

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

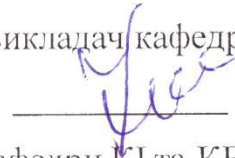
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект системи безпечного управління
привілейованими обліковими записами у середовищі
Microsoft Active Directory»

Виконав: студент 4-го курсу групи КІ-21-1
спеціальності 123 «Комп'ютерна інженерія»

 Вадим Тарнопольський

Керівник: Старший викладач кафедри КІ та КБ,

 Ігор Фальковський

Рецензент: Доцент кафедри КІ та КБ, к.т.н.,

 Олексій Шелуха

Житомир – 2025

Державний університет «Житомирська політехніка»

Факультет інформаційно-комп'ютерних технологій

Кафедра комп'ютерної інженерії та кібербезпеки

Спеціальність 123 «Комп'ютерна інженерія»

Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Тарнопольський Вадим Олександрович

Тема роботи: «Проект системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory»

затверджена Наказом університету від 3 березня 2025 р. № 97/с

Термін здачі студентом закінченої роботи 4 червня 2025 р.

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

Предметом дослідження є методи та засоби захисту привілейованих облікових записів у середовищі Microsoft Active Directory.

Об'єктом дослідження є середовище Microsoft Active Directory.

Обладнання та програмне забезпечення:

1. Гіпервізор VirtualBox
2. Операційні системи: Windows 10, Windows Server 2019
3. Служба Active Directory Domain Services (AD DS)

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Фальковський І.Г.	03.03.2025	03.03.25
2	Фальковський І.Г.	03.03.2025	03.03.25
3	Фальковський І.Г.	03.03.2025	03.03.25

Студент Вадим Тарнопольський

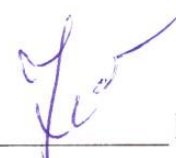
Керівник Ігор Фальковський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Терміни виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	
2	Створення плану роботи	23.03.2025	
3	Аналіз літературних джерел	03.04.2025 – 12.04.2025	
4	Аналіз об'єкта дослідження	13.04.2025 – 20.04.2025	
5	Розробка структурної моделі	22.04.2025 – 28.04.2025	
6	Проектування та створення структури домену AD	01.05.2025 – 10.05.2025	
7	Налаштування базових функцій домену	11.05.2025 – 15.05.2025	
8	Налаштування прикладних служб, технологій та функцій домену	15.05.2025 – 20.05.2025	

9	Перевірка працездатності системи	21.05.2025 – 23.05.2025	
10	Оформлення пояснювальної записки	24.05.2025 – 28.05.2025	
11	Захист	19.06.2025	

Студент  Вадим Тарнопольський

Керівник  Ігор Фальковський

АНОТАЦІЯ

Завданням на кваліфікаційну роботу було створення системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory. Пояснювальна записка до кваліфікаційної роботи на тему "Проект системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory" складається зі вступу, трьох розділів, висновків, списку використаної літератури та додатків. Текстова частина викладена на 76 сторінках друкованого тексту.

Пояснювальна записка має 6 сторінок додатків.

Список використаних джерел містить 20 найменувань і займає 2 сторінки.

В роботі наведено 75 рисунків, 4 таблиці. Загальний обсяг роботи – 85 сторінок.

У результаті роботи розроблено та впроваджено систему безпечного управління обліковими записами з підвищеними правами у середовищі Microsoft Active Directory. Така система дозволяє централізовано контролювати доступ до критично важливих ресурсів, забезпечувати розмежування прав користувачів, зменшувати ризики несанкціонованого доступу та посилювати захист від внутрішніх загроз. Особливу увагу приділено обмеженню використання привілейованих облікових записів, моніторингу дій адміністраторів та впровадженню політик безпеки. Запропоновані рішення сприятимуть підвищенню загального рівня інформаційної безпеки та ефективному управлінню ІТ-інфраструктурою організації.

КЛЮЧОВІ СЛОВА: АДМІНІСТРУВАННЯ, СИСТЕМА, БЕЗПЕКА, ПРИВІЛЕЙОВАНІ ОБЛІКОВІ ЗАПИСИ, «ACTIVE DIRECTORY».

					ККІКБ.КР.Б – 123 – 14 – ПЗ			
Змн.	Арк.	№ докум.	Підпис	Дата	Проект системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory	Лім.	Арк.	Аркушів
Розроб.		Тарнопольський		11.06.25				
Керівник		Фальковський І.Г.		11.06.25			5	85
Реценз.		Шелуха О.О.		11.06.25		ФІКТ, Гр. КІ-21-1		
Н. контр.		Фальковський І.Г.		11.06.25				
Затверд.		Єфіменко А.А.		11.06.25				

ANNOTATION

The task for the qualification work was to create a system for secure management of privileged accounts in the Microsoft Active Directory environment. The explanatory note to the qualification work on the topic "Project for a system for secure management of privileged accounts in the Microsoft Active Directory environment" consists of an introduction, three sections, conclusions, a list of used literature and appendices. The text part is set out on 76 pages of printed text.

The explanatory note has 6 pages of appendices.

The list of used sources contains 20 items and occupies 2 pages.

The work contains 75 figures, 4 tables. The total volume of work is 85 pages.

As a result of the work, a system for secure management of accounts with elevated rights in the Microsoft Active Directory environment will be developed and implemented. Such a system will allow centralized control of access to critical resources, ensure the separation of user rights, reduce the risks of unauthorized access and strengthen protection against internal threats. Special attention will be paid to restricting the use of privileged accounts, monitoring administrator actions, and implementing security policies. The proposed solutions will contribute to increasing the overall level of information security and effective management of the organization's IT infrastructure.

KEYWORDS: ACTIVE DIRECTORY, ADMINISTRATION, PRIVILEGED ACCOUNTS, SECURITY, SYSTEM.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		6

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IPv4 – Internet Protocol version 4.

DHCP – Dynamic Host Configuration Protocol.

ПК – Персональний комп'ютер.

DNS - Domain Name System

JEA — Just Enough Administration

DSC — Desired State Configuration

AD — Active Directory

AD DS - Active Directory Domain Services

IP - Internet Protocol

IPv4 - Internet Protocol version 4

GPO — Group Policy Object

OU — Organizational Unit

LAPS – Local Administrator Password Solution

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

VPN – Virtual Private Network

ACL – Access Control List

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		7

ЗМІСТ

ВСТУП	10
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА ІНСТРУМЕНТИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ У MICROSOFT ACTIVE DIRECTORY.....	12
1.1 Роль та структура Microsoft Active Directory у керуванні привілейованими обліковими записами	12
1.2 Загрози та вразливості привілейованих облікових записів у AD	15
1.3 Політики групової безпеки (GPO) як засіб контролю доступу у AD....	17
1.4 Захист паролів адміністратора за допомогою Local Administrator Password Solution (LAPS).....	19
1.5 Використання Just Enough Administration (JEA) для обмеження дій адміністраторів у AD	22
1.6 Автоматизація конфігурацій безпеки за допомогою Desired State Configuration (DSC) у AD	25
РОЗДІЛ 2. Проектування системи.....	28
2.1 Проектування фізичної топології мережі	28
2.2 Проектування логічної топології мережі	31
2.3 Вибір середовища для реалізації курсового проєкту	32
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ФУНКЦІОНУВАННЯ МЕРЕЖІ, ЗАСОБІВ ЇЇ АДМІНІСТРУВАННЯ ТА БЕЗПЕКИ.	35
3.1 Вибір обладнання для організації роботи мережі	35
3.2 Створення середовища AD	39
3.3 Налаштування групових політик (GPO)	49
3.4 Впровадження LAPS.....	54
3.5 Налаштування JEA.....	57

3.6 Використання DSC.....	61
3.7 Тестування роботи системи	64
ВИСНОВКИ	75
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	77
ДОДАТКИ.....	79

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				9
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Проектування системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory є ключовим завданням для забезпечення захисту IT-інфраструктури, збереження конфіденційності даних та підтримки безперервності бізнес-процесів. Привілейовані облікові записи відіграють важливу роль в адмініструванні та управлінні мережею, але водночас вони є однією з головних цілей для злоумисників.

Розробка такої системи передбачає впровадження ефективних механізмів контролю доступу, обмеження використання облікових записів із підвищеними правами, посилення процедур автентифікації та моніторинг дій користувачів із розширеними привілеями. Це дозволяє запобігати несанкціонованому доступу, зменшувати ризики внутрішніх загроз і відповідати сучасним вимогам інформаційної безпеки.

Впровадження запропонованих рішень сприятиме підвищенню рівня захищеності середовища Active Directory, дозволить мінімізувати потенційні уразливості та забезпечить ефективне управління доступом до критично важливих ресурсів організації.

Метою кваліфікаційної роботи є розробка та впровадження системи безпечного управління привілейованими обліковими записами для забезпечення ефективного управління, моніторингу та діагностики привілейованих користувачів.

Основними **завданнями** проекту є вивчення теоретичних основ і методів управління привілейованими обліковими записами у Microsoft Active Directory, аналіз існуючих рішень для їхнього захисту, розробка архітектури системи безпечного управління, налаштування середовища Active Directory з урахуванням механізмів обмеження доступу, впровадження інструментів моніторингу та аудиту, тестування розробленої системи, оцінювання її ефективності та формування рекомендацій щодо подальшого використання.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Предметом дослідження є методи та засоби захисту привілейованих облікових записів у середовищі Microsoft Active Directory, що спрямовані на зниження ризиків несанкціонованого доступу та підвищення рівня безпеки ІТ-інфраструктури.

Об'єктом дослідження є середовище Microsoft Active Directory, яке включає облікові записи, групи, політики контролю доступу та механізми автентифікації, що використовуються для управління ресурсами організації.

Методи дослідження включають аналіз літературних джерел і нормативної документації, проєктування системи управління привілейованими обліковими записами в тестовому середовищі, експериментальне налаштування та перевірку механізмів контролю доступу, а також аналіз отриманих результатів з метою оцінки ефективності впроваджених заходів.

Під час виконання кваліфікаційної роботи було розроблено Проєкт системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		11

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ТА ІНСТРУМЕНТИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ У MICROSOFT ACTIVE DIRECTORY

1.1 Роль та структура Microsoft Active Directory у керуванні привілейованими обліковими записами

Active Directory (AD) – це ієрархічна служба каталогу від компанії Microsoft, яка використовується в доменному середовищі Windows для організації та централізованого керування різними типами об'єктів: комп'ютерами, користувачами, серверами, принтерами. AD є центральним елементом керування та аутентифікації у мережах Windows. Active Directory тісно пов'язана та інтегрована з безліччю служб та програм Microsoft, таких як DNS, DHCP, поштова служба Exchange Server, і т.д. Завдяки тому, що всі облікові записи користувачі зберігаються в єдиній базі AD, користувач може увійти під своїм обліковим записом та паролем на будь-який комп'ютер у домені AD (на відміну від workgroup, де на кожному комп'ютері зберігається власна база користувачів).

AD організовано в ієрархічну структуру. В архітектурі AD є такі елементи:

Ліс AD (forest) – найвищий рівень ієрархії Active Directory. Він являє собою набір пов'язаних доменів, які поділяють загальну схему, структуру та глобальний каталог

Домен – окрема область усередині лісу AD, зі своїм кордоном безпеки та реплікацією. Містить користувачів, комп'ютери, групи та інші об'єкти.

Організаційна одиниця (OU) – контейнери всередині домену для логічного угруповання об'єктів (аналог – папки на диску). OU є точки призначення GPO та делегування повноважень.

Для встановлення домену Active Directory необхідно встановити роль Active Directory Domain Services (ADDS) на комп'ютері з Windows Server. Такий сервер називається контролер домену Active Directory (DC). У домені

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		12

може бути один або кілька контролерів домену, залежно від потреб та розміру домену. Контролери домену виконують аутентифікацію користувачів та обслуговують запити на доступ до ресурсів мережі (використовується як logon server);

На контролері домену зберігається база Active Directory (NTDS.DIT). Кожен контролер домену зберігає свою копію бази AD та реплікує нові/змінені дані з іншим DC.

Сайт AD – об'єкти AD, що є однією або кількома фізичними IP підмережами, пов'язаними швидкими каналами. Зазвичай сайти AD відображають фізичні географічні чи логічні межі у корпоративній мережі. Клієнти виконують автентифікацію, отримують політики з контролерів домену у своїх сайтах. У кожному сайті може бути один або кілька контролерів домену. Між веб-сайтами можна налаштувати інтервали реплікації для зменшення навантаження на WAN канали.

Global Catalog (GC) – ця роль може бути призначена для будь-якого контролера домену. Такий DC буде зберігати коротку інформацію про весь ліс і використовуватиметься для пошуку та автентифікації в різних доменах;

Групові політики (GPO) – дозволяють адміністраторам налаштовувати параметри комп'ютерів та користувачів у мережі з використанням централізованих політик

Схема AD – визначає структуру та можливі атрибути об'єктів у Active Directory.

Ключовим рішенням при проектуванні AD є рішення щодо поділу інформаційної інфраструктури на ієрархічні домени та підрозділи верхнього рівня. Типовими моделями, що використовуються для такого поділу, є моделі поділу за функціональними підрозділами компанії, за географічним розташуванням, і за ролями в інформаційній інфраструктурі компанії. Часто використовуються комбінації цих моделей.[1]

Active Directory відіграє центральну роль у впровадженні привілейованими обліковими записами завдяки своїм функціональним можливостям:

Централізоване управління ідентичностями:

- Забезпечення єдиного репозиторію для облікових записів користувачів, адміністраторів і сервісів
- Стандартизація процесів створення, зміни та деактивації облікових записів
 - Можливість застосування глобальних політик безпеки до всіх об'єктів

Розмежування прав доступу:

- Створення груп безпеки, таких як «Domain Admins»
- Делегування обмежених прав адміністраторам окремих підрозділів або серверів
- Розподіл об'єктів за організаційними одиницями (OU) для логічної структури

Аудит та моніторинг:

- Ведення журналу входів і виходів користувачів
- Фіксація змін до конфігурацій та облікових записів
- Виявлення та розслідування підозрілої активності

Інтеграція з рішеннями для PAM (Privileged Access Management):

- Підтримка Microsoft Identity Manager (MIM)
- Вбудований механізм Privileged Access Management у Windows Server
- Інтеграція з Azure AD Privileged Identity Management (PIM) для хмарних ресурсів

Отже, Active Directory — це рішення, яке забезпечує контроль над доступом до ресурсів, захищає дані та спрощує управління мережею. Це особливо важливо для компаній, які працюють з конфіденційною інформацією та мають складну IT-інфраструктуру.[2]

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				14
Змн.	Арк.	№ докум.	Підпис	Дата		

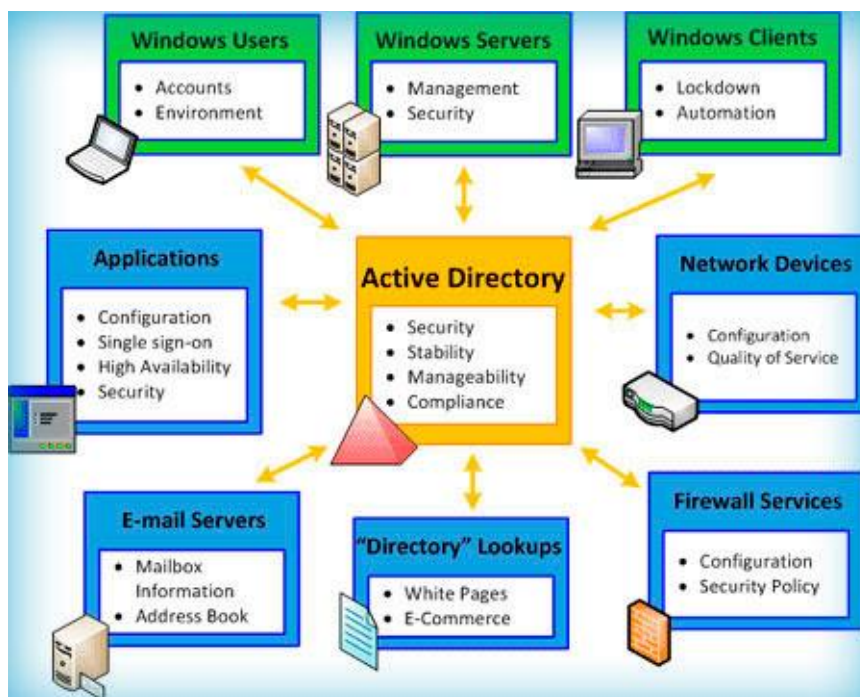


Рисунок 1.1 – Організація Active Directory

1.2 Загрози та вразливості привілейованих облікових записів у AD

Останнім часом все більше атак спрямовані безпосередньо на AD. Зокрема, кіберзлочинні групи, що використовують програми-вимагачі, активно атакують цю службу, оскільки вона є критичною частиною ІТ-інфраструктури організацій. Наприклад, група, що використовує програму-вимагач Conti, була причетна до понад 400 атак по всьому світу, застосовуючи нові уразливості Active Directory, як-от PrintNightmare (CVE-2021-34527) і Zerologon (CVE-2020-1472), для підвищення привілеїв та подальшого проникнення в мережі.[3]

Отже, серед основних загроз та вразливостей для облікових записів Active Directory можна виділити наступні:

- Надмірні привілеї — облікові записи мають більше прав, ніж потрібно, що збільшує ризик зловживання або компрометації.
- Слабкі або спільні паролі — використання передбачуваних або однакових паролів полегшує злам через brute-force або фішингові атаки.

- Відсутність розмежування доступу — коли адміністратори мають необмежений доступ без сегментації, це відкриває шлях до повного контролю над системою в разі компрометації.
- Недостатній аудит дій — відсутність моніторингу дій привілейованих користувачів ускладнює виявлення підозрілої або шкідливої активності.
- Кешування облікових даних — збереження облікових даних у пам'яті системи або на диску дає змогу зловмисникам витягувати їх за допомогою спеціальних інструментів (наприклад, Mimikatz).
- Застарілі протоколи автентифікації — використання NTLM або інших слабких механізмів дозволяє проводити атаки типу Pass-the-Hash.
- Відсутність багатофакторної автентифікації (MFA) — використання лише паролів залишає систему вразливою до компрометації облікових записів.
- Підвищення привілеїв — зловмисник може скористатися конфігураційними помилками або вразливостями для отримання адміністративного доступу.
- Постійні облікові записи з привілеями — існування постійно активних облікових записів відкриває вікно можливостей для атаки навіть у періоди бездіяльності.
- Фішинг та соціальна інженерія — привілейовані користувачі можуть стати жертвами обману, внаслідок чого віддають облікові дані або запускають шкідливий код.

Враховуючи популярність та статичність Active Directory, зловмисники змогли знайти нові інноваційні бекдори для проникнення в інфраструктуру. Ці хитрі шляхи атаки дозволяють отримувати інформацію за допомогою облікових записів користувачів або взагалі за допомогою привілейованих облікових записів, а отже потрібно подбати про їхню безпеку.[4]

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				16
Змн.	Арк.	№ докум.	Підпис	Дата		

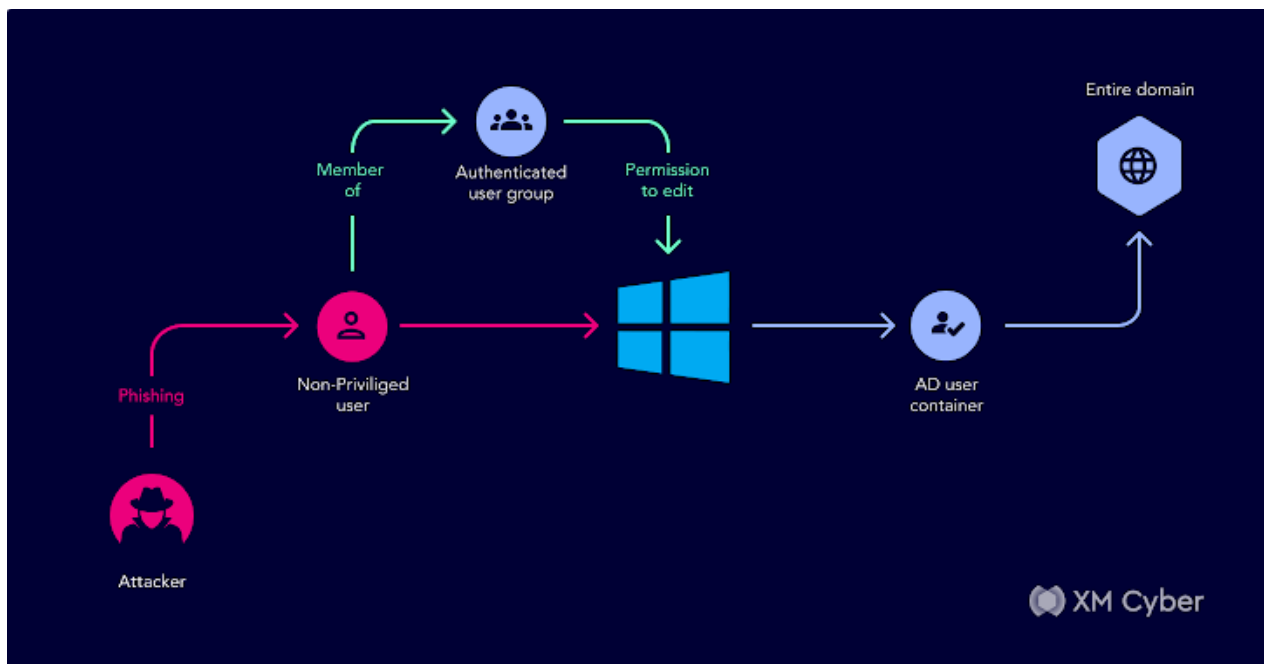


Рисунок 1.2 – принцип дії авторизації в Active Directory

1.3 Політики групової безпеки (GPO) як засіб контролю доступу у AD

Групова політика - це інструмент, доступний адміністраторам, що працюють з архітектурою Active Directory. Це дозволяє централізовано керувати налаштуваннями на клієнтських комп'ютерах і серверах, підключених до домену, а також забезпечує простий спосіб розповсюдження програмного забезпечення.

Групові політики дозволяють налаштовувати параметри для певного набору користувачів або комп'ютерів у домені Active Directory. Також дозволяють вказати політики в одному місці для групи та застосувати цільовий набір користувачів.

Наприклад, можна використовувати стандартний набір та конфігурації для груп користувачів або комп'ютерів у домені або на запит. У всіх компаніях зазвичай є різні відділи, наприклад відділ системних адміністраторів, розробників, дизайнерів, кожному з відділу необхідний свій стандартний набір програмного забезпечення, їх робочі комп'ютери повинні бути налаштовані під спеціальні завдання та потреби. За допомогою групових

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		17

політик можна створити налаштування для конкретних груп користувачів у домені. За допомогою адміністрування Active Directory можна встановити та керувати окремими уніфікованими наборами налаштувань, безпосередньо для дизайнерів або розробників.

Часто групові політики застосовуються саме до підрозділів. Групові політики самі є об'єктами. Підрозділ є найнижчим рівнем, на якому можуть делегуватися адміністративні повноваження.[5]

Конфігурації для комп'ютерів чи користувачів простіше та ефективніше, т.к. розташовані в одному місці та не вимагають повтору на кожному комп'ютері. Налаштування різних об'єктів групової політики можуть перекриватись або конфліктувати. За замовчуванням об'єкти групової політики обробляються у такому порядку (причому створені пізніше мають пріоритет над створеними раніше): [6]

- Локальний (індивідуальний комп'ютер)
- Сайт
- Домен
- Організаційна одиниця

Для керування груповими політиками Microsoft надає консоль керування груповими політиками (GPMC). Використовуючи цей безкоштовний редактор групової політики, ІТ-адміністратори можуть створювати, копіювати, імпортувати, створювати резервні копії та відновлювати об'єкти групової політики, а також складати звіти щодо них. Microsoft також пропонує цілий набір інтерфейсів GPMC, які можна використовувати для програмного доступу до багатьох операцій, що підтримуються консоллю. [6]

За замовчуванням будь-який член групи адміністраторів домену може створювати об'єкти групової політики та керувати ними. Крім того, існує глобальна група під назвою "Власники-творці групових політик"; його члени можуть створювати об'єкти групової політики, але вони можуть змінювати

лише створені ними політики, якщо їм спеціально не надано дозволи на редагування інших об'єктів групової політики. [6]

У цій же консолі можна делегувати допоміжним ІТ-адміністраторам дозволи на різні дії: створення, редагування та створення зв'язків для певних об'єктів групової політики. Делегування – цінний інструмент; наприклад, можна надати групі, відповідальній за керування Microsoft Office, можливість редагувати об'єкти групової політики, які використовуються для керування налаштуваннями Office на робочому столі користувачів. [6]



Рисунок 1.3 – принцип роботи GPO в Active Directory

1.4 Захист паролів адміністратора за допомогою Local Administrator Password Solution (LAPS)

LAPS (Local Administrator Password Solution) дозволяє централізовано керувати паролями локальних адміністраторів на комп'ютерах домену. Поточний пароль локального адміністратора зберігаються в захищених атрибутах об'єктів Computer Active Directory, регулярно змінюється автоматично і може бути отриманий авторизованими користувачами.

Функціонал LAPS заснований на використанні спеціального функціоналу GPO, який заснований на Group Policy Client Side Extension (CSE) і є невеликим модулем, який встановлюється на робочі станції. Дане розширення GPO використовується для створення унікального пароля

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		19

локального адміністратора (SID — 500) на кожному комп'ютері домену. Пароль адміністратора автоматично змінюється із зазначеною періодичністю (за замовчуванням, кожні 30 днів). Значення поточного пароля зберігається в конфіденційному атрибуті облікового запису комп'ютера в Active Directory, доступ до перегляду вмісту атрибута регулюється групами безпеки AD.

Використання Windows LAPS для регулярної зміни та керування паролями локальних облікових записів адміністратора має такі переваги:

- Захист від атак типу «pass-the-hash» та «lateral-traversal».
- Покращена безпека для сценаріїв віддаленої служби підтримки
- Можливість входити в систему та відновлювати дані на пристроях, які інакше недоступні
- Деталізована модель безпеки (списки контролю доступу та додаткове шифрування паролів) для захисту паролів, що зберігаються в Active Directory Windows Server
- Підтримка моделі керування доступом на основі ролей Microsoft Entra для захисту паролів, що зберігаються в Microsoft Entra ID.[7]

Схема архітектури Windows LAPS має кілька ключових компонентів:

- IT-адміністратор: представляє спільно різні ролі IT-адміністратора, які можуть брати участь у розгортанні Windows LAPS. Ролі IT-адміністратора беруть участь у налаштуванні політики, закінченні терміну дії або отриманні збережених паролів та взаємодії з керованими пристроями.
- Керований пристрій: представляє приєднаний до Microsoft Entra пристрій або пристрій, приєднаний до Windows Server Active Directory, на якому потрібно керувати обліковим записом локального адміністратора. Ця функція складається з декількох двійкових файлів ключів: laps.dll для основної логіки, lapscsp.dll для логіки постачальника конфігураційних служб (CSP) і lapsps.dll для логіки командлета PowerShell. Ви також можете налаштувати Windows LAPS за допомогою групової політики. Windows LAPS відповідає на

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				20
Змн.	Арк.	№ докум.	Підпис	Дата		

сповіщення про зміни об'єктів групової політики. Керований пристрій може бути контролером домену Windows Server Active Directory і налаштований для резервного копіювання паролів облікових записів служб каталогів (DSRM).

- Windows Server Active Directory : локальне розгортання Windows Server Active Directory.
- Ідентифікатор Microsoft Entra: розгортання Microsoft Entra , яке виконується у хмарі.
- Microsoft Intune Переважне рішення для управління політиками пристроїв Майкрософт, яке також працює у хмарі.[8]

Архітектура LAPS складається з двох частин. Модуль керування встановлюється на машині адміністратора, а клієнтська частина встановлюється на серверах та ПК, на яких потрібно регулярно міняти пароль локального адміністратора.

Отже, LAPS відкриває нам наступні можливості:

- Безпечне зберігання паролів окремих робочих станцій в Active Directory
- Встановлення нових правил для створення паролів
- Зміни адміністраторських паролів, підключивши захищений канал та обминаючи безпосереднє підключення до системи за допомогою Active Directory
- Регулювання "часу життя" паролів, а також автоматизація процесу їх автоматичних замінів.[9]

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				21
Змн.	Арк.	№ докум.	Підпис	Дата		

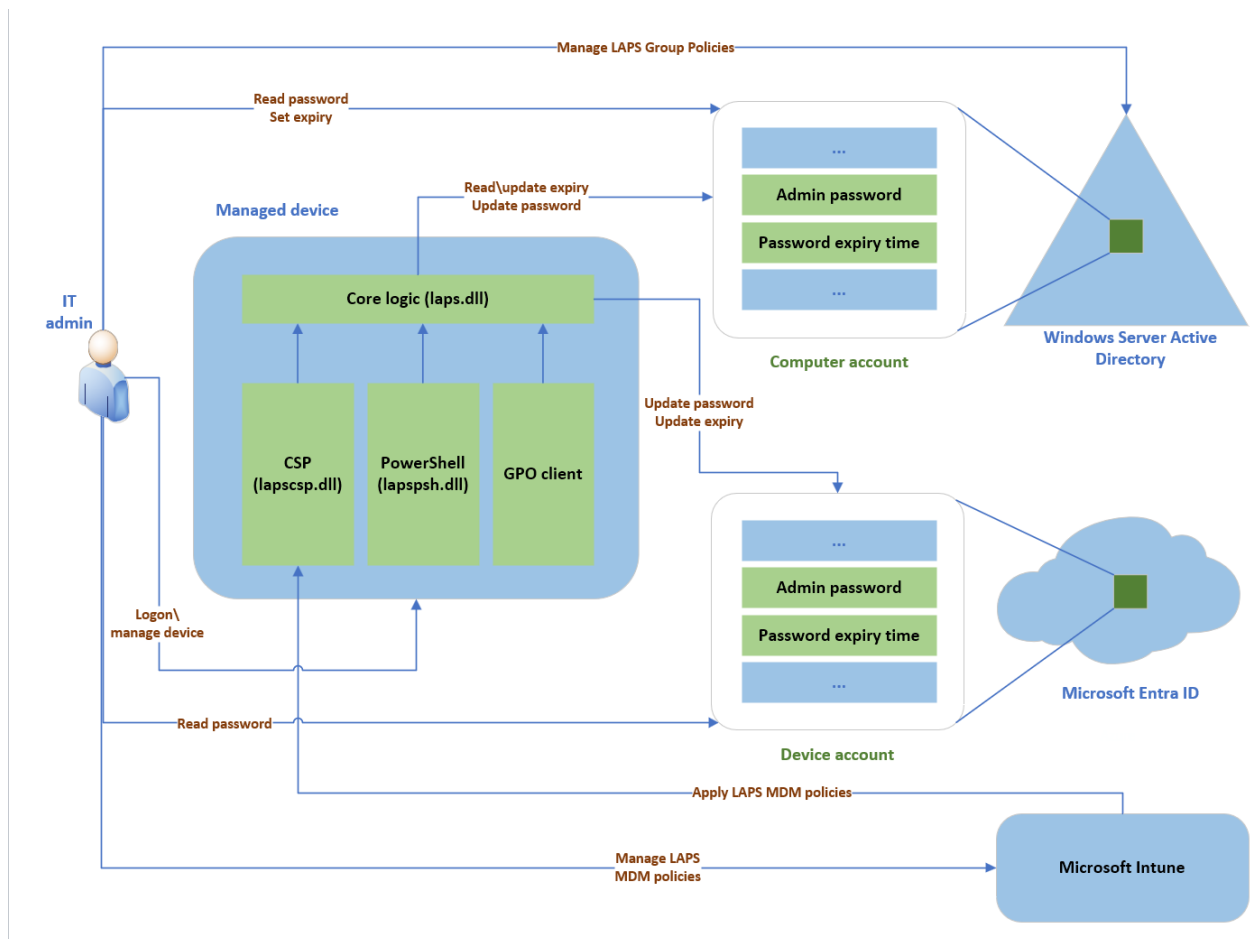


Рисунок 1.4 – принцип дії LAPS в Active Directory

1.5 Використання Just Enough Administration (JEA) для обмеження дій адміністраторів у AD

Технологія Just Enough Administration (JEA), яка з'явилася у версії PowerShell 5.0, дає змогу делегувати адміністративні повноваження на все, чим можна керувати за допомогою PowerShell. JEA дозволяє надати вашим користувачам права на виконання певних адміністративних завдань, не надаючи їм права адміністратора сервера або сервісу (AD, Exchange, SharePoint і т.д.) За допомогою JEA ви можете вказати яким користувачам можна запускати певні командлети, функції або PowerShell скрипти з правами привілейованих користувачів, а також докладно логувати.

Адміністратор створює на сервері конфігураційний файл сесії PowerShell та файл із командами, які може виконувати користувач. На основі цих файлів створюється точка підключення JEA (endpoint), до якої може

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		22

підключитися користувач і виконати в цю сесію будь-яку з доступних команд або програм.

Ви можете зменшити кількість адміністраторів на комп'ютерах , використовуючи віртуальні облікові записи або групові керовані облікові записи служби, які допускають виконання привілейованих дій від імені звичайних користувачів.[10]

Обмежити доступні користувачам дії, вказавши, які командлети, функції та зовнішні команди можуть виконувати користувачі.[10]

Краще зрозуміти, що роблять ваші користувачі за допомогою деталізованих записів і журналів, що показують виконувані користувачами команди під час сеансу.[10]

Високопривілейовані облікові записи , які використовуються для адміністрування серверів, становлять серйозну загрозу для безпеки. обслуговування та інших небажаних операцій.[10]

JEА вирішує цю проблему, дотримуючись принципу найменших прав доступу . За наявності JEА ви можете налаштувати для адміністраторів DNS кінцеву точку керування, що надає їм доступ тільки до команд PowerShell, які потрібні для роботи. Це означає, що ви можете надати відповідні права доступу для відновлення пошкодженого кешу DNS або перезапуску DNS-сервера без випадкового надання прав доступу до Active Directory, перегляд файлової системи або запуск потенційно небезпечних сценаріїв. Більше того, якщо в сеансі JEА налаштовано використання тимчасових привілейованих віртуальних облікових записів, ваші адміністратори DNS зможуть підключатися до сервера за допомогою облікових даних без адміністративних повноважень і виконувати команди, для яких зазвичай потрібні права адміністратора. JEА дозволяє видалити користувачів з ролей локальних адміністраторів та адміністраторів домену з великими правами доступу, а також детально налаштувати операції, доступні на кожному комп'ютері.[10]

Завдяки Just Enough Administration (JEА) організації можуть реалізувати потужну модель контрольованого доступу на основі ролей, яка дозволяє

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				23
Змн.	Арк.	№ докум.	Підпис	Дата		

виконання лише строго визначених адміністративних дій. Це значно зменшує площу атаки та ризики, пов'язані з людським фактором або зловмисним використанням привілеїв.

Ключові переваги JEA:

- Зменшення ризику компрометації критичних облікових записів.
- Аудит і відповідність: всі дії в рамках JEA-сеансів логуються, що спрощує розслідування інцидентів і відповідає вимогам регуляторів.
- Гнучкість налаштування: адміністратори можуть створювати спеціалізовані кінцеві точки для різних ролей – від операторів резервного копіювання до обслуговування DNS або IIS.
- Масштабованість: JEA підтримує розгортання через групову політику, Desired State Configuration (DSC) та інші інструменти автоматизації.

Таким чином, JEA — це не просто функціональність PowerShell, а стратегія мінімізації прав і підвищення безпеки у сучасному IT-середовищі.

Головна мета JEA — обмежити привілеї. Ми можемо дуже детально вказати, що може робити користувач. Наприклад, якщо ви хочете обмежити користувача лише перезапуском служби спулерів, тоді використовуйте JEA.[11]

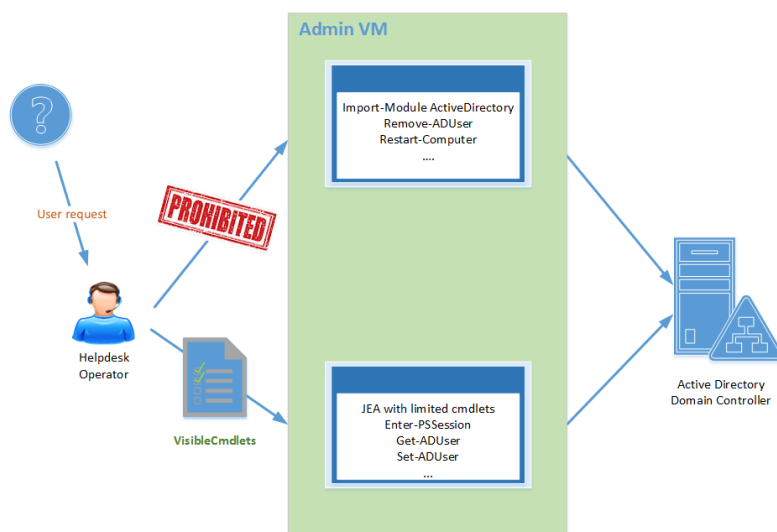


Рисунок 1.5 – принцип дії JEA в Active Directory

1.6 Автоматизація конфігурацій безпеки за допомогою Desired State Configuration (DSC) у AD

Microsoft Desired State Configuration (DSC) – це декларативна платформа конфігурації. При використанні DSC стан комп'ютера описується за допомогою формату, який має бути зрозумілим, навіть якщо читач не є експертом на тему. На відміну від імперативних інструментів, при визначенні середовища застосування визначення середовища застосування відрізняється від логіки скрипта, що реалізує спосіб доставки.[12]

Використовуючи DSC, ми описуємо як хочемо, щоб виглядала система зрештою, не вдаючись у подробиці — система автоматично налаштовується відповідно до заданих вимог.[13]

Тобто, якщо нам потрібно щоб у реєстрі був певний ключ, щоб якась служба була запущена, якийсь компонент Windows встановлений (або навпаки – щоб чогось не було, або було вимкнено), то при традиційному підході ми повинні самі написати перевірку кожної вимоги, і якщо щось не відповідає – поправити (знов-таки самі) створити, зупинити.[13]

Наприклад, адміністратор може створити конфігурацію, яка визначає, що групи привілейованих користувачів мають певні права доступу або що облікові записи адміністратора повинні відповідати політикам безпеки. DSC автоматично створює облікові записи з необхідними правами та налаштуваннями, а також керує додаванням чи видаленням користувачів з привілейованих груп, таких як Domain Admins або Enterprise Admins. Однією з основних функцій DSC є постійне підтримання бажаного стану системи. Якщо привілейовані облікові записи були змінені або видалені, DSC автоматично виправляє ситуацію, приводячи систему до бажаного стану. Це зменшує ймовірність помилок або зловмисних змін у системі. DSC також слідкує за тим, щоб система залишалася в тому стані, який був заданий адміністратором. DSC дозволяє вести детальний аудит змін у конфігураціях, що дає змогу відстежувати будь-які зміни в привілейованих облікових записах і виявляти несанкціоновані або нещодавно внесені зміни. Автоматичне генерування

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		25

звітів дозволяє адміністратору перевіряти стан конфігурацій, зокрема щодо привілейованих облікових записів, що дає змогу швидко виявляти порушення політик безпеки. DSC також обмежує доступ до критичних облікових записів лише для тих, хто має на це відповідні повноваження, що знижує ймовірність помилок або зловмисних дій. Адміністратори можуть налаштовувати доступ до привілейованих облікових записів за допомогою політик доступу на основі ролей (RBAC). DSC може бути інтегрована з іншими інструментами безпеки, такими як системи моніторингу та управління подіями безпеки (SIEM). Це дозволяє автоматично реагувати на підозрілі або несанкціоновані зміни в конфігураціях привілейованих облікових записів.

Використання DSC забезпечує автоматизацію, стандартизацію та сталий стан системи, що є важливим для безпечного адміністрування привілейованими обліковими записами. Ці функції знижують людський фактор, підвищують безпеку та забезпечують відповідність політикам безпеки організації

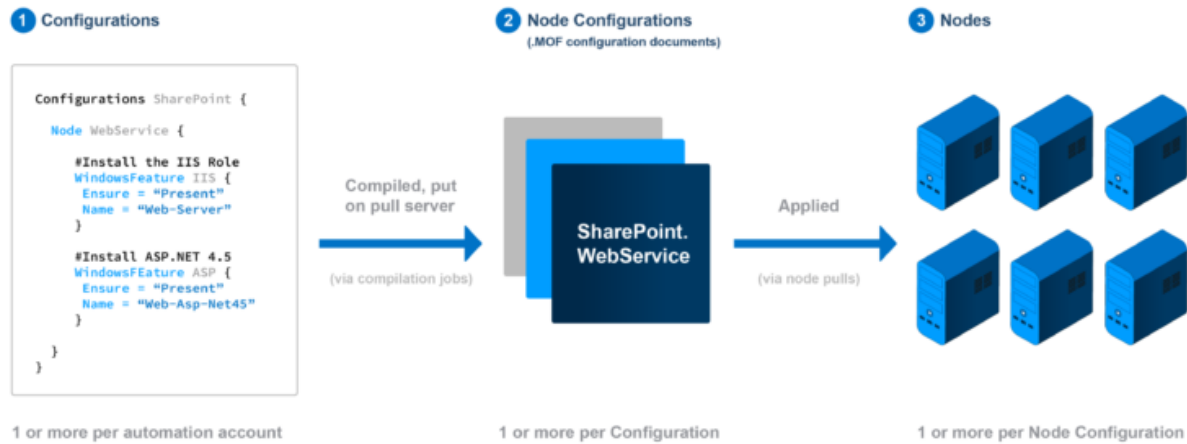


Рисунок 1.6 – принцип дії DSC в Active Directory

Висновки до першого розділу

В даному розділі було розглянуто теоретичні відомості та основні функції Active Directory, також було приділено увагу ролі та структури Microsoft Active Directory у керуванні привілейованими обліковими записами.

Розглянуто загрози та вразливості привілейованих облікових записів у AD, оскільки привілейовані облікові записи в Active Directory є основною цілью для зловмисників, адже надають доступ до критично важливих ресурсів.

Задля безпеки системи було розглянуто важливі інструменти та засоби для запобігання дій зловмисників, наприклад - політики групової безпеки (GPO), оскільки це є ключовим інструментом у Microsoft Active Directory для централізованого управління налаштуваннями безпеки та контролю доступу. Вони дозволяють ефективно застосовувати обмеження до користувачів і комп'ютерів, забезпечуючи дотримання корпоративних стандартів безпеки.

Для безпеки паролів було обрано сучасний засіб Local Administrator Password Solution (LAPS), який забезпечує автоматичне керування паролями локальних адміністраторів на комп'ютерах у домені Active Directory. Не менш важливим був розгляд використання Just Enough Administration (JEA) для обмеження дій адміністраторів у AD. Значну увагу було приділено Desired State Configuration (DSC) як сучасному інструменту для автоматизації конфігурацій безпеки.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		27

РОЗДІЛ 2. Проектування системи

2.1 Проектування фізичної топології мережі

Робоча станція— комп'ютер, призначений переважно для вирішення наукових, технічних та інженерних завдань. Є частиною локальної мережі і працює під керуванням багатозадачної й багатокористувацької операційної системи.[14]

У доменній мережі дві робочі станції, які є частиною домену, виконують ключову роль у забезпеченні доступу користувачів до необхідних ресурсів і сервісів. Обидві робочі станції можуть бути налаштовані для виконання різних завдань, але всі вони підключені до єдиної інфраструктури домену, що дозволяє централізовано управляти їх налаштуваннями, безпекою та доступом.

Одна з робочих станцій може використовуватися як основна для повсякденних задач, таких як робота з документами, використання програмного забезпечення, доступ до спільних ресурсів (файлів, принтерів), та інших необхідних інструментів. Вона підключена до домену, що дозволяє автоматично застосовувати політики безпеки, налаштування доступу та обмеження, визначені в Active Directory, а також централізовано управляти обліковими записами користувачів та правами доступу. Інша робоча станція може використовуватися для специфічних функцій або для резервного доступу. Це може бути робоча станція для адміністраторів, тестувальників або користувачів, які мають обмежений доступ до системи, але їм необхідні певні адміністративні функції або специфічний доступ до ресурсів в домені. Вона також підключена до домену, що дозволяє застосовувати потрібні політики та забезпечує користувачам доступ лише до тих ресурсів, які їм необхідні для виконання їх завдань.

Оскільки обидві станції знаходяться в одному домені, адміністратори можуть централізовано контролювати їх доступ до мережевих ресурсів, застосовувати правила безпеки, забезпечувати єдину політику для всіх

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		28

користувачів і пристроїв, а також здійснювати моніторинг діяльності в межах домену. Це значно полегшує управління великою кількістю робочих станцій і забезпечує відповідність вимогам безпеки та управління в організації.

Windows Server це сімейство серверних операційних систем від Microsoft (лінійка Windows NT), розроблена в 1993 році (NT 3.1 в редакції Advanced Server) для розгортання та управління корпоративною IT-інфраструктурою. Починаючи з 2003 року, Microsoft використовує маркетингову назву Windows Server. Важливим етапом у розвитку стала Windows 2000 Server, саме в ній вперше з'явилися Active Directory, DNS, DHCP і Group Policy.

Windows Server дуже відрізняється від настільних версій Windows (для ПК і ноутбуків). Вона створена не для прямого користування кінцевим користувачем, а для роботи різних сервісів та програм у фоновому режимі: файлові сховища, бази даних, віртуальні машини, Active Directory, служби віддаленого доступу та багато іншого. Може працювати без графічного інтерфейсу користувача (GUI) — у так званому Server Core режимі, що дозволяє знизити навантаження, зменшити площу кібератак та заощадити ресурси. Адміністрування найчастіше здійснюють через PowerShell, консоль і віддалено по мережі.

Контролер домену в комп'ютерних мережах, побудованих на Microsoft Servers — це сервер, який контролює область комп'ютерної мережі (домен).[15]

Контролери домену не обмежуються лише управлінням користувачами та ресурсами в межах одного домену; вони є невід'ємною частиною функціонування доменів Active Directory, які можуть охоплювати кілька фізичних розташувань, підтримуючи складну мережу служб каталогів на підприємстві.[16]

Аутентифікація та Авторизація: центральним елементом ролі контролера домену є можливість аутентифікації облікових даних користувача.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Цей процес забезпечує доступ до мережевих ресурсів тільки дійсним користувачам, підвищуючи безпеку мережі.[16]

Управління користувачами та групами: крім окремих користувачів, контролери домену також здатні керувати політиками груп та членством у групах.[16]

Забезпечення політик та управління конфігурацією: вони відіграють важливу роль у впровадженні об'єктів групової політики (GPO), які застосовують політики та конфігурації на комп'ютери та користувачів у домені.[16]

Служби каталогів та Active Directory: в основі можливостей контролера домену лежить Active Directory (AD) — база даних, яка зберігає інформацію про мережеві об'єкти, такі як користувачі, групи, комп'ютери, принтери та послуги.[16]

Відмовостійкість та реплікація: для середовищ з кількома контролерами домену реплікація забезпечує узгодженість та надійність даних у мережі.[16]

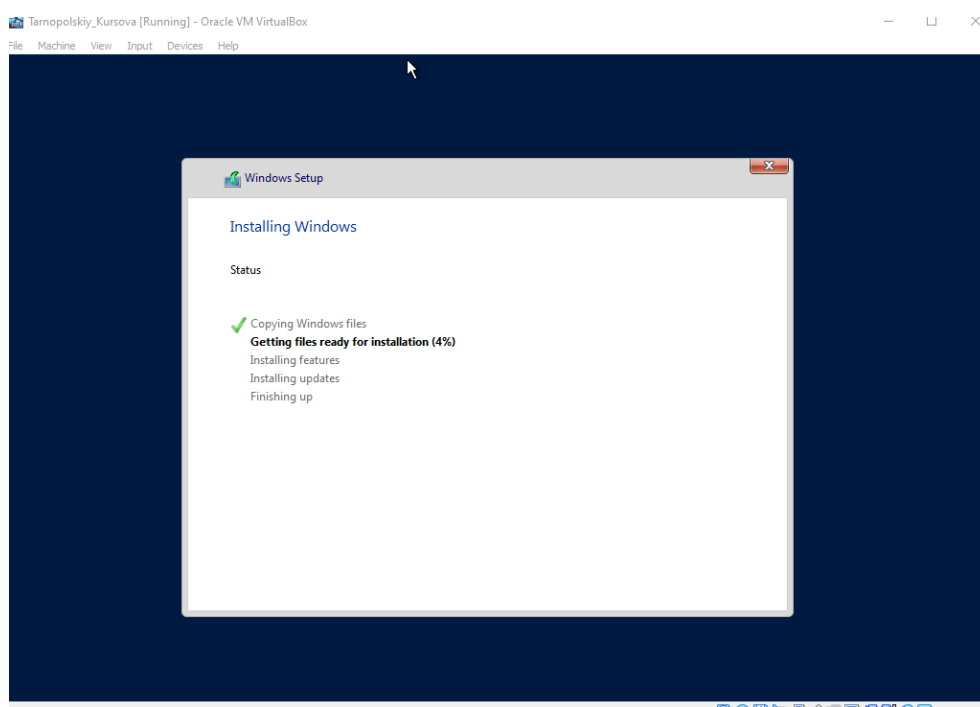


Рисунок 2.1 – інсталяція Windows сервер

2.2 Проектування логічної топології мережі

IPv4 (англ. Internet Protocol version 4) — четверта версія мережевого протоколу IP. Перша версія протоколу, яка набула широкого розповсюдження. Протокол IPv4, описаний у RFC 791 (вересень 1981 року), прийшов на заміну описаному у RFC 760 (січень 1980 року). Використовує 4-байтну форму запису адрес пристроїв в комп'ютерній мережі.[17]

Він забезпечує унікальну адресу для кожного пристрою, підключеного до мережі, що дозволяє цим пристроям знаходити один одного та обмінюватися даними. Кожна IPv4-адреса складається з 32 бітів і зазвичай записується у вигляді чотирьох чисел, розділених крапками (наприклад, 192.168.1.1). Загальна кількість можливих IPv4-адрес становить приблизно 4,3 мільярда, що колись здавалося достатнім, але з часом цього простору стало не вистачати через стрімке зростання кількості пристроїв, підключених до мережі. Незважаючи на те, що поступово впроваджується новіший протокол IPv6, IPv4 залишається надзвичайно важливим, оскільки більшість Інтернету все ще працює на його основі. Його значення полягає в тому, що без нього пристрої просто не змогли б "побачити" одне одного в мережі, а Інтернет не зміг би функціонувати як єдина глобальна система.

Таблиця 2.1 адресація мережі

Пристрій	Канал	IP-адреси	Маска	Префікс
Мережа	-	192.168.1.0	255.255.255.0	/24
Srv-Tarnopolskiy	Мережний адаптер	192.168.1.3	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	-	-
Comp1-Tarnopolskiy	Мережний адаптер	192.168.1.4	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	-	-
Comp2-Tarnopolskiy	Мережний адаптер	192.168.1.5	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.1.1	-	-

2.3 Вибір середовища для реалізації курсового проєкту

Для реалізації курсового проєкту було обрано віртуалізаційне середовище Oracle VM VirtualBox.

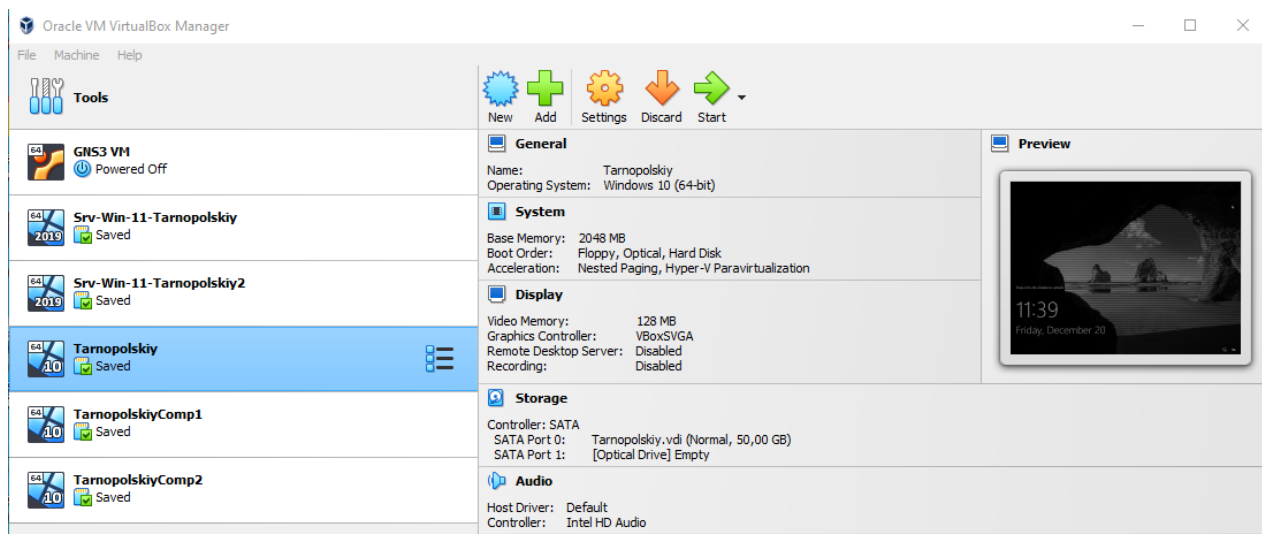


Рисунок 2.2 – Середовище VirtualBox

Для реалізації мережевої інфраструктури, включаючи контролер домену та робочі станції, було обрано VirtualBox — безкоштовну віртуалізаційну платформу, яка дозволяє створювати та запускати віртуальні машини (VM) на фізичному комп'ютері.

VirtualBox — це програмне забезпечення, яке імітує справжній комп'ютер, що дає користувачеві можливість встановлювати, запускати й використовувати інші операційні системи, наче звичайні застосунки. [18]

VirtualBox підтримує різноманітні операційні системи, що дає змогу створювати та тестувати різні конфігурації мережі без необхідності виділяти додаткове фізичне обладнання.

Використання VirtualBox для розгортання контролера домену та робочих станцій має кілька переваг:

- Економія ресурсів: оскільки VirtualBox дозволяє запускати кілька віртуальних машин на одному фізичному сервері, можна створити віртуальний контролер домену Windows Server та декілька робочих станцій Windows без потреби в додатковому обладнанні.

- Гнучкість та простота налаштування: VirtualBox дозволяє швидко створювати, конфігурувати та змінювати віртуальні машини. Це забезпечує легкість у налаштуванні різних ролей (наприклад, контролера домену, клієнтських робочих станцій, серверів) в одному середовищі.

- Тестування та ізоляція: віртуальні машини можна ізолювати від основної системи, що дозволяє тестувати конфігурації, політики безпеки та налаштування без ризику вплинути на основну операційну систему чи мережу. Це ідеально підходить для навчальних цілей та тестових середовищ.

- Зручність у відновленні та міграції: завдяки можливості створення моментальних знімків (snapshots) віртуальних машин, можна зберігати поточний стан середовища і, у разі потреби, відновлювати його до попереднього стану. Це особливо корисно для тестування змін у конфігураціях домену чи робочих станцій.

- Масштабованість: VirtualBox дозволяє створювати та налаштовувати кілька віртуальних машин на одному фізичному сервері. Це дає змогу масштабувати інфраструктуру віртуальних мереж без додаткових витрат на фізичні сервери, що є великим плюсом для малих і середніх організацій або для лабораторій.

Завдяки цим можливостям VirtualBox є відмінним вибором для реалізації середовища, що включає контролер домену та робочі станції, дозволяючи створити ефективну, гнучку і недорогу інфраструктуру для тестування та навчання.

Висновки до другого розділу

У другому розділі було проведено аналіз робочих станцій та сервера, досліджено програмне забезпечення мережевих пристроїв, було виявлено їх переваги, особливості та вразливості. Також було розглянуто загальну топологію мережі та її схему.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		33

Досліджено також протокол IPv4, його важливість та необхідність, було розроблено схему адресації на основі даного протоколу з урахуванням кількості пристроїв в мережі.

Особливу увагу було приділено VirtualBox — безкоштовній віртуалізаційній платформі, яка дозволяє створювати та запускати віртуальні машини (VM) на фізичному комп'ютері. Було досліджено її гнучкість, масштабованість, зручність та особливості реалізації.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		34

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ ФУНКЦІОНУВАННЯ МЕРЕЖІ, ЗАСОБІВ ЇЇ АДМІНІСТРУВАННЯ ТА БЕЗПЕКИ.

3.1 Вибір обладнання для організації роботи мережі

Microsoft Windows або Windows (англ. вікна, скор. Win) — група комерційних пропрієтарних операційних систем корпорації Microsoft, орієнтованих на управління за допомогою графічного інтерфейсу.[19]

Вибір операційної системи Windows для робочих станцій у доменному середовищі має кілька важливих причин, пов'язаних з її перевагами, зручністю та інтеграцією з іншими компонентами мережі:

- Інтеграція з Active Directory: Windows є основною операційною системою для роботи з Active Directory, що забезпечує централізоване управління користувачами, комп'ютерами та іншими мережевими ресурсами. Оскільки Active Directory є важливим компонентом для управління доменом, використання Windows на робочих станціях дозволяє безшовно інтегрувати ці пристрої в мережу та використовувати можливості аутентифікації, авторизації та управління безпекою.

- Сумісність з корпоративними додатками: Windows є однією з найпоширеніших операційних систем у корпоративному середовищі. Багато стандартних програм та корпоративних додатків розроблені саме для Windows, що забезпечує сумісність з широким спектром програмного забезпечення. Це дозволяє без проблем використовувати необхідні програми для офісної роботи, фінансів, управління проектами та іншого.

- Підтримка безпеки та оновлень: операційна система Windows забезпечує регулярні оновлення безпеки, що допомагає захистити робочі станції від останніх загроз і вразливостей. Вона також підтримує налаштування політик безпеки через Group Policy, що дозволяє централізовано контролювати доступ, паролі, шифрування та інші важливі аспекти безпеки на всіх робочих станціях.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		35

- Підтримка віддаленого доступу та управління: Windows має вбудовані інструменти для віддаленого доступу, такі як Remote Desktop, що дозволяє адміністраторам дистанційно працювати з робочими станціями для налаштування, підтримки та управління. Це важливо для забезпечення зручності адміністрування, особливо в великих організаціях.

- Широка підтримка та документація: оскільки Windows є однією з найбільш популярних операційних систем, вона має величезну кількість ресурсів для підтримки, як у вигляді офіційної документації, так і в онлайн-спільнотах. Це значно полегшує вирішення проблем, налаштування та оптимізацію робочих станцій.

- Зручність у використанні: Windows має такий інтерфейс, що забезпечує зручність для користувачів, навіть тих, хто не має спеціалізованих технічних знань. Це дозволяє забезпечити високу продуктивність та ефективність роботи співробітників без потреби в додатковому навчанні або підвищенні кваліфікації.

Завдяки цим перевагам Windows є ідеальним вибором для робочих станцій у доменній мережі, забезпечуючи стабільність, безпеку та зручність для користувачів і адміністраторів.

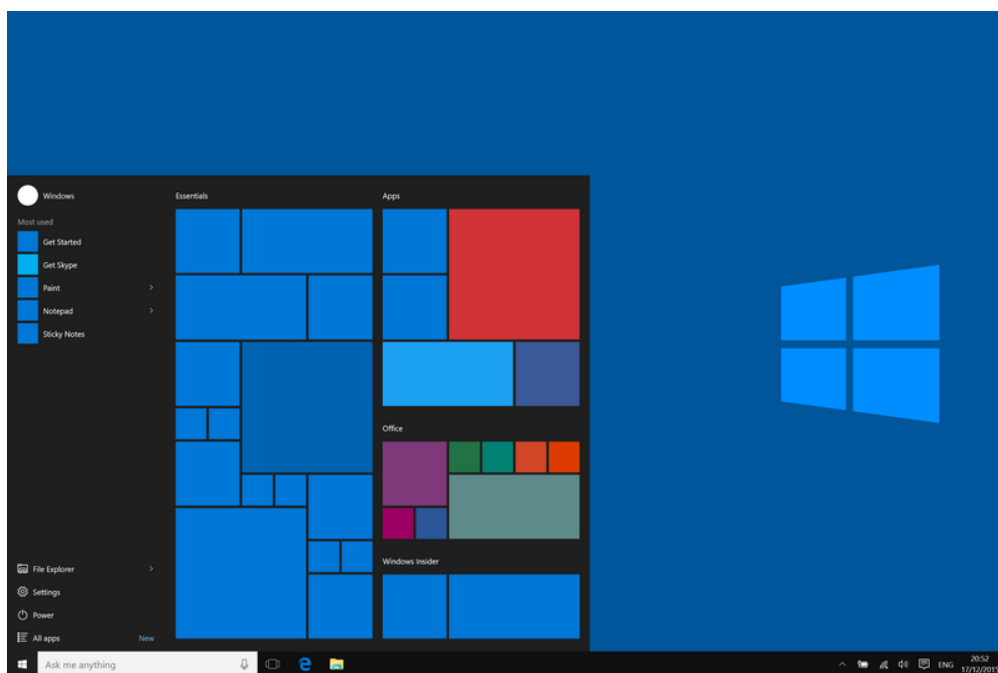


Рисунок 3.1 – ОС Windows

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		36

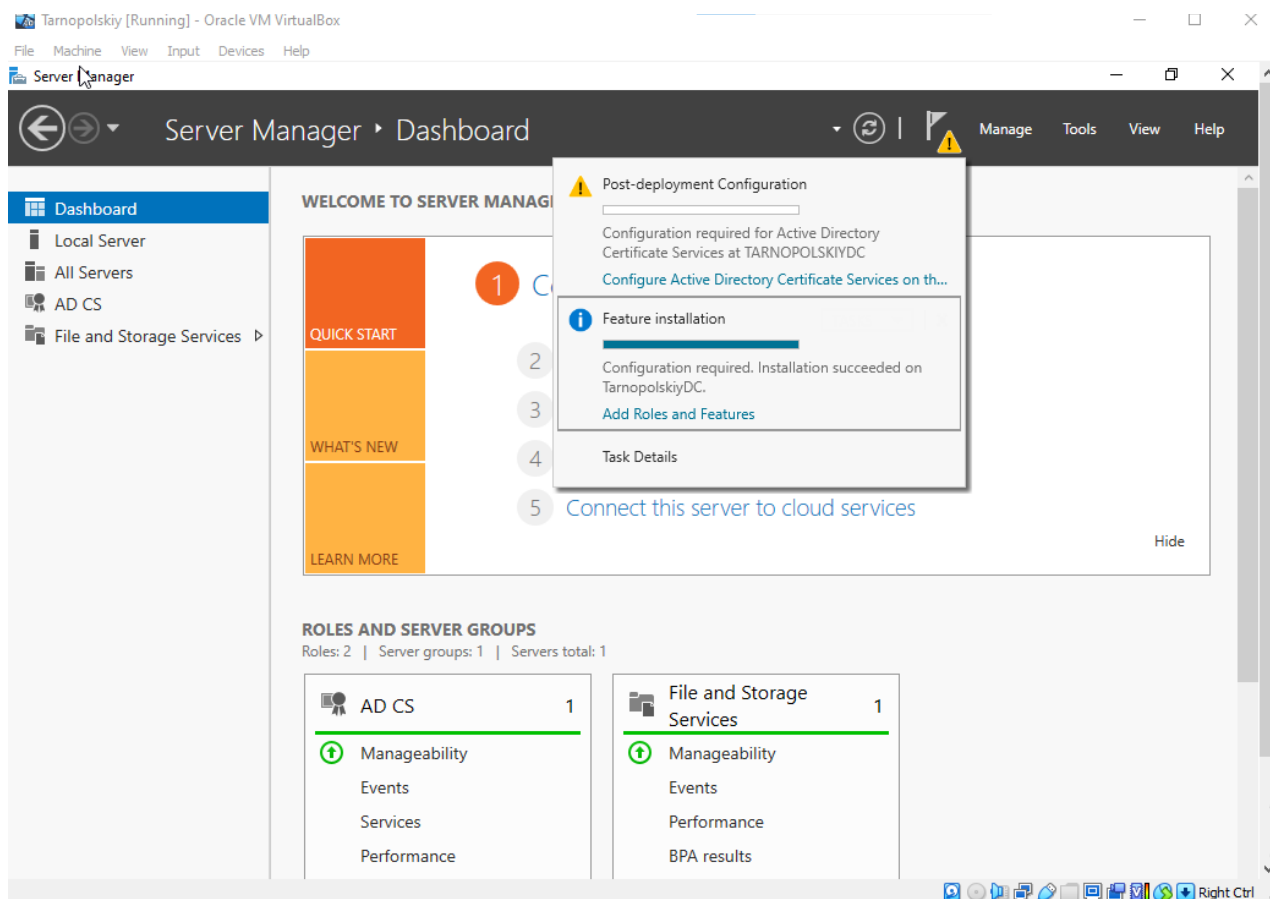


Рисунок 3.2 – Windows Server

Вибір Windows Server 2019 для реалізації контролера домену та серверних функцій має кілька вагомих переваг, що обґрунтовують цей вибір у корпоративному середовищі:

- Підтримка Active Directory: Windows Server 2019 є потужною платформою для налаштування і підтримки Active Directory (AD). Оскільки AD є критично важливим для управління доменом, а також для забезпечення централізованої аутентифікації, авторизації та управління обліковими записами, Windows Server 2019 забезпечує найкращу інтеграцію з цією технологією. Це дозволяє ефективно адмініструвати користувачів, групи та пристрої у домені.

- Посилена безпека: Windows Server 2019 містить покращені функції безпеки, включаючи підтримку Windows Defender Advanced Threat Protection (ATP), що допомагає виявляти і нейтралізовувати загрози.

- Крім того, підтримка шифрування за допомогою функцій, таких як BitLocker та Windows Defender Application Control, забезпечує високий рівень захисту даних і системи від несанкціонованого доступу.

- Гнучкість у віртуалізації: Windows Server 2019 підтримує технології віртуалізації через Hyper-V, що дозволяє створювати віртуальні машини для розгортання додаткових служб, таких як тестові сервери, резервні копії або додаткові контролери домену. Це забезпечує гнучкість при управлінні серверами та ресурсами, а також дозволяє економити на фізичному обладнанні.

- Розширена інтеграція з хмарними сервісами: Windows Server 2019 має вбудовані функції інтеграції з хмарними платформами, такими як Microsoft Azure. Це дозволяє легко здійснювати гібридні розгортання, де частина ресурсів або служб може бути перенесена в хмару, забезпечуючи більш ефективне управління та масштабованість інфраструктури.

- Підтримка контейнерів та мікросервісів: Windows Server 2019 має підтримку контейнерів Windows і Linux, що дає змогу розгортати сучасні додатки та сервіси за допомогою технологій контейнеризації. Це може бути важливим для розгортання новітніх додатків, що працюють в середовищах мікросервісів, та для підвищення ефективності роботи серверів.

- Управління через PowerShell та Windows Admin Center: Windows Server 2019 має вдосконалені інструменти для адміністрування, такі як PowerShell, а також Windows Admin Center для централізованого управління серверами. Це дозволяє адміністраторам зручно виконувати операції з налаштування та моніторингу системи, а також автоматизувати процеси.

- Покращення в продуктивності: Windows Server 2019 має низку покращень у продуктивності, що дозволяє більш ефективно використовувати ресурси серверів. Оптимізація роботи з пам'яттю, швидкість обробки запитів та підтримка сучасних архітектурних рішень дозволяють серверам працювати з максимальною ефективністю.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		38

Таким чином, вибір Windows Server 2019 для реалізації контролера домену та серверних функцій забезпечує надійність, масштабованість і безпеку інфраструктури в доменному середовищі, зручність адміністрування, а також підтримку новітніх технологій для розвитку і інтеграції з хмарними та контейнерними платформами.

3.2 Створення середовища AD

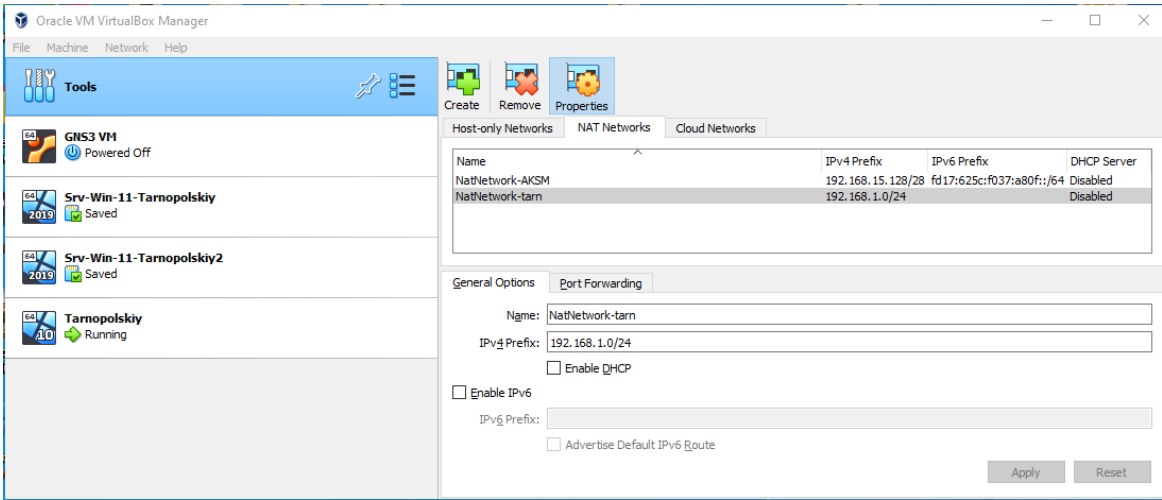


Рисунок 3.3 – створення NAT-Network

Проектуємо мережу, налаштовуємо IP-адреси на пристроях та інсталуємо програмне забезпечення. Схема мережі наведена у додатку А.

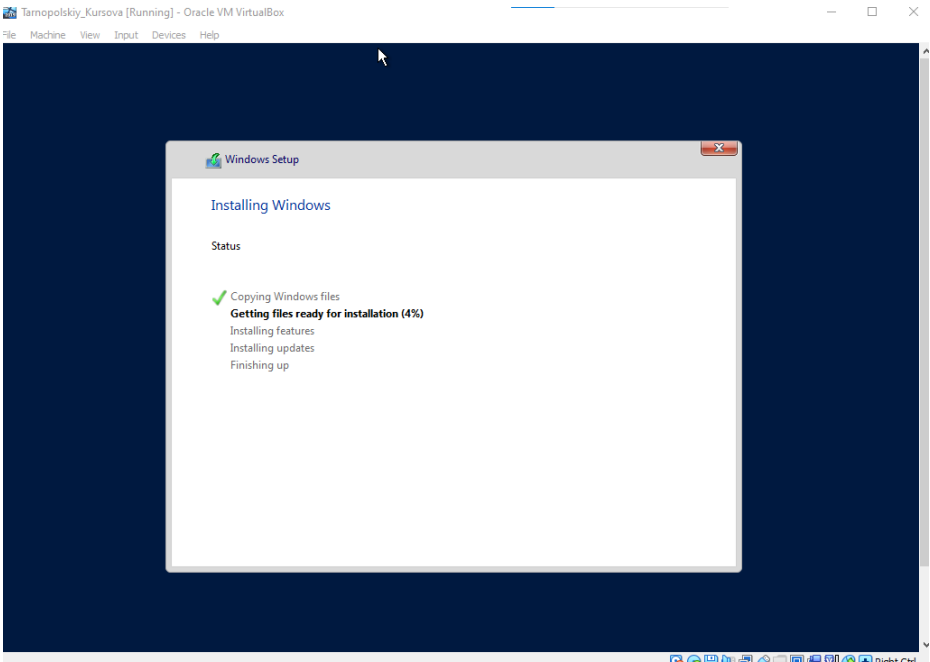


Рисунок 3.4 – інсталяція Windows Server

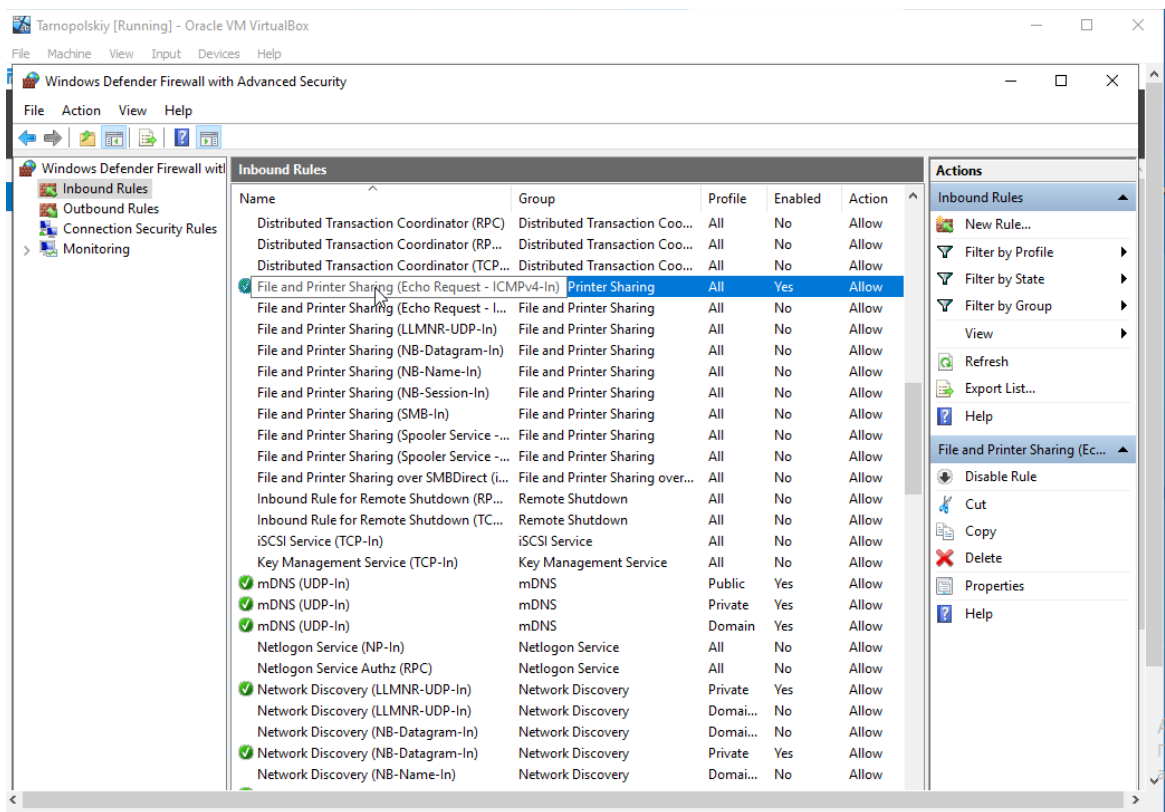


Рисунок 3.5 – налаштування потрібних дозволів

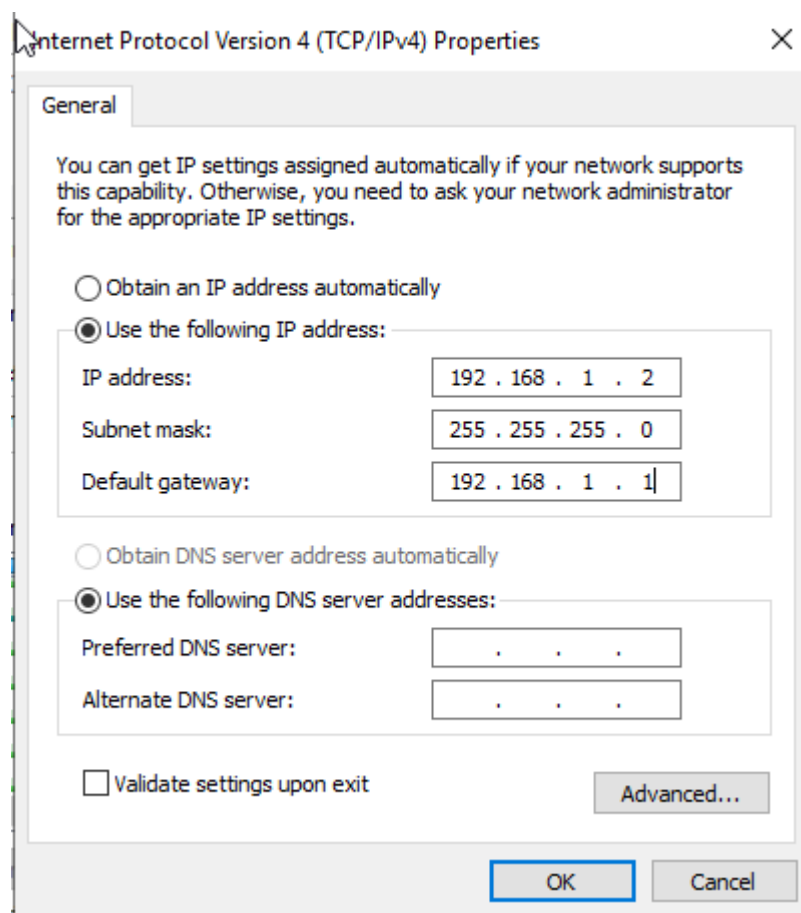


Рисунок 3.6 – ip-address на контролері домену

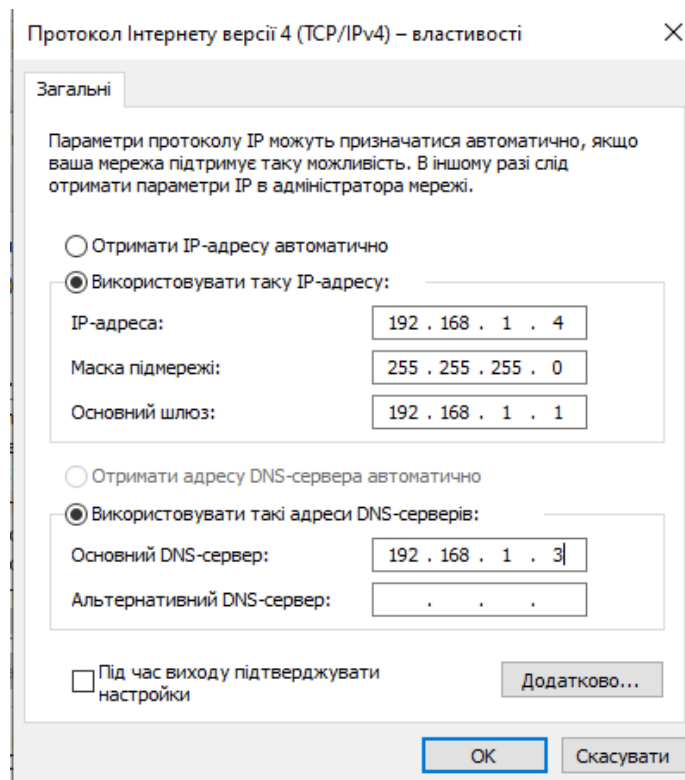


Рисунок 3.7 – ip-address на першій робочій станції

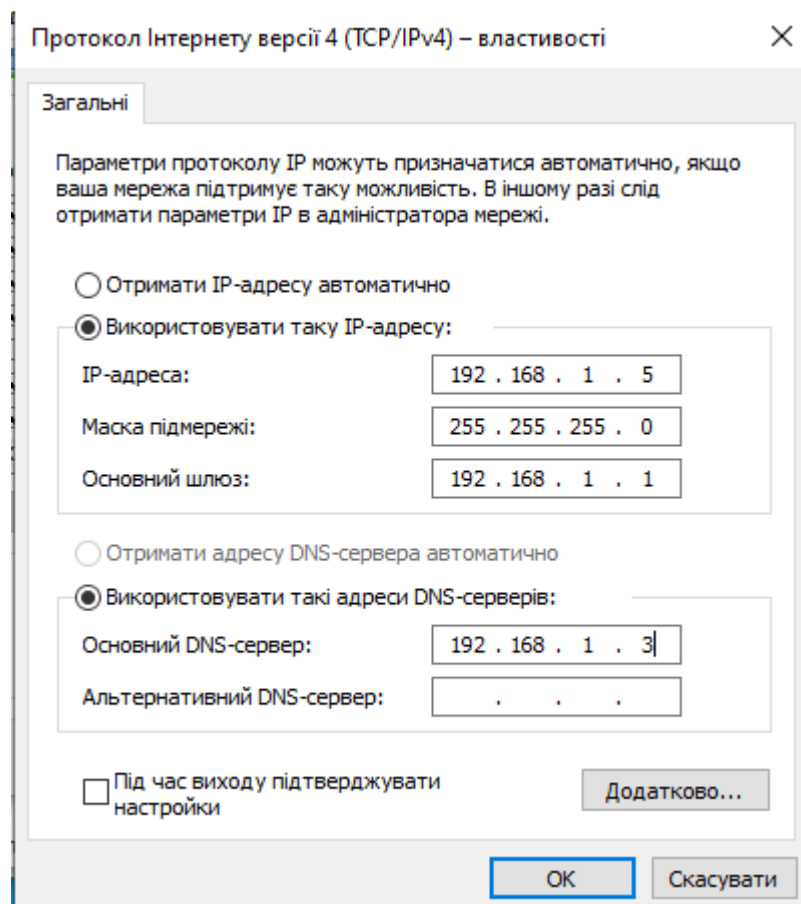


Рисунок 3.8 – ip-address на другій робочій станції

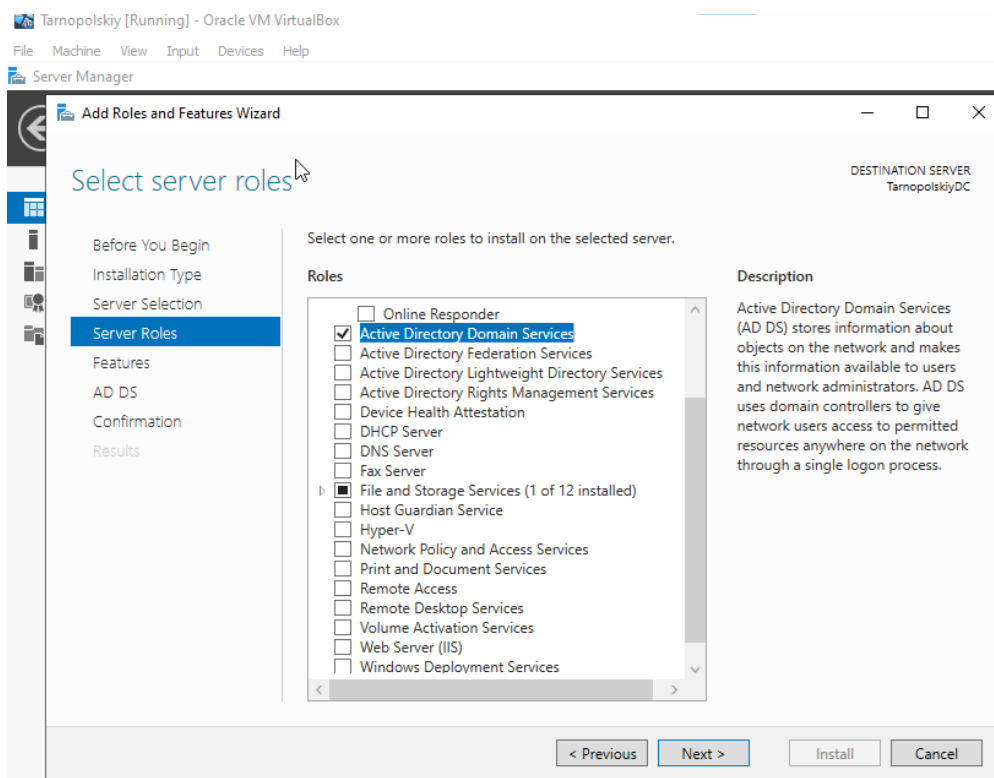


Рисунок 3.9 – встановлення ролі на сервері

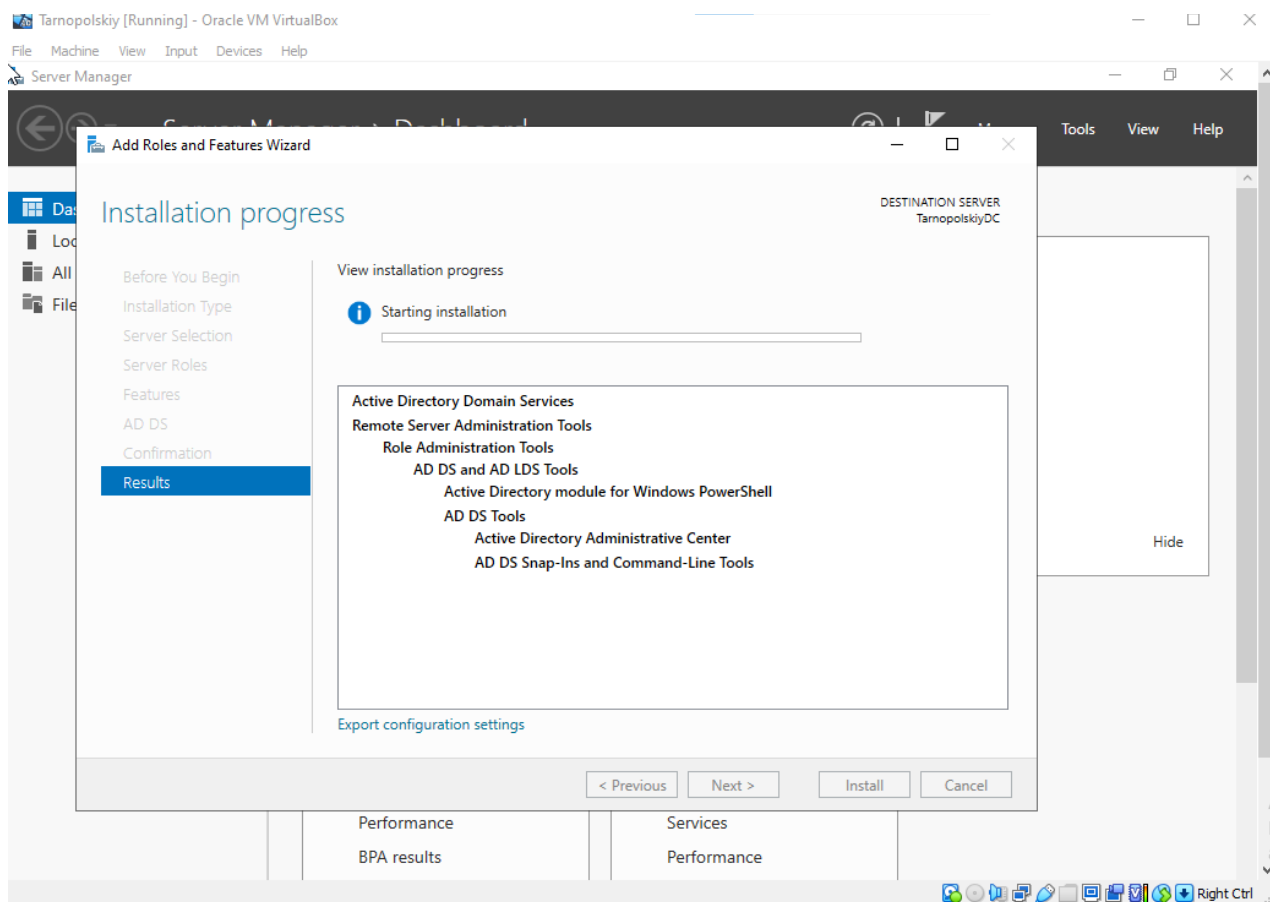


Рисунок 3.10 – встановлення ролей

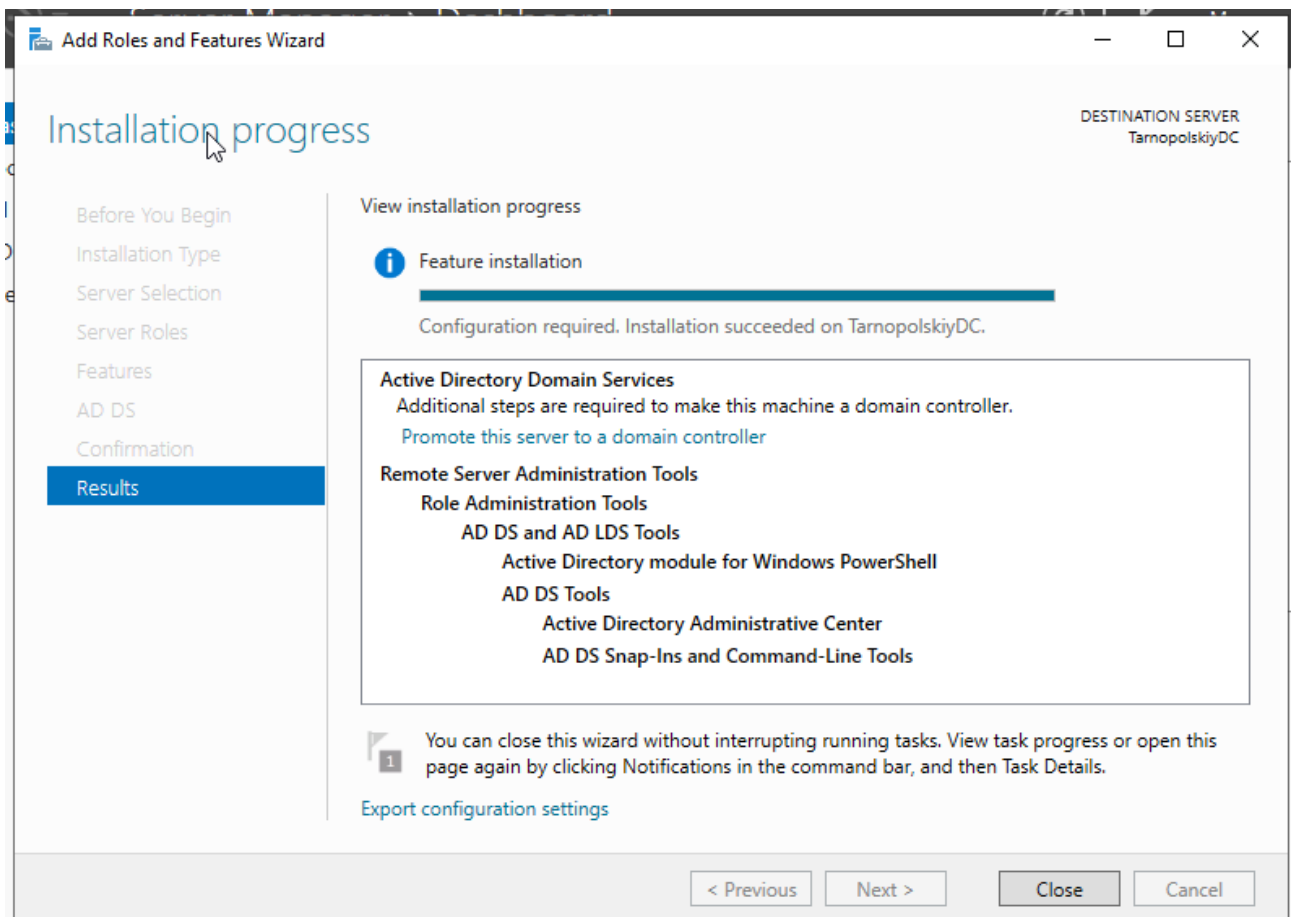


Рисунок 3.11 – успішне встановлення

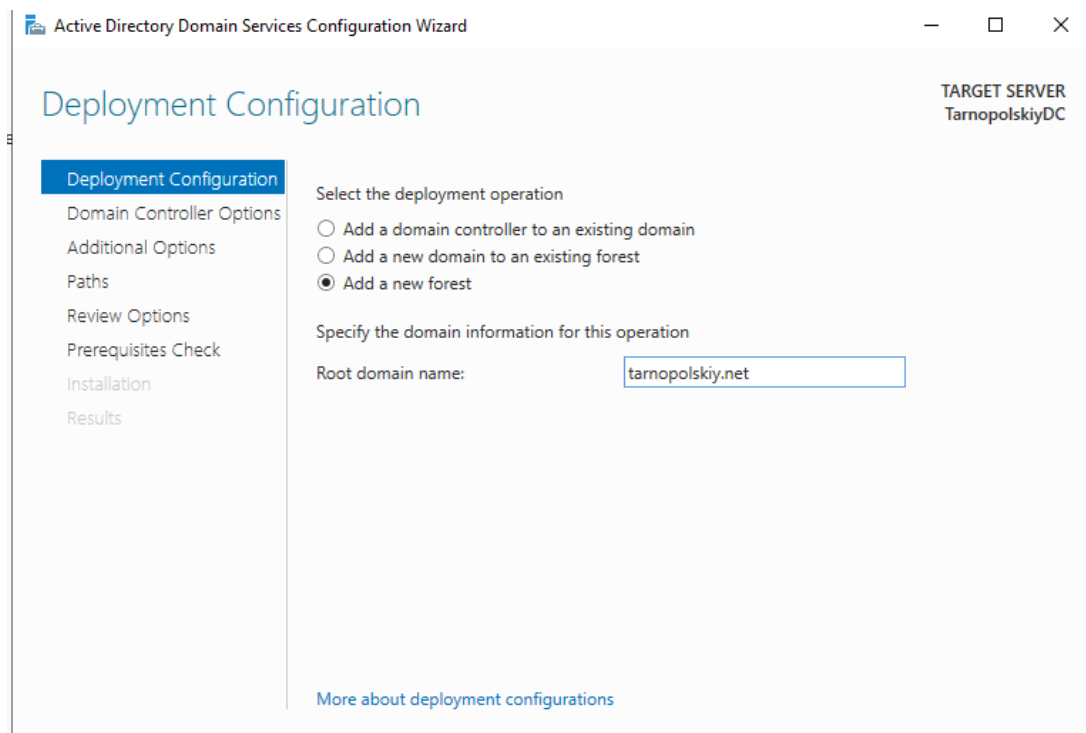


Рисунок 3.12 – створення домену

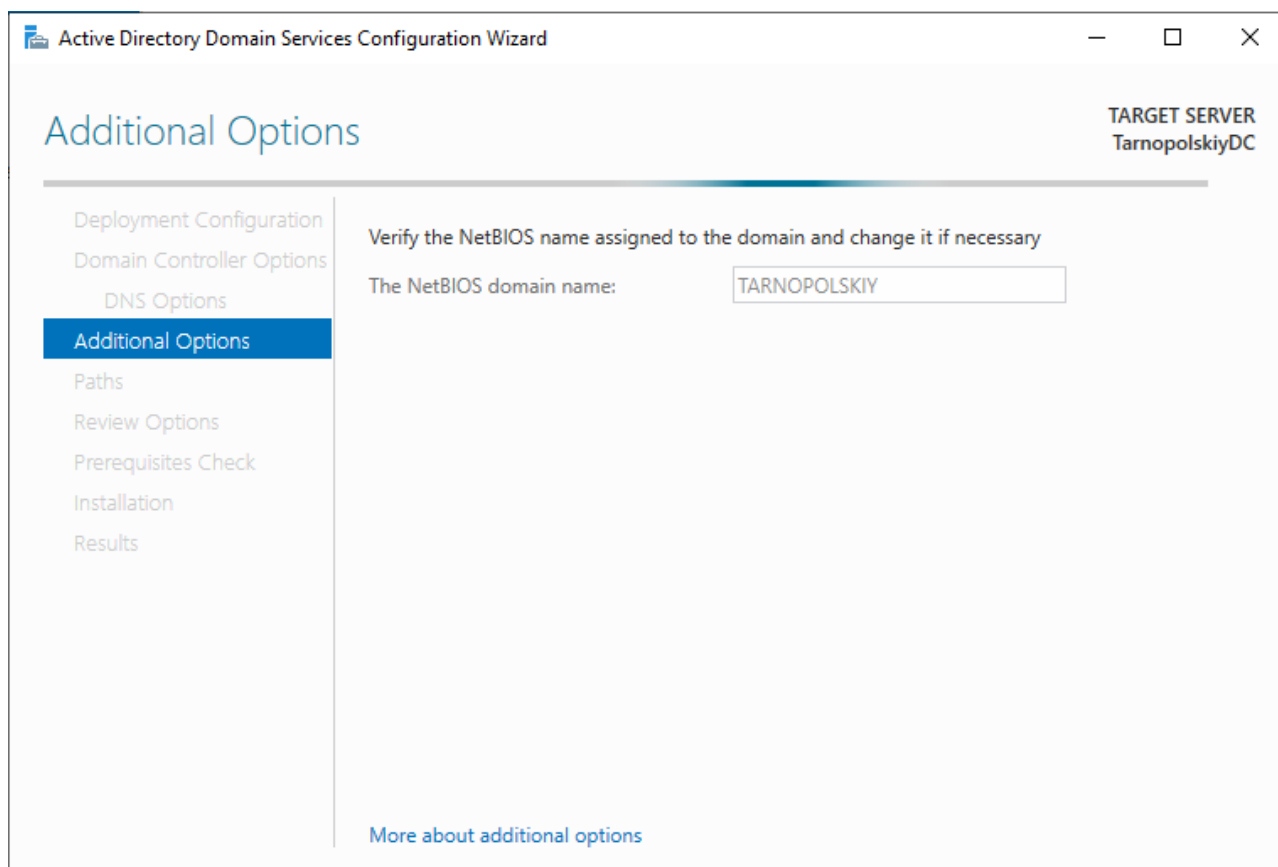


Рисунок 3.13 – створення домену

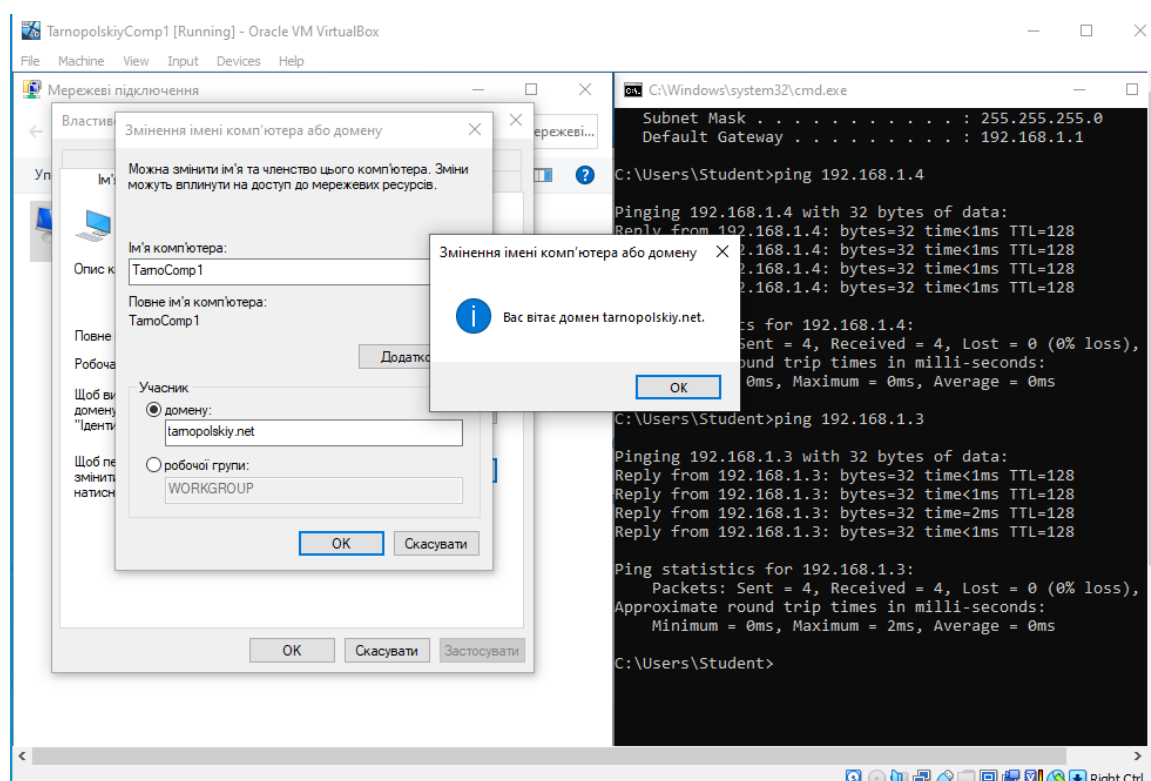


Рисунок 3.14 – підключення до домену, а також перевірка зв'язку на першій робочій станції

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				44
Змн.	Арк.	№ докум.	Підпис	Дата		

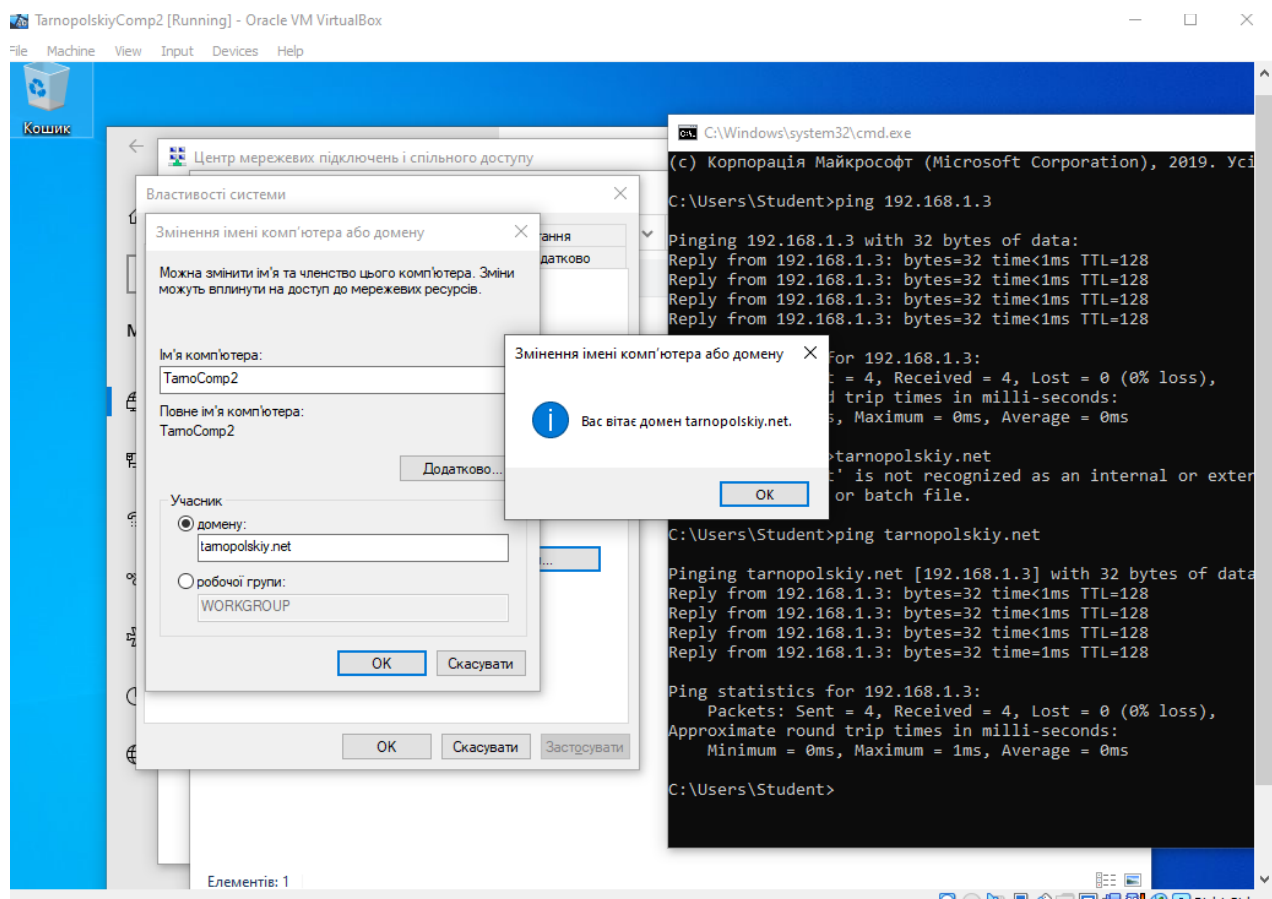


Рисунок 3.15 – підключення до домену, а також перевірка зв'язку на другій робочій станції

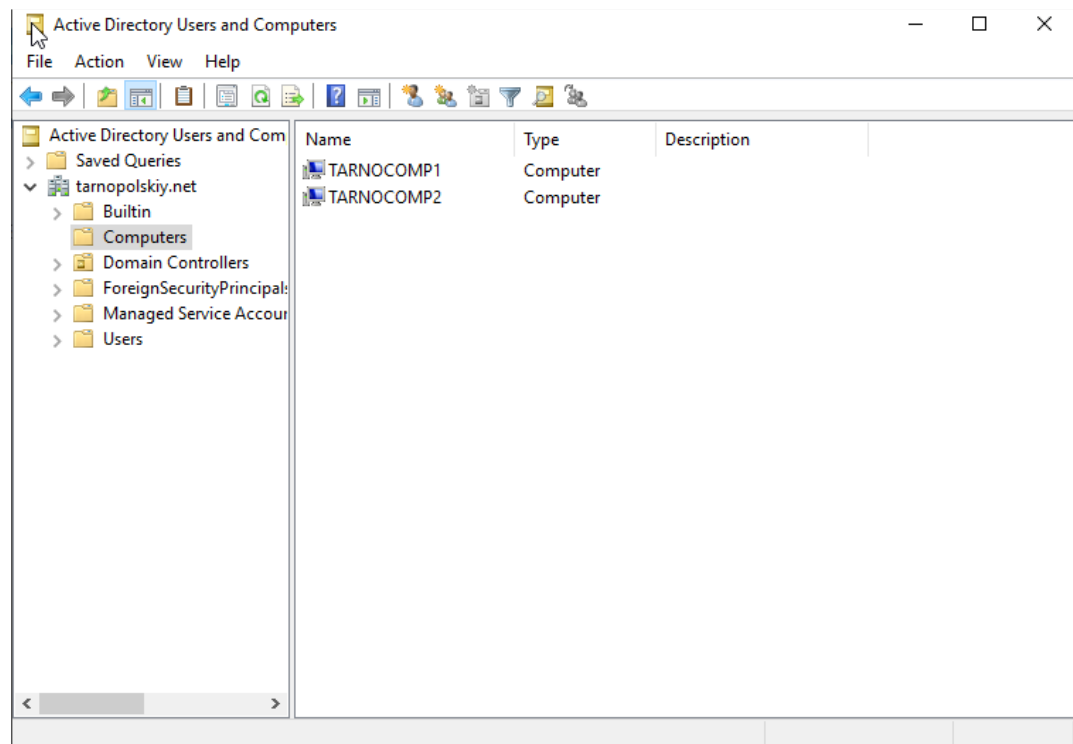


Рисунок 3.16 – підключені до домену робочі станції

New Object - Group

Create in: tarnopolskiy.net/AdminAccounts

Group name:
Server\Admins

Group name (pre-Windows 2000):
Server Admins

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

OK Cancel

Рисунок 3.17 – створення групи адмінів

New Object - Group

Create in: tarnopolskiy.net/UsersAccounts

Group name:
Server Users

Group name (pre-Windows 2000):
Server Users

Group scope

☐ Domain local

☒ Global

☐ Universal

Group type

☒ Security

☐ Distribution

OK Cancel

Рисунок 3.18 – створення групи користувачів

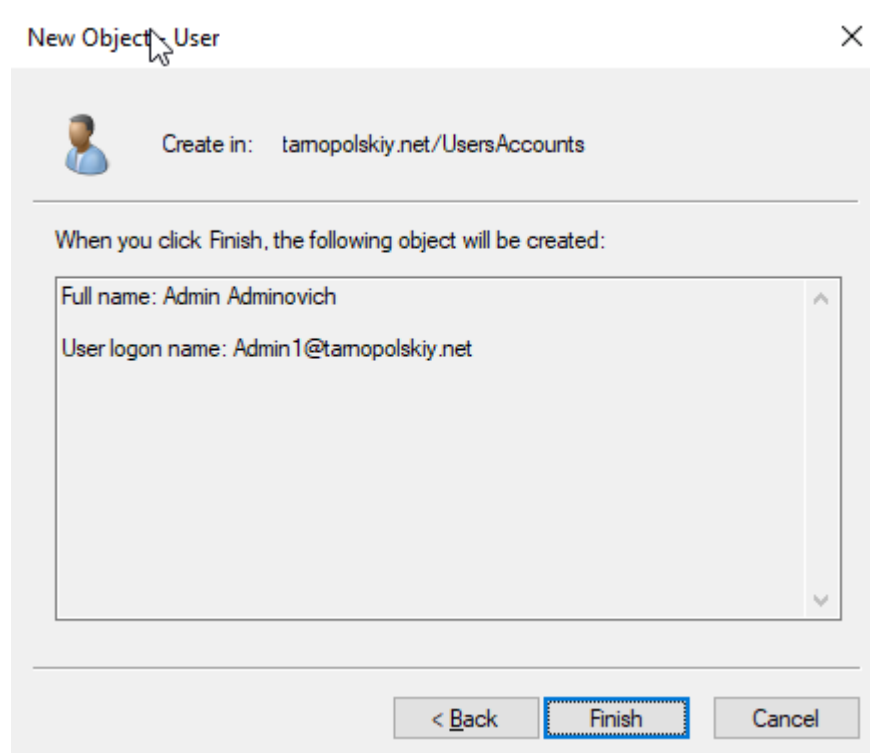


Рисунок 3.19 – приклад створення облікового запису

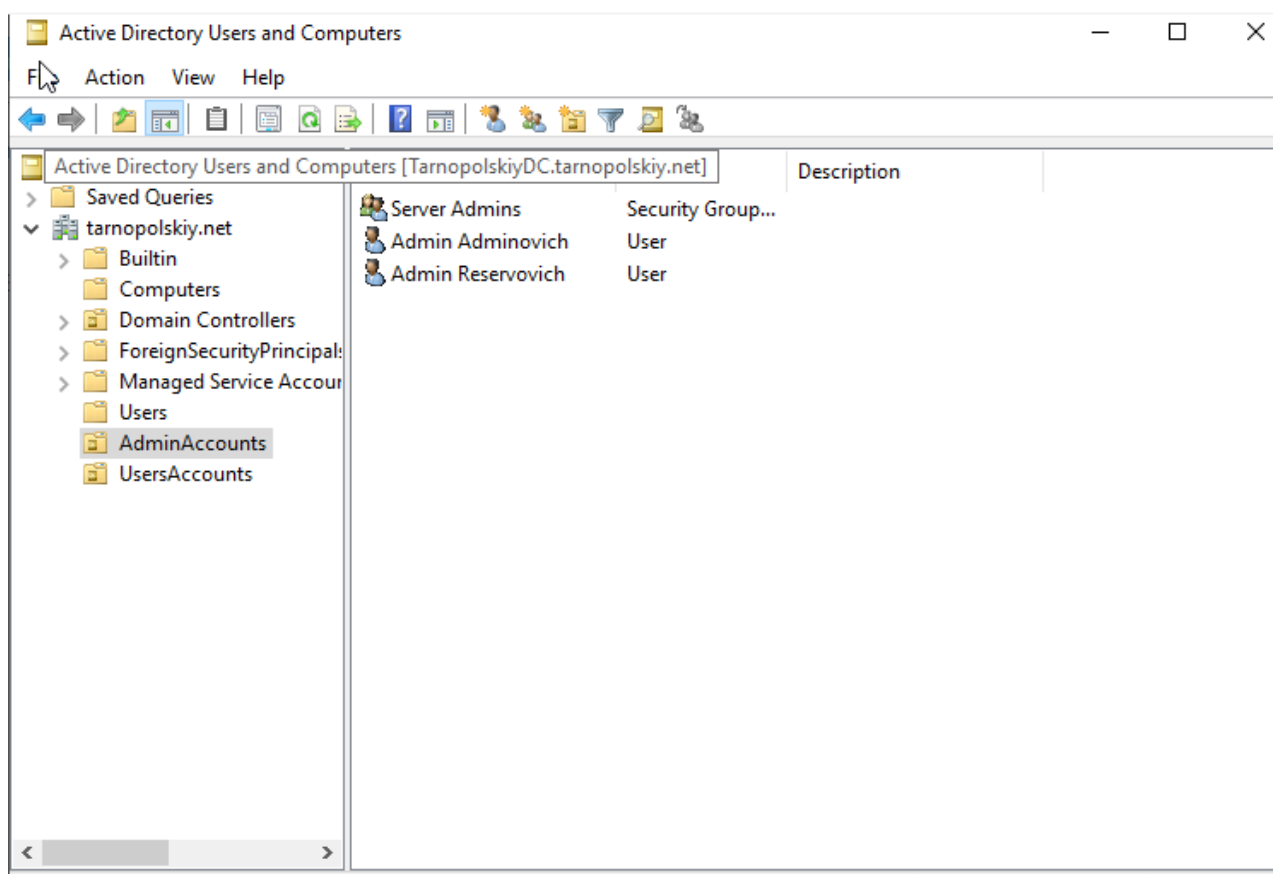


Рисунок 3.20 – створені облікові записи адміністраторів в групі

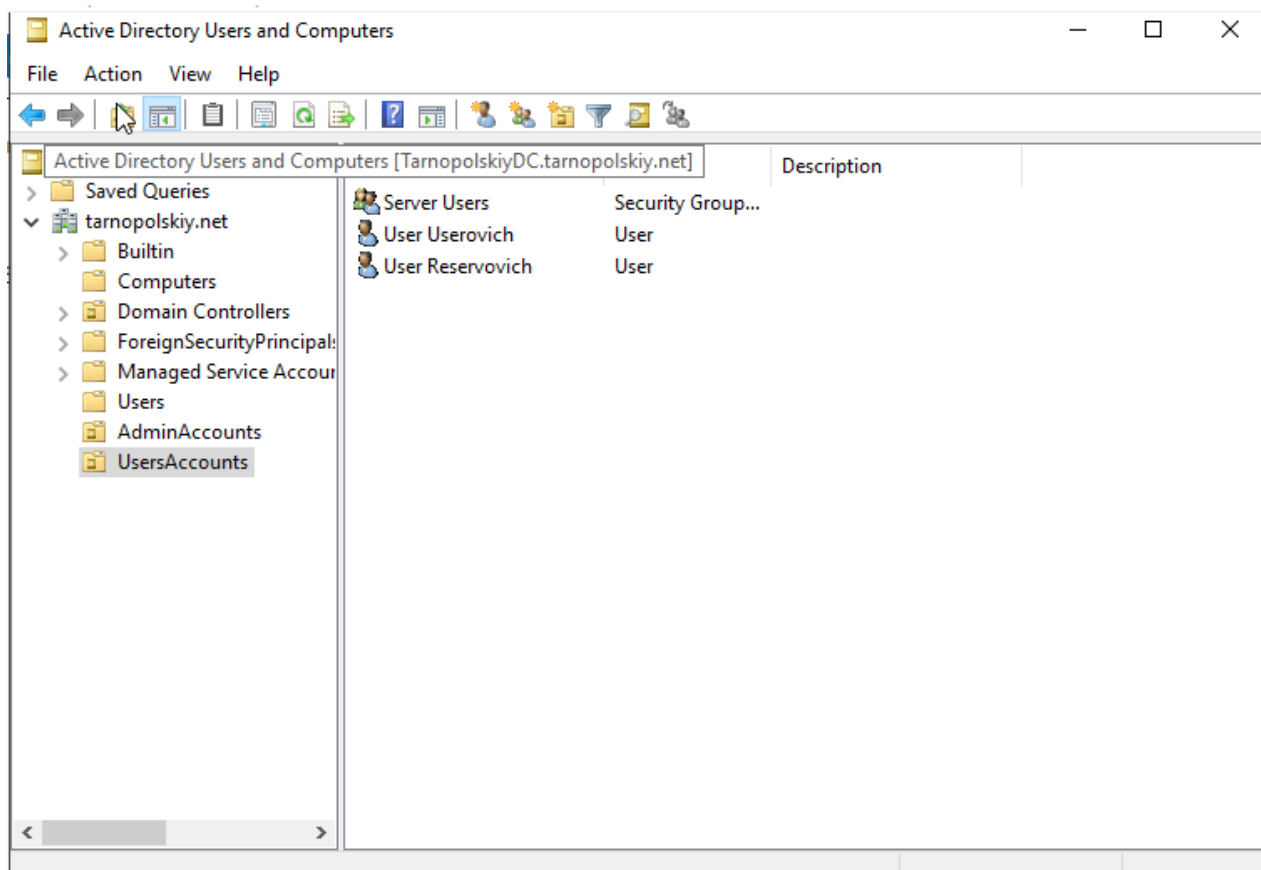


Рисунок 3.21 – створені облікові записи користувачів у групі

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ADGroupMember "Server Admins"

distinguishedName : CN=Admin Adminovich,OU=AdminAccounts,DC=tarnopolskiy,DC=net
name              : Admin Adminovich
objectClass       : user
objectGUID        : 9d639839-9d15-4ce8-8ca3-df735b00edab
SamAccountName    : Admin1
SID               : S-1-5-21-2802516665-2336818053-4112535548-1109

distinguishedName : CN=Admin Reservovich,OU=AdminAccounts,DC=tarnopolskiy,DC=net
name              : Admin Reservovich
objectClass       : user
objectGUID        : 963938ec-7559-4b32-9d73-f64e80fdac40
SamAccountName    : Admin2
SID               : S-1-5-21-2802516665-2336818053-4112535548-1110

PS C:\Users\Administrator> Get-ADGroupMember "Server Users"

distinguishedName : CN=User Userovich,OU=UsersAccounts,DC=tarnopolskiy,DC=net
name              : User Userovich
objectClass       : user
objectGUID        : af785f24-2f19-4f96-8509-f05e00a3204d
SamAccountName    : User1
SID               : S-1-5-21-2802516665-2336818053-4112535548-1111

distinguishedName : CN=User Reservovich,OU=UsersAccounts,DC=tarnopolskiy,DC=net
name              : User Reservovich
objectClass       : user
objectGUID        : a8d99343-5c39-4d84-9942-41bc62ff2a38
SamAccountName    : User2
SID               : S-1-5-21-2802516665-2336818053-4112535548-1112

```

Рисунок 3.22 – перевірка наявних груп та користувачів

3.3 Налаштування групових політик (GPO)

За допомогою Group Policy Management Console (GPMC) можна централізовано контролювати політики для користувачів та комп'ютерів в організації. Далі надано налаштування загальних групових політик для безпеки домену, незалежно від рангу облікових записів чи груп.

Default Domain Policy

Scope Details Settings Delegation

Links

Display links in this location: tamopolskiy.net

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
tamopolskiy.net	No	Yes	tamopolskiy.net

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
Authenticated Users

Add... Remove Properties

WMI Filtering

This GPO is linked to the following WMI filter:

<none> Open

Activate Windows
Go to Settings to activate Windows

Рисунок 3.23 – вкладка scope

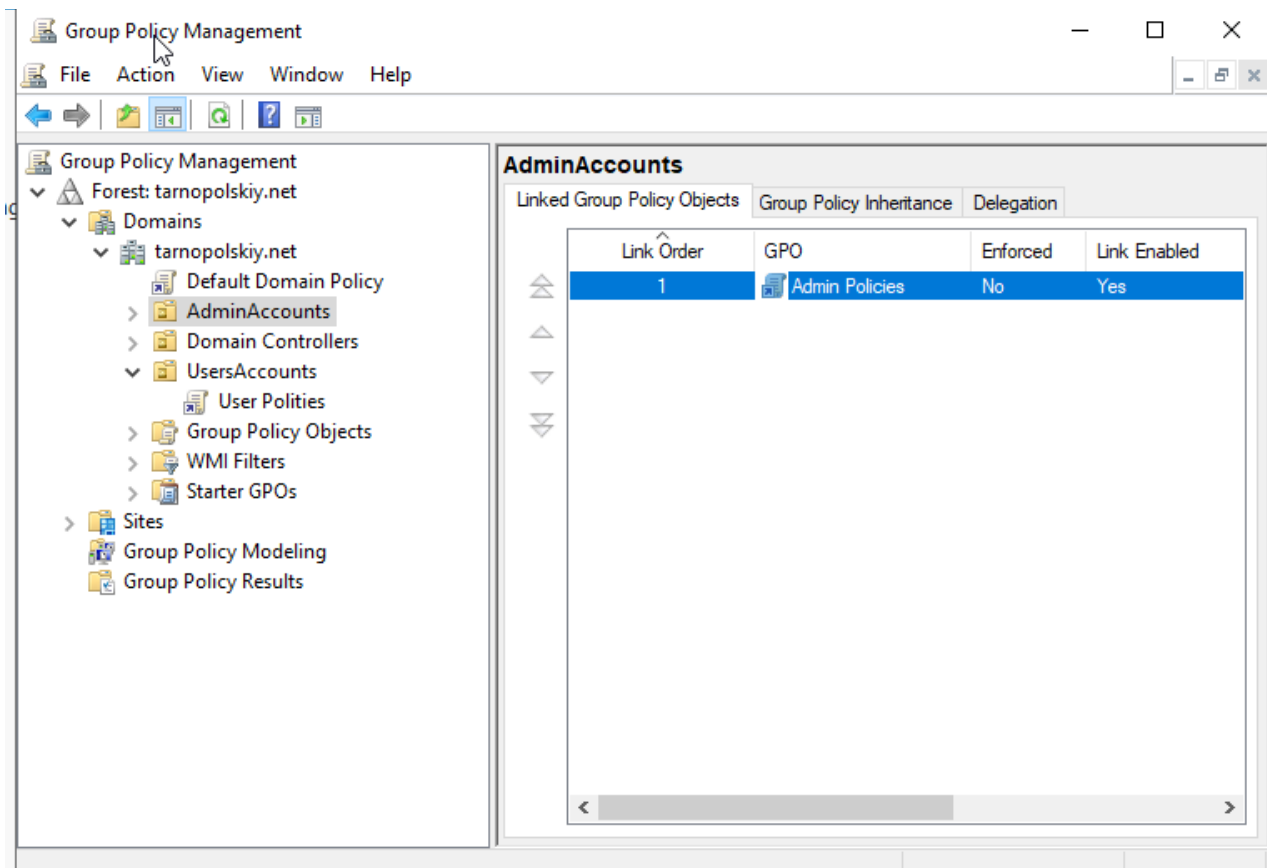


Рисунок 3.24 – створення групових політик для адмінів

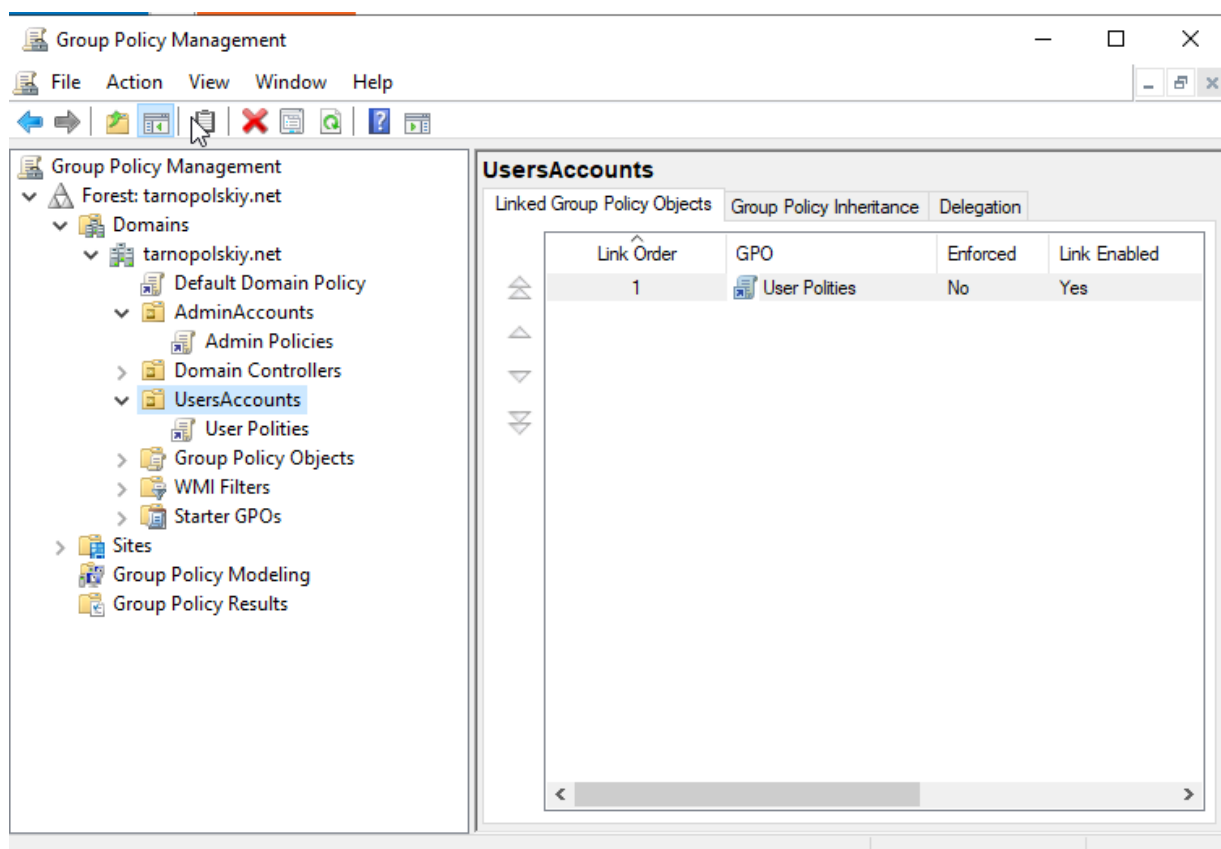


Рисунок 3.25 – створення групових політик для користувачів

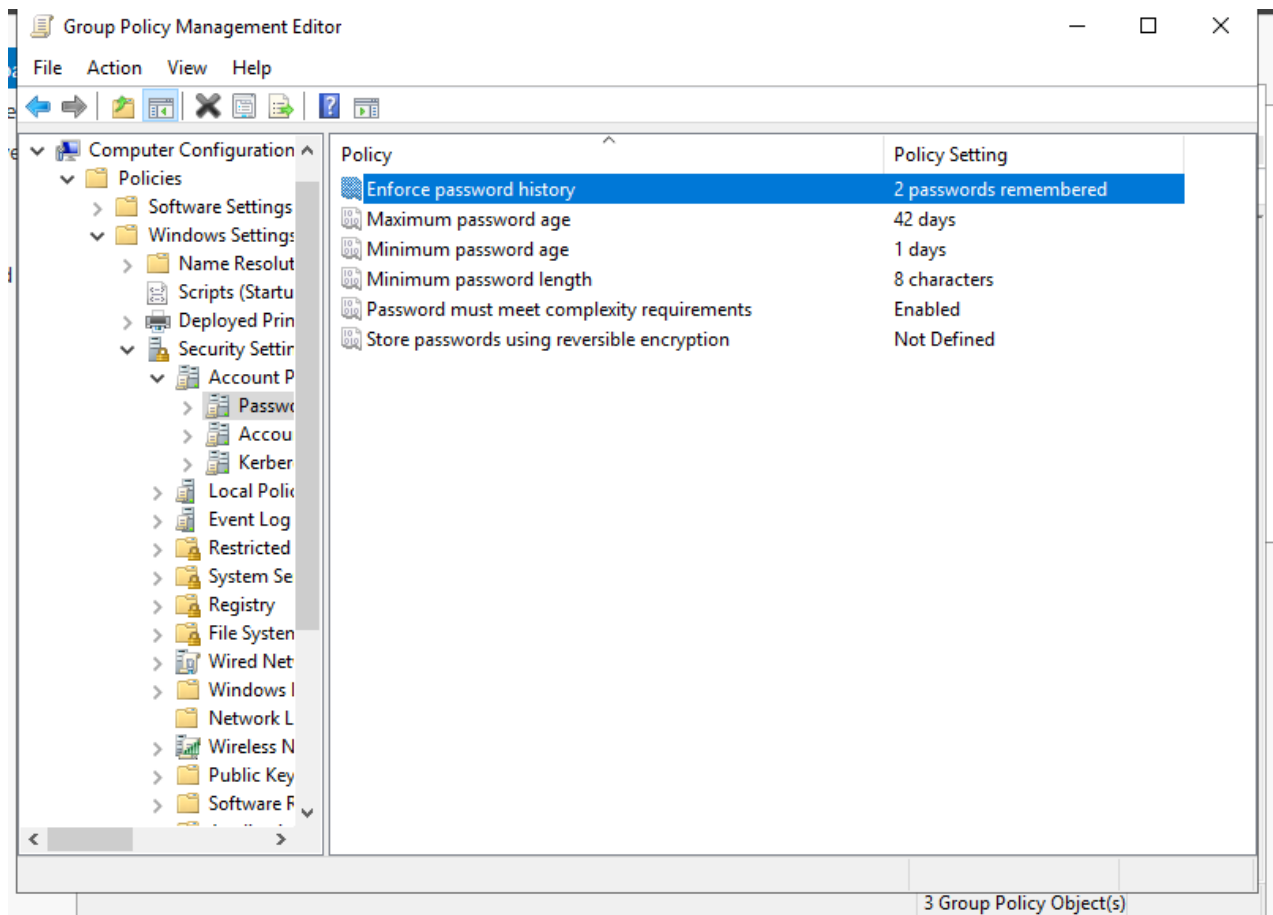


Рисунок 3.26 – налаштування групових політик, яке стосується паролів

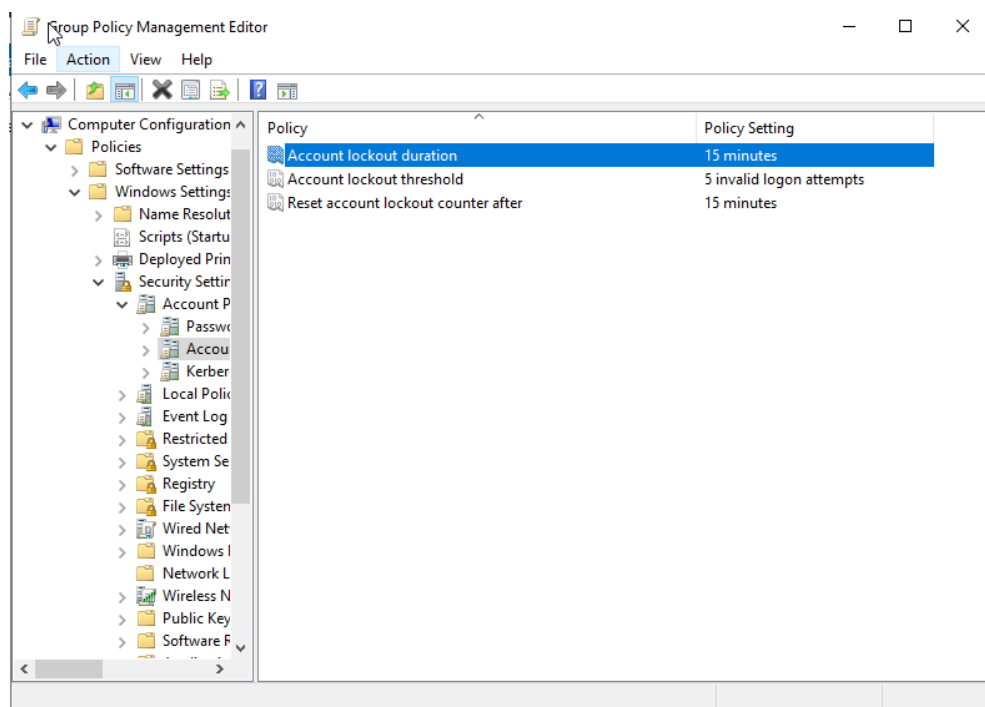


Рисунок 3.27 – налаштування групових політик, яке стосується акаунту

Попередні політики стосувались як групи адмінів, так і групи користувачів. Налаштування в них було однакове. Далі налаштування будуть тільки для групи звичайних користувачів, які обмежують певні можливості:

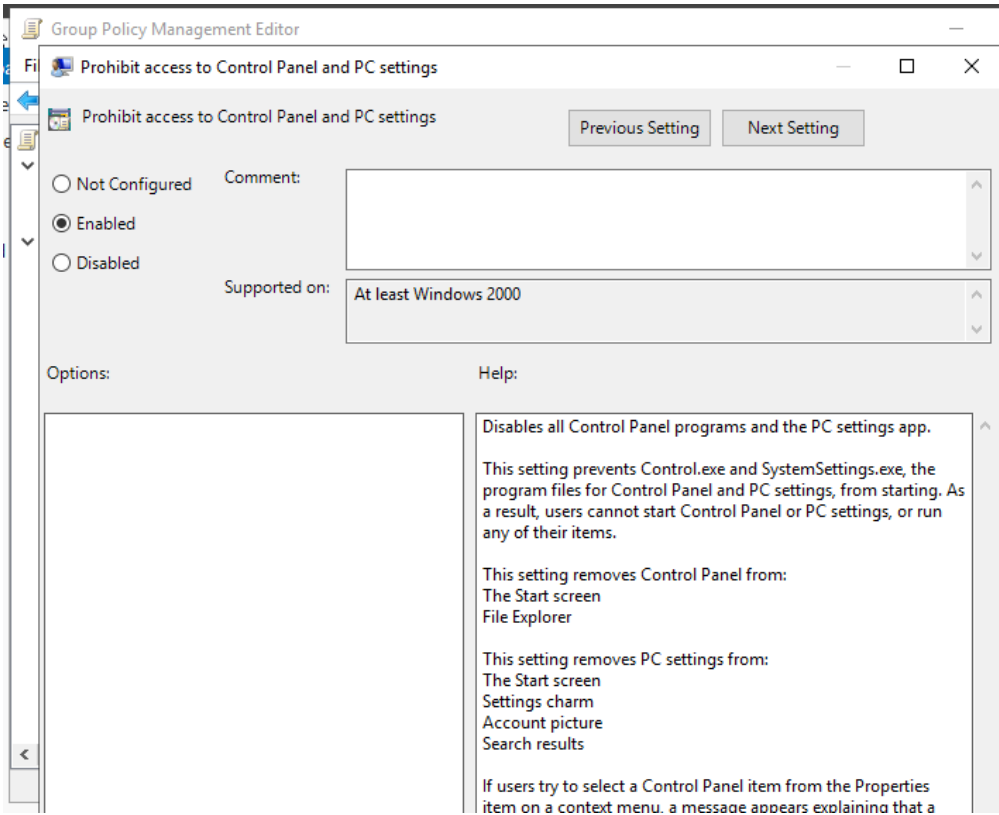


Рисунок 3.28 – налаштування control panel для користувачів

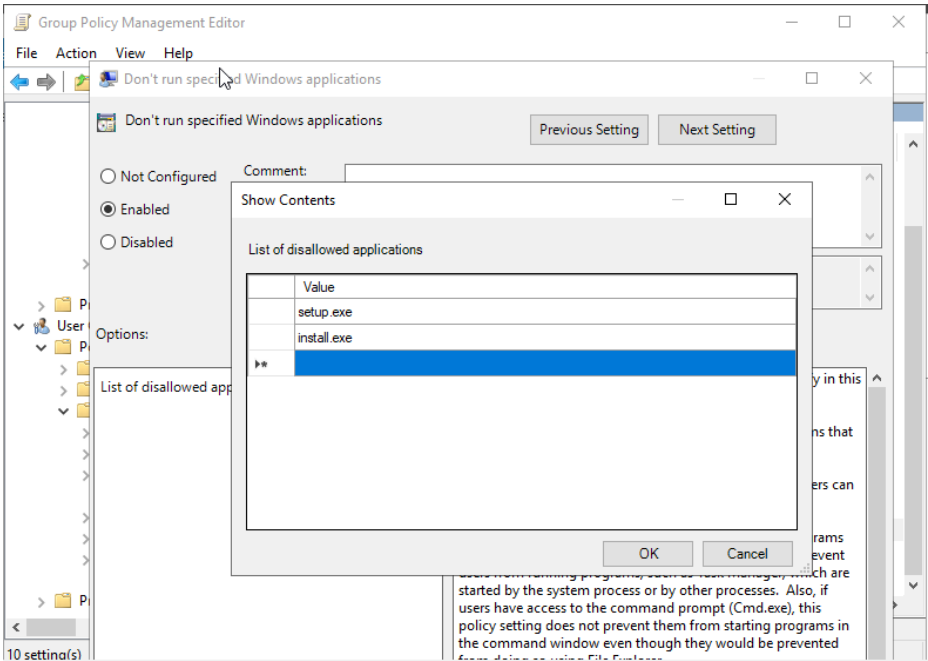


Рисунок 3.29 – обмеження застосування певних файлів для звичайних користувачів

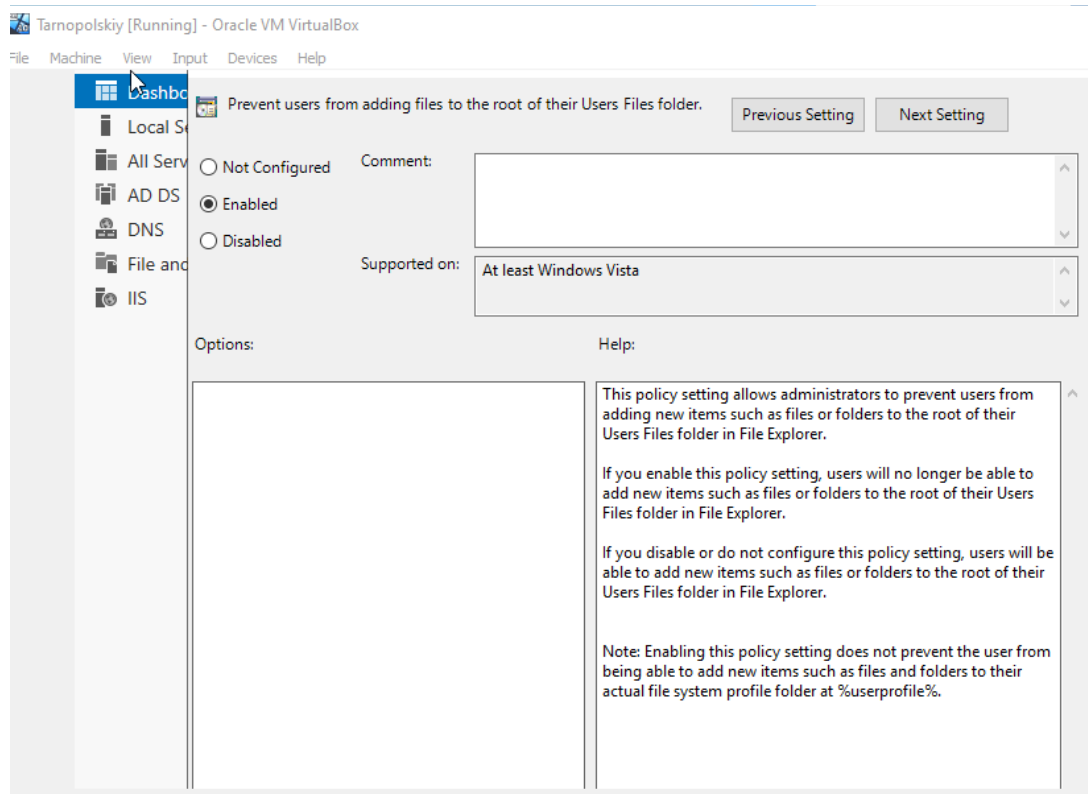


Рисунок 3.30 – налаштування обмеження для звичайних користувачів

Ця політика дозволяє адміністраторам заборонити користувачам додавати нові елементи, такі як файли або папки, до кореневої теки їхніх Users Files у Провіднику файлів.

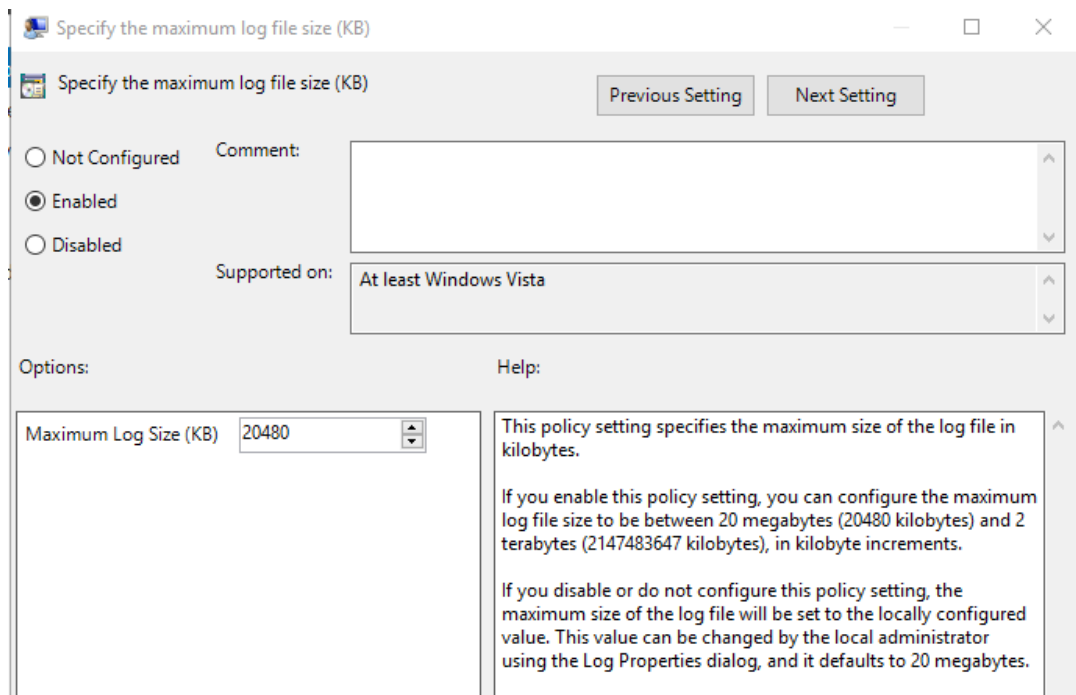


Рисунок 3.31 – встановлення розміру логів

```
C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
C:\Users\Administrator>
```

Рисунок 3.32 – оновлення політик

3.4 Впровадження LAPS

Рішення Microsoft Local Administrator Password Solution (LAPS) забезпечує керування паролями облікових записів локального адміністратора для комп'ютерів, приєднаних до домену. Паролі рандомізовані та зберігаються в Active Directory (AD), захищені списками керування доступом, тому лише відповідні користувачі можуть прочитати їх або запросити скидання.[20]

Для початку необхідно завантажити оснащення LAPS на офіційному сайті Microsoft та встановити:

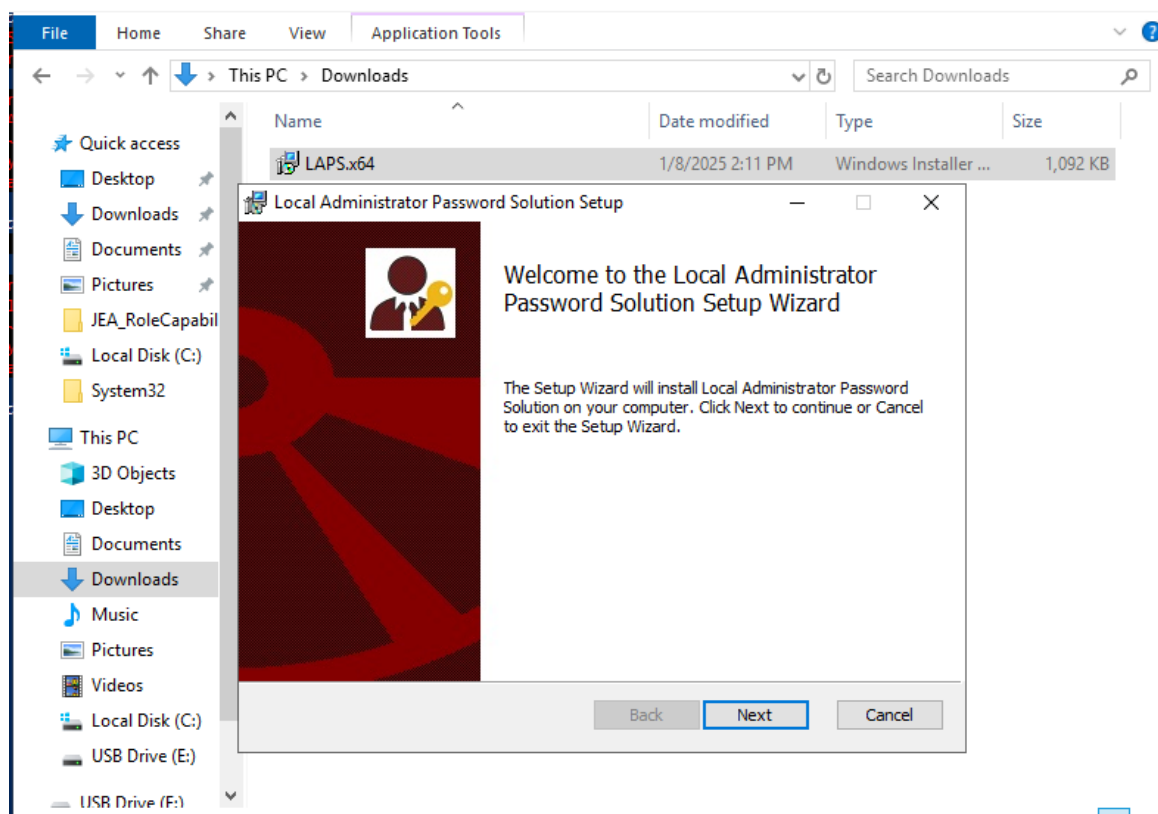


Рисунок 3.33 – Встановлення LAPS

```
PS C:\Users\Administrator> Get-WindowsFeature RSAT-AD-Tools

Display Name                                     Name                                     Install State
-----
[X] AD DS and AD LDS Tools                      RSAT-AD-Tools                          Installed

PS C:\Users\Administrator>
```

Рисунок 3.34 – перевірка встановлення

Команда `Get-WindowsFeature RSAT-AD-Tools` перевіряє наявність встановленого компоненту RSAT-AD-Tools. Результат показує, що AD DS and AD LDS Tools встановлені (Installed), тобто можна використовувати утиліти для управління Active Directory.

```
PS C:\> Get-Module -ListAvailable AdmPwd.PS

Directory: C:\Windows\system32\WindowsPowerShell\v1.0\Modules

ModuleType Version      Name                                ExportedCommands
-----
Binary      5.0.0.0      AdmPwd.PS                          {Update-AdmPwdADSchema, Get-AdmPwdPassword, Reset-AdmPwdPa...

PS C:\>
```

Рисунок 3.35 – перевірка наявності необхідних модулів

Команда `Get-Module -ListAvailable AdmPwd.PS` перевіряє наявність модуля AdmPwd.PS, який використовується для LAPS (Local Administrator Password Solution).

```
PS C:\> Update-AdmPwdADSchema

Operation                DistinguishedName                                Status
-----
AddSchemaAttribute       cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=t... Success
AddSchemaAttribute       cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=tarnopolskiy,DC... Success
ModifySchemaClass        cn=computer,CN=Schema,CN=Configuration,DC=tarnopolskiy,DC=net    Success

PS C:\>
```

Рисунок 3.36 – встановлення атрибутів

Команда `Update-AdmPwdADSchema` оновлює схему Active Directory для підтримки LAPS. Результат показує, що операції виконані успішно (Success) для таких атрибутів. Це означає, що Active Directory готова до роботи з LAPS. Далі потрібно налаштувати GPO та дозволи на читання паролів.

```

PS C:\> Set-AdmPwdReadPasswordPermission -OrgUnit "OU=AdminAccounts,DC=tarnopolskiy,DC=net" -AllowedPrincipals "Server Admins"

Name           DistinguishedName           Status
-----
AdminAccounts  OU=AdminAccounts,DC=tarnopolskiy,DC=net  Delegated

PS C:\> Set-AdmPwdResetPasswordPermission -OrgUnit "OU=AdminAccounts,DC=tarnopolskiy,DC=net" -AllowedPrincipals "Server Admins"

Name           DistinguishedName           Status
-----
AdminAccounts  OU=AdminAccounts,DC=tarnopolskiy,DC=net  Delegated

PS C:\>

```

Рисунок 3.37 – встановлення дозволів для групи адміністраторів

Було успішно налаштовано делегування прав для LAPS у організаційному підрозділі AdminAccounts. Групі "Server Admins" було надано дозвіл на перегляд збережених паролів локальних адміністраторів за допомогою команди Set-AdmPwdReadPasswordPermission, а також дозвіл на їх скидання через Set-AdmPwdResetPasswordPermission. Обидві операції було виконано успішно, що підтверджується статусом "Delegated". Відтепер учасникам групи "Server Admins" дозволено використовувати команди Get-AdmPwdPassword для отримання паролів і Reset-AdmPwdPassword для їх зміни.

```

PS C:\Users\Administrator> Set-AdmPwdComputerSelfPermission -Identity "OU=ComputersT,DC=tarnopolskiy,DC=net"

Name           DistinguishedName           Status
-----
ComputersT     OU=ComputersT,DC=tarnopolskiy,DC=net  Delegated

```

Рисунок 3.38 – дозволи для самостійного оновлення паролів

Було налаштовано необхідні дозволи для самостійного оновлення пароля локального адміністратора комп'ютерами в організаційному підрозділі ComputersT. Використання команди Set-AdmPwdComputerSelfPermission дозволило об'єктам комп'ютерів у OU-ComputersT змінювати та оновлювати свої паролі в Active Directory. Операція була виконана успішно, що підтверджується статусом "Delegated".

Перейдемо до налаштування групової політики LAPS. Це необхідно, оскільки для алгоритмів LAPS потрібні налаштування часу та правил зміни паролю та його структури.

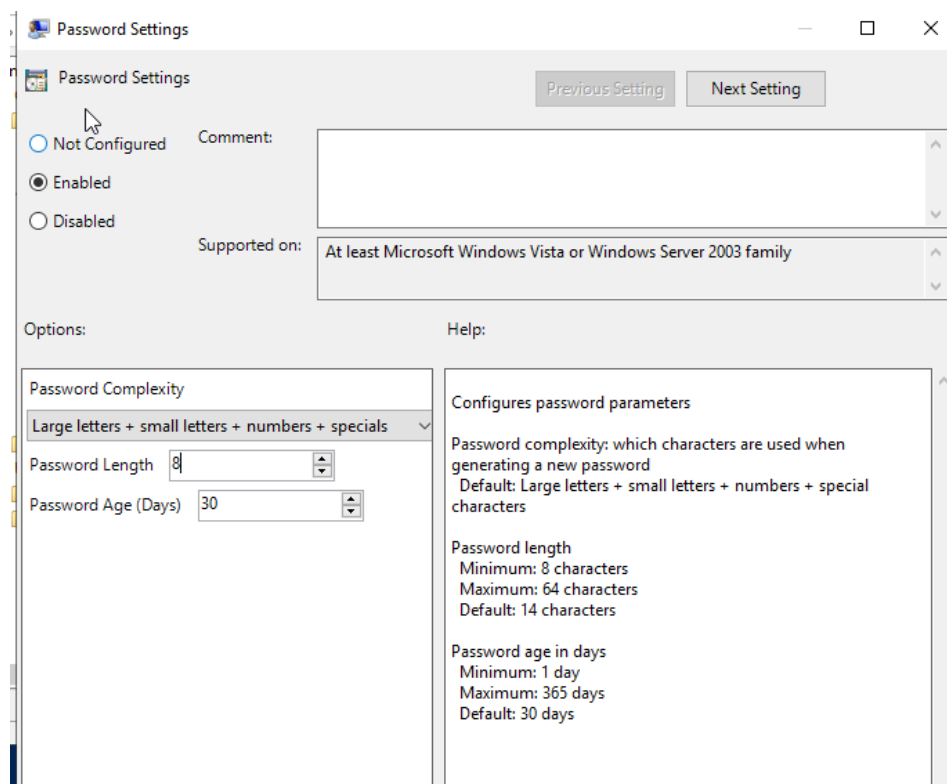


Рисунок 3.39 – налаштування GPO для LAPS

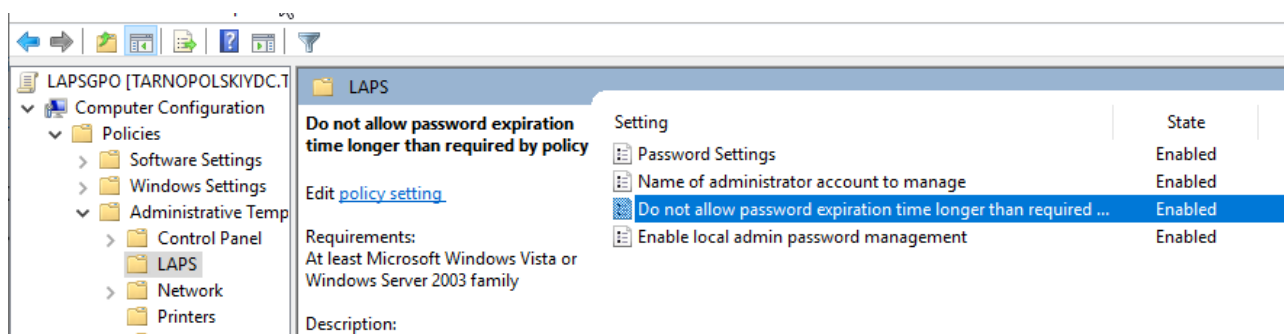


Рисунок 3.40 – налаштування GPO для LAPS

Скрипт для налаштування LAPS наведено у додатку Е.

3.5 Налаштування JEA

JEA – важливий і необхідний інструмент для безпеки привілейованих облікових записів. Для унеможливлення компрометації локальних облікових записів було впроваджено LAPS, проте варто окремо краще подбати і про привілейовані облікові записи. Для цього використано JEA, адже цей інструмент обмежує права навіть при наявності доменного доступу.

```

PS C:\Users\Administrator> New-Item -ItemType Directory -Path "C:\Program Files\WindowsPowerShell\Modules\MyJEARole" -Force

Directory: C:\Program Files\WindowsPowerShell\Modules

Mode                LastWriteTime         Length Name
----                -
d-----         2/9/2025   6:52 AM                MyJEARole

PS C:\Users\Administrator> New-Item -ItemType Directory -Path "C:\Program Files\WindowsPowerShell\Modules\MyJEARole\RoleCapabilities" -Force

Directory: C:\Program Files\WindowsPowerShell\Modules\MyJEARole

Mode                LastWriteTime         Length Name
----                -
d-----         2/9/2025   6:52 AM                RoleCapabilities

PS C:\Users\Administrator> New-Item -ItemType Directory -Path "C:\Program Files\WindowsPowerShell\Modules\MyJEARole\SessionConfigurations" -Force

Directory: C:\Program Files\WindowsPowerShell\Modules\MyJEARole

Mode                LastWriteTime         Length Name
----                -
d-----         2/9/2025   6:53 AM                SessionConfigurations

```

Рисунок 3.41 – Створення структури каталогів

Було створено необхідну структуру каталогів для налаштування JEА. В каталозі "MyJEARole" в C:\Program Files\WindowsPowerShell\Modules було створено підкаталоги "Role Capabilities" та "SessionConfigurations", де зберігатимуться відповідні конфігурації для ролі JEА. Тепер можна додавати необхідні файли для визначення дозволів і налаштувань для сесій.

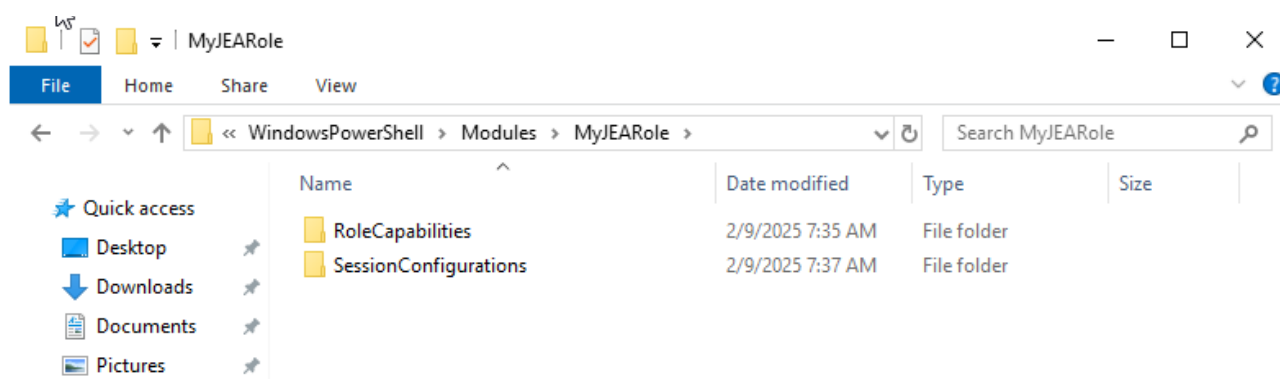


Рисунок 3.42 – Структура каталогів

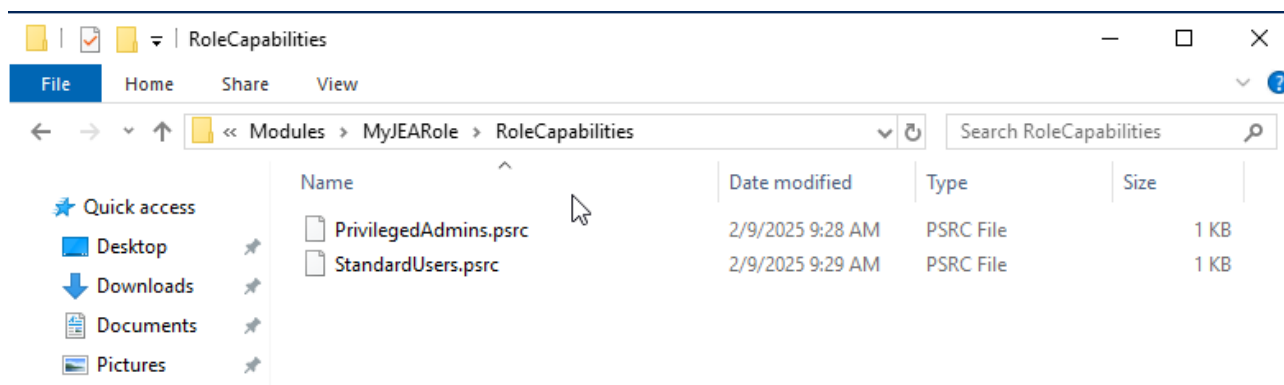


Рисунок 3.43 – Створені файли для скриптів

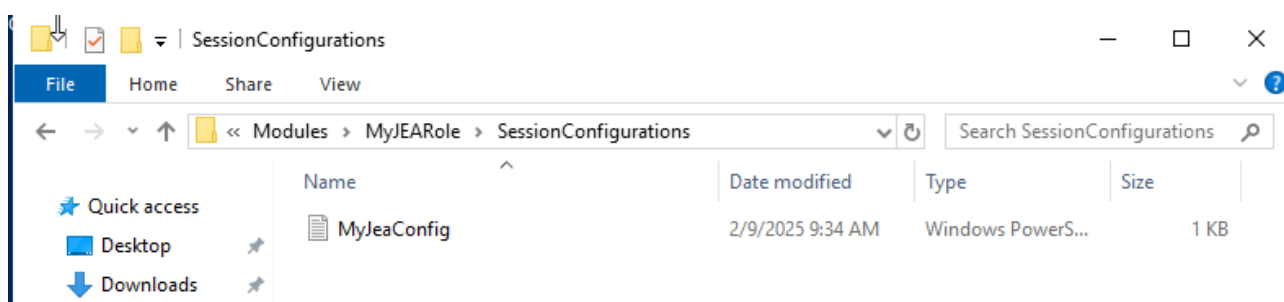


Рисунок 3.44 – Створений файл для скрипта



Рисунок 3.45 – Створений скрипт

У цьому файлі налаштовується конфігурація для JEA (Just Enough Administration), зокрема, визначаються властивості для певної ролі та її здатності до виконання операцій у сесії.

Цей файл є частиною налаштування, яке визначає, які ролі та дозволи мають користувачі під час роботи з JEA. Описаний скрипт – наведений у додатку Б.

```

@{
    GUID = '11111111-1111-1111-1111-111111111111'
    Author = "Vadim"
    CompanyName = "Diplom"
    Description = "Admins"
    PowerShellVersion = '5.1'

    VisibleCmdlets = @(
        'Get-Service',
        'Restart-Service',
        'Stop-Service',
        'Start-Service',
        'Get-Process',
        'Stop-Process',
        'Restart-Computer'
    )
}

```

Рисунок 3.46 – Створений скрипт

Файл PrivilegedAdmins.psre є частиною конфігурації JEA і визначає, які команди будуть доступні для користувачів, які мають роль PrivilegedAdmins.

Він визначає набір команд для адміністраторів, які мають певні дозволи в сесії JEA. Скрипт зазначено у додатку В.

```

@{
    GUID = '22222222-2222-2222-2222-222222222222'
    Author = "Vadim"
    CompanyName = "Diplom"
    Description = "Users"
    PowerShellVersion = '5.1'

    VisibleCmdlets = @(
        'Get-Service',
        'Restart-Service'
    )
}

```

Рисунок 3.47 – Створений скрипт

Файл StandardUsers.psre є частиною конфігурації JEA для StandardUsers, що визначає, які команди будуть доступні користувачам цієї ролі.

Цей файл визначає набір дозволених команд для менш привілейованих користувачів у сесії JEA. Зображений на рисунку скрипт наведено у додатку Г.

```

PS C:\Users\Administrator> Register-PSSessionConfiguration -Name MyJEAConfig -Path "C:\Program Files\WindowsPowerShell\Modules\MyJEARole\SessionConfigurations\MyJeaConfig.pssc"
WARNING: Register-PSSessionConfiguration may need to restart the WinRM service if a configuration using this name has recently been unregistered, certain system data structures may still be cached. In that case, a restart of WinRM may be required.
All WinRM sessions connected to Windows PowerShell session configurations, such as Microsoft.PowerShell and session configurations that are created with the Register-PSSessionConfiguration cmdlet, are disconnected.

WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Plugin
Type          Keys          Name
----          -
Container     {Name=MyJEAConfig} MyJEAConfig
WARNING: Set-PSSessionConfiguration may need to restart the WinRM service if a configuration using this name has recently been unregistered, certain system data structures may still be cached. In that case, a restart of WinRM may be required.
All WinRM sessions connected to Windows PowerShell session configurations, such as Microsoft.PowerShell and session configurations that are created with the Register-PSSessionConfiguration cmdlet, are disconnected.
WARNING: Waiting for service 'Windows Remote Management (WS-Management) (winrm)' to stop...
WARNING: Waiting for service 'Windows Remote Management (WS-Management) (winrm)' to stop...
WARNING: Register-PSSessionConfiguration may need to restart the WinRM service if a configuration using this name has recently been unregistered, certain system data structures may still be cached. In that case, a restart of WinRM may be required.
All WinRM sessions connected to Windows PowerShell session configurations, such as Microsoft.PowerShell and session configurations that are created with the Register-PSSessionConfiguration cmdlet, are disconnected.
PS C:\Users\Administrator>

```

Рисунок 3.48 – Реєстрація сесії JEA

Команда `Register-PSSessionConfiguration` була успішно виконана для реєстрації нової сесії PowerShell JEA з ім'ям `MyJEAConfig`. В результаті була створена конфігурація для обмеженого доступу до PowerShell за допомогою JEA, що дозволяє точно визначити, які команди будуть доступні для виконання користувачам із певними ролями. Скрипт для налаштування JEA наведено у додатку Є.

3.6 Використання DSC

Desired State Configuration (DSC) — це інструмент автоматизації в PowerShell, який дозволяє забезпечити конфігурацію та управління інфраструктурою, гарантуючи, що налаштування системи відповідають заданому "бажаному стану".

Оскільки DSC забезпечує автоматичну перевірку та відновлення заданої конфігурації, гарантуючи, що параметри LAPS і JEA залишаються актуальними та незмінними після змін, оновлень чи втручань.

Отже, налаштування:

```

PS C:\Users\Administrator> $PSVersionTable.PSVersion

Major Minor Build Revision
-----
5      1      17763 1007

PS C:\Users\Administrator> Install-Module -Name PSDscResources -Force

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Administrator\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet provider by
running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet to install
and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y
PS C:\Users\Administrator> Install-Module -Name PSDscResources -Force
PS C:\Users\Administrator> Get-Module -ListAvailable -Name PSDscResources

Directory: C:\Program Files\WindowsPowerShell\Modules

ModuleType Version Name ExportedCommands
-----
Manifest 2.12.0.0 PSDscResources

PS C:\Users\Administrator>

```

Рисунок 3.49 – встановлення та інсталяція DSC

```

dsc: Блокнот
Файл Редагування Формат Вигляд Довідка
Configuration EnvironmentVariable_Path
{
    param ()

    Import-DscResource -ModuleName 'PSDscResources'

    Node localhost
    {
        Environment CreatePathEnvironmentVariable
        {
            Name = 'TestPathEnvironmentVariable'
            Value = 'TestValue'
            Ensure = 'Present'
            Path = $true
            Target = @('Process', 'Machine')
        }
    }
}

EnvironmentVariable_Path -OutputPath "C:\Users\Administrator\EnvironmentVariable_Path"

```

Рисунок 3.50 – dsc-скрипт

Скрипт наведено у додатку Г.

```
PS C:\Users\Administrator> Get-InstalledModule -Name 'PSDscResources'

Version      Name              Repository        Description
-----      -
2.12.0.0     PSDscResources    PSGallery         This module contains the standard DSC resources....

PS C:\Users\Administrator> notepad .\LCMConfigggg.ps1
PS C:\Users\Administrator> Set-WsManQuickConfig -Force
WinRM is already set up to receive requests on this computer.
WinRM is already set up for remote management on this computer.
PS C:\Users\Administrator> Start-DscConfiguration -Path 'C:\Users\Administrator\EnvironmentVariable_Path' -Wait -Verbose

VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, 'methodName' =
SendConfigurationApply,'className' = MSFT_DSCLocalConfigurationManager,'namespaceName' =
root/Microsoft/Windows/DesiredStateConfiguration'.
VERBOSE: An LCM method call arrived from computer TARNOPOLSKIYDC with user sid
S-1-5-21-2802516665-2336818053-4112535548-500.
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Set ]
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Resource ] [[Environment]CreatePathEnvironmentVariable]
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Test ] [[Environment]CreatePathEnvironmentVariable]
```

Рисунок 3.51 – виконання скрипта

```
PS C:\Users\Administrator> Start-DscConfiguration -Path 'C:\Users\Administrator\EnvironmentVariable_Path' -Wait -Verbose
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, 'methodName' =
SendConfigurationApply,'className' = MSFT_DSCLocalConfigurationManager,'namespaceName' =
root/Microsoft/Windows/DesiredStateConfiguration'.
VERBOSE: An LCM method call arrived from computer TARNOPOLSKIYDC with user sid
S-1-5-21-2802516665-2336818053-4112535548-500.
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Set ]
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Resource ] [[Environment]CreatePathEnvironmentVariable]
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Test ] [[Environment]CreatePathEnvironmentVariable]
VERBOSE: [TARNOPOLSKIYDC]: [[Environment]CreatePathEnvironmentVariable] Environment variable
'TestPathEnvironmentVariable' does not exist.
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ End Test ] [[Environment]CreatePathEnvironmentVariable] in 4.4400 seconds.
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ Start Set ] [[Environment]CreatePathEnvironmentVariable]
VERBOSE: [TARNOPOLSKIYDC]: [[Environment]CreatePathEnvironmentVariable] Environment variable
'TestPathEnvironmentVariable' created with value 'TestValue'.
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ End Set ] [[Environment]CreatePathEnvironmentVariable] in 0.4530 seconds.
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ End Resource ] [[Environment]CreatePathEnvironmentVariable]
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ End Set ]
VERBOSE: [TARNOPOLSKIYDC]: LCM: [ End Set ] in 16.3150 seconds.
VERBOSE: Operation 'Invoke CimMethod' complete.
VERBOSE: Time taken for configuration job to complete is 18.11 seconds
PS C:\Users\Administrator> Get-DscConfiguration
```

Рисунок 3.52 – продовження виконання

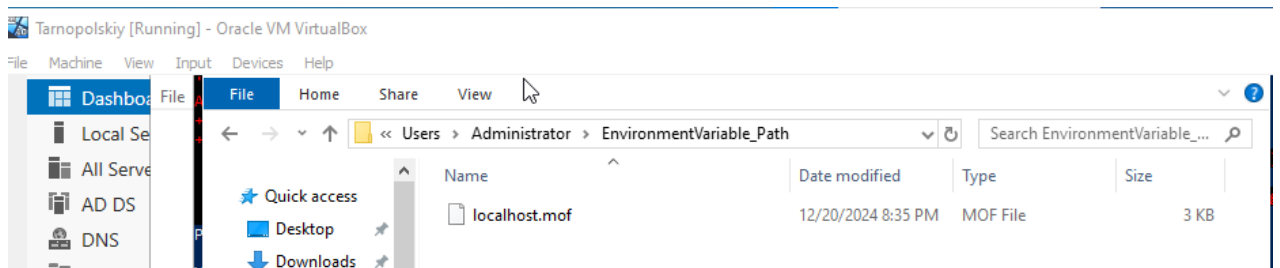


Рисунок 3.53 – результат виконання: створений MOF-файл

Скрипт для налаштування LAPS наведено у додатку Ж.

3.7 Тестування роботи системи

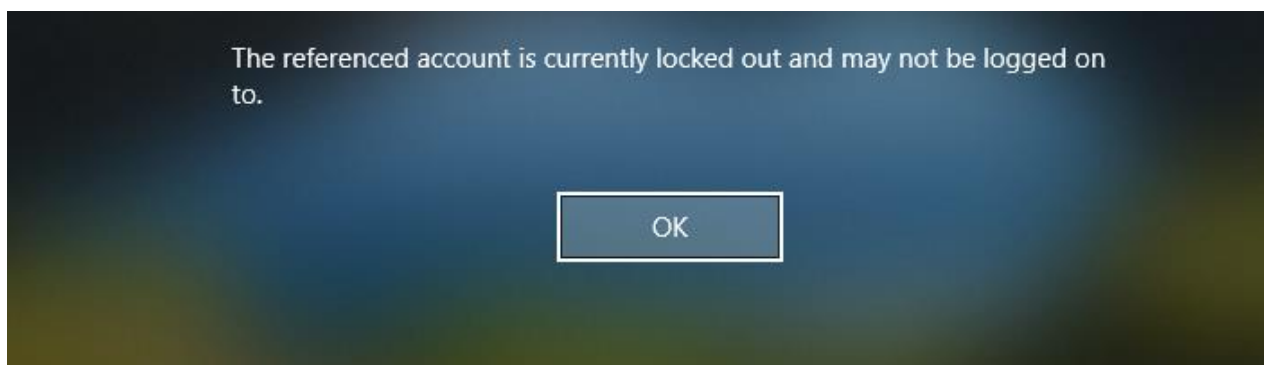


Рисунок 3.54 – результат при перевищенні спроб вводу паролю

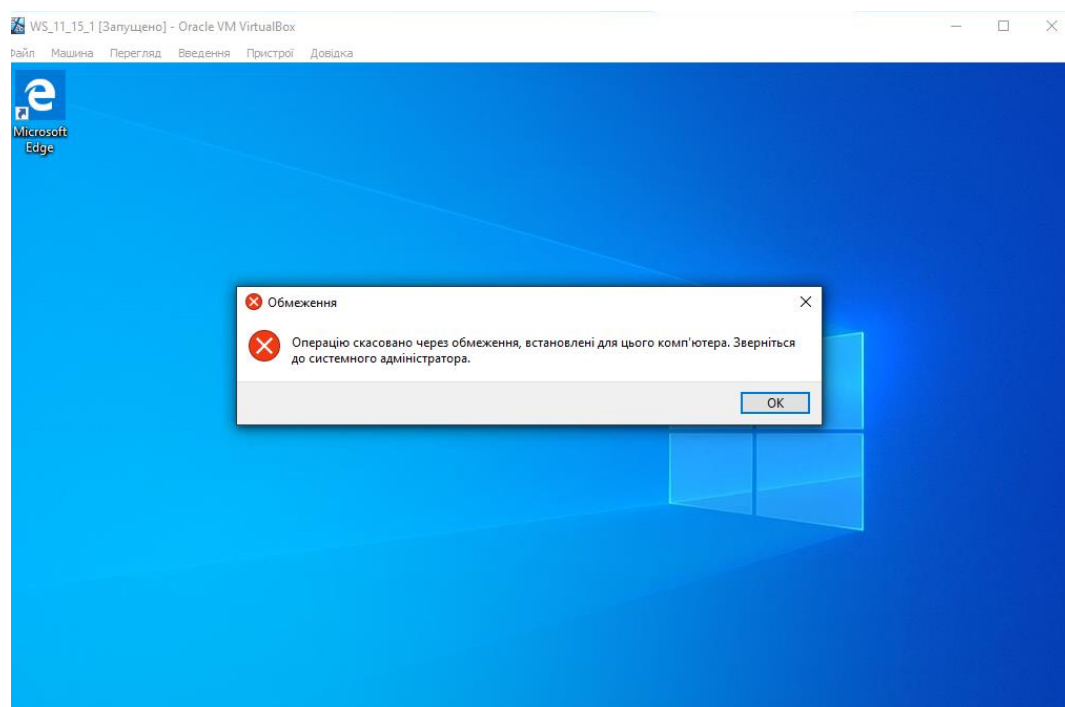


Рисунок 3.55 – результат при спробі виконати файл, виконання яких заборонено адміністратором

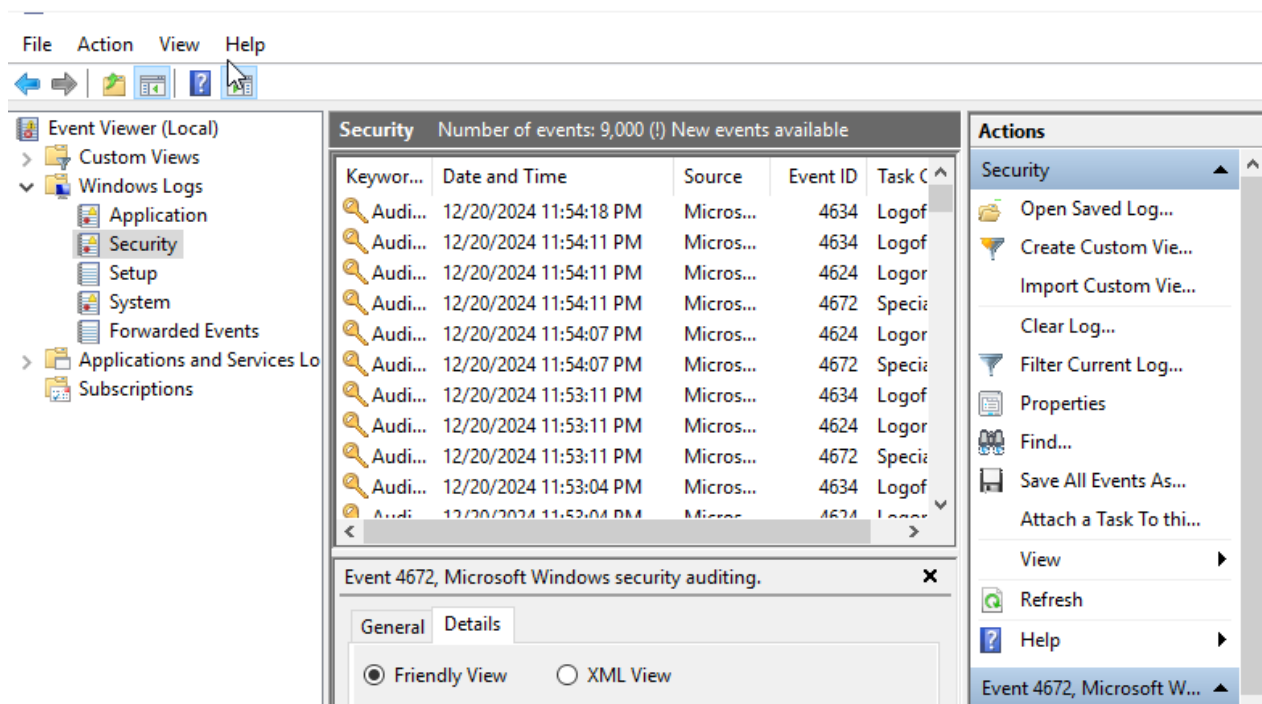


Рисунок 3.56 – логи в Event viewer

Перевірка роботи LAPS:

```
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> Reset-AdmPwdPassword -ComputerName "TARNOCOMP1"

DistinguishedName                                Status
-----
CN=TARNOCOMP1,OU=ComputersT,DC=tarnopolskiy,DC=net PasswordReset

PS C:\Users\Administrator> Get-AdmPwdPassword -ComputerName "TARNOCOMP1"

ComputerName    DistinguishedName                                Password                                ExpirationTimestamp
-----
TARNOCOMP1      CN=TARNOCOMP1,OU=ComputersT,DC=tarnopolski... Q{A}33)8wh%mx3 2/9/2025 6:22:33 AM

PS C:\Users\Administrator>
```

Рисунок 3.57 – Генерація паролю LAPS

Було виконано скидання пароля локального адміністратора для комп'ютера TARNOCOMP1 за допомогою команди Reset-AdmPwdPassword. Операція завершилася успішно, що підтверджується статусом "PasswordReset".

Після цього було отримано новий пароль за допомогою Get-AdmPwdPassword. Для комп'ютера TARNOCOMP1 було згенеровано новий пароль Q{A}33)8wh%mx3

```

PS C:\Users\Administrator> Get-AdmPwdPassword -ComputerName "TARNOCOMP1"

ComputerName      DistinguishedName      Password      ExpirationTimestamp
-----
TARNOCOMP1        CN=TARNOCOMP1,OU=ComputersT,DC=tarnopolski... Q{A)33)8wh%mx3 2/9/2025 6:22:33 AM

PS C:\Users\Administrator> Get-ADComputer -Identity "TARNOCOMP1" -Properties ms-Mcs-AdmPwd

DistinguishedName : CN=TARNOCOMP1,OU=ComputersT,DC=tarnopolskiy,DC=net
DNSHostName       : TarnoComp1.tarnopolskiy.net
Enabled           : True
ms-Mcs-AdmPwd     : Q{A)33)8wh%mx3
Name              : TARNOCOMP1
ObjectClass       : computer
ObjectGUID        : 9a59740e-2595-4efc-8cfa-0734888a03da
SamAccountName    : TARNOCOMP1$
SID               : S-1-5-21-2802516665-2336818053-4112535548-1103
UserPrincipalName :

PS C:\Users\Administrator>

```

Рисунок 3.58 – Запит для отримання локального паролю

Було виконано запит до Active Directory для отримання пароля локального адміністратора комп'ютера TARNOCOMP1 через атрибут ms-Mcs-AdmPwd. Результат підтверджує, що пароль Q{A)33)8wh%mx3 збережено в Active Directory для цього комп'ютера.

Таблиця 3.1 – перевірка роботи LAPS

№	Дія	Опис операції	Очікуваний результат	Фактичний результат	Статус
1	Запуск Reset-AdmPwdPassword	Скидання пароля локального адміністратора на комп'ютері TARNOCOMP1	Команда виконується без помилок, статус — PasswordReset	PasswordReset	Успішно
2	Отримання нового пароля	Виконання Get-AdmPwdPassword -ComputerName TARNOCOMP1	Новий пароль відображається	Q{A)33)8wh%mx3	Успішно
3	Перевірка збереження пароля в AD	Отримання значення атрибуту ms-Mcs-AdmPwd для об'єкта TARNOCOMP1	Значення атрибута відповідає новому паролю	Q{A)33)8wh%mx3	Успішно
4	Перевірка прав доступу	Перевірка, чи користувач має доступ до читання атрибута ms-Mcs-AdmPwd	Доступ дозволений (відповідно до GPO)	Доступ дозволено	Успішно
5	Перевірка журналу подій	Перевірка на наявність запису про скидання пароля	Подія про скидання наявна в Event Viewer	Подія знайдена	Успішно

Описана таблиця – перша таблиця у додатку Д.

Перевірка роботи JEA:

```
All WinRM sessions connected to Windows PowerShell session configurations, such as Microsoft.PowerShell and session configurations that are created with the Register-PSSessionConfiguration cmdlet, are disconnected.

PS C:\Users\Administrator> Get-PSSessionConfiguration

Name       : microsoft.powershell
PSVersion  : 5.1
StartupScript :
RunAsUser   :
Permission  : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed, BUILTIN\Remote
              Management Users AccessAllowed

Name       : microsoft.powershell.workflow
PSVersion  : 5.1
StartupScript :
RunAsUser   :
Permission  : BUILTIN\Administrators AccessAllowed, BUILTIN\Remote Management Users AccessAllowed

Name       : microsoft.powershell32
PSVersion  : 5.1
StartupScript :
RunAsUser   :
Permission  : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed, BUILTIN\Remote
              Management Users AccessAllowed

Name       : microsoft.windows.servermanagerworkflows
PSVersion  : 3.0
StartupScript :
RunAsUser   :
Permission  : NT AUTHORITY\INTERACTIVE AccessAllowed, BUILTIN\Administrators AccessAllowed

Name       : MyJEAConfig
PSVersion  : 5.1
StartupScript :
RunAsUser   :
Permission  : TARNOPOLSKIY\Server Admins AccessAllowed, TARNOPOLSKIY\Server Users AccessAllowed

PS C:\Users\Administrator>
```

Рисунок 3.59 – Наявна зареєстрована сесія JEA

```
Function Get-Help
Function Measure-Object
Function Out-Default
Function Select-Object
Cmdlet Get-Process 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Get-Service 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Restart-Computer 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Restart-Service Microsoft.PowerShell.Management
Cmdlet Start-Service Microsoft.PowerShell.Management
Cmdlet Stop-Process Microsoft.PowerShell.Management
Cmdlet Stop-Service Microsoft.PowerShell.Management

[localhost]: PS>Get-Command

CommandType Name
-----
Function Clear-Host
Function Exit-PSSession
Function Get-Command
Function Get-FormatData
Function Get-Help
Function Measure-Object
Function Out-Default
Function Select-Object
Cmdlet Get-Process
Cmdlet Get-Service 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Restart-Computer 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Restart-Service 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Start-Service 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Stop-Process 3.0.0.0 Microsoft.PowerShell.Management
Cmdlet Stop-Service 3.0.0.0 Microsoft.PowerShell.Management

[localhost]: PS>Exit-PSSession
PS C:\Users\Administrator> Enter-PSSession -ComputerName localhost -ConfigurationName MyJEAConfig -Credential (Get-Credential)

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

Рисунок 3.60 – Вхід з привілейованого облікового запису

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				67
Змн.	Арк.	№ докум.	Підпис	Дата		

```
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
[localhost]: PS>Get-Command
```

CommandType	Name	Version	Source
Function	Clear-Host		
Function	Exit-PSSession		
Function	Get-Command		
Function	Get-FormatData		
Function	Get-Help		
Function	Measure-Object		
Function	Out-Default		
Function	Select-Object		
Cmdlet	Get-Process	3.0.0.0	Microsoft.PowerShell.Management
Cmdlet	Get-Service	3.0.0.0	Microsoft.PowerShell.Management
Cmdlet	Restart-Computer	3.0.0.0	Microsoft.PowerShell.Management
Cmdlet	Restart-Service	3.0.0.0	Microsoft.PowerShell.Management
Cmdlet	Start-Service	3.0.0.0	Microsoft.PowerShell.Management
Cmdlet	Stop-Process	3.0.0.0	Microsoft.PowerShell.Management
Cmdlet	Stop-Service	3.0.0.0	Microsoft.PowerShell.Management

```
[localhost]: PS>Get-Process
```

Handles	NPM(K)	PM(K)	WS(K)	CPU(s)	Id	SI	ProcessName
257	16	4016	23368	0.63	4352	1	ApplicationFrameHost
252	13	4768	6332	25.03	2624	1	conhost
349	13	2224	5220	1.98	344	0	csrss
371	17	2424	5892	18.06	416	1	csrss
389	15	3728	15496	2.09	1928	1	ctfmon
384	32	16132	21952	8.55	1996	0	dfsrs
176	11	2208	7424	0.09	1740	0	dfssvc
228	16	3392	11376	0.48	3688	1	dllhost
203	13	15728	16168	0.11	4760	1	dllhost

Рисунок 3.61 – Перевірка доступних команд привілейованого облікового запису

```
762 43 10328 29496 42.63 296 0 svchost
795 23 7512 27340 4.92 740 0 svchost
812 21 6148 12508 8.78 776 0 svchost
170 9 3496 12072
1606 48 59600 101220
583 31 11920 23328
869 22 19744 32100
620 34 9000 27748
214 12 1760 7608
396 32 8656 17764
280 16 3352 12864
312 13 2008 8720
199 10 2264 8308
382 24 3300 12016
168 11 3788 10576
226 14 4688 11628
374 16 15388 17400
519 22 19336 34504
471 21 6868 32164
148 8 1500 7124
452 25 4188 14352
1808 0 192 136
232 24 4868 13984 0.38 3052 1 taskhostw
171 11 1364 6696 0.09 432 0 wininit
257 12 2520 11216 0.33 472 1 winlogon
631 32 52220 71188 1.52 2792 0 WmiPrvSE
603 21 12836 27080 28.16 3004 0 WmiPrvSE
639 27 48920 67344 1.81 4704 0 wsmprovhost
```

Windows PowerShell credential request

Enter your credentials.

User name: TARNOPOLSKIY\User1

Password: [masked]

OK Cancel

```
[localhost]: PS>Exit-PSSession
PS C:\Users\Administrator> Enter-PSSession -ComputerName localhost -ConfigurationName MyJEACConfig -Credential (Get-Cred
ntial)
```

```
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
```

Рисунок 3.62 – вхід в обліковий запис звичайного користувача

```

[localhost]: PS>Exit-PSSession
PS C:\Users\Administrator> Enter-PSSession -ComputerName localhost -ConfigurationName MyJEAConfig -Credential (Get-Cred
ntial)

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
[localhost]: PS>Get-Command

CommandType      Name                                           Version      Source
-----
Function         Clear-Host                                     3.0.0.0      Microsoft.PowerShell.Management
Function         Exit-PSSession                                3.0.0.0      Microsoft.PowerShell.Management
Function         Get-Command                                    3.0.0.0      Microsoft.PowerShell.Management
Function         Get-FormatData                                3.0.0.0      Microsoft.PowerShell.Management
Function         Get-Help                                       3.0.0.0      Microsoft.PowerShell.Management
Function         Measure-Object                                3.0.0.0      Microsoft.PowerShell.Management
Function         Out-Default                                   3.0.0.0      Microsoft.PowerShell.Management
Function         Select-Object                                 3.0.0.0      Microsoft.PowerShell.Management
Cmdlet           Get-Service                                   3.0.0.0      Microsoft.PowerShell.Management
Cmdlet           Restart-Service                               3.0.0.0      Microsoft.PowerShell.Management

[localhost]: PS>Get-Process
The term 'Get-Process' is not recognized as the name of a cmdlet, function, script file, or operable program. Check
the spelling of the name, or if a path was included, verify that the path is correct and try again.
+ CategoryInfo          : ObjectNotFound: (Get-Process:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

[localhost]: PS>Get-Service

Status      Name                DisplayName
-----
Running     ADWS                Active Directory Web Services
Stopped     AJRouter            AllJoyn Router Service
Stopped     ALG                 Application Layer Gateway Service
Running     AppHostSvc          Application Host Helper Service

```

Рисунок 3.63 – Перевірка заборонених і дозволених команд звичайного користувача

Таблиця 3.2 – Перевірка роботи JEА

№	Дія	Обліковий запис	Команда	Очікуваний результат	Фактичний результат	Статус
1	Перегляд конфігурації сесії	Привілейований	Get-PSSessionConfiguration	Є MYJEAConfig	Є MYJEAConfig	Успішно
2	Вхід у JEА-сесію	Привілейований	Enter-PSSession	Вхід дозволено	Вхід успішний	Успішно
3	Дозволена команда	Привілейований	Restart-Service spooler	Виконується	Виконано	Успішно
4	Заборонена команда	Привілейований	Get-Process	Помилка доступу	Помилка	Успішно
5	Вихід із сесії	Привілейований	Exit-PSSession	Вихід з сесії	Вийшов	Успішно
6	Вхід у JEА-сесію	Звичайний	Enter-PSSession	Вхід дозволено	Вхід успішний	Успішно
7	Дозволена команда	Звичайний	Get-Service	Виконується	Виконано	Успішно
8	Заборонена команда	Звичайний	Remove-Item	Помилка доступу	Помилка	Успішно
9	Вихід із сесії	Звичайний	Exit-PSSession	Вихід з сесії	Вийшов	Успішно

Описана таблиця – друга таблиця у додатку Д.

Перевірка роботи DSC:

```
PS C:\Users\Administrator> Get-DscLocalConfigurationManager

ActionAfterReboot      : ContinueConfiguration
AgentId                : 1A37A44F-BF4E-11EF-B06A-08002727DC36
AllowModuleOverWrite   : False
CertificateID          : 
ConfigurationDownloadManagers : {}
ConfigurationID        : 
ConfigurationMode      : ApplyAndMonitor
ConfigurationModeFrequencyMins : 15
Credential             : 
DebugMode              : {NONE}
DownloadManagerCustomData : 
DownloadManagerName    : 
LCMCompatibleVersions  : {1.0, 2.0}
LCMState               : Idle
LCMStateDetail         : 
LCMVersion             : 2.0
StatusRetentionTimeInDays : 10
SignatureValidationPolicy : NONE
SignatureValidations   : {}
MaximumDownloadSizeMB  : 500
PartialConfigurations  : 
RebootNodeIfNeeded     : False
RefreshFrequencyMins   : 30
RefreshMode            : PUSH
ReportManagers         : {}
ResourceModuleManagers : {}
PSComputerName         :
```

Рисунок 3.64 – отримання налаштувань локального керівника

Команда `Get-DscLocalConfigurationManager` використовується для отримання налаштувань локального керівника конфігурації DSC (Desired State Configuration) на комп'ютері. DSC дозволяє автоматизувати конфігурацію й управління системами, забезпечуючи, щоб вони залишалися в визначеному стані.

```
PS C:\Users\Administrator> Get-WinEvent -LogName "Microsoft-Windows-Dsc/Operational" | Select -Last 20

ProviderName: Microsoft-Windows-DSC

TimeCreated      Id LevelDisplayName Message
-----
12/20/2024 7:55:09 PM 4102 Information Job {5E79D736-BF4F-11EF-B06A-08002727DC36} : ...
12/20/2024 7:55:09 PM 4271 Information The local configuration manager started.
12/20/2024 7:47:10 PM 4270 Information The local configuration manager was shut down.
12/20/2024 7:46:39 PM 4252 Error Job {2E806E7F-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:39 PM 4102 Information Job {2E806E7F-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:28 PM 4513 Information Job {286BA14C-BF4E-11EF-B06A-08002727DC36} : Details logging com...
12/20/2024 7:46:28 PM 4252 Error Job {286BA14C-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:28 PM 4512 Information Job {286BA14C-BF4E-11EF-B06A-08002727DC36} : Details logging sta...
12/20/2024 7:46:28 PM 4102 Information Job {286BA14C-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:06 PM 4252 Error Job {1A37A451-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:06 PM 4102 Information Job {1A37A451-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:05 PM 4271 Information The local configuration manager started.
12/20/2024 7:46:05 PM 4413 Information Job {1A37A44E-BF4E-11EF-B06A-08002727DC36} : ...
12/20/2024 7:46:05 PM 4407 Information Job {1A37A44E-BF4E-11EF-B06A-08002727DC36} : ...
```

Рисунок 3.65 – інформація про події DSC

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				70
Змн.	Арк.	№ докум.	Підпис	Дата		

Команда `Get-WinEvent -LogName "Operational" | Select-Object -Last 20` була використана для отримання останніх 20 подій із журналу подій "Operational" на комп'ютері. Цей журнал містить інформацію про різні системні події та процеси, пов'язані з керуванням конфігурацією DSC (Desired State Configuration), серед інших.

```
PS C:\Users\Administrator> Test-DscConfiguration
True
PS C:\Users\Administrator> Get-DscConfiguration

ConfigurationName : EnvironmentVariable_Path
DependsOn          :
ModuleName         : PSDscResources
ModuleVersion      : 2.12.0.0
PsDscRunAsCredential :
ResourceId          : [Environment]CreatePathEnvironmentVariable
SourceInfo         :
Ensure             : Present
Name               : TestPathEnvironmentVariable
Path               :
Target             :
Value              : TestValue
PSComputerName     :
CimClassName       : MSFT_EnvironmentResource
```

Рисунок 3.66 – робота та конфігурація DSC

Команда `Test-DscConfiguration` повертає результат `True`, що означає, що поточна конфігурація на комп'ютері відповідає очікуваним значенням, і налаштування DSC (Desired State Configuration) виконуються без помилок.

Команда `Get-DscConfiguration` виводить налаштування, які застосовані в поточній конфігурації:

```
PS C:\Users\Administrator> Get-Service -Name DsmSvc

Status Name          DisplayName
-----
Running DsmSvc          Device Setup Manager
```

Рисунок 3.67 – перевірка статусу служби

Команда `Get-Service -Name DsmSvc` використовується для перевірки статусу служби `DsmSvc`, яка відповідає за керування налаштуваннями пристроїв і їх конфігурацією в системі.

Таблиця 3.3 – Перевірка роботи DSC

Команда	Призначення	Результат
Get-DscLocalConfigurationManager	Отримання параметрів локального керівника конфігурації DSC	Відображено поточні налаштування LCM
Get-DscConfiguration	Перегляд застосованої конфігурації DSC	Виведено конфігурацію: змінні середовища, налаштування ресурсів
Test-DscConfiguration	Перевірка відповідності системи визначеній конфігурації	Результат: True – конфігурація в нормі
Get-WinEvent -LogName "Operational" Select-Object -Last 20	Перегляд останніх 20 подій у журналі DSC	Отримано останні події, пов'язані з DSC
Get-Service -Name DsmSvc	Перевірка стану служби DsmSvc (служба керування конфігурацією пристроїв)	Служба працює (Running)

Описана таблиця – третя таблиця у додатку Д.

У результаті проведених налаштувань та тестувань маємо наступні особливості роботи системи:

- Коректність підключення до домену: обидві робочі станції успішно приєднано до домену, перевірено наявність зв'язку через ping та nslookup.

- LAPS: політика LAPS була застосована, паролі локальних адміністраторів оновлювались згідно з вказаним інтервалом. Отримання та скидання паролів вдалося лише уповноваженим адміністраторам. Таблиця перевірок – перша у додатку Д.

- GPO: політики успішно застосовані. Користувачі не могли змінювати налаштування панелі керування, запускати заборонені файли, створювати об'єкти в кореневому каталозі.

- JEA: адміністративна роль дозволяла лише строго визначені командлети PowerShell. Спроба запуску команд поза визначеним переліком блокувалась. Таблиця перевірок – друга у додатку Д.

- DSC: при ручній зміні критичних налаштувань (наприклад, членство у групі «Адміністратори»), конфігурація була автоматично повернута до бажаного стану. Таблиця перевірок – третя у додатку Д.

- Моніторинг: у журналах подій зафіксовано всі входи користувачів, зміни політик та спроби запуску заблокованих програм.

На основі реалізованої системи було проведено оцінку ефективності запропонованих рішень у контексті управління привілейованими обліковими записами в середовищі Microsoft Active Directory. Основні результати:

- Зниження ризику компрометації привілейованих облікових записів: Завдяки впровадженню LAPS усі локальні паролі адміністратора стали унікальними та автоматично змінюваними, що зменшує ймовірність lateral movement та атак типу pass-the-hash.

- Підвищення контрольованості привілеїв: Завдяки JEА було введено контрольований доступ до адміністративних функцій. Адміністратори можуть виконувати лише дозволені командлети, що відповідає принципу мінімальних привілеїв.

- Покращення аудиту та відповідності: Усі дії адміністраторів логуються, забезпечуючи просте трасування інцидентів. Це відповідає вимогам ISO 27001 щодо аудиту та журналювання.

- Автоматизація відповідності налаштувань: DSC підтримує критичну конфігурацію без втручання адміністратора. У разі несанкціонованої зміни — вона автоматично відновлюється до безпечного стану.

- Умовне скорочення "поверхні атаки" на близько 60–80 відсотків: За оцінками на основі сценаріїв типових атак (brute-force, credential theft), застосовані заходи дозволяють мінімізувати принаймні 4 із 5 векторів проникнення, пов'язаних із привілейованими обліковими записами.

Висновки до третього розділу

У третьому розділі було вибрано обладнання, на якому буде базуватись наша система. Вибір був зроблений на користь операційної системи Windows та Active Directory, де було проведено базове налаштування системи, а саме: встановлено ролі, налаштування ір-адрес, тестування на наявність помилок зв'язку.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі були налаштовані групові політики – важлива частина роботи, адже за допомогою Group Policy Management Console (GPMC) можна централізовано контролювати політики для користувачів та комп'ютерів в організації. Було налаштовано як загальні політики, такі як складність паролів, особливості входу в систему, терміни дії, так і окремо для звичайних користувачів, які стали обмеженими в плані дій, що при певних обставинах могли завдати шкоди системі. Налаштування були успішно впроваджені та випробувані.

Особливу увагу було приділено рішення Microsoft Local Administrator Password Solution (LAPS), що забезпечує керування паролями облікових записів локального адміністратора для комп'ютерів, приєднаних до домену. Рішення було успішно впроваджено та протестовано.

Не менш важливим було налаштування JEA. Для унеможливлення компрометації локальних облікових записів було впроваджено LAPS, проте варто було окремо краще подбати і про привілейовані облікові записи, адже цей інструмент обмежує права навіть при наявності доменного доступу. Налаштування передбачає написання власних скриптів, що й було зроблено. Пізніше було все протестовано та випробувано успішно.

Також увагу було приділено DSC, оскільки він забезпечує автоматичну перевірку та відновлення заданої конфігурації, гарантуючи, що параметри LAPS і JEA залишаються актуальними та незмінними після змін, оновлень чи втручань. Його налаштування також передбачає написання скрипту. У підсумку рішення було успішно впроваджено та випробувано.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		74

ВИСНОВКИ

У кваліфікаційній роботі було розроблено та реалізовано проєкт системи безпечного управління привілейованими обліковими записами у середовищі Microsoft Active Directory з використанням сучасних інструментів адміністрування, таких як LAPS, JEA, DSC, GPO та VirtualBox. Метою роботи — створення ефективного рішення для централізованого, контрольованого та захищеного управління обліковими записами з підвищеними правами — досягнуто повністю.

У першому розділі теоретично обґрунтовано доцільність використання Active Directory для централізованого управління доступом, проаналізовано загрози, пов'язані з привілейованими обліковими записами, та розглянуто сучасні засоби їх нейтралізації. Окрему увагу приділено впровадженню GPO, LAPS, JEA та DSC як засобів зміцнення політик безпеки, контролю привілеїв і забезпечення стабільної конфігурації системи.

У другому розділі виконано проектування фізичної та логічної структури мережі із врахуванням вимог до безпечного адміністрування. Обґрунтовано вибір віртуального середовища VirtualBox, здійснено розподіл IP-адрес, визначено топологію та конфігурацію інфраструктури, що дозволило забезпечити масштабованість та ізольованість системи.

Третій розділ присвячено практичній реалізації та тестуванню системи. Налаштовано доменну інфраструктуру, реалізовано контроль доступу через групові політики, впроваджено LAPS для автоматичного управління паролями, обмежено адміністративні дії через JEA та впроваджено DSC для автоматизації підтримки бажаного стану конфігурації. Результати тестування підтвердили відповідність системи очікуваним вимогам щодо безпеки, керованості та надійності.

Запропоноване рішення продемонструвало високу практичну ефективність та здатність до впровадження в умовах малого або середнього підприємства. Система дозволяє зменшити ризики компрометації критичних

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				75
Змн.	Арк.	№ докум.	Підпис	Дата		

облікових записів, забезпечити відповідність політикам безпеки та підвищити загальний рівень інформаційної безпеки організації.

		Тарнопольський			ККІКБ.КР.Б – 123 – 14 – ПЗ	Арк.
		Фальковський І.Г				
Змн.	Арк.	№ докум.	Підпис	Дата		76

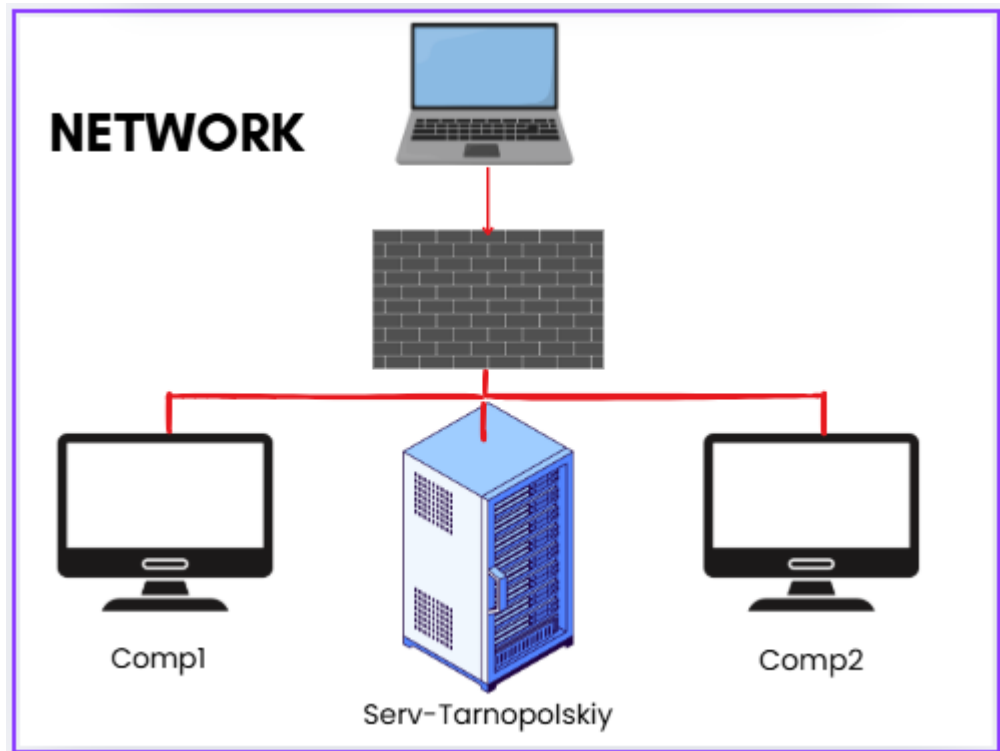
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Active Directory [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Active_Directory?utm_source=chatgpt.com
2. Переваги використання централізованої системи авторизації Active Directory від Microsoft [Електронний ресурс] – Режим доступу: <https://xn--80ahcnklsjod4a9r.xn--j1amh/articles/perevagi-vikoristannya-centralizovanoyi-sistemi-avtorizaciyi-active-directory-vid-microsoft>
3. Захист мережі: як правильно налаштувати та захистити Active Directory [Електронний ресурс] – Режим доступу: <https://hackyourmom.com/osvita/zahyst-merezhi-yak-pravylno-nalashtuvaty-ta-zahystyty-active-directory/>
4. Attacks on Active Directory [Електронний ресурс] – Режим доступу: <https://tenable.bakotech.com/ru-attacks-on-active-directory>
5. Active Directory [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Active_Directory
6. Концепция Active Directory: что нужно знать [Електронний ресурс] – Режим доступу: <https://habr.com/ru/companies/galssoftware/articles/543588/>
7. LAPS management policy settings [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-management-policy-settings>
8. Обзор концепции LAPS [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/ru-ru/windows-server/identity/laps/laps-concepts-overview>
9. Управление паролями с помощью LAPS [Електронний ресурс] – Режим доступу: <https://itfb.com.ua/upravlenie-parolyami-s-pomoshhyu-laps/>
10. PowerShell Remoting: Just Enough Administration (JEA) [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/ru-ru/powershell/scripting/security/remoting/jea/overview?view=powershell-7.5>

11. PowerShell: Implementing Just Enough Administration (JEA) step-by-step [Електронний ресурс] – Режим доступу: <https://sid-500.com/2018/02/11/powershell-implementing-just-enough-administration-jea-step-by-step/>
12. DSC Overview [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/ru-ru/powershell/dsc/overview?view=dsc-3.0>
13. Що таке PowerShell? Посібник для початківців [Електронний ресурс] – Режим доступу: <https://corewin.ua/blog/what-is-powershell-guide/>
14. Робоча станція [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D0%B1%D0%BE%D1%87%D0%B0%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F>
15. Контролер домену [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D0%B5%D1%80%D0%B4%D0%BE%D0%BC%D0%B5%D0%BD%D1%83>
16. Що таке контролер домену – VPN Unlimited [Електронний ресурс] – Режим доступу: https://www.vpnunlimited.com/ua/help/cybersecurity/domain-controller?srsId=AfmBOooL-3bellFYNPoBKjaGwAGL_cNm15-jVJmaBGnMBLZ16KhWxqpS
17. IPv4 [Електронний ресурс] – Режим доступу: <https://uk.wikipedia.org/wiki/IPv4>
18. Що таке VirtualBox і як ним користуватись [Електронний ресурс] – Режим доступу: <https://geekkies.in.ua/software/what-is-virtualbox-and-how-to-use-it.html>
19. Microsoft Windows [Електронний ресурс] – Режим доступу: https://uk.wikipedia.org/wiki/Microsoft_Windows
20. Оцінювання безпеки LAPS – Microsoft Defender for Identity [Електронний ресурс] – Режим доступу: <https://learn.microsoft.com/ru-ru/defender-for-identity/security-assessment-laps>

ДОДАТКИ

Додаток А – Схема мережі



Додаток Б

Скрипт MyJeaConfig.ps1

```
@{
    GUID = '33333333-3333-3333-3333-333333333333'
    Author = 'Vadim'
    CompanyName = 'Diplom'
    Description = 'JEA'
    SessionType = 'RestrictedRemoteServer'
    RunAsVirtualAccount = $true
    RoleDefinitions = @{
        'TARNOPOLSKIY\Server Admins' = @{ RoleCapabilities = @('PrivilegedAdmins') }
        'TARNOPOLSKIY\Server Users' = @{ RoleCapabilities = @('StandardUsers') }
    }
}
```

Додаток В

Скрипт PrivilegedAdmins.ps1

```
@{
    GUID = '11111111-1111-1111-1111-111111111111'
    Author = 'Vadim'
```

```

CompanyName = 'Diplom'
Description = 'Admins'
PowerShellVersion = '5.1'

VisibleCmdlets = @(
    'Get-Service',
    'Restart-Service',
    'Stop-Service',
    'Start-Service',
    'Get-Process',
    'Stop-Process',
    'Restart-Computer'
)
}

```

Додаток Г

Скрипт StandardUsers.psrc

```

@{
    GUID = '22222222-2222-2222-2222-222222222222'
    Author = 'Vadim'
    CompanyName = 'Diplom'
    Description = 'Users'
    PowerShellVersion = '5.1'

    VisibleCmdlets = @(
        'Get-Service',
        'Restart-Service'
    )
}

```

Додаток Г

Скрипт DSC

```

configuration EnvironmentVariable_Path
{
    param ()

    Import-DscResource -ModuleName 'PSDscResources'
}

```

Node localhost

```
{  
  Environment CreatePathEnvironmentVariable  
  {  
    Name   = 'TestPathEnvironmentVariable'  
    Value  = 'TestValue'  
    Ensure = 'Present'  
    Path   = $true  
    Target = @('Process', 'Machine')  
  }  
}  
  
EnvironmentVariable_Path -OutputPath "C:\Users\Administrator\EnvironmentVariable_Path"
```

Додаток Д

Таблиця перевірки роботи LAPS

№	Дія	Опис операції	Очікуваний результат	Фактичний результат	Статус
1	Запуск Reset-AdmPwdPassword	Скидання пароля локального адміністратора на комп'ютері TARNOCOMP1	Команда виконується без помилок, статус — PasswordReset	PasswordReset	Успішно
2	Отримання нового пароля	Виконання Get-AdmPwdPassword -ComputerName TARNOCOMP1	Новий пароль відображається	Q{A}33)8wh%mx3	Успішно
3	Перевірка збереження пароля в AD	Отримання значення атрибута ms-Mcs-AdmPwd для об'єкта TARNOCOMP1	Значення атрибута відповідає новому паролю	Q{A}33)8wh%mx3	Успішно
4	Перевірка прав доступу	Перевірка, чи користувач має доступ до читання атрибута ms-Mcs-AdmPwd	Доступ дозволений (відповідно до GPO)	Доступ дозволено	Успішно
5	Перевірка журналу подій	Перевірка журналу подій на наявність запису про скидання пароля	Подія про скидання наявна в Event Viewer	Подія знайдена	Успішно

Таблиця перевірки роботи JEA

№	Дія	Обліковий запис	Команда	Очікуваний результат	Фактичний результат	Статус
1	Перегляд конфігурацій сесії	Привілейований	Get-PSSessionConfiguration	Є MYJEAConfig	Є MYJEAConfig	Успішно
2	Вхід у JEA-сесію	Привілейований	Enter-PSSession	Вхід дозволено	Вхід успішний	Успішно
3	Дозволена команда	Привілейований	Restart-Service spooler	Виконується	Виконано	Успішно
4	Заборонена команда	Привілейований	Get-Process	Помилка доступу	Помилка	Успішно
5	Вихід із сесії	Привілейований	Exit-PSSession	Вихід з сесії	Вийшов	Успішно
6	Вхід у JEA-сесію	Звичайний	Enter-PSSession	Вхід дозволено	Вхід успішний	Успішно
7	Дозволена команда	Звичайний	Get-Service	Виконується	Виконано	Успішно
8	Заборонена команда	Звичайний	Remove-Item	Помилка доступу	Помилка	Успішно
9	Вихід із сесії	Звичайний	Exit-PSSession	Вихід з сесії	Вийшов	Успішно

Таблиця перевірки роботи DSC

Команда	Призначення	Результат
Get-DscLocalConfigurationManager	Отримання параметрів локального керівника конфігурації DSC	Відображено поточні налаштування LCM
Get-DscConfiguration	Перегляд застосованої конфігурації DSC	Виведено конфігурацію: змінні середовища, налаштування ресурсів
Test-DscConfiguration	Перевірка відповідності системи визначеній конфігурації	Результат: True – конфігурація в нормі
Get-WinEvent -LogName "Operational" Select-Object -Last 20	Перегляд останніх 20 подій у журналі DSC	Отримано останні події, пов'язані з DSC
Get-Service -Name DsmSvc	Перевірка стану служби DsmSvc (служба керування конфігурацією пристроїв)	Служба працює (Running)

Скрипт для налаштування LAPS

```
# Імпорт модуля LAPS
Import-Module AdmPwd.PS

# Оновлення схеми Active Directory (потрібно виконати лише один раз у домені)
Update-AdmPwdADSchema

# Делегування комп'ютерам прав змінювати власний пароль
Set-AdmPwdComputerSelfPermission -Identity "OU=ComputersT,DC=tarnopolskiy,DC=net"

# Делегування прав на читання пароля локального адміністратора
Set-AdmPwdReadPasswordPermission -OrgUnit
"OU=AdminAccounts,DC=tarnopolskiy,DC=net" -AllowedPrincipals "Server Admins"

# Делегування прав на скидання пароля локального адміністратора
Set-AdmPwdResetPasswordPermission -OrgUnit
"OU=AdminAccounts,DC=tarnopolskiy,DC=net" -AllowedPrincipals "Server Admins"

# Отримання збереженого пароля комп'ютера
Get-AdmPwdPassword -ComputerName "TARNOCOMP1"

# Перевірка властивостей комп'ютера (перевірка поля ms-Mcs-AdmPwd)
Get-ADComputer -Identity "TARNOCOMP1" -Properties ms-Mcs-AdmPwd
```

Скрипт для налаштування JEA

```
# Використовуються файли:
# - MyJeaConfig.pssc (конфігурація сесії)
# - PrivilegedAdmins.psrc (рольові можливості адміністраторів)
# - StandardUsers.psrc (рольові можливості звичайних користувачів)

# Створення каталогу модуля JEA і каталогу RoleCapabilities
$modulePath = "$env:ProgramFiles\WindowsPowerShell\Modules\MyJEARole\1.0.0"
$roleCapPath = Join-Path $modulePath "RoleCapabilities"
New-Item -Path $roleCapPath -ItemType Directory -Force | Out-Null

# Копіювання файлів рольових можливостей у каталог RoleCapabilities
Copy-Item -Path "C:\Users\Administrator\PrivilegedAdmins.psrc" -Destination
"$roleCapPath\PrivilegedAdmins.psrc"
```

```
Copy-Item -Path "C:\Users\Administrator\StandardUsers.psrc" -Destination  
"$roleCapPath\StandardUsers.psrc"
```

```
# Створення каталогу для зберігання конфігурації сесії
```

```
$sessionConfigPath = "C:\Program  
Files\WindowsPowerShell\Modules\MyJEARole\SessionConfigurations"
```

```
New-Item -Path $sessionConfigPath -ItemType Directory -Force | Out-Null
```

```
# Копіювання конфігураційного файлу сесії
```

```
Copy-Item -Path "C:\Users\Administrator\MyJeaConfig.pssc" -Destination  
"$sessionConfigPath\MyJeaConfig.pssc"
```

```
# Реєстрація конфігурації сесії JEA
```

```
Register-PSSessionConfiguration -Name "MyJEAConfig" -Path  
"$sessionConfigPath\MyJeaConfig.pssc" -Force
```

```
# Перезапуск служби WinRM для застосування змін (якщо потрібно)
```

```
Restart-Service WinRM
```

Додаток Ж

Скрипт для налаштування DSC

```
# Перевірка версії PowerShell
```

```
$PSVersionTable.PSVersion
```

```
# Встановлення DSC-модуля зі стандартними ресурсами
```

```
Install-Module -Name PSDscResources -Force
```

```
# Перевірка, чи встановлено модуль PSDscResources
```

```
Get-InstalledModule -Name 'PSDscResources'
```

```
Get-Module -ListAvailable -Name 'PSDscResources'
```

```
# Відкриття файлу LCMConfigggg.ps1
```

```
notepad .\LCMConfigggg.ps1
```

```
# Увімкнення та налаштування WinRM для DSC
```

```
Set-WSManQuickConfig -Force
```

```
#Окремо існує DSC-конфігураційний скрипт EnvironmentVariable_Path.ps1, який створює  
конфігурацію для змінної середовища TestPathEnvironmentVariable
```

```
# Застосування конфігурації (створення змінної середовища)
```

```
Start-DscConfiguration -Path 'C:\Users\Administrator\EnvironmentVariable_Path' -Wait -Verbose
```