

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

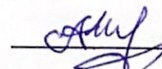
## ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра  
на тему: «Проект системи автоматизованого розгор-  
тання контролерів домену корпоративної мережі на  
базі Active Directory»

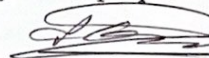
Виконав: студент 4-го курсу групи КІ-20-1  
спеціальності 123 «Комп'ютерна інженерія»

 Богдан МАРКЕЄВ

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

 Олексій ШЕЛУХА

Рецензент: завідувач кафедри КІ та КБ, к.т.н., доцент

 Андрій ЄФІМЕНКО

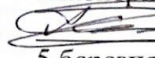
Житомир – 2024

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної  
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО  
5 березня 2024 р.

### ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Маркеєв Богдан Володимирович

Тема роботи: «Проект системи автоматизованого розгортання контролерів  
домену корпоративної мережі на базі Active Directory»

затверджена Наказом університету від 5 березня 2024 р. № 97

Термін здачі студентом закінченої роботи 9 червня 2024 р.

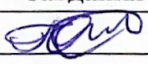
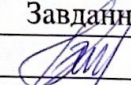
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

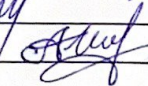
- процес розгортання контролерів домену мережі на базі Active Directory;
- відомості про скрипти у PowerShell;
- схема мережі компанії

Обладнання та програмне забезпечення:

1. мережевий емулятор GNS3, VirtualBox
2. операційні системи Windows Server 2019, Windows 10
3. образи мережевих пристроїв

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

| Розділ  | Консультант             | Підпис, дата                                                                        |                                                                                       |
|---------|-------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|         |                         | Завдання видав                                                                      | Завдання прийняв                                                                      |
| 1,2,3,4 | Головня Олена Сергіївна |  |  |

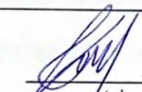
Студент  Богдан МАРКЕЄВ  
Керівник  Олексій ШЕЛУХА

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назви етапів<br>випускної кваліфікаційної роботи                  | Термін виконання<br>етапів роботи | Примітка |
|-------|-------------------------------------------------------------------|-----------------------------------|----------|
| 1     | Постановка завдання                                               | до 10.03.2024                     | виконано |
| 2     | Аналіз об'єкта дослідження                                        | до 01.04.2024                     | виконано |
| 3     | Постановка задачі дослідження                                     | до 01.04.2024                     | виконано |
| 4     | Опрацювання літературних джерел                                   | до 01.05.2024                     | виконано |
| 5     | Підготовка вимог до проєкту                                       | до 15.05.2024                     | виконано |
| 6     | Розробка теоретичного макету                                      | до 20.05.2024                     | виконано |
| 7     | Налаштування автоматизованого розгортання домену Active Directory | до 05.05.2024                     | виконано |
| 8     | Тестування готової системи                                        | до 07.06.2024                     | виконано |
| 9     | Оформлення пояснювальної записки                                  | до 09.06.2024                     | виконано |
| 10    | Отримання відгуку керівника та рецензії на кваліфікаційну роботу  | до 14.06.2024                     | виконано |
| 11    | Захист                                                            | до 29.06.2024                     | виконано |

Студент

Керівник проєкту

  
 (підпис)  
  
 (підпис)

Богдан МАРКЕЄВ

(прізвище та ініціали)

Олексій ШЕЛУХА

(прізвище та ініціал)

## АНОТАЦІЯ

Кваліфікаційна робота присвячена розробці автоматизованих рішень котрі пришвидшать та покращать процес розгортання контролерів домену мереж підприємств. Також дана тематика дозволить глибше зрозуміти тонкощі взаємодії з середовищем Active Directory.

Пояснювальна записка до випускної кваліфікаційної роботи на тему «Проект системи автоматизованого розгортання контролерів домену корпоративної мережі на базі Active Directory» складається з вступу, трьох розділів, висновків, списку використаних джерел та 3 додатків обсягом 38 сторінок.

Загальний обсяг роботи займає 96 сторінок, містить 56 рисунків та 5 таблиць. Список використаних джерел містить 23 найменувань і займає 3 сторінки.

В першому розділі проведено аналіз літературних джерел за темою кваліфікаційної роботи, виділено місце автоматизації в загальній систем та виконано постановку технічного завдання, яке формує необхідні вимоги для майбутніх автоматизованих рішень.

В другому розділі розглянуто методи та засоби вирішення поставлених завдань, проведено проектування та налаштування мережі.

В третьому розділі проведено розгортання проекту, налаштування системи захисту та проведено тестування роботи скриптів.

Висновок містить в собі результати виконаної роботи.

У додатках до роботи наведено конфігураційні файли та лістинг скриптів для розгортання контролерів домену.

Ключові слова: MICROSOFT, ACTIVE DIRECTORY, ПРОГРАМНИЙ ЕМУЛЯТОР GNS, NAT, POWERSHELL, РОЗМЕЖУВАННЯ ДОСТУПУ, USERS, СКРИПТИ, GPO, PSO, ОРГАНІЗАЦІЙНІ ОДИНИЦІ, КОМАНДЛЕТИ.

|           |      |               |                 |          |                                                                                                              |                          |      |         |
|-----------|------|---------------|-----------------|----------|--------------------------------------------------------------------------------------------------------------|--------------------------|------|---------|
|           |      |               |                 |          | <b>ККІК.КР.Б – 123 – 20 – ПЗ</b>                                                                             |                          |      |         |
| Зм.       | Арк. | № докум.      | Підпис          | Дата     |                                                                                                              | Літ.                     | Арк. | Аркушів |
| Розроб.   |      | Маркєв Б.В.   | <i>[Підпис]</i> | 18.06.24 | Проект системи автоматизованого розгортання контролерів домену корпоративної мережі на базі Active Directory |                          |      |         |
| Керівник  |      | Шелуха О.О.   | <i>[Підпис]</i> | 18.06.24 |                                                                                                              |                          | 4    | 59      |
| Реценз.   |      | Сфіменко А.А. | <i>[Підпис]</i> | 18.06.24 |                                                                                                              | <b>ФІКТ, Гр. КІ-20-1</b> |      |         |
| Н. контр. |      | Шелуха О.О.   | <i>[Підпис]</i> | 18.06.24 |                                                                                                              |                          |      |         |
| Затверд.  |      | Сфіменко А.А. | <i>[Підпис]</i> | 18.06.24 |                                                                                                              |                          |      |         |

## ANNOTATION

The qualification work is devoted to the development of automated solutions that will speed up and improve the process of deploying domain controllers for enterprise networks. Also, this topic will allow you to better understand the intricacies of interaction with the Active Directory server.

The explanatory note to the final qualification work on the topic "Project of the system of automated deployment of corporate network domain controllers based on Active Directory" consists of a list of abbreviations, introduction, three chapters, conclusions, a list of references and 3 appendices of 38 volume.

The total volume of the work occupies 96 pages, contains 56 figures and 5 tables. The list of references includes 23 titles that occupies 3 pages.

The first chapter analyzes the literature on the topic of the qualification work, highlights the place of automation in the overall system and formulates the terms of reference that form the necessary requirements for future automated solutions.

The second section discusses the methods and means of solving the tasks, designing and configuring the network.

In the third section, the project is deployed, the security system is configured, and the scripts are tested. Using PowerShell scripts, we created a domain structure, all OUs and users in them, configured access control, password policies, and event auditing on the server. I will add backups and a control panel

The appendices to the paper contain configuration files and a list of scripts for deploying domain controllers.

**Keywords:** MICROSOFT, ACTIVE DIRECTORY, GNS SOFTWARE EMULATOR, NAT, GPO, POWERSHELL, ACCESS CONTROL, US-ERS, SCRIPTS, GPO, PSO, ORGANIZATIONAL UNITS, COMMANDLETS.

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 5    |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

## ЗМІСТ

|                                                                                                  |    |
|--------------------------------------------------------------------------------------------------|----|
| ВСТУП                                                                                            | 8  |
| РОЗДІЛ 1. ОГЛЯД ДОСЛІДЖЕНЬ ТА ІНСТРУМЕНТІВ ЗА ТЕМОЮ РОБОТИ<br>ТА ПОСТАНОВКА ТЕХНІЧНОГО ЗАВДАННЯ. | 9  |
| 1.1 Аналіз методів та технологій управління контролером домену .....                             | 9  |
| 1.2 Класифікація систем автоматизації процесів в Active Directory .....                          | 14 |
| 1.3 Визначення можливостей PowerShell для автоматизації процесів. ....                           | 18 |
| 1.4 Постановка технічного завдання .....                                                         | 20 |
| Висновки до розділу .....                                                                        | 20 |
| РОЗДІЛ 2. ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ .....                                            | 21 |
| 2.1 Розробка топології комп'ютерної мережі .....                                                 | 21 |
| 2.2 Розробка схеми адресації мережі .....                                                        | 23 |
| 2.3 Розмежування доступу користувачів .....                                                      | 25 |
| Висновки до розділу .....                                                                        | 30 |
| РОЗДІЛ 3. РОЗГОРТАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЗАСОБАМИ АВ-<br>ТОМАТИЗАЦІЇ.                      | 31 |
| 3.1 Встановлення та розгортання Microsoft Active Directory .....                                 | 31 |
| 3.2 Налаштування групових політик .....                                                          | 42 |
| 3.3 Налаштування мережевих пристроїв .....                                                       | 53 |
| Висновки до розділу .....                                                                        | 57 |
| ВИСНОВКИ                                                                                         | 58 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ                                                                   | 59 |
| ДОДАТКИ                                                                                          | 62 |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

MS – Microsoft

AD – Active Directory

DHCP - Dynamic Host Configuration Protocol

OU – Organization Unit

WS – Work Station

GPO – Group Policy Object

PS – Power Shell

PSO – Password Settings Object

ПЗ – Програмне забезпечення

ПК – персональний комп'ютер

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 7    |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

## ВСТУП

**Актуальність теми.** У сучасному інформаційно-технологічному середовищі, що стрімко розвивається та збільшує обсяги даних, корпоративні мережі стають все більш складними та вимогливими з точки зору ефективного управління. Одним з ключових компонентів таких мереж є контролери доменів, які забезпечують централізоване управління користувачами, комп'ютерами та мережевими ресурсами на основі Active Directory. Традиційні методи розгортання контролерів доменів часто вимагають значних ресурсів, часу і людських зусиль, що може негативно вплинути на продуктивність і безперервність роботи організації.

**Метою випускної кваліфікаційної роботи** є розробка системи автоматизованого розгортання контролерів домену корпоративної мережі на базі Active Directory. Для досягнення поставленої мети було сформульовано наступні задачі:

- провести аналіз сучасних досліджень та технологій автоматизації процесів в ОС Windows, визначити необхідні компоненти для розгортання захищеного ядра системи на базі Active Directory
- провести проектування мережевої інфраструктури підприємства, що забезпечить надійну та продуктивну роботу її домену
- розробити скрипти для автоматизованого розгортання контролерів домену корпоративної мережі на базі Active Directory
- перевірити роботоспроможність розробленої системи та створених автоматизованих сценаріїв

**Об'єктом дослідження** є процес автоматизації розгортання та налаштування мережевої інфраструктури, контролерів домену, процес створення користувачів, групових політик, мережевих пристроїв тощо.

**Предметом дослідження** є методи та засоби засоби налаштування мережевої інфраструктури з використанням командлетів PowerShell, написання скриптів для автоматизації цих процесів.

У процесі виконання кваліфікаційної роботи було розроблено: структуру мережі підприємства, розмежування доступу користувачів, автоматизовані рішення для розгортання доменних контролерів та виконання базових налаштувань.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 8    |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

## РОЗДІЛ 1. ОГЛЯД ДОСЛІДЖЕНЬ ТА ІНСТРУМЕНТІВ ЗА ТЕМОЮ РОБОТИ ТА ПОСТАНОВКА ТЕХНІЧНОГО ЗАВДАННЯ.

### 1.1 Аналіз методів та технологій управління контролером домену

Active Directory (AD) - це служба управління каталогами та ідентичностями від Microsoft для доменних мереж Windows. Вона була представлена в Windows 2000, входить до складу більшості операційних систем MS Windows Server і використовується різними рішеннями Microsoft, такими як Exchange Server і SharePoint Server, а також додатками і службами сторонніх розробників.

Служби доменів Active Directory - це основна служба Active Directory. Вона використовується для автентифікації користувачів і контролю доступу до мережеских ресурсів. Сервер, на якому працює AD DS, називається контролером домену. Більшість доменних мереж Windows мають два або більше контролерів домену: основний контролер домену та один або більше резервних контролерів домену для забезпечення відмовостійкості. Під час входу користувачі проходять автентифікацію на контролері домену і отримують доступ до певних ресурсів на основі адміністративно визначених політик [1].

Існує цілий ряд функціональних переваг, які надає Active Directory, і вони включають в себе наступні:

- Безпека - безпека підвищується за рахунок контролю доступу до мережеских ресурсів.
- Розширюваність - компанії можуть легко організувати дані Active Directory відповідно до своєї організаційної структури та бізнес-потреб.
- Простота - адміністратори можуть централізовано керувати ідентичностями користувачів і привілеями доступу в масштабах підприємства, що допомагає знизити операційні витрати.
- Відмовостійкість - оскільки Active Directory підтримує дублювання компонентів і реплікацію даних, це сприяє безперервності бізнесу.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 9    |

Основною службою Active Directory є служба доменів Active Directory Domain Services (AD DS), яка є частиною операційної системи Windows Server. Після встановлення Active Directory Domain Services на сервері він стає контролером домену (DC). На цьому сервері зберігається вся база даних AD, включно з об'єктами, деревами та їхніми зв'язками. Зазвичай організації мають кілька контролерів доменів, і кожен з них має копію каталогу для всього домену. Зміни, внесені до каталогу на одному контролері домену, наприклад, оновлення пароля, додавання або видалення даних, реплікуються на інші контролери домену, щоб усі вони залишалися актуальними. Настільні комп'ютери, ноутбуки та інші пристрої під керуванням Windows (а не Windows Server) можуть бути частиною середовища Active Directory, але на них не працюють служби домену Active Directory.

Важливо зазначити, що Active Directory призначений лише для локальних середовищ Microsoft. У хмарних середовищах Microsoft використовується Azure Active Directory. Azure Active Directory - це хмарне рішення наступного покоління для керування ідентичностями від Microsoft, яке використовується для контролю доступу до рішень SaaS, таких як Microsoft 365, хмарних додатків власної розробки, що працюють на Azure, а також традиційних корпоративних додатків. AD і Azure AD є окремими, але можуть певною мірою працювати разом, якщо у вашій організації використовується гібридне розгортання локального та хмарного IT-середовищ.

Active Directory складається з наступної ієрархічної структури:

- **Домени:** Домен представляє групу об'єктів, таких як користувачі, групи і пристрої, які мають спільну базу даних AD. Ви можете уявити собі домен як гілку дерева. Домен має таку саму структуру, як і стандартні домени та під-домени, наприклад, *yourdomain.com* і *sales.yourdomain.com*.
- **Дерева:** Дерево - це один або кілька доменів, згрупованих разом у логічній ієрархії. Оскільки домени в дереві пов'язані між собою, вважається, що вони «довіряють» один одному.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 10   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

- Ліс: Ліс є найвищим рівнем організації в AD і містить групу дерев. Дерева в лісі також можуть довіряти одне одному, а також ділитися схемами каталогів, каталогами, інформацією про програми та конфігураціями доменів.

- Організаційні одиниці: OU використовується для організації користувачів, груп, комп'ютерів та інших організаційних одиниць.

- Контейнери: Контейнер схожий на OU, однак, на відміну від OU, неможливо зв'язати об'єкт групової політики (GPO) із загальним контейнером Active Directory [2].

Kerberos, NTLM і LDAP – протоколи автентифікації які Active Directory підтримує.

Протокол Kerberos - це протокол автентифікації, що використовується для перевірки ідентифікації користувача або вузла мережі. Вперше розроблений Масачусетським технологічним інститутом (MIT) у 1980-х роках, Kerberos став широко використовуваним протоколом автентифікації для комп'ютерних мереж.

Kerberos використовує систему на основі квитків для забезпечення автентифікації, яка працює наступним чином:

1. Користувач намагається отримати доступ до мережевого ресурсу, такого як файловий сервер або база даних.
2. Комп'ютер користувача надсилає запит на сервер автентифікації Kerberos з запитом на квиток для потрібного ресурсу.
3. Сервер Kerberos перевіряє облікові дані користувача, такі як ім'я користувача та пароль, і створює квиток для надання (TGT).
4. TGT шифрується секретним ключем і надсилається назад на комп'ютер користувача.
5. Комп'ютер користувача розшифровує TGT за допомогою його пароля та надсилає запит на сервер надання квитків (TGS) для отримання квитка для доступу до потрібного ресурсу.
6. TGS перевіряє особу користувача за допомогою TGT і створює службовий квиток для потрібного ресурсу.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 11   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

7. Сервісний квиток шифрується сеансовим ключем і надсилається назад на комп'ютер користувача.

8. Комп'ютер користувача розшифровує службовий квиток і надсилає його на сервер ресурсу разом із запитом на доступ до ресурсу.

9. Сервер ресурсів перевіряє квиток служби за допомогою ключа сеансу та надає доступ до ресурсу, якщо квиток є дійсним [3].

NTLM (NT LAN Manager) — це протокол автентифікації Microsoft, який використовується для автентифікації користувачів і комп'ютерів у мережевому середовищі Windows. Він був представлений в операційній системі Windows NT як наступник протоколу автентифікації LM (LAN Manager), який був менш безпечним.

Windows New Technology LAN Manager (NTLM) - це набір протоколів безпеки, запропонований Microsoft для автентифікації користувачів, захисту цілісності та конфіденційності їхньої діяльності. За своєю суттю, NTLM є інструментом єдиного входу (SSO), який покладається на протокол «запит-відповідь» для підтвердження користувача, не вимагаючи від нього введення пароля.

Незважаючи на відомі вразливості, NTLM продовжує широко використовуватися навіть у нових системах, щоб підтримувати сумісність із застарілими клієнтами та серверами. Хоча NTLM все ще підтримується Microsoft, він був замінений на Kerberos як протокол автентифікації за замовчуванням в Windows 2000 і наступних доменах Active Directory (AD).

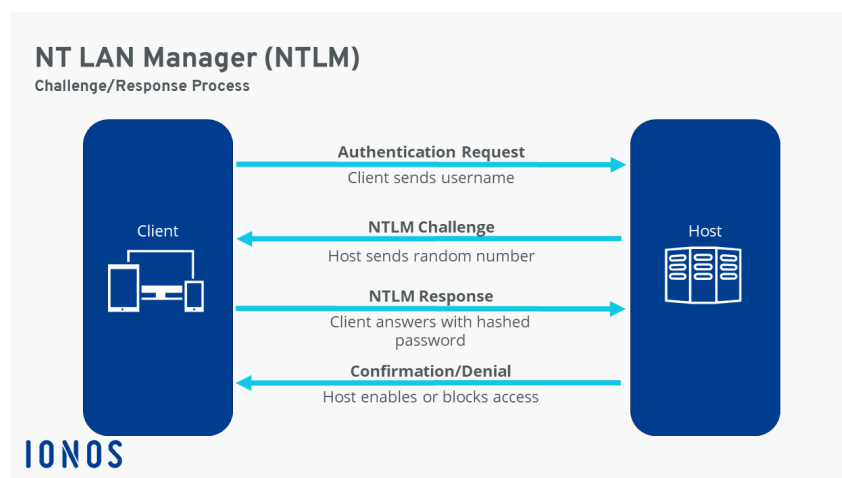


Рис. 1.1.1 - Принцип роботи NTLM

Основна відмінність між NTLM і Kerberos полягає в тому, як ці два протоколи керують автентифікацією. NTLM покладається на тристороннє рукошлякування між клієнтом і сервером для автентифікації користувача. Kerberos використовує двосторонній процес, який використовує службу видачі квитків або центр розподілу ключів [4].

Полегшений протокол доступу до каталогів (LDAP) - це протокол, який дозволяє програмам швидко запитувати інформацію про користувача.

Компанії зберігають імена користувачів, паролі, адреси електронної пошти, підключення до принтерів та інші статичні дані в каталогах. LDAP - це відкритий, незалежний від постачальника прикладний протокол для доступу до цих даних. LDAP також може обробляти автентифікацію, тому користувачі можуть увійти в систему лише один раз і отримати доступ до багатьох різних файлів на сервері. Принцип роботи зображено на Рис. 1.1

LDAP - це протокол, тому він не визначає, як працюють програми для роботи з каталогами. Замість цього, це форма мови, яка дозволяє користувачам дуже швидко знаходити потрібну інформацію [5].

LDAP не залежить від постачальника, тому його можна використовувати з різними програмами для роботи з каталогами. Зазвичай каталог містить дані, які є:

- Описові. Кілька пунктів, таких як ім'я та місцезнаходження, об'єднуються для визначення ресурсу.
- Статичними. Інформація не дуже часто змінюється, а якщо і змінюється, то малопомітно.
- Цінні. Дані, що зберігаються в каталозі, є критично важливими для основних бізнес-функцій, і до них звертаються знову і знову.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 13   |

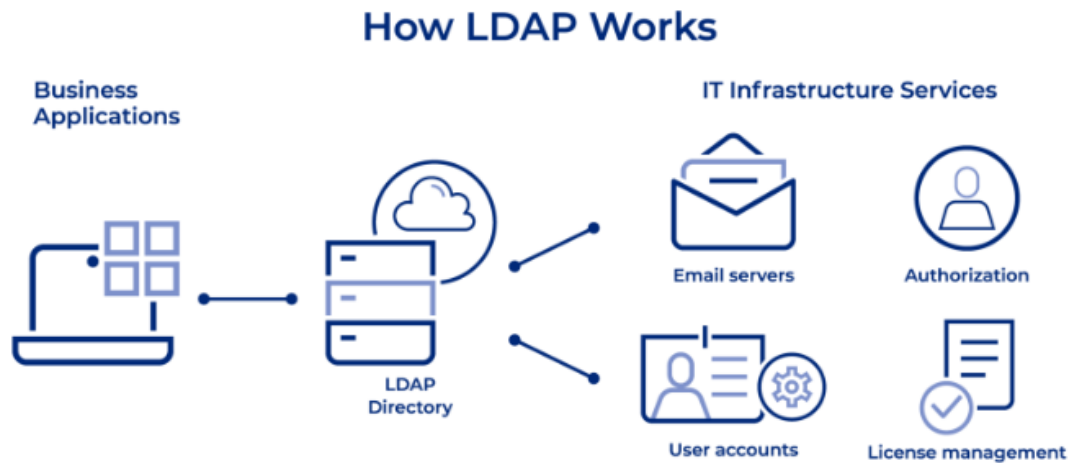


Рис. 1.1.2 - LDAP Directory Tree

Детальна політика паролів (Fine-grained password policy, FGPP) надає можливість встановлювати різні політики блокування паролів і облікових записів для різних груп користувачів в одному домені, тим самим роблячи середовище AD більш захищеним. FGPP розширює сферу безпеки паролів за рахунок наявності декількох політик паролів в одному домені. Детальна політика паролів розгортається за допомогою об'єктів параметрів паролів (PSO). PSO містить ті самі параметри паролів, що й інші об'єкти GPO. Щоб застосувати різні налаштування до груп користувачів, адміністраторам потрібно створити новий PSO і налаштувати параметри відповідно до вимог. Коли PSO застосовано до користувача, користувач більше не використовує політику паролів, розгорнуту у груповій політиці. Замість цього він використовує вказані параметри PSO [6].

## 1.2 Класифікація систем автоматизації процесів в Active Directory

З розвитком технологій, розширенням підприємств котрі використовують Active Directory у своїх цілях виникала потреба у рішеннях, котрі значно спростили б процес налаштування і розгортання контролерів домену і пов'язаних з ним інструментів та речей.

Таким чином сьогодні існує декілька рішень, котрі задовольняють вимоги більшості спеціалістів.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 14   |

Серед них:

- Швидкість та ефективність розгортання
- Надійність та безпека
- Легкість у використанні
- Гнучкість та адаптивність
- Інтеграція з існуючими системами
- Моніторинг та звітність

Ansible - це програмне забезпечення для автоматизації ІТ з відкритим вихідним кодом, написане мовою Python. Він може налаштовувати системи, розгортати програмне забезпечення та організовувати розширені робочі процеси для підтримки розгортання додатків, оновлення системи тощо.

Основними сильними сторонами Ansible є простота і легкість у використанні. Він також приділяє особливу увагу безпеці та надійності, маючи мінімальну кількість рухомих частин. Він використовує OpenSSH для транспортування (з іншими способами транспортування і витягування як альтернативи), а також використовує зрозумілу для людини мову, яка призначена для швидкого початку роботи без тривалого навчання.

Спільний дистрибутив Ansible містить набір потужних інструментів командного рядка, які підтримуються на більшості операційних систем, де встановлено Python. Сюди входять Red Hat Enterprise Linux, Debian, Ubuntu, MacOS, FreeBSD, Microsoft Windows та інші.

Ansible виконується з керуючого вузла - наприклад, коли користувач запускає команду `ansible-playbook`. Керовані вузли - це пристрої, які автоматизуються, наприклад, сервер Microsoft Windows.

Для автоматизації Linux і Windows Ansible підключається до керованих вузлів і виштовхує на них невеликі програми, які називаються модулями Ansible. Ці програми написані як ресурсні моделі бажаного стану системи. Потім Ansible виконує ці модулі (за замовчуванням через SSH) і видаляє їх після завершення. Ці модулі розроблені так, щоб бути ідемпотентними, коли це можливо, щоб вони вносили зміни в систему лише тоді, коли це необхідно.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 15   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

Для автоматизації мережевих пристроїв та інших ІТ-пристроїв, де модулі не можуть бути виконані, Ansible запускається на керуючому вузлі. Оскільки Ansible не має агентів, він може взаємодіяти з пристроями, не вимагаючи встановлення додатків чи сервісів на керованому вузлі. Щоб збільшити потужність виконання для пристроїв без можливості запуску модулів, Ansible Automation Platform може розподіляти завдання автоматизації між вузлами виконання, використовуючи технологію, яка називається «сітка автоматизації» (automation mesh).

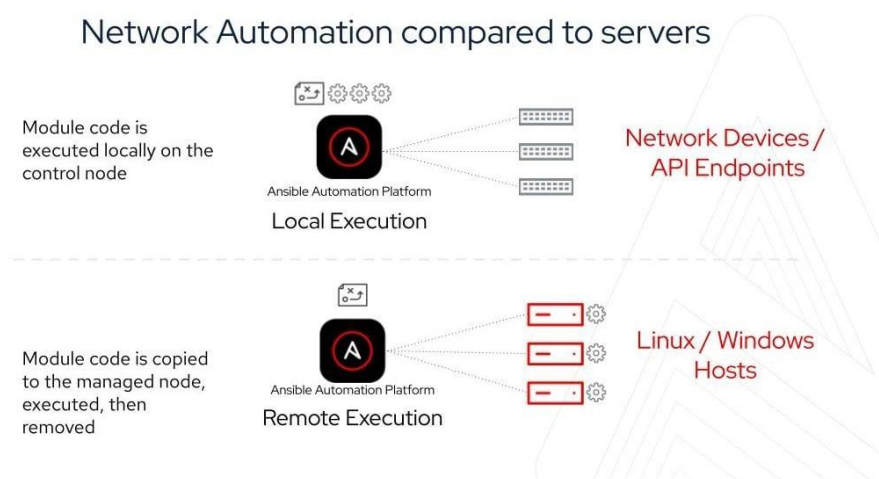


Рис. 1.1.3 – Порівняння Network Automation до серверів

Ansible – чудовий інструмент але при роботі з Windows Server 2019 та Active Directory можуть виникати деякі обмеження та проблеми:

#### Обмежена підтримка Windows

- **Linux-орієнтований:** Ansible спочатку був розроблений для роботи з Linux-системами, і хоча підтримка Windows була додана, вона все ще менш розвинена в порівнянні з Linux.

- **Модулі для Windows:** Хоча існує багато модулів для управління Windows, деякі специфічні функції Windows Server 2019 та Active Directory можуть бути не повністю підтримані або вимагати додаткових налаштувань.

#### Складність налаштування:

- **Windows Remote Management (WinRM):** Ansible використовує WinRM для зв'язку з Windows-системами. Налаштування WinRM може бути складним і вимагати додаткових зусиль для забезпечення безпечного та стабільного з'єднання.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 16   |

- Додаткові налаштування: Деякі функції, такі як управління Active Directory, можуть вимагати складних налаштувань та налаштувань безпеки, що ускладнює використання Ansible у порівнянні з іншими інструментами.

#### Обмежені можливості автоматизації для Active Directory

- Обмежена функціональність модулів: Існуючі модулі Ansible для управління Active Directory можуть не покривати всі необхідні аспекти управління доменними контролерами та об'єктами Active Directory.

- Складність у сценаріях: Для деяких складних сценаріїв розгортання та управління Active Directory може знадобитися написання кастомних скриптів або використання інших інструментів у поєднанні з Ansible [7].

Chef - це DevOps інструмент для управління конфігурацією, який керує інфраструктурою за допомогою написання коду, а не за допомогою ручного процесу, тому його можна дуже легко автоматизувати, тестувати і розгортати. Chef має клієнт-серверну архітектуру і підтримує різні платформи, такі як Windows, Ubuntu, Centos, Solaris тощо. Він також може бути інтегрований з хмарними платформами, такими як AWS, Google Cloud Platform, Open Stack тощо.

Перш ніж заглибитись у Chef, давайте розберемось, що таке управління конфігурацією. Керування конфігураціями відстежує всю інформацію, пов'язану з програмним і апаратним забезпеченням організації, а також ремонтує, розгортає та оновлює всю програму за допомогою автоматизованих процедур. Керування конфігураціями виконує роботу кількох системних адміністраторів і розробників, які керують сотнями серверів і додатків. Деякі інструменти, що використовуються для управління конфігурацією: Chef, Puppet, Ansible, CF Engine, SaltStack тощо.

Chef автоматизував конфігурацію, розгортання та управління додатками в мережі, навіть якщо ми працюємо в хмарному або гібридному середовищі. Ми можемо використовувати Chef для прискорення розгортання додатків. Chef є чудовим інструментом для прискорення доставки програмного забезпечення, швидкість розробки програмного забезпечення відноситься до того, наскільки швидко програмне забезпечення здатне змінюватися у відповідь на нові вимоги або умови [8].

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 17   |



Рис. 1.1.4 - Використання Chef Infra для розгортання коду

### Переваги Chef

- Одне з найбільш гнучких рішень для керування ОС та проміжним програмним забезпеченням.
- Розроблено для програмістів.
- Chef пропонує гібридні та SaaS рішення для серверів Chef Servers
- Послідовний порядок виконання
- Дуже стабільний, надійний і зрілий, особливо для великих розгортань як в публічних, так і в приватних середовищах.

### Мінуси Chef

- Потребує тривалого навчання
- Початкове налаштування складне.
- Бракує поштовху, тому немає негайних дій щодо змін. Процес витягування відбувається за визначеним графіком.

Ще існують такі інструменти як MDT(Microsoft Deployment Toolkit), який використовується для автоматизації розгортання операційних систем та базового налаштування [9] та DSC (Desired State Configuration) [10], але усі ці рішення, як і попередні використовують у своїх оболонках можливості Powershell, тому наступним засобом автоматизації було розглянуто саме створення скриптів за допомогою Powershell.

## 1.3 Визначення можливостей PowerShell для автоматизації процесів.

PowerShell - це кросплатформне рішення для автоматизації завдань, що складається з оболонки командного рядка, мови сценаріїв і середовища керування конфігурацією. PowerShell працює на Windows, Linux та macOS[11].

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 18   |

PowerShell - це сучасна командна оболонка, яка включає в себе найкращі можливості інших популярних оболонок. На відміну від більшості оболонок, які приймають і повертають лише текст, PowerShell приймає і повертає об'єкти .NET. Оболонка має наступні можливості:

- Надійна історія командного рядка
- Заповнення табуляції та передбачення команд
- Підтримка псевдонімів команд і параметрів
- Конвеєр для ланцюжкового виконання команд
- Консольна довідкова система, подібна до довідкових сторінок Unix

Як і описані вище рішення, PowerShell вимагає вивчення та набуття навичок написання скриптів за допомогою командлетів вбудованих у Windows. Але це у свою чергу дає нам змогу напряду вирішувати як саме працюватимуть скрипти для автоматизації тих чи інших процесів, адже на кожному виконувану графічну дію є відповідна дія у вигляді коду.

Серед них:

- встановлення модулів Active Directory,
- розгортання домену,
- налаштування IP-конфігурації робочі станції/контролера домену,
- налаштування DHCP та DNS,
- створення та розподіл OU всередині структури домену,
- налаштування та керування груповими політиками,
- використання сервісів AD DS та ін.

До того ж більшість готових рішень використовують саме командлети PowerShell для виконання тих чи інших налаштувань, тому розуміння принципів роботи оболонки дає змогу гнучко керувати системою в цілому [12].

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 19   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

#### 1.4 Постановка технічного завдання

В результаті аналізу літератури за темою кваліфікаційної роботи було визначено актуальність розробки системи автоматизованого розгортання контролерів домену корпоративної мережі на базі Active Directory. Для досягнення зазначеної мети слід виконати наступні задачі:

- Автоматизоване встановлення і налаштування контролеру домену Active Directory
- Автоматизоване налаштування DNS-ролі серверу
- Автоматизоване налаштування DHCP-ролі серверу та IP конфігурації
- Налаштування IP та DHCP конфігурацій
- Створення користувачів на основі сформованого переліку співробітників підприємства
- Створення OU(відділів) та розмежування доступу в їх структурі
- Забезпечення автентифікації користувачів у системі
- Забезпечення авторизації користувачів у системі
- Створення та керування груповими політиками[13]
- Моніторинг подій у системі

Результатом виконаної роботи мають бути автоматизовані рішення, котрі дадуть змогу швидко і безпечно розгорнути контролер домену в залежності від функціональних вимог підприємства.

Посилаючись на вищевказані вимоги, архітектура системи буде реалізована на базі рішень Microsoft Active Directory з використанням інструментів вбудованих у операційні системи Windows [14].

#### Висновки до розділу

У першому розділі були проведені теоретичні дослідження технологій необхідних для реалізації проекту, згідно теми кваліфікаційної роботи було визначене технічне завдання, яке формує необхідні вимоги для майбутніх автоматизованих рішень.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 20   |

## РОЗДІЛ 2. ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ.

### 2.1 Розробка топології комп'ютерної мережі

Для підприємства була розроблена топологія захищеної мережі, під час проектування особлива увага була приділена наступним особливостям:

- Мережа локальна
- Доступ до інтернету
- Масштабованість, тобто підтримка підключення нових пристроїв

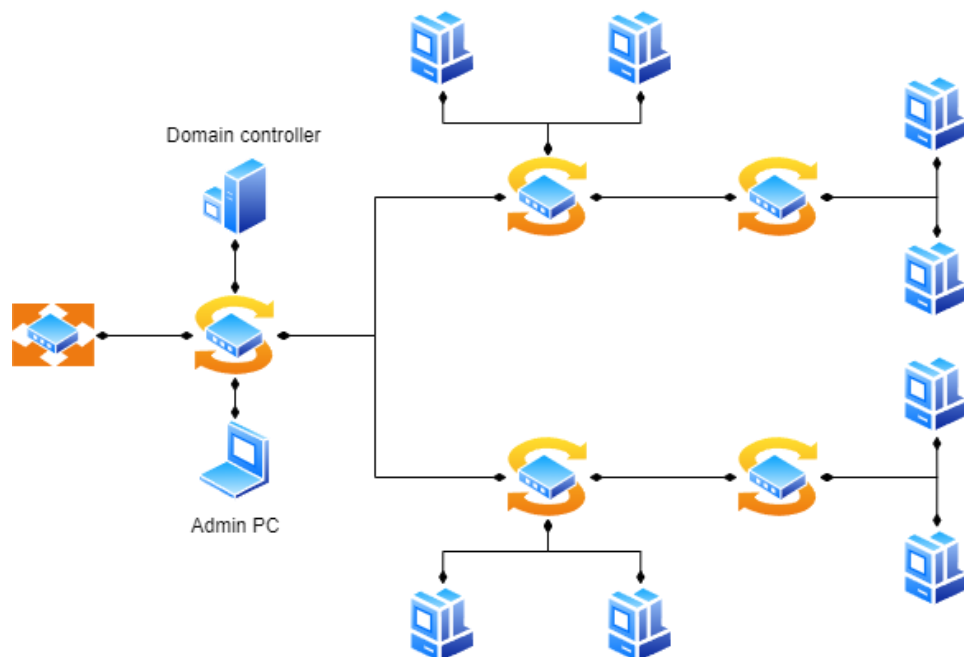


Рисунок 2.1 - Схематична топологія мережі

Спроектована мережа, що представлена на рисунку 2.1 – складається з: 1 маршрутизатора, 5 комутаторів з можливістю розширення, головного контролера домену і довільної кількості кінцевих пристроїв, наявність певної кількості кінцевих пристроїв в топології мережі не відображує їх реальну кількість, адже для тестування реалізованих надалі рішень не потрібна велика кількість ресурсів. Доступ до інтернету буде забезпечено за допомогою використання протоколу NAT і його функції перевантаження(overload) [15].

Перевантаження NAT - це найпоширеніший метод NAT, який використовується у всіх мережах, що підключаються до Інтернету. Це пов'язано з тим, як він функціонує і з обмеженнями, які він може подолати.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 21   |

Незалежно від того, чи використовуєте ви маршрутизатор, брандмауер, функцію спільного доступу до Інтернету від Microsoft або будь-яку сторонню програму, яка дозволяє всім вашим домашнім комп'ютерам підключатися до Інтернету через одне з'єднання, ви використовуєте перевантаження NAT.

Цей режим NAT також відомий під іншими назвами, такими як NAPT (Network Address Port Translation - перетворення мережевої адреси на порт), IP-маскування і NAT з PAT (Port Address Translation - перетворення адреси порту).

Це також допоможе нам налаштувати з'єднання з мережею інтернет в межах мережевого емулятора GNS [16].

На комутаторах мережі будуть застосовані мінімальні заходи безпеки базовим і найпростішим з яких є – Port Security.

За замовчуванням всі інтерфейси на комутаторах Cisco увімкнені. Це означає, що зловмисник може підключитися до вашої мережі через розетку і потенційно загрожувати вашій мережі. Якщо ви знаєте, які пристрої будуть підключені до яких портів, ви можете використовувати функцію безпеки Cisco, яка називається Port Security. Використовуючи захист портів, мережевий адміністратор може пов'язати певні MAC-адреси з інтерфейсом, що може перешкодити зловмиснику підключити свій пристрій. Таким чином, ви можете обмежити доступ до інтерфейсу, щоб тільки авторизовані пристрої могли ним користуватися. Якщо підключено несанкціонований пристрій, ви можете вирішити, яку дію виконає комутатор, наприклад, відкинути трафік або вимкнути порт.

Щоб налаштувати Port Security, потрібно виконати три кроки:

1. визначити інтерфейс як інтерфейс доступу за допомогою команди `switchport mode access interface`
2. увімкнути безпеку порту за допомогою команди `switchport port-security interface`
3. визначити, з яких MAC-адрес дозволено надсилати кадри через цей інтерфейс за допомогою команди `switchport port-security mac-address MAC_ADDRESS interface` або за допомогою команди `switchport port-security mac-address sticky`

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 22   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

interface для динамічного вивчення MAC-адреси підключеного в даний момент хоста [17].

## 2.2 Розробка схеми адресації мережі

Робочі станції всередині мережі будуть отримувати динамічні IP-адреси за допомогою протоколу DHCP, але контролер домену та мережеві пристрої повинні мати статичні адреси.

Протокол динамічної конфігурації хоста (DHCP) - це протокол клієнт/сервер, який автоматично надає хосту Інтернет-протоколу (IP) його IP-адресу та іншу пов'язану з нею конфігураційну інформацію, таку як маска підмережі та шлюз за замовчуванням. RFC 2131 і 2132 визначають DHCP як стандарт Робочої групи з розробки інтернету (IETF), заснований на протоколі Bootstrap (BOOTP), протоколі, з яким DHCP має багато спільних деталей реалізації. DHCP дозволяє хостам отримувати необхідну інформацію про конфігурацію TCP/IP від сервера DHCP.

До складу Windows Server 2016 входить DHCP-сервер, який є додатковою роллю мережевого сервера, яку ви можете розгорнути у своїй мережі для надання IP-адрес та іншої інформації клієнтам DHCP. Усі клієнтські операційні системи на базі Windows включають клієнт DHCP як частину TCP/IP, і клієнт DHCP увімкнено за замовчуванням [18].

Для забезпечення адресації нижче наведено розрахунки у Таблиці 2.1

Таблиця 2.1

### Інформація про мережу

| Призначення                         | IP-адреса                 |
|-------------------------------------|---------------------------|
| Мережева адреса:                    | 205.8.15.0/24             |
| Використовуваний діапазон IP адрес: | 205.8.15.1 - 205.8.15.254 |
| Широкомовна адреса:                 | 205.8.15.255              |
| Загальна кількість хостів:          | 256                       |
| Кількість доступних хостів:         | 254                       |
| Маска підмережі:                    | 255.255.255.0             |

|                                     |                          |
|-------------------------------------|--------------------------|
| Обернена маска:                     | 0.0.0.255                |
| Шлюз по замовчуванню(маршрутизатор) | 205.8.15.1               |
| Діапазон адрес комутаторів          | 205.8.15.3-205.8.15.7    |
| Адреса серверу                      | 205.8.15.2               |
| Вільний діапазон IP адрес           | 205.8.15.10-205.8.15.254 |
| Діапазон адрес робочих станцій      | DHCP                     |

У Таблиці 2.1 проведений розподіл IP адрес для усіх мережевих пристроїв, а саме для: шлюзу за замовчуванням (маршрутизатора), комутаторів, серверів, вільний діапазон виділений для робочих станцій та інших пристроїв.

Таблиця 2.2

## Параметри IP-адресації мережі

| Мережа/<br>Пристрій | Інтерфейс/Мереж-<br>ний адаптер/Шлюз | IP-адреса  | Маска         | /   |
|---------------------|--------------------------------------|------------|---------------|-----|
| corpmarkeiev.net    |                                      | 205.8.15.0 | 255.255.255.0 | /24 |
| LAN_A               |                                      | 10.1.1.0   | 255.255.255.0 | /24 |
| Маршрутизатор<br>R1 | Інтерфейс fe0/0                      | DHCP       |               |     |
|                     | Інтерфейс fe0/1                      | 10.1.1.254 | 255.255.255.0 | /24 |
| Комутатор<br>SW-1   | Інтерфейс Vlan 1                     | 205.8.15.3 | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           | 205.8.15.1 | -             | -   |
| Комутатор<br>SW-2   | Інтерфейс Vlan 1                     | 205.8.15.4 | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           | 205.8.15.1 | -             | -   |

|                   |                       |             |               |     |
|-------------------|-----------------------|-------------|---------------|-----|
| Комутатор<br>SW-3 | Інтерфейс Vlan 1      | 205.8.15.4  | 255.255.255.0 | /24 |
|                   | Шлюз за замовчуванням | 205.8.15.1  | -             | -   |
| Комутатор<br>SW-4 | Інтерфейс Vlan 1      | 205.8.15.5  | 255.255.255.0 | /24 |
|                   | Шлюз за замовчуванням | 205.8.15.1  | -             | -   |
| Комутатор<br>SW-5 | Інтерфейс Vlan 1      | 205.8.15.6  | 255.255.255.0 | /24 |
|                   | Шлюз за замовчуванням | 205.8.15.1  | -             | -   |
| Комутатор<br>SW-6 | Інтерфейс Vlan 1      | 192.168.0.7 | 255.255.255.0 | /24 |
|                   | Шлюз за замовчуванням | 205.8.15.1  | -             | -   |
| SRV-MRKV          | Інтерфейс E0/0        | 205.8.15.2  | 255.255.255.0 | /24 |
| AdminPC           | Інтерфейс E0/0        | 205.8.15.3  | 255.255.255.0 | /24 |

### 2.3 Розмежування доступу користувачів

Проект спрямовано на автоматизацію розгортання контролера домену і мережі підприємства. Для моделювання бази виконання даного проекту обрано офіс невеликого підприємства, з нечисленним штатом співробітників різних відділів і структур. Можна зазначити, що програмна автоматизація може бути реалізована на базі будь-якого малого підприємства, незалежно від вибору.

Керування доступом може здійснюватися за допомогою утиліти Ntrights, котра є одним з компонентів серверного ресурсного комплексу Microsoft Windows 2000 Server Resource Kit.

Ця утиліта командного рядка дозволяє вам змінювати права користувачів або груп на локальних і віддалених машинах. У наш час більшість адміністраторів Windows, ймовірно, використовують графічний інтерфейс для керування правами користувачів, але утиліта командного рядка не втратила своєї цінності і у багатьох випадках може бути кращим вибором, ніж версія з графічним інтерфейсом. Наприклад, ви можете включити Ntrights у скрипти і командні файли для виконання багатьох складних адміністративних завдань на декількох машинах.[\[19\]](#)

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 25   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

## Синтаксис Ntrights

Під час інсталяції набору ресурсів Ntrights за замовчуванням встановлюється у каталог %systemroot%\program filesresource kit. Щоб скористатися утилітою, потрібно увійти до системи під обліковим записом, який має достатні права для внесення змін на цільовому комп'ютері, на якому ви хочете, щоб зміни набули чинності.[20]

Також розподілити можливості користувачів можна за допомогою групових політик або ж GPO, вони використовуються для доступу до ресурсів у домені: робочі станції, групи користувачів, користувачі тощо. За їх же допомогою будуть впроваджуватись норми безпеки для користувачів: паролі, їх складність, кількість спроб для входу тощо.

Об'єкт групової політики (GPO) - це віртуальна колекція параметрів політики. GPO має унікальне ім'я, наприклад GUID [21].

Параметри групової політики містяться в об'єкті GPO. GPO може представляти параметри політики у файловій системі і в Active Directory. Параметри GPO оцінюються клієнтами, використовуючи ієрархічну природу Active Directory.

Створювати їх можна за допомогою GPMC (Group Policy Management Console) або ж за допомогою командлетів Powershell імпортуючи модулі для роботи з груповими політиками, відмінність полягає лише в тому, що потрібно знати параметри котрі приймає командлет пов'язаний з GPO, а також дослідити шляхи реєстрів політик, котрі потрібні для виконання задач [22].

У Таблиці 2.3 наведено список користувачів, їх приналежність до відділу та роль яку вони виконують на підприємстві. Це означає, що під час реалізації структури домену, потрібно буде враховувати значимість кожного з користувачів, а якщо конкретніше то користувачів відділу System Administrators, котрі виконують найголовнішу роль у середовищі домену

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 26   |

Таблиця 2.3

## Користувачі та відділи домену

| Користувач       | Відділ                 | Роль          |
|------------------|------------------------|---------------|
| John Doe         | Accountancy Department | Accounter     |
| Jane Smith       | Accountancy Department | Accounter     |
| Michael Thompson | HR Department          | HR Specialist |
| Sara Brown       | HR Department          | HR Specialist |
| Alex Davis       | Digital Transformation | Designer      |
| Anna Klein       | Digital Transformation | Photograph    |
| Tom Parker       | Engineering Department | Lead engineer |
| Emma Peterson    | Engineering Department | Engineer      |
| Chris Morris     | System Administrators  | DC Admin      |
| Olivia Nelson    | System Administrators  | System Admin  |

Розмежування доступу змодельовано таким чином, аби користувачі мали змогу виконувати локальний вхід лише на робочих станціях свого відділу. Виключенням є адміністратори системи, один з яких відповідає за управління контролером домену і має доступ лише до нього, інший же виступає в ролі системного адміністратора, котрий має доступ до усіх робочих станцій відділу. Відповідно до розмежування мають бути створені OU для розміщення кожного з відділів підприємства з розподілом користувачів у них.

У Таблиці 2.4 детальніше продемонстровано як буде розмежовано доступ між користувачами домену

Таблиця 2.4

## Доступ користувачів всередині домену

|                     | Адміністратор контролеру | Системний адміністратор | Користувач департаменту |
|---------------------|--------------------------|-------------------------|-------------------------|
| Власний департамент | +                        | +                       | +                       |
| Інший департамент   | -                        | +                       | -                       |
| Мережеві пристрої   | -                        | +                       | -                       |

Також звичайним користувачам домену необхідно обмежити доступ до певних функцій на робочих станціях, задля захисту від неправомірних дій.

Таблиця 2.5

#### Заборони користувачам

|                                       | Системний адміністратор | Користувач департаменту |
|---------------------------------------|-------------------------|-------------------------|
| Доступ до панелі керування            | +                       | -                       |
| Доступ до рядка Powershell            | +                       | -                       |
| Доступ до налаштувань                 | +                       | -                       |
| Підключення USB пристроїв             | +                       | -                       |
| Встановлення програмного забезпечення | +                       | -                       |
| Доступ до реєстру                     | +                       | -                       |
| Заборона завантажень з браузера       | +                       | -                       |
| Встановлення ПЗ                       | +                       | -                       |

Чому це важливо:

#### 1. Доступ до панелі керування

- **Безпека:** Панель керування надає доступ до налаштувань системи, які можуть бути змінені зловмисно або помилково, що призведе до збоїв у роботі системи.
- **Адміністративний контроль:** Обмеження доступу дозволяє адміністраторам централізовано керувати налаштуваннями системи, запобігаючи небажаним змінам.

#### 2. Доступ до рядка Powershell

- **Зловживання правами адміністратора:** PowerShell є потужним інструментом для адміністрування Windows, і його використання зловмисниками може призвести до серйозних проблем безпеки.
- **Шкідливе програмне забезпечення:** Багато шкідливих програм використовують PowerShell для виконання шкідливих дій.

### 3. Доступ до налаштувань

- Запобігання змінам конфігурації: Обмеження доступу до налаштувань запобігає змінам конфігурації системи, що може призвести до нестабільної роботи.
- Захист системних налаштувань: Багато системних налаштувань можуть впливати на безпеку системи. Обмеження доступу знижує ризик змін цих налаштувань.

### 4. Підключення USB пристроїв

- Запобігання витоку даних: USB-пристрої можуть бути використані для копіювання конфіденційних даних.
- Захист від шкідливого ПЗ: USB-пристрої можуть бути носіями шкідливих програм, які можуть інфікувати систему при підключенні.

### 5. Встановлення програмного забезпечення

- Контроль за програмами: Обмеження дозволяє контролювати, які програми встановлюються на комп'ютерах користувачів, що запобігає встановленню небажаного або шкідливого ПЗ.
- Сумісність та стабільність: Неконтрольоване встановлення програм може призвести до конфліктів програмного забезпечення та зниження продуктивності системи.

### 6. Доступ до реєстру

- Захист системи: Реєстр Windows містить критично важливі налаштування системи. Неконтрольований доступ може призвести до серйозних проблем у роботі системи.
- Запобігання змінам конфігурації: Зміни в реєстрі можуть впливати на безпеку та стабільність системи.

### 7. Заборона завантажень з браузера

- Запобігання завантаженню шкідливого ПЗ: Заборона завантажень знижує ризик того, що користувачі випадково завантажуть та встановлять шкідливі програми.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 29   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

- Контроль за контентом: Обмеження допомагає контролювати, які файли та дані можуть бути завантажені з Інтернету, що сприяє підвищенню безпеки мережі.

## 8. Встановлення ПЗ

- Запобігання встановленню небажаного ПЗ: Обмеження дозволяє адміністраторам контролювати, яке програмне забезпечення може бути встановлено на комп'ютерах користувачів.
- Зниження ризику інфекцій: Багато шкідливих програм можуть маскуватися під корисне програмне забезпечення. Обмеження встановлення ПЗ знижує ризик інфікування системи.

## Висновки до розділу

У другому розділі було спроектовано модель мережі, котра ґрунтується на розглянутих технологіях, протоколах та готових рішеннях описаних у першому розділі. Було розроблено топологічну структуру мережі підприємства, схему розмежування доступу користувачів та їх місце у межах домену. Окреслено якими функціями буде заборонено користуватись звичайним користувачам і які на це причини.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 30   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

## РОЗДІЛ 3. РОЗГОРТАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ЗАСОБАМИ АВТОМАТИЗАЦІЇ.

### 3.1 Встановлення та розгортання Microsoft Active Directory

Для початку роботи з AD сервером необхідно пройти процес його встановлення, він подібний до інсталяції звичайної ОС Windows, тому розберемо лише деякі моменти.

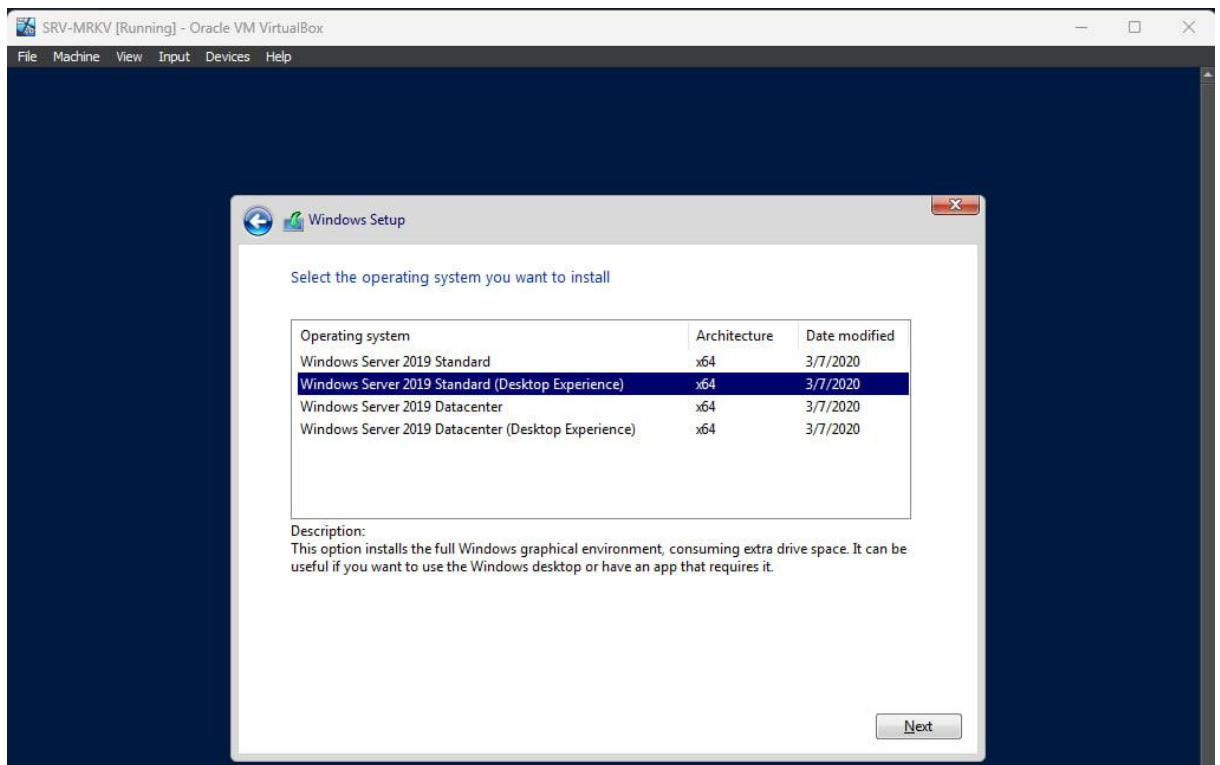


Рис. 3.1.1 - Вибір ОС для встановлення

Після вибору типу встановлення «Custom: Install Windows only (advanced)» виконуємо розбиття диску на розділи, на даному етапі можна керувати доступним місцем на ньому, форматовувати та розбивати його на томи. Було створено один загальний том, адже немає жодної потреби у розбитті його на частини.

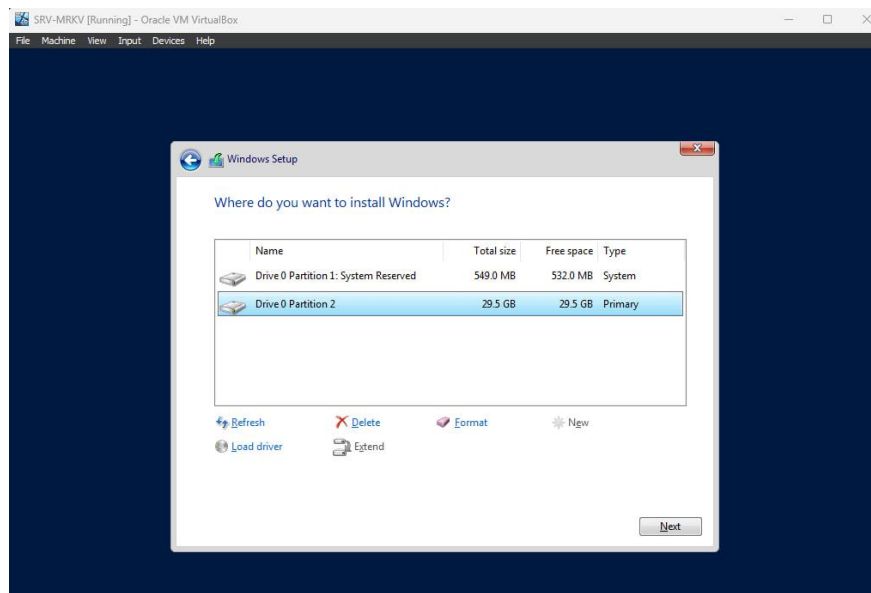


Рис. 3.1.2 - Розбиття диску на розділи

Після очікування завершення процесу встановлення, нас зустрічає вікно створення Адміністратора пристрою та входу під цим обліковим записом, після чого вже є можливим початок налаштування Active Directory.

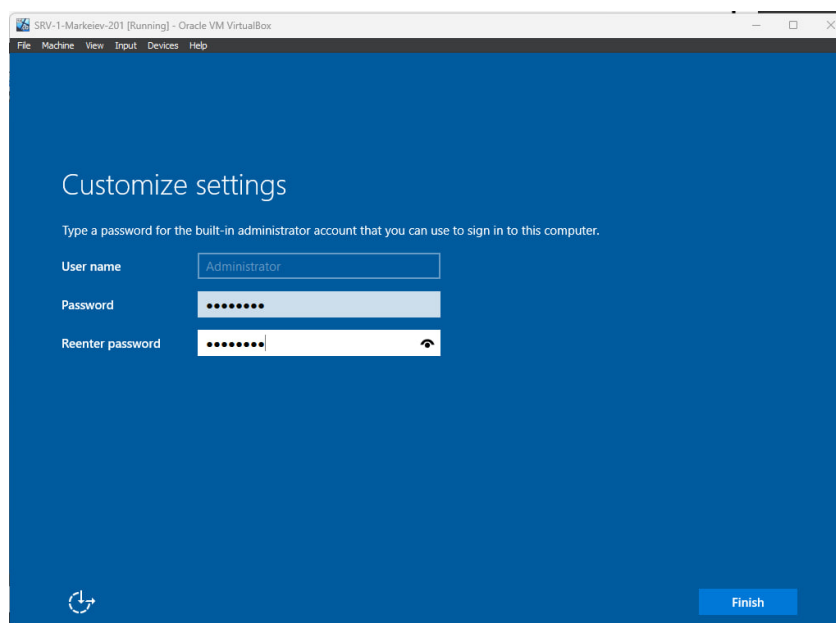


Рис. 3.1.3 - Створення користувача адміністратора

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 32   |

Розгортання контролеру домену, а також налаштування та імплементація усіх потрібних функцій, буде відбуватись автоматизовано за допомогою сценаріїв PowerShell з передвчасно заданими параметрами. Для початку процесу розгортання контролеру від імені адміністратора запускаємо наступний сценарій “FOREST\_INST.ps1”.

Серед передбачених параметрів:

- Назва домену: corpmarkeiev.net
- NetBios: CORPMARKEIEV
- ComputerName: SRV-MRKV
- Встановити DNS: \$true

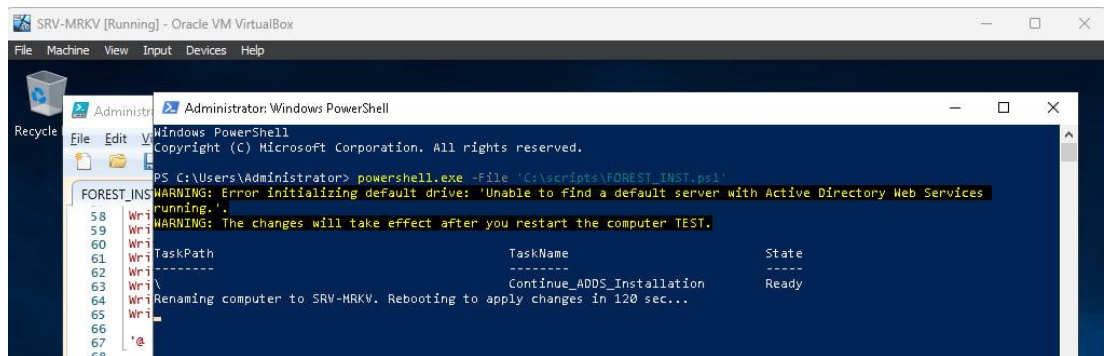


Рис. 3.1.4 - Ініціалізація сценарію “FOREST\_INST.ps1”

Даний сценарій спрацьовує у два етапи:

- у першому змінюється назва контролера домена на завчасно вказану у тілі сценарію, створюється та зберігається ще один сценарій “FOREST\_INST\_Continue.ps1”, створюється задача у Task Scheduler для його запуску одразу після перезавантаження.
- У другому продовжується налаштування контролера домену як головного контролера домену і виводяться всі вчинені зміни, після чого очікується перезавантаження для збереження змін.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 33   |

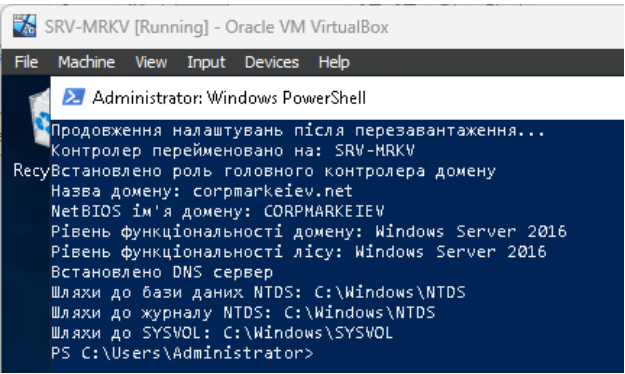


Рис. 3.1.5 - Закінчення роботи скрипта

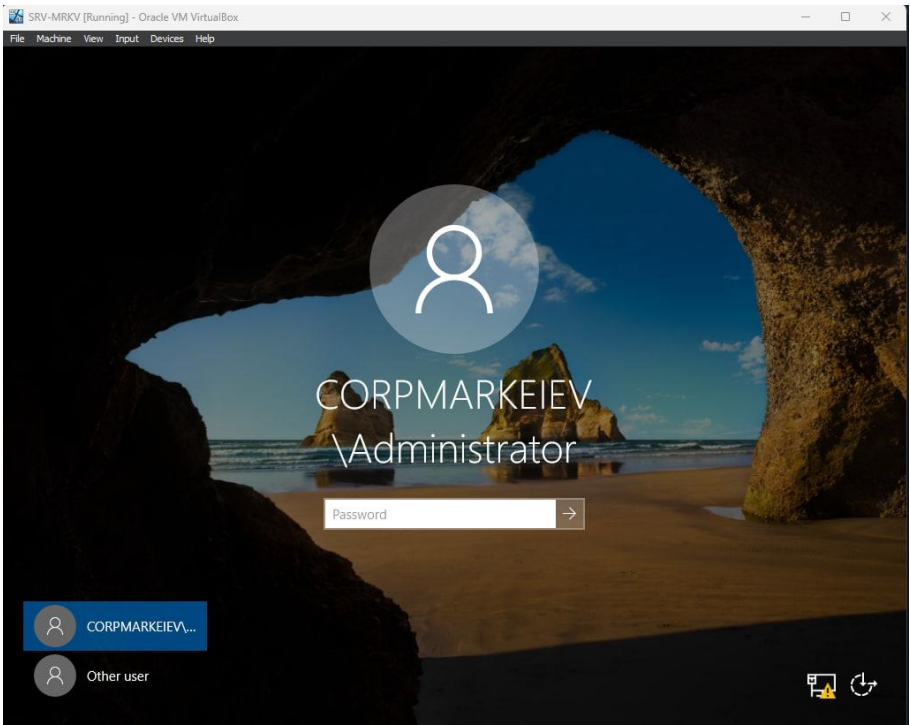


Рис. 3.1.6 - Вхід вже як локального адміністратора домену

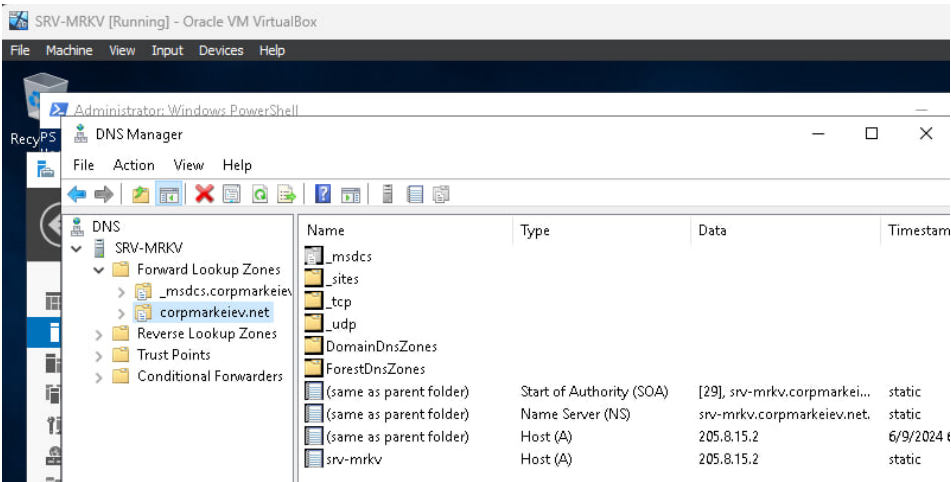


Рис. 3.1.7 - Створені та налаштовані функції DNS сервера

Наступним етапом буде налагодження статичної IP-конфігурації контролера з встановленням модуля DHCP і виконання відповідних для його роботи налаштувань.

```

Administrator: Windows PowerShell
PS C:\Users\Administrator> powershell.exe -File "C:\script\DHCP_IP.ps1"
Налаштування IP-конфігурації контролера та встановлення модуля DHCP з подальшими налаштуваннями

Success Restart Needed Exit Code      Feature Result
-----
True      No      NoChangeNeeded {}
True      No      NoChangeNeeded {}

IP Configuration:

ComputerName           : SRV-MRKV
InterfaceAlias          : Ethernet
InterfaceIndex          : 3
InterfaceDescription    : Intel(R) PRO/1000 MT Desktop Adapter
ComponentId             : 1
NetAdapter              : MSFT_NetAdapter (CreationClassName = "MSFT_NetAdapter", DeviceID =
                        : "{1B631FEC-7A21-4E35-A010-071AC2EBC62E}", SystemCreationClassName = "CIM_NetworkPort",
                        : SystemName = "SRV-MRKV.corpmarkeiev.net")
NetCompartment          : MSFT_NetCompartment (InstanceID = "{557955}"; CreationClassName = "", SystemCreationClassName = "",
NetIPv6Interface        : MSFT_NetIPv6Interface (Name = "{557955}"; CreationClassName = "", SystemCreationClassName = "",
NetIPv4Interface        : MSFT_NetIPv4Interface (Name = "{557955}"; CreationClassName = "", SystemCreationClassName = "",
NetProfile               : MSFT_NetConnectionProfile (InstanceID = "{1B631FEC-7A21-4E35-A010-071AC2EBC62E}")
AllIPAddresses           : {205.8.15.2, fe80::91b6:a837:bf19:354%3}
IPv6Address              : {}
IPv6TemporaryAddress     : {}
IPv6LinkLocalAddress     : {fe80::91b6:a837:bf19:354%3}
IPv4Address              : {205.8.15.2}
IPv6DefaultGateway       :
IPv4DefaultGateway       :
DNSServer                : {MSFT_DNSClientServerAddress (Name = "3", CreationClassName = "", SystemCreationClassName = "",
                        : SystemName = "23"), MSFT_DNSClientServerAddress (Name = "3", CreationClassName = "",
                        : SystemCreationClassName = "", SystemName = "2")}
Detailed                : False
  
```

Рис. 3.1.8 - Ініціалізація скрипта “DHCP\_IP.ps1”

По закінченню роботи скрипта, отримуємо повідомлення про успішне налаштування DHCP scope з виведенням встановлених параметрів, серед яких:

- Проміжок адрес DHCP: 205.8.15.0 - 205.8.15.254
- Пул адрес для виключення: 205.8.15.1 - 205.8.15.7
- Адреса DHCP сервера та одночасно контролера домену
- Маска підмережі

```

Exclusion range successfully added to the DHCP scope.
Configured DHCP Scope Parameters:
Scope Name: MainScope
Scope ID: 205.8.15.0
Start Range: 205.8.15.8
End Range: 205.8.15.254
Subnet Mask: 255.255.255.0
DNS Server: 205.8.15.2
DNS Domain: corpmarkeiev.net
Router (Gateway): 205.8.15.1
Exclusion Range 1: 205.8.15.1 - 205.8.15.7
  
```

Рис. 3.1.9 - Результат роботи скрипта “DHCP\_IP.ps1”

Після закінчення роботи скрипта, перевіряємо дійсність виконаних налаштувань всередині Server Manager, а також переглядаємо IP-конфігурацію мережевого адаптера контролера домену.

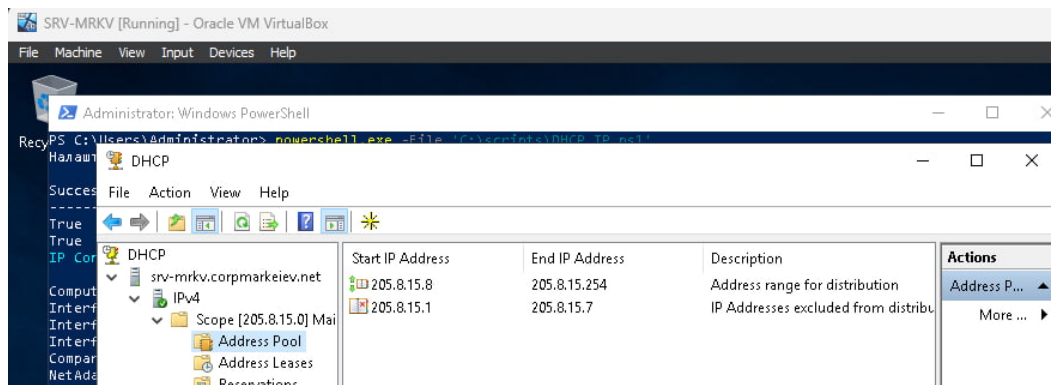


Рис. 3.1.10 - Успішно створений DHCP Scope

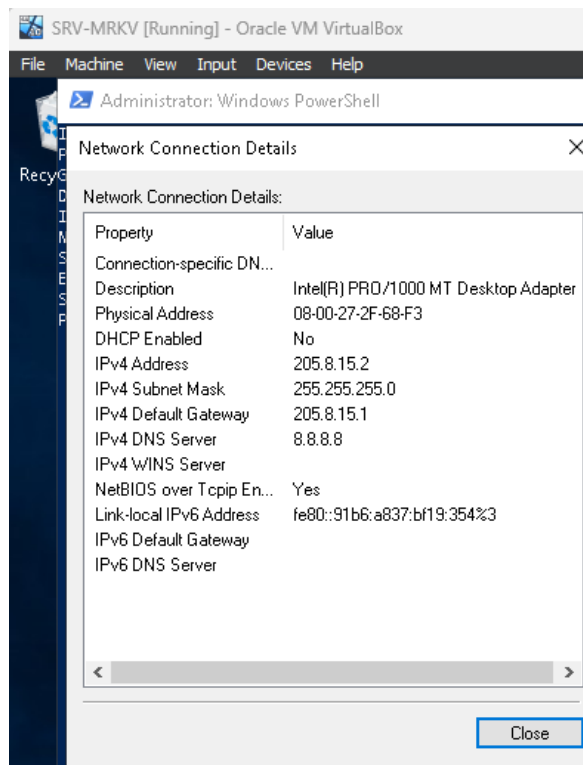


Рис. 3.1.11 - Конфігурація мережевого адаптера

Як ми бачимо на поданих рисунках, скрипт вірно налаштував DHCP для автоматичного розподілення адрес між робочими станціями домену, а також змінив конфігурацію мережевого адаптера контролера домену. На цьому етапі завершується налаштування ролей серверу та мінімально необхідних служб потрібних для подальшого створення користувачів і розподілу їх по організаційним одиницям задля встановлення додаткових налаштувань.

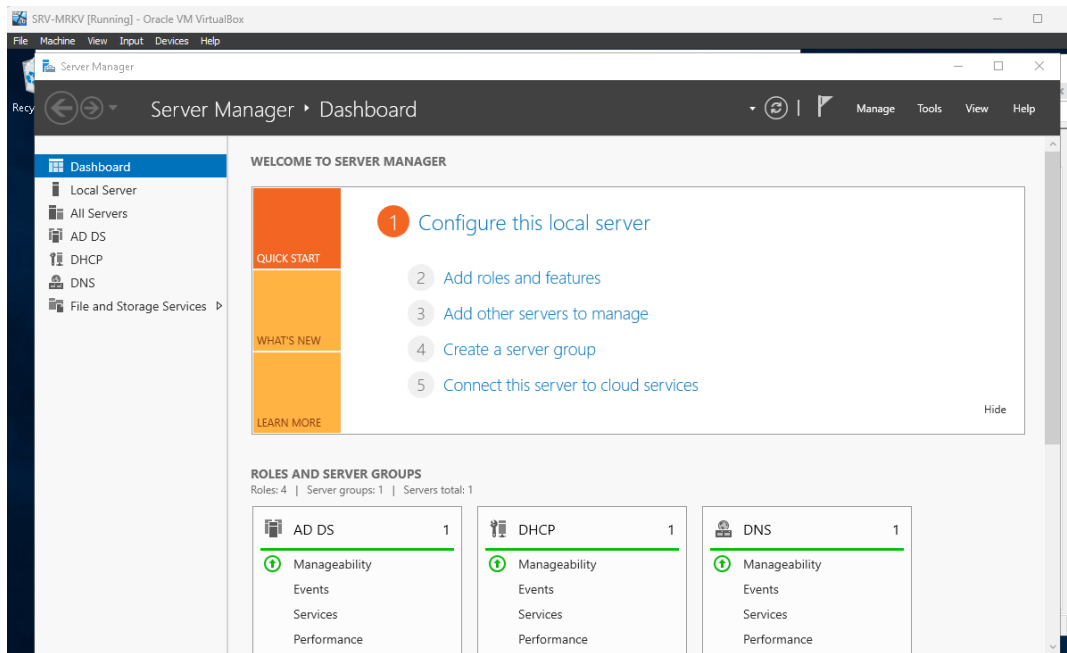


Рис. 3.1.12 - Відображення встановлених служб всередині Server Manager

Для перевірки роботи автоматизованих сценаріїв вручну додамо робочу станцію, за допомогою якої перевіримо можливість приєднання до домену, роботу DHCP сервера, а також авторизації під обліковим записом користувача одного з відділів.

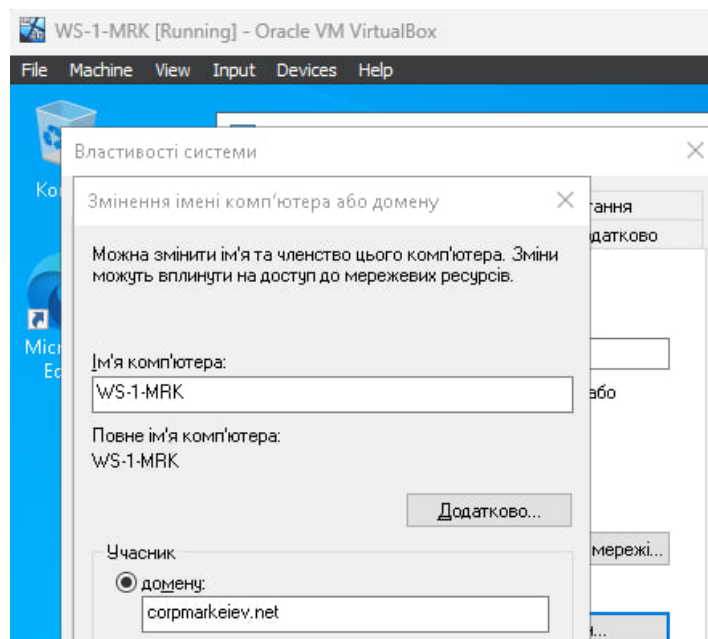


Рис. 3.1.13 - Додавання робочої станції до домену

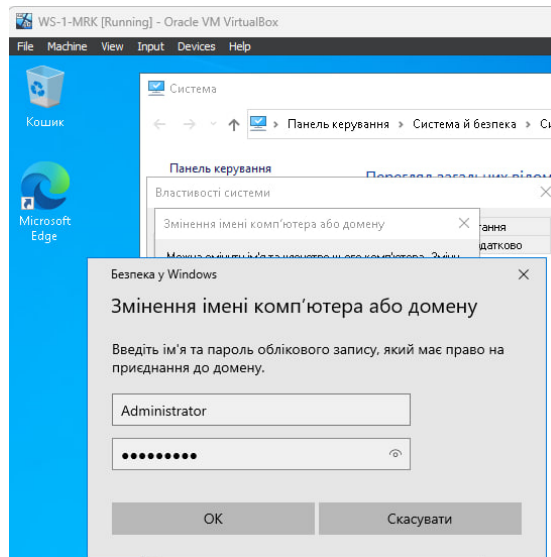


Рис. 3.1.14 - Авторизація під обліковим записом локального адміністратора

Далі переходимо до побудови і налаштування структури домену, для цього ініціалізуємо скрипт “OU\_GRP.ps1” котрий створює організаційні одиниці та групи для майбутніх користувачів всередині домену, відповідно до тих, котрі були зазначені у попередньому розділі. Варто зазначити, що серед OU потрібних для розміщення користувачів, також будуть створені OU котрі міститимуть в собі робочі станції домену відокремлені одна від одної, відповідно до відділів котрій належить, а також OU Company groups, котра міститиме групи користувачів для зручнішої навігації всередині структури домену.[\[23\]](#)

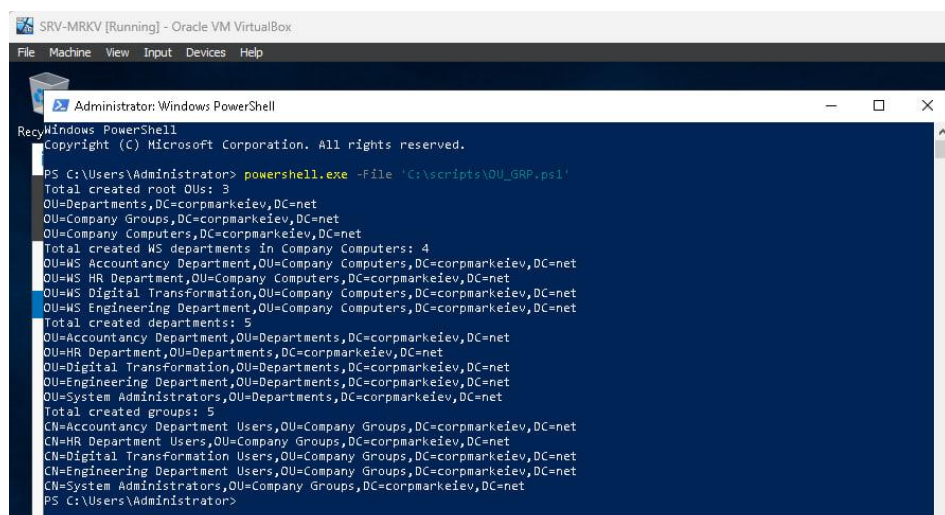


Рис. 3.1.15 - Ініціалізація скрипта OU\_GRP.ps1

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 38   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

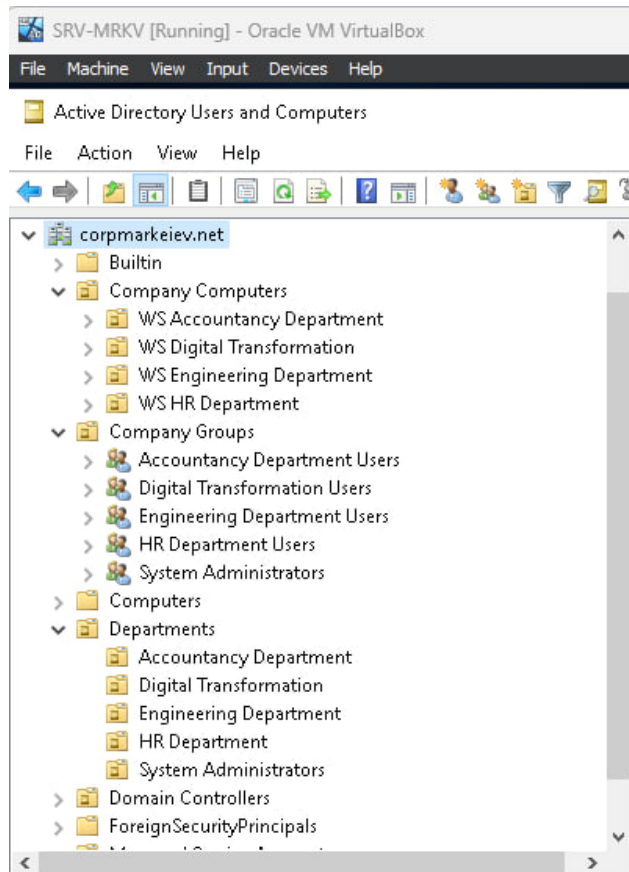


Рис. 3.1.16 - Створені OU та групи користувачів

Згідно ієрархії користувачів домену у підприємства є список співробітників, їх посад та відділів котрим вони належать. Даний список потрібно імпортувати у файл CSV та після чого його можна буде застосувати при ініціалізації відповідного сценарію. Таким чином будуть занесені дані про користувачів домену та групи, до яких вони належатимуть.

Спираючись на структуру підприємства та відділи, в яких працюють співробітники, автоматизований сценарій USERS.ps1 додасть до домену: 10 співробітників, і створить 6 відділів. Серед даних користувачів, присутні також одноразові паролі, котрі будуть змінені під час першого входу в систему, тому ризики виникнення загроз безпеці суттєво зменшуються. Дані про користувачів можна побачити у ДОДАТКУ В серед лістингу скриптів.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 39   |

```

PS C:\Users\Administrator> powershell.exe -File 'C:\scripts\USERS.ps1'
Total added users: 10

-----
Firstname Lastname Username Department Group OU
-----
John Doe John.Doe Accountancy Department Accountancy Department Users OU=Accountancy Department,OU=...
Jane Smith Jane.Smith Accountancy Department Users OU=Accountancy Department,OU=...
Michael Thompson Michael.Thompson HR Department HR Department Users OU=HR Department,OU=Departme...
Sara Brown Sara.Brown HR Department HR Department Users OU=HR Department,OU=Departme...
Alex Davis Alex.Davis Digital Transformation Digital Transformation Users OU=Digital Transformation,OU=...
Anna Klein Anna.Klein Digital Transformation Digital Transformation Users OU=Digital Transformation,OU=...
Tom Parker Tom.Parker Engineering Department Engineering Department Users OU=Engineering Department,OU=...
Emma Peterson Emma.Peterson Engineering Department Users OU=Engineering Department,OU=...
Chris Morris Chris.Morris System Administrators System Administrators OU=System Administrators,OU=...
Olivia Nelson Olivia.Nelson System Administrators System Administrators OU=System Administrators,OU=...

User distribution by OU:
-----
Name Value
-----
OU=Accountancy Department,OU=Departments,DC=corpmarkeiev,DC=net 2
OU=Digital Transformation,OU=Departments,DC=corpmarkeiev,DC=net 2
OU=Engineering Department,OU=Departments,DC=corpmarkeiev,DC=net 2
OU=HR Department,OU=Departments,DC=corpmarkeiev,DC=net 2
OU=System Administrators,OU=Departments,DC=corpmarkeiev,DC=net 2

User distribution by Groups:
-----
Name Value
-----
Accountancy Department Users 2
Digital Transformation Users 2
Engineering Department Users 2
HR Department Users 2
System Administrators 2

```

Рис. 3.1.17 - Ініціалізація скрипта USERS.ps1

Після того як скрипт завершив роботу перевіримо наявність створених користувачів у відповідних OU всередині домену.

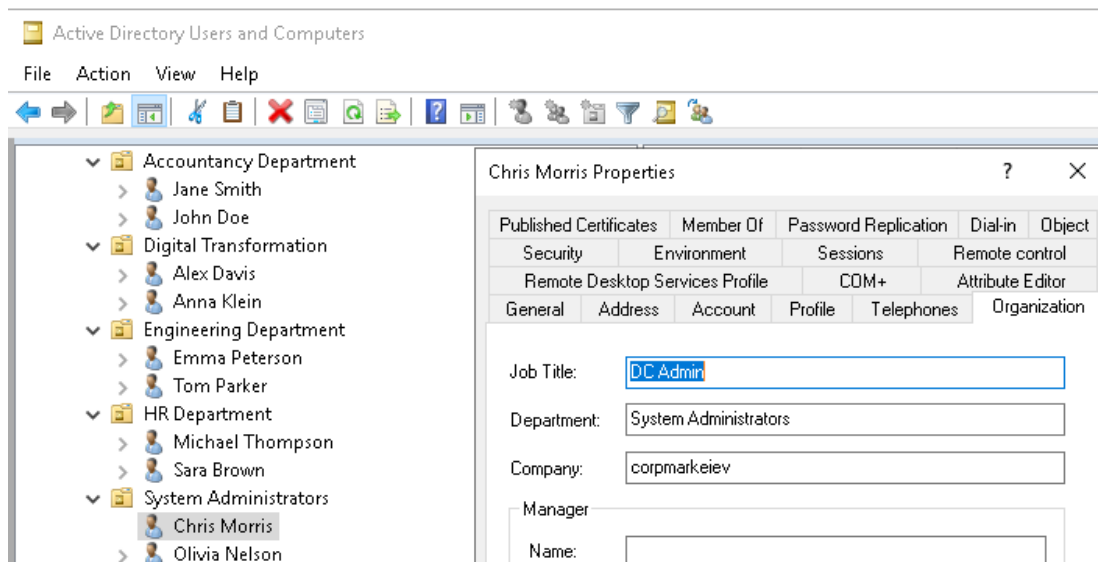


Рис. 3.1.18 - Перелік користувачів розподілених по відділам котрим вони належать

Після цього виконаємо спробу авторизуватись на одній з робочих станцій мережі, котру було підключено раніше.

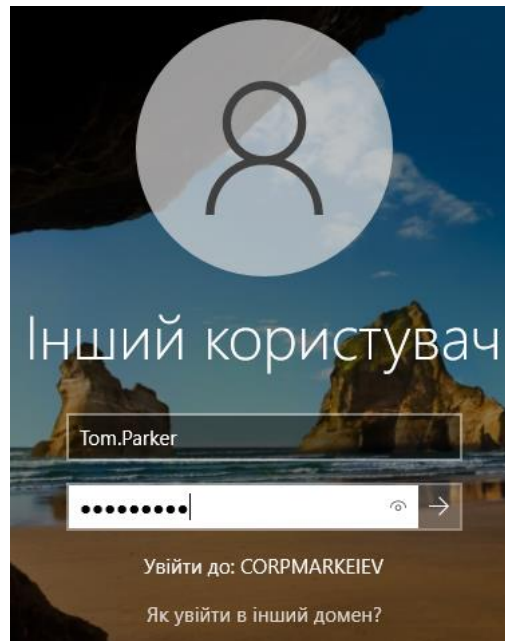


Рис. 3.1.19 - Авторизація під користувачем відділу Engineering Department

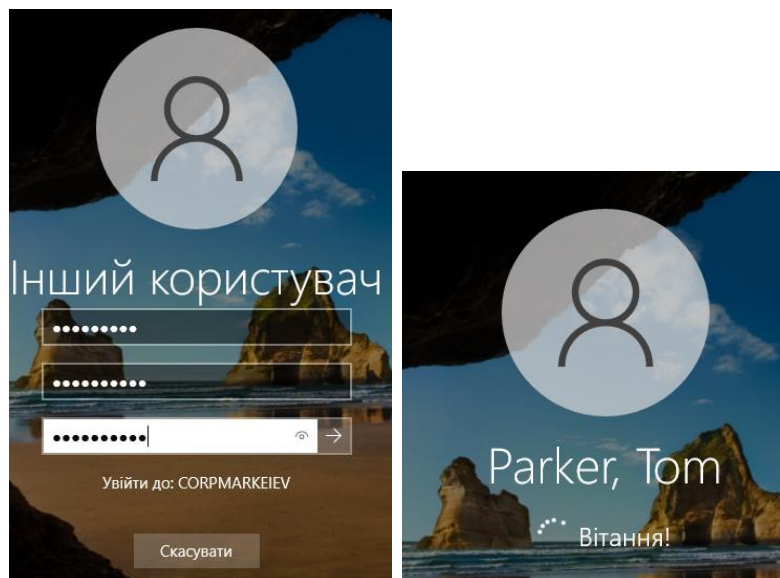


Рис. 3.1.20 - Вимога змінити пароль під час першого входу та успішний вхід

Після успішного приєднання робочої станції та подальшого входу під обліковим записом одного з користувачів відділів перевіряємо якість роботи DHCP сервера

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 41   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

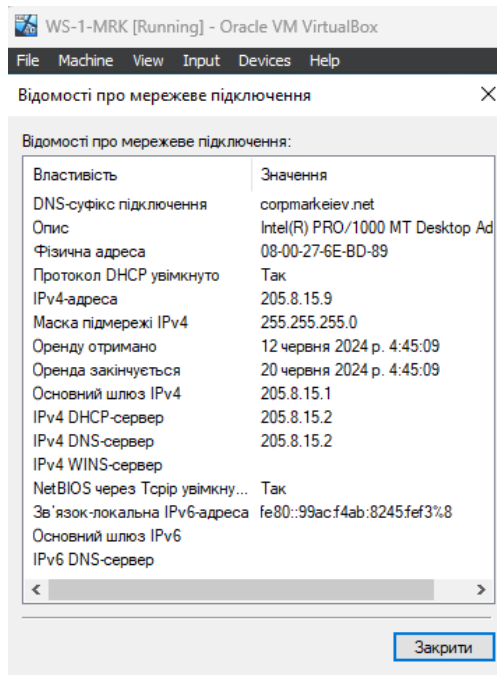


Рис. 3.1.21 - Успішне отримання конфігурацій робочою станцією

### 3.2 Налаштування групових політик

З міркувань безпеки головними завданнями буде забезпечення доступу користувачам до комп'ютерів лише свого відділу, обмежений доступ до функцій операційної системи, налаштування політик паролів та блокування облікових записів. Також будуть налаштовані моніторингові системи та резервне копіювання даних. Для досягнення цих цілей будуть налаштовані GPO відповідно для кожної OU робочих станцій відділів, а також безпосередніх відділів.

Почнемо з розмежування доступу до робочих станцій домену. Як було зазначено раніше – політики дозволятимуть вхід лише вказаним користувачам або групам, унеможливлючи несанкціонований вхід.

Варто зазначити, що у адміністраторів домену будуть особливі повноваження, а саме користувач Chris Morris матиме роль DC Admin, яка дає змогу локального входу на доменному контролері. Користувач Olivia Nelson в свою чергу має роль System Admin, вона дає змогу авторизуватись на робочих станціях користувачів інших відділів.

Для досягнення цих цілей скористаємось автоматизованим скриптом “LOGIN\_GPO.ps1”, він створює та прив'язує GPO до OU всередині Company

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 42   |

Computers, відповідно до створених відділів. Даний скрипт додає групи користувачів у список дозволених на виконання локального входу разом з обліковими записами, котрі належать групам. Окрім них завжди дозволяється вхід локальному адміністратору домену.

Так як цей скрипт використовує шаблон GPO “Allow log on locally”, то відповідно він звертається до запису у системному реєстрі під назвою назвою “SeInteractiveLogonRight”. Користувачів які не мають доступу до робочих станцій відділу, скрипт додає у список заборонених записів, використовуючи протилежну політику “Deny log on locally”, їй відповідним є запис реєстру “SeDenyInteractiveLogonRight”

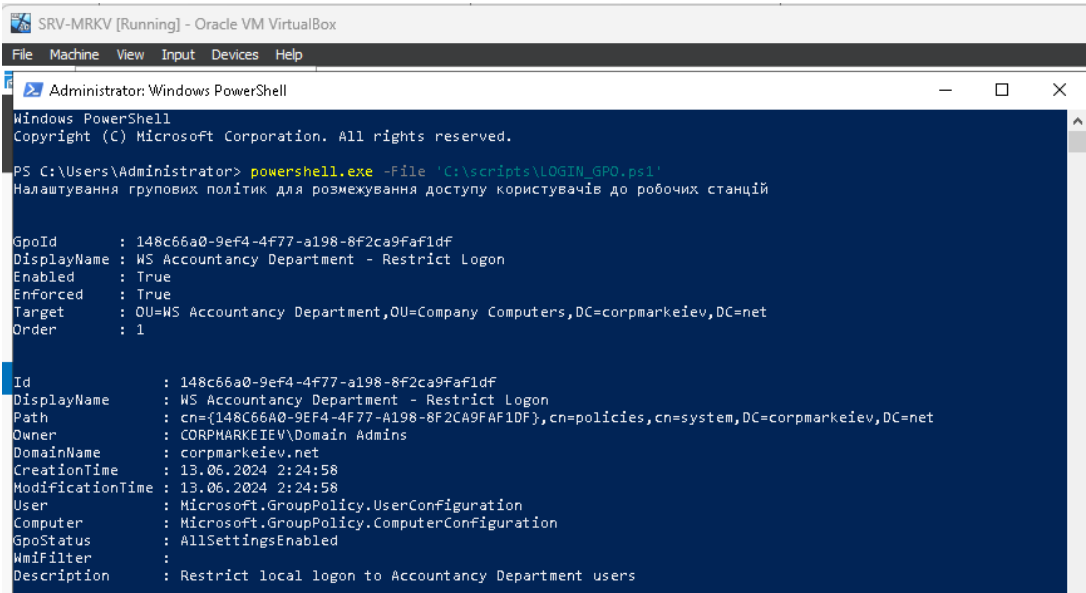


Рис. 3.2.1 - Ініціалізація скрипта LOGIN\_GPO.ps1

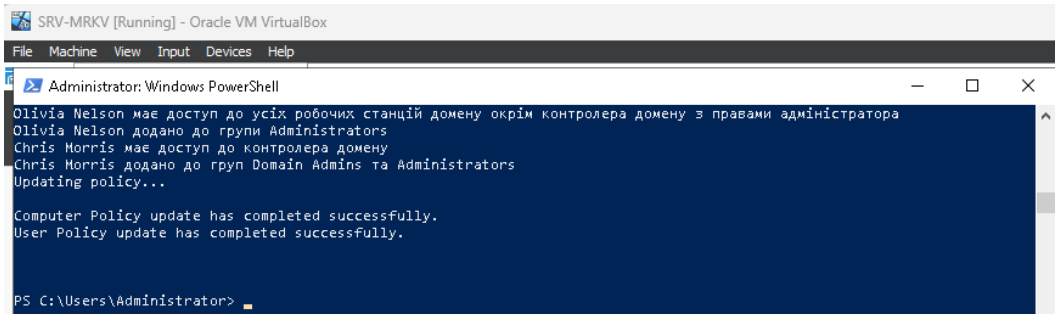


Рис. 3.2.2 - Завершення роботи скрипта

Спробуємо виконати вхід під користувачем відділу Digital Transformation на робочій станції відділу Accountancy

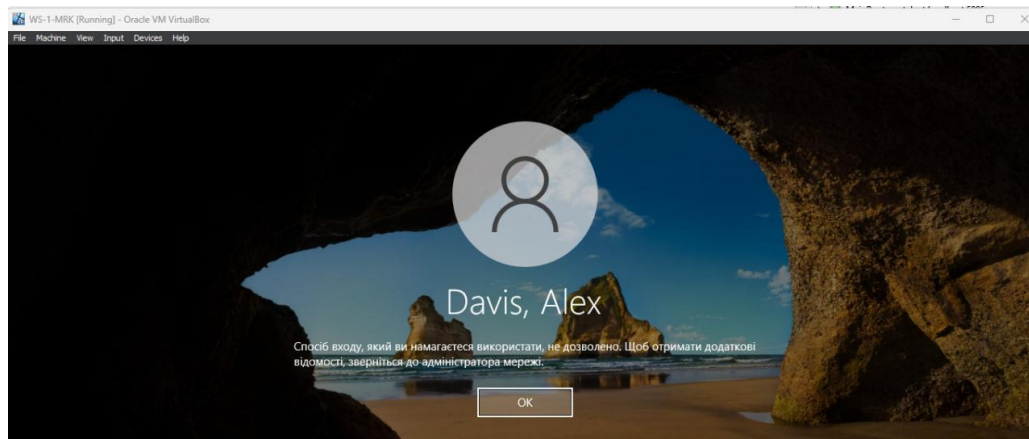


Рис. 3.2.3 - Безуспішна спроба входу під даними користувача невідповідного відділу

Також даний автоматизований сценарій додає користувача Chris Morris до групи Domain Admin та Administrators, що в свою чергу дає можливість входу на доменному контролері. Так як користувач Olivia Nelson має роль System Admin, то вона може авторизуватись на робочих станціях користувачів інших відділів з правами адміністратора.

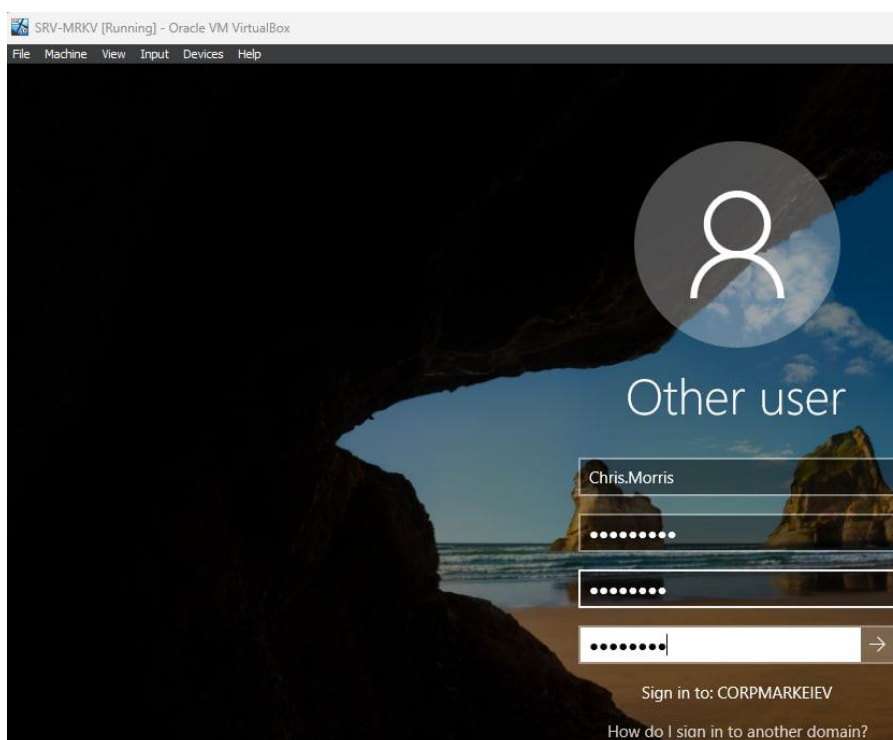


Рис. 3.2.4 - Спроба входу під даними користувача System Admin на контролері домену

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 44   |

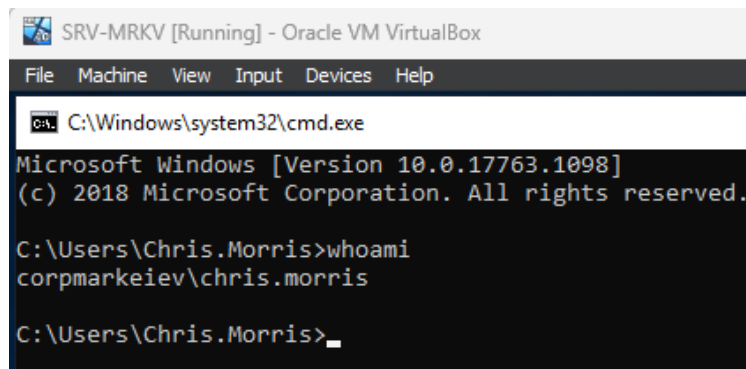


Рис. 3.2.5 – Перевірка на успішність входу в CMD

Тепер налаштуємо політику аудиту, аби слідкувати які зміни відбувались з користувачами у середовищі Server Manager. При спробі змінити пароль, відповідний запис має з'явитись у Event Viewer з описом того коли була здійснена спроба, ким і на якій робочій станції.

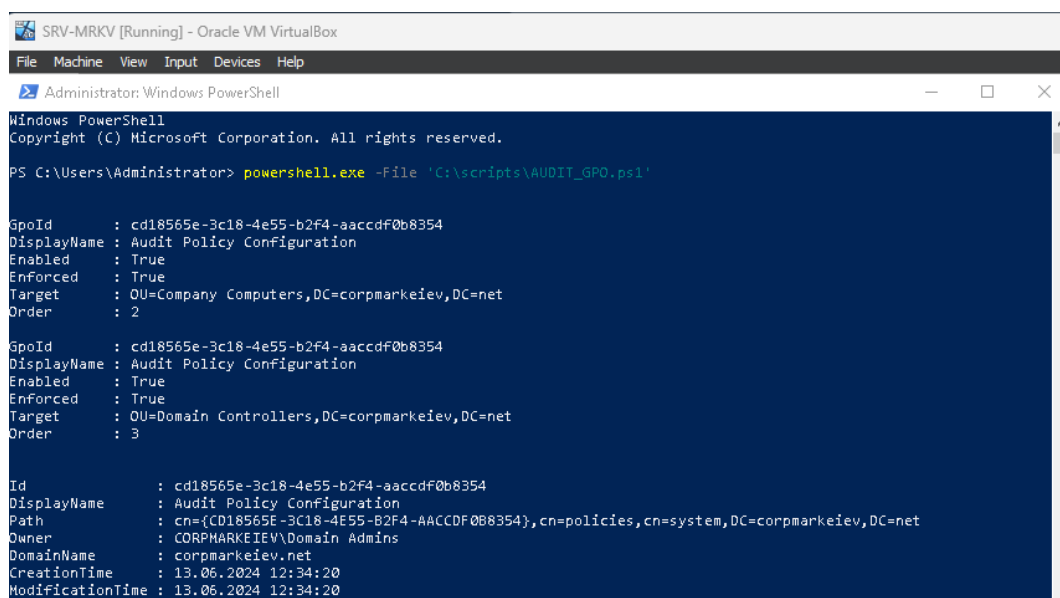


Рис. 3.2.6 - Політики для аудиту дій користувачів, груп та інших подій пов'язаних з авторизацією

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 45   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

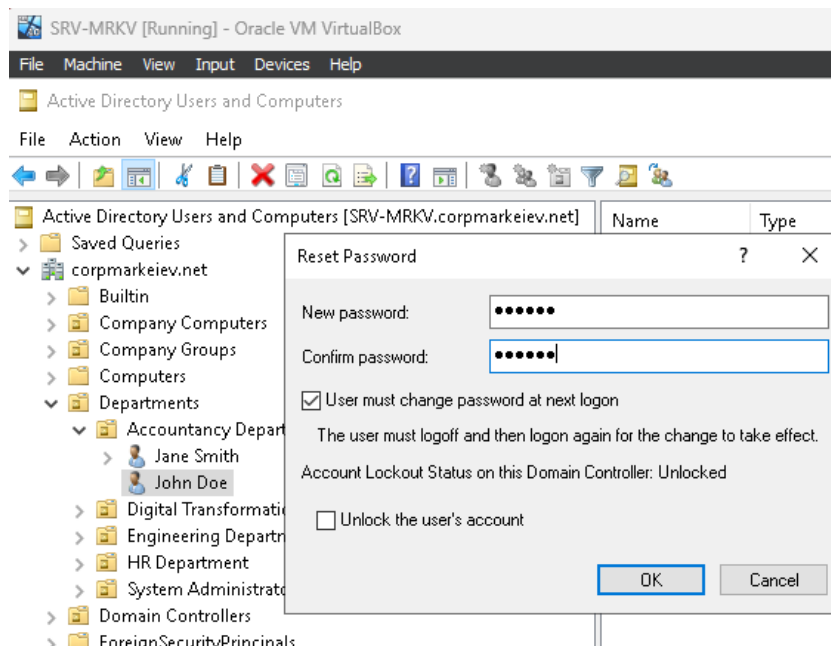


Рис. 3.2.7 - Спроба змінити пароль користувача

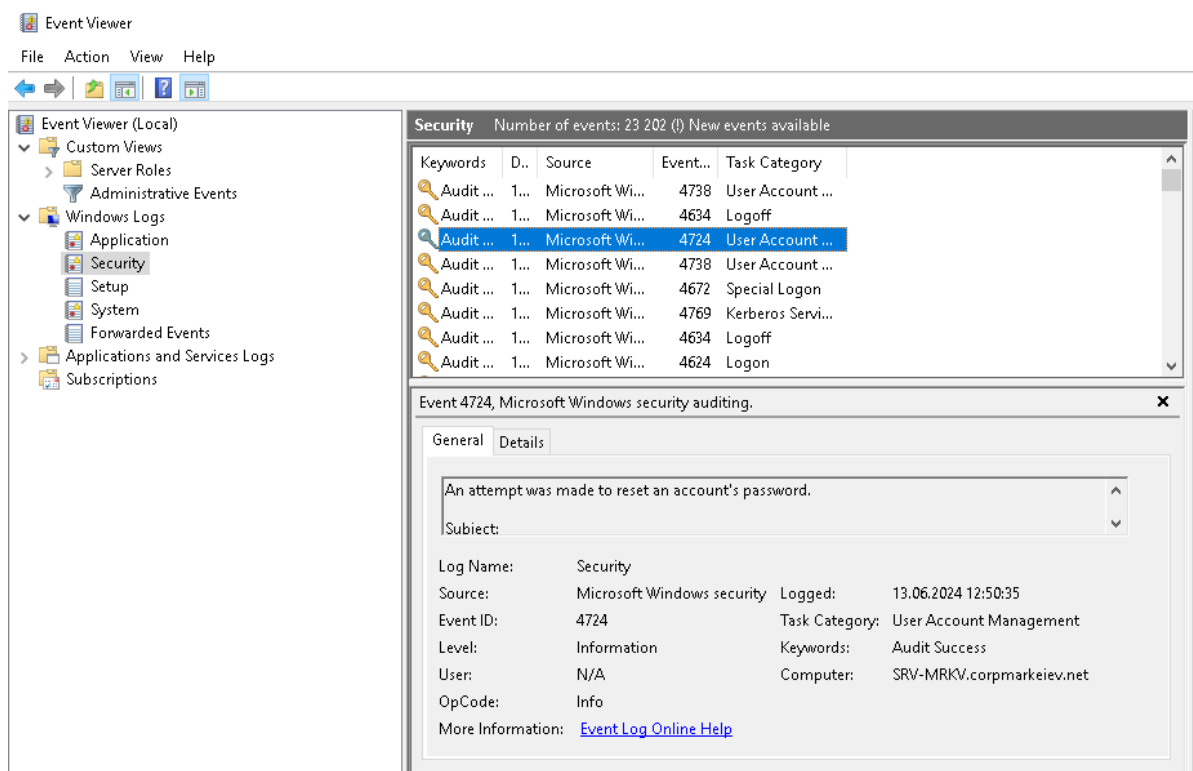


Рис. 3.2.8 - Відображення змін у Журналі подій

Наступним кроком було налаштовано політики паролів та блокування користувачів при неуспішних спробах увійти до системи. Вони відрізнятимуться для користувачів відділів та системних адміністраторів. Це зроблено для забезпечення вищого рівня захисту для користувачів з повноваженнями адміністратора.

Виконуємо ініціалізацію сценарію PASS\_LOCK\_PSO.ps1, для налаштування блокування користувачів і політик паролів відповідно. Були використані саме PSO, через те що вони містять ті самі параметри паролів, що й інші об'єкти GPO. Щоб застосувати різні налаштування до груп користувачів, адміністраторам потрібно створити новий PSO і налаштувати параметри відповідно до вимог. Коли PSO застосовано до користувача, користувач більше не використовує політику паролів, розгорнуту у груповій політиці. Замість цього він використовує вказані параметри PSO. Це в свою чергу дозволяє гнучко налаштовувати параметри авторизації для різних користувачів, без потреби налаштовувати GPO.

```

SRV-MRKV [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Administrator: Windows PowerShell

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

PS C:\Users\Administrator> powershell.exe -File 'C:\scripts\PASS_LOCK_PSO.ps1'
Configuring PSO for users...
Configured PSO for System Administrators:
- Name: PSO for System Administrators
- Precedence: 1
- Password History Count: 24
- Reversible Encryption Enabled: False
- Complexity Enabled: True
- Minimum Password Length: 12
- Minimum Password Age: 1.00:00:00
- Maximum Password Age: 42.00:00:00
- Lockout Threshold: 3
- Lockout Observation Window: 01:00:00
- Lockout Duration: 01:00:00
Configured PSO for Other Users:
- Name: PSO for Other Users
- Precedence: 2
- Password History Count: 12
- Reversible Encryption Enabled: False
- Complexity Enabled: True
- Minimum Password Length: 8
- Minimum Password Age: 1.00:00:00
- Maximum Password Age: 42.00:00:00
- Lockout Threshold: 6
- Lockout Observation Window: 00:10:00
- Lockout Duration: 00:10:00
PSO policies configured successfully and linked to specified groups.
Updating Policies...
Updating policy...

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

PS C:\Users\Administrator>
  
```

Рис. 3.2.9 - Ініціалізація сценарію PASS\_LOCK\_PSO.ps1

Після запровадження політик перевіримо їх безпосередню роботу, спробуємо змінити пароль користувача на менший аніж зазначено в політиці, а саме менше 8 символів. Тимчасовий пароль що був заданий користувачу містить 7 символів (B1234567m), пароль з яким виконується спроба здійснити вхід 6 символів (B123456m).

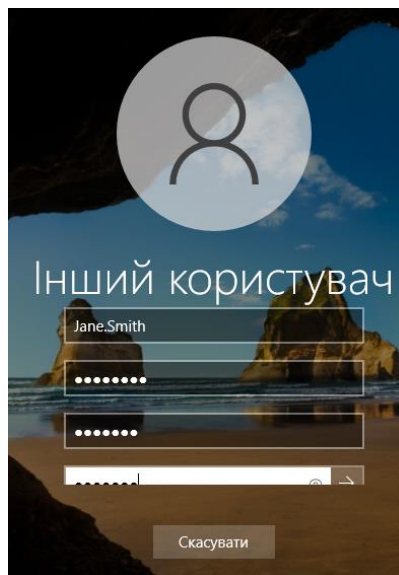


Рис. 3.2.10 - Перевірка роботи політики паролів для користувачів

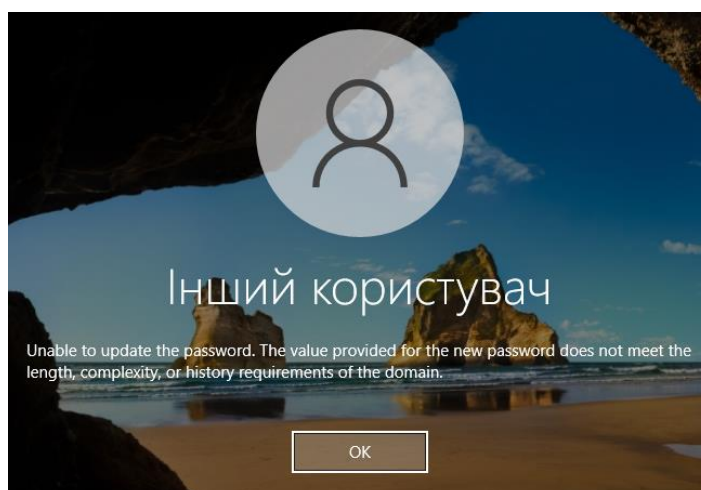


Рис. 3.2.11 - Помилка при невідповідності пароля політиці

Також перевіримо роботу кількості можливих спроб уводити неправильний пароль, для звичайних користувачів ця кількість складає 6 спроб.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 48   |

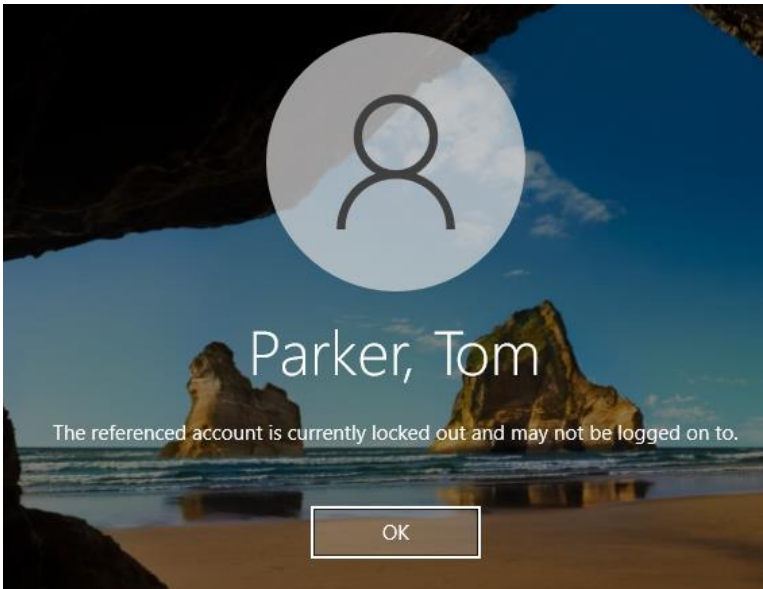


Рис. 3.2.12 - Блокування звичайного користувача при 6 невдалих спробах

Далі налаштуємо групові політики, котрі обмежуватимуть доступ звичайних користувачів до системних інструментів та функцій. Для цього ініціалізуємо скрипт RESTRICT\_GPO.ps1 котрий вимкне вказані функції для користувачів та робочих станцій всередині зазначених OU.

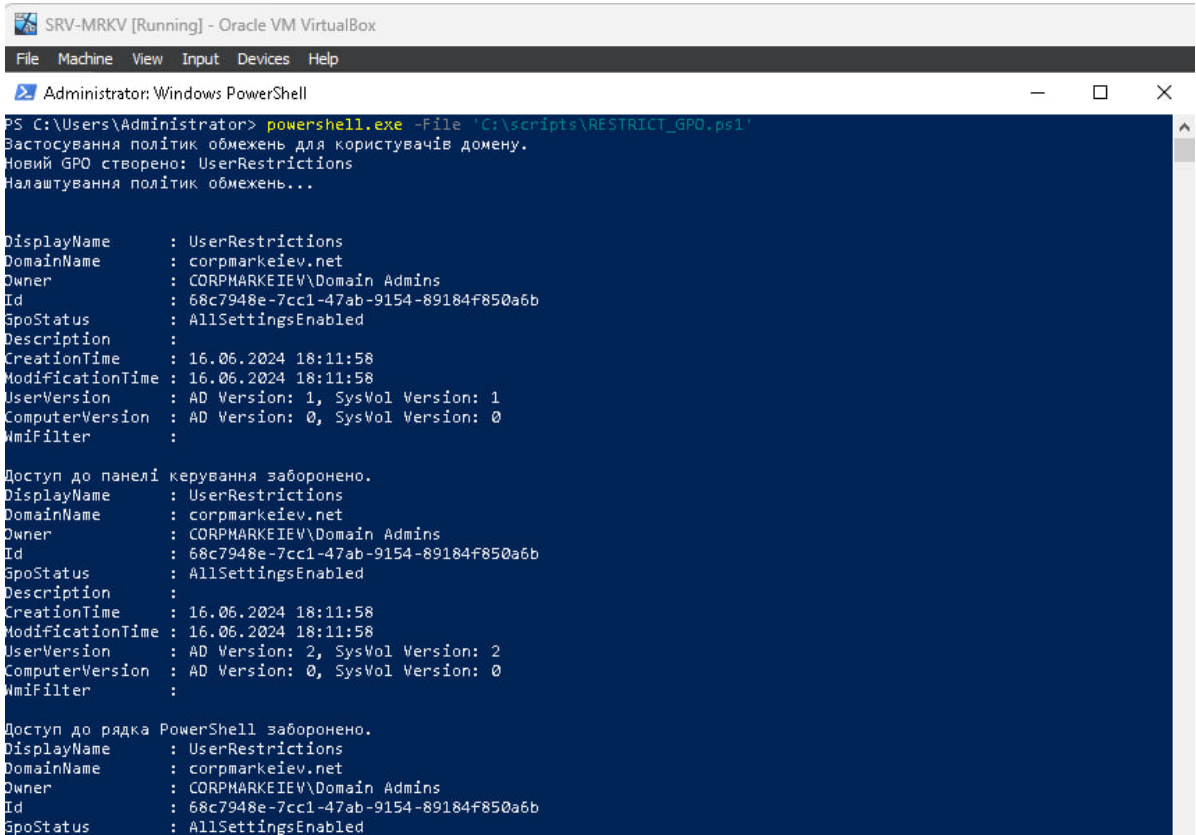


Рис. 3.2.13 – Ініціалізація скрипта RESTRICT\_GPO.ps1

Даний скрипт має прибрати можливість запуску наступних функцій та інструментів:

- Панель керування
- Командний рядок
- Налаштування
- Запуск з'ємних носіїв (USB)
- Встановлення програмного забезпечення
- Реєстр

Але при цьому, всі ці функції будуть доступні для користувачів групи System Administrators, так як на них ці обмеження накладатись не будуть, так само і на робочі станції, які вони використовують.

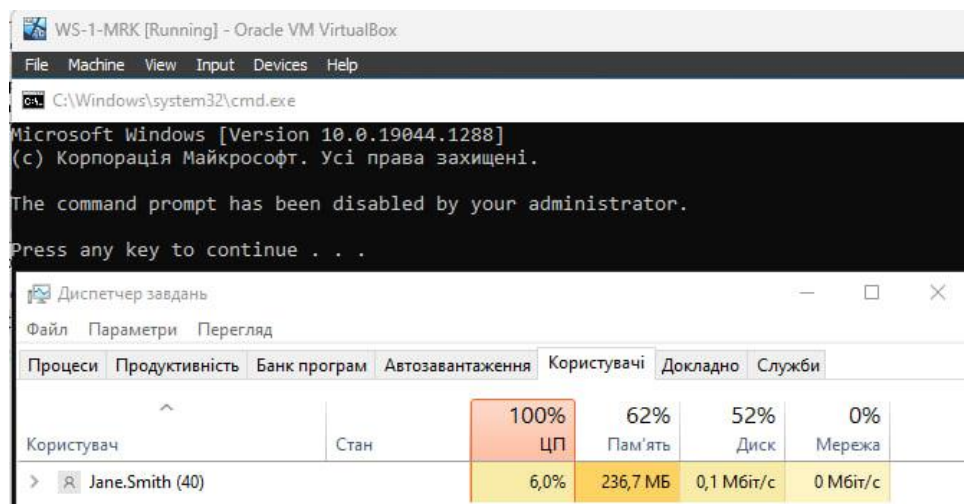


Рис. 3.2.14 – Заборона використання командного рядка звичайному користувачеві

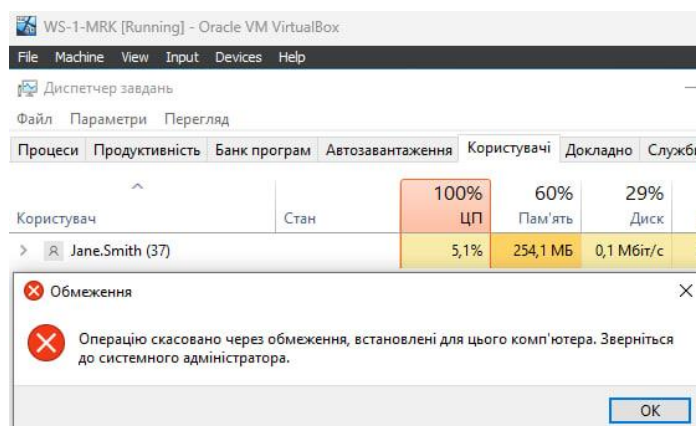


Рис. 3.2.15 – Заборона використання панелі керування звичайному користувачеві

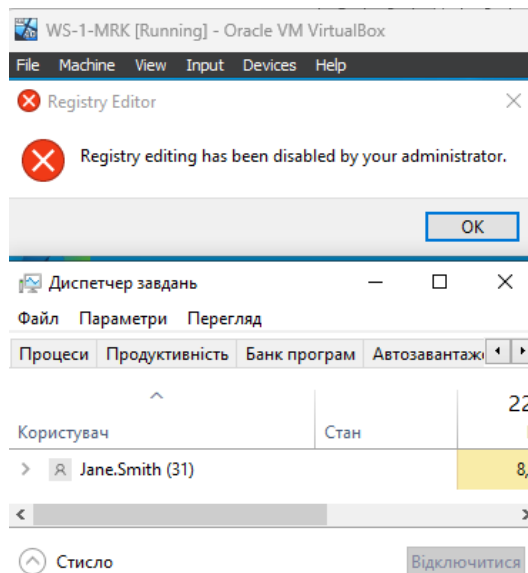


Рис. 3.2.16– Заборона використання реєстру звичайному користувачеві

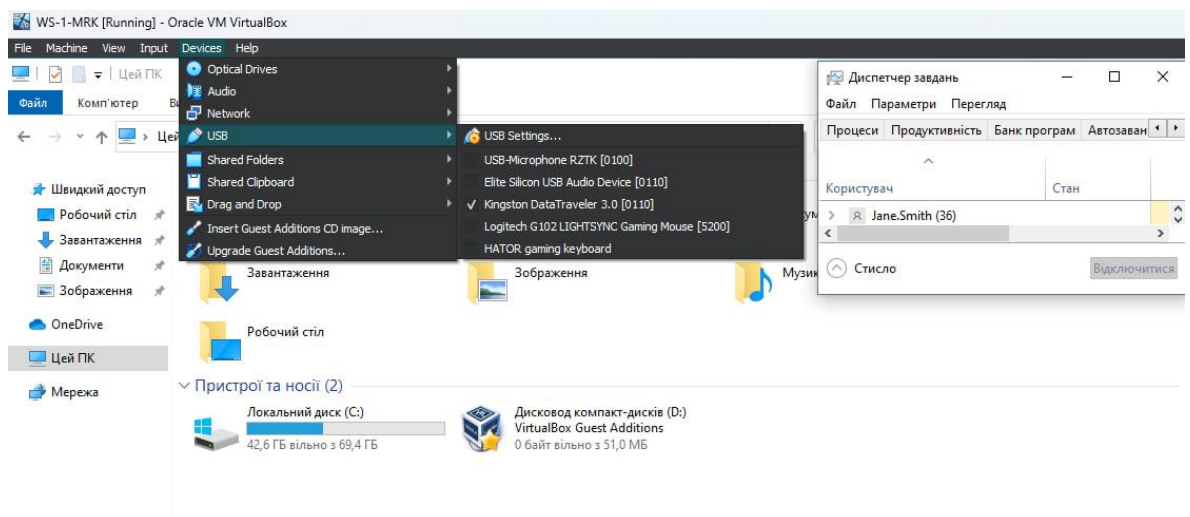


Рис. 3.2.17 – Заборона запуску з’ємних пристроїв (USB) звичайному користувачеві

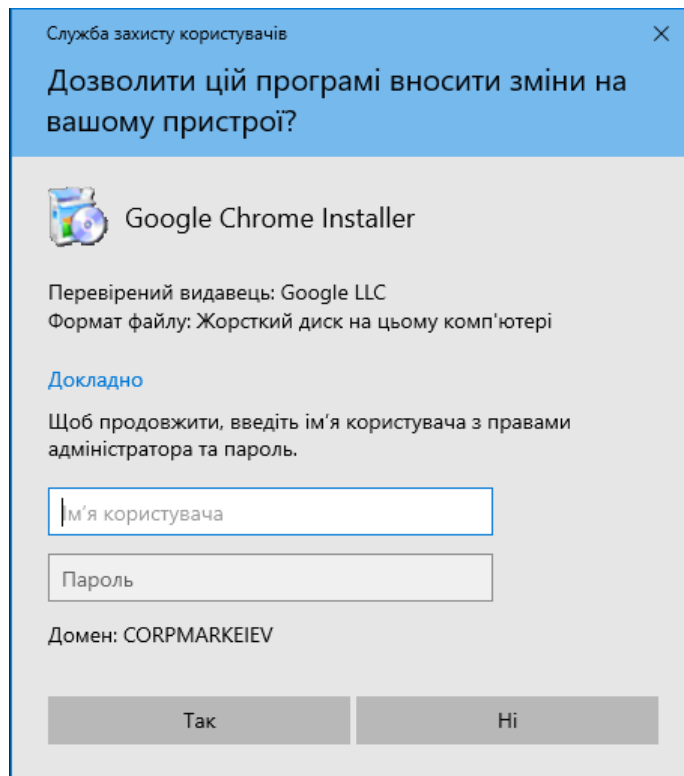


Рис. 3.2.18 – Заборона інсталяції програмного забезпечення звичайному користувачеві

Тепер перевіримо чи доступні ці ж функції при вході на робочій станції адміністратору.

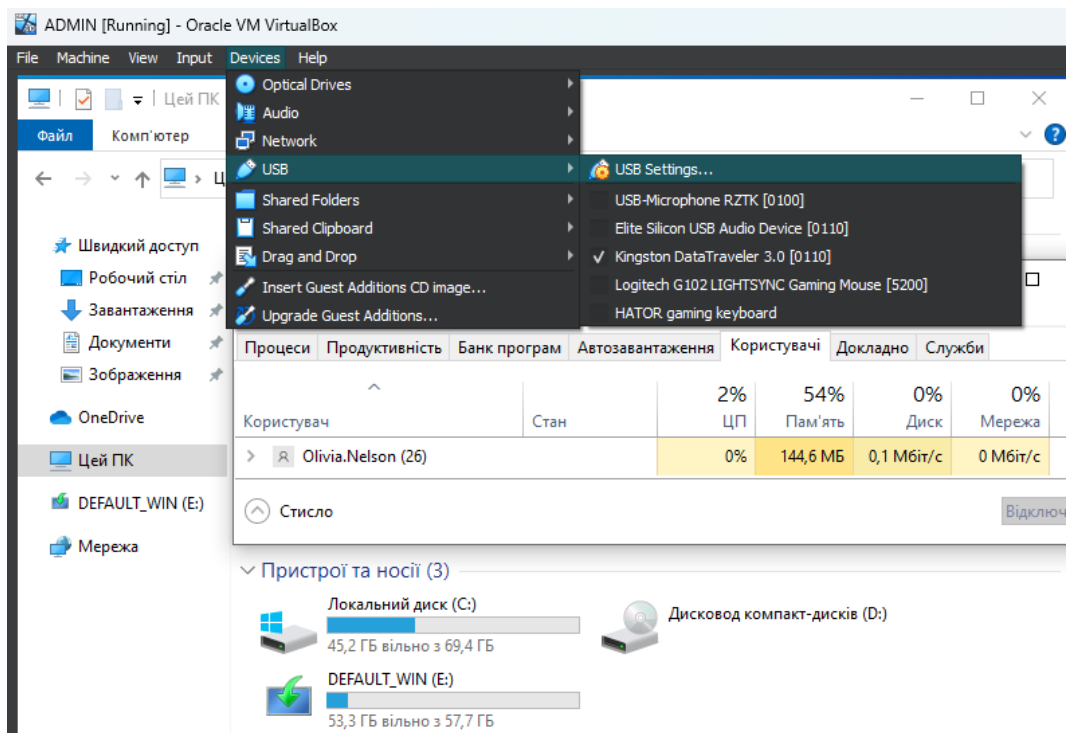


Рис. 3.2.19– Доступний запуск з'ємних пристроїв (USB) адміністратору

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 52   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

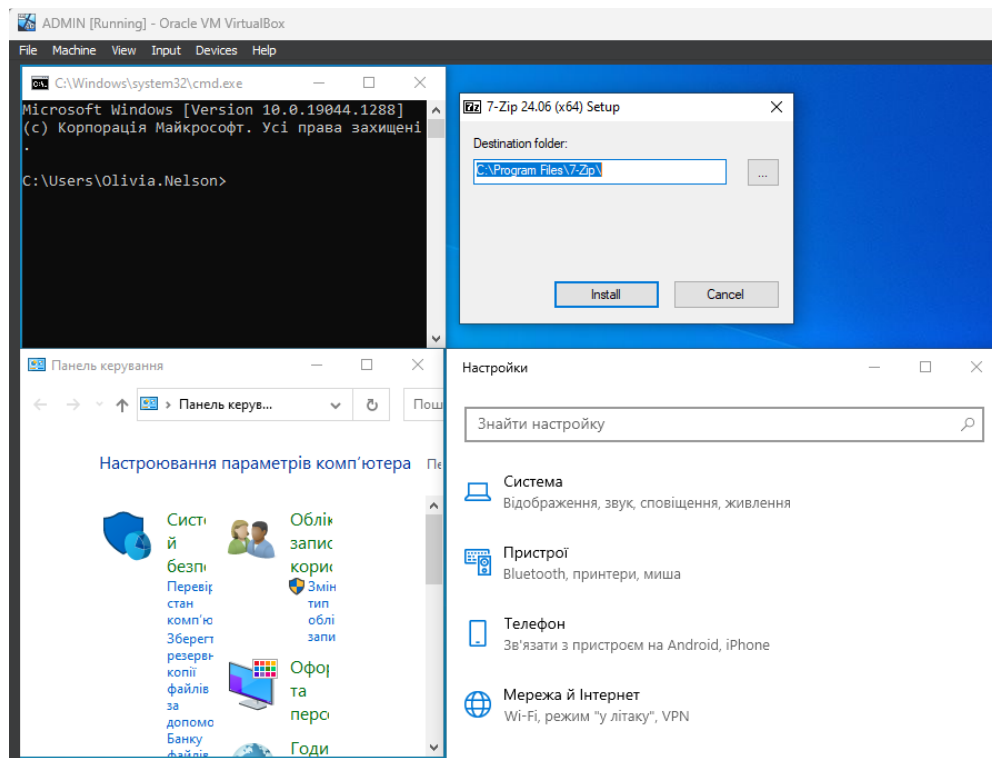


Рис. 3.2.20 – Доступні панель керування, командний рядок, налаштування та встановлення програмного забезпечення адміністратора.

### 3.3 Налаштування мережевих пристроїв

За поставленими вимогами у попередніх розділах, пристрої всередині структури мають мати доступ до глобальної мережі Інтернету, це стає можливим за використання NAT Overflow на головному маршрутизаторі. Загальну схему мережі в середовищі GNS3 можна переглянути у Додатку Б.

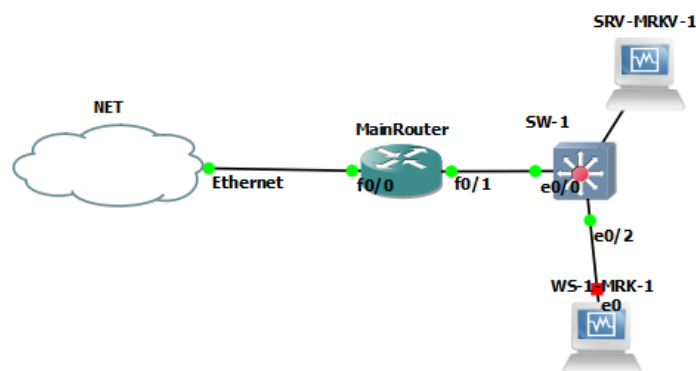


Рис. 3.3.1 - Схема підключення маршрутизатора до мережі Інтернет у програмному емуляторі GNS3

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 53   |

Для реалізації достатньо використати 1 маршрутизатор, два інтерфейси якого будуть налаштовані на отримання IP-адреси наданої провайдером за допомогою DHCP та зв'язок з пристроями домену відповідно.

```

MainRouter
*Mar 1 00:00:03.151: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar 1 00:00:03.215: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*Mar 1 00:00:04.151: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to down
*Mar 1 00:00:04.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
MainRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainRouter(config)#int f0/0
MainRouter(config-if)#ip address dhcp
MainRouter(config-if)#no sh
MainRouter(config-if)#exi
*Mar 1 00:05:49.335: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:05:50.335: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
MainRouter(config-if)#exi
MainRouter(config)#
*Mar 1 00:06:01.383: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned
DHCP address 192.168.0.102, mask 255.255.255.0, hostname MainRouter
MainRouter(config)#
  
```

Рис. 3.3.2 - Отримання IP-адреси від провайдера

```

MainRouter
[OK]
MainRouter#
MainRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainRouter(config)#ip domain-lookup
MainRouter(config)#ip name-server 8.8.8.8
MainRouter(config)#exi
MainRouter#int fa
*Mar 1 04:31:46.426: %SYS-5-CONFIG_I: Configured from console by console
MainRouter#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MainRouter(config)#int fa0/0
MainRouter(config-if)#ip nat outside
MainRouter(config-if)#int fa0/1
MainRouter(config-if)#ip nat inside
MainRouter(config-if)#ip nat inside source list 1 int fa0/0 overload

%Dynamic mapping in use, cannot change
MainRouter(config)#access-list 1 permit 205.0.0.0 0.255.255.255
MainRouter(config)#int fa0/1
MainRouter(config-if)#ip addr 205.8.15.1 255.255.255.0
MainRouter(config-if)#no sh
MainRouter(config-if)#exi
MainRouter(config)#
  
```

Рис. 3.3.3 - Налаштування NAT та інтерфейсу для зв'язку з пристроями домену

```

MainRouter
oing a cold start
*Mar 1 00:00:08.215: %LINK-5-CHANGED: Interface NVI0, changed state to administratively down
*Mar 1 00:00:09.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface NVI0, changed state to down
MainRouter#
*Mar 1 00:00:16.295: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 192.168.0.102, mask 255.255.255.0, hostname MainRouter
MainRouter#P7P?
% Unrecognized command
MainRouter#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/25/28 ms
MainRouter#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/24 ms
MainRouter#

```

Рис. 3.3.4 - Перевірка з'єднання з адресою Google

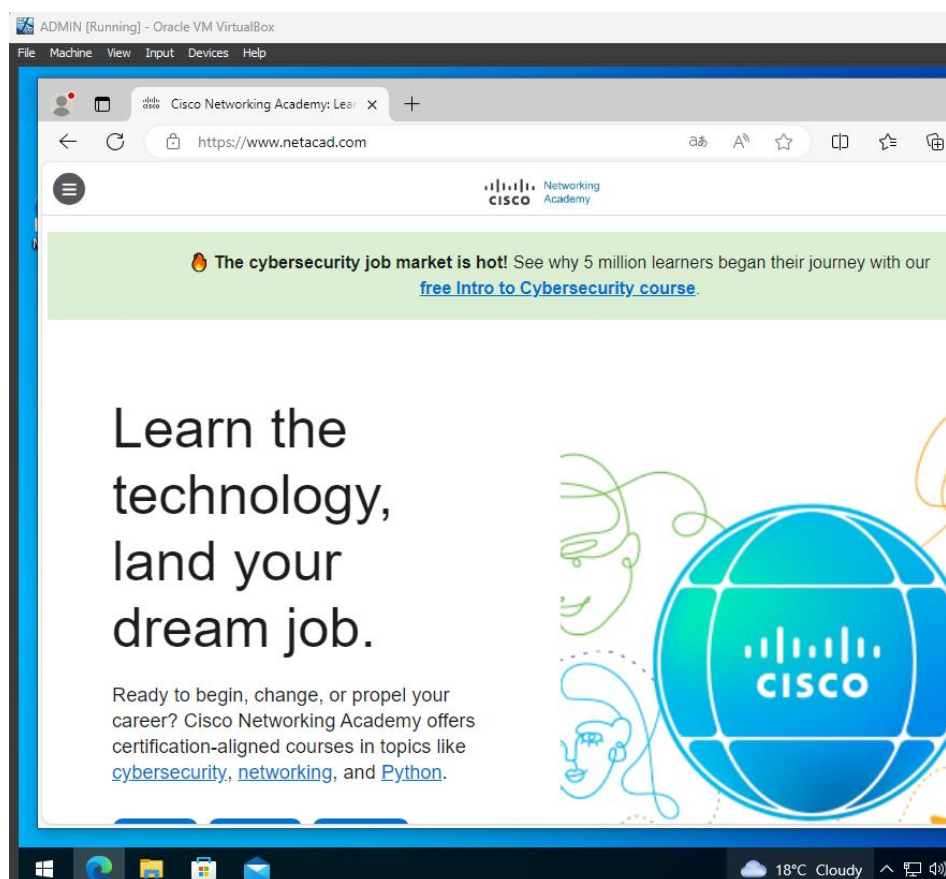


Рис. 3.3.5 - Перевірка наявності доступу до інтернету на робочій станції домену

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 55   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

Далі налаштуємо мережеві параметри на комутаторах домену:

```

IOU1(config)#int vlan 1
IOU1(config-if)#ip addr 205.8.15.
*Jun 16 19:58:04.426: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethe
rnet0/0 (not full duplex), with MainRouter FastEthernet0/1 (full duplex).
IOU1(config-if)#ip addr 205.8.15.4 255.255.255.0
IOU1(config-if)#no sh
IOU1(config-if)#exi
IOU1(config)#ip default-ga
IOU1(config)#ip default-
IOU1(config)#ip default-gateway 205.8.15.1
IOU1(config)#

```

Рис. 3.3.6 – Налаштування IP-конфігурації комутатора SW-1

Наступним кроком налаштуємо захист портів комутаторів, аби унеможливити приєднання невідомих пристроїв до мережі.

```

IOU1(config)#int range e0/1-2, e1/0, e2/0
IOU1(config-if-range)#switchport mode access
IOU1(config-if-range)#switchport port-security
IOU1(config-if-range)#switchport port-security maximum 1
IOU1(config-if-range)#switchport port-security mac-address sticky
IOU1(config-if-range)#ip arp inspection trust
IOU1(config-if-range)#ip dhcp snooping trust
IOU1(config-if-range)#ip dhcp snooping limit rate 256
IOU1(config-if-range)#exi
IOU1(config)#in
*Jun 16 20:07:04.430: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethe
rnet0/0 (not full duplex), with MainRouter FastEthernet0/1 (full duplex).
IOU1(config-if-range)#ip dhcp snooping limit rate 256
IOU1(config-if-range)#exi
IOU1(config)#in
*Jun 16 20:08:04.435: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethe
rnet0/0 (not full duplex), with MainRouter FastEthernet0/1 (full duplex).
IOU1(config)#int range e0/1-2, e1/0, e2/0
IOU1(config-if-range)#spanning
*Jun 16 20:09:04.438: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethe
rnet0/0 (not full duplex), with MainRouter FastEthernet0/1 (full duplex).
IOU1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 4 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
IOU1(config-if-range)#

```

Рис. 3.3.7 – Налаштування Port-security для мережевих пристроїв та робочих станцій на комутаторі SW1

```

SW-1 - PuTTY
IOU1(config)#int range e0/3, e1/1-3, e2/1-3, e3/0-3
IOU1(config-if-range)#switchport mode access
IOU1(config-if-range)#switchport port-security
IOU1(config-if-range)#switchport port-security maximum 3
IOU1(config-if-range)#switchport port-security mac-address sticky
IOU1(config-if-range)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast will be configured in 11 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
IOU1(config-if-range)#s
*Jun 16 20:11:04.435: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on Ethe
rnet0/0 (not full duplex), with MainRouter FastEthernet0/1 (full duplex).
IOU1(config-if-range)#spanning-tree bpduguard enable
IOU1(config-if-range)#switchpor access vlan 1
IOU1(config-if-range)#switchpor access vlan 99
% Access VLAN does not exist. Creating vlan 99
IOU1(config-if-range)#

```

Рис. 3.3.7 – Налаштування Port-security невикористаних портів.

Аналогічні налаштування були проведені на інших комутаторах мережі.

### Висновки до розділу

У третьому розділі було розгорнуто та налаштовано контролер домену за допомогою автоматизованих сценаріїв, також встановлено надбудови для мінімального функціонування домену. За допомогою сценаріїв PowerShell створено структуру домену, усі OU та користувачів у них, налаштовано розмежування доступу, політики паролів та аудит подій на сервері. Також було мінімально налаштовано мережеві пристрої мережі, а також реалізовано доступ до мережі Інтернет всередині програмного емулятора GNS3.

## ВИСНОВКИ

При виконанні випускової кваліфікаційної роботи було проведено аналіз її теми, було розглянуто технології MS Active Directory, засоби автоматизованого керування контролерами домену та їх налаштування. Було вирішено якими засобами можна досягнути виконання роботи, а саме за допомогою використання командлетів оболонки PowerShell та об'єднання їх у скрипти.

Було спроектовано мережу підприємства, котра може забезпечити роботу підприємства, було враховано потребу прорахунку IP-адресації та описано розподіл адрес між пристроями у мережі. Було обрано за допомогою якого протоколу буде здійснюватися присвоєння адрес пристроям домену.

На основі мети кваліфікаційної роботи було поставлено технічне завдання, котре включало в себе перелік рішень, які мають реалізувати автоматизовані сценарії. Було досліджено яким чином мають працювати ці автоматизовані сценарії.

Далі було побудовано мережу підприємства, після чого виконано розгортання контролеру домену за допомогою автоматизованого сценарію, котрий включав в себе встановлення важливих модулів та функцій, для забезпечення повноцінного функціонування домену. Після цього було створено організаційні одиниці та користувачів в них, між якими було розмежовано доступ до певних функцій домену, його ресурсів тощо. Ці рішення включали в себе різницю у повноваженнях серед користувачів, їх можливості в домену, а саме локальний вхід на робочих станціях лише свого відділу, політики паролів в залежності від ролі користувача.

За допомогою скриптів, було налагоджено обмеження для звичайних користувачів до системних функцій та інструментів на робочих станціях такі як: панель керування, налаштування, завантаження та встановлення програмного забезпечення, доступ до командного рядка та рядка PowerShell.

В результаті роботи побудовану мережу підприємства було створено автоматизовані рішення для розгортання контролеру домену та імплементації важливих модулів для його роботи.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 58   |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. MS AD: [Електронний ресурс] / CyberArk – <https://www.cyberark.com/what-is/active-directory/> – Загол. з екрану.
2. What Is Active Directory and How Does It Work? [Електронний ресурс] / Lepide – <https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/> – 24.04.2024. – Загол. з екрану.
3. Kerberos Authentication [Електронний ресурс] / Fortinet. – <https://www.fortinet.com/resources/cyberglossary/kerberos-authentication>
4. NTLM EXPLAINED [Електронний ресурс] / Crowdstrike. – <https://www.crowdstrike.com/cybersecurity-101/ntlm-windows-new-technology-lan-manager/>
5. What is LDAP? [Електронний ресурс] / okta. – <https://www.okta.com/identity-101/what-is-ldap/> – Загол. з екрану
6. AD DS: Fine-Grained Password Policies: [Електронний ресурс] / Microsoft – [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770394(v=ws.10)?redirectedfrom=MSDN) – Загол. з екрану.
7. Ansible: [Електронний ресурс] / Ansible – <https://www.ansible.com/how-ansible-works/> – Загол. з екрану.
8. CHEF: [Електронний ресурс] / Intellipaat – <https://intellipaat.com/blog/what-is-chef/> – Загол. з екрану.
9. MDT: [Електронний ресурс] / SmartDeploy – <https://www.smartdeploy.com/blog/microsoft-deployment-toolkit-pros-cons-of-a-free-tool/> – Загол. з екрану.
- 10.DSC: [Електронний ресурс] / Microsoft – <https://learn.microsoft.com/en-us/powershell/dsc/overview?view=dsc-2.0> – Загол. з екрану.
- 11.Powershell: [Електронний ресурс] / Microsoft – <https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.4>

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 59   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

- 12.Setting up Active Directory via PowerShell: [Електронний ресурс] / Microsoft – <https://www.microsoft.com/en-gb/industry/blog/technetuk/2016/06/08/setting-up-active-directory-via-powershell/> – Загол. з екрану.
- 13.Group Policy Examples: Most Useful GPOs for Security [Електронний ресурс] / ActiveDirectoryPRO – <https://activedirectorypro.com/group-policy-examples-most-useful-gpos-for-security/> – Загол. з екрану.
- 14.Powershell and domain controller: [Електронний ресурс] / Microsoft DevBlogs – <https://devblogs.microsoft.com/scripting/use-powershell-to-deploy-a-new-active-directory-forest/> – Загол. з екрану.
- 15.Network Address Translation (NAT): [Електронний ресурс] / GeeksforGeeks – <https://www.geeksforgeeks.org/network-address-translation-nat/> – Загол. з екрану.
- 16.Connect GNS3 to the Internet [Електронний ресурс] / gns3. - <https://docs.gns3.com/docs/using-gns3/advanced/connect-gns3-internet> - 05.02.2023. – Загол. з екрану
- 17.Port Security [Електронний ресурс] / - <https://study-ccna.com/port-security/> – Загол. з екрану
- 18.DHCP: [Електронний ресурс] / Microsoft – <https://learn.microsoft.com/uk-ua/windows-server/networking/technologies/dhcp/dhcp-top> – Загол. з екрану.
- 19.Ntrights: [Електронний ресурс] / ItProToday – <https://www.itprotoday.com/it-management/ntrights> – Загол. з екрану.
- 20.NTRIGHTS.exe (2003 Resource Kit): [Електронний ресурс] / vs-rennweg – <https://vs-rennweg.ksn.at/allmann/allgemeines/1/scripts%20kommandozeile/An%20A-Z%20Index%20of%20the%20Windows%20CMD%20command%20line/NTrights%20-%20User%20Privileges%20%20Windows%20CMD%20%20SS64.com.html> – Загол. з екрану.
- 21.Group Policy Objects: [Електронний ресурс] / Microsoft – <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects> – Загол. з екрану.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 60   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

22.GPO and Powershell: [Електронний ресурс] / CloudBrothers – <https://cloudbrothers.info/en/manage-group-policies-powershell/> – Загол. з екрану.

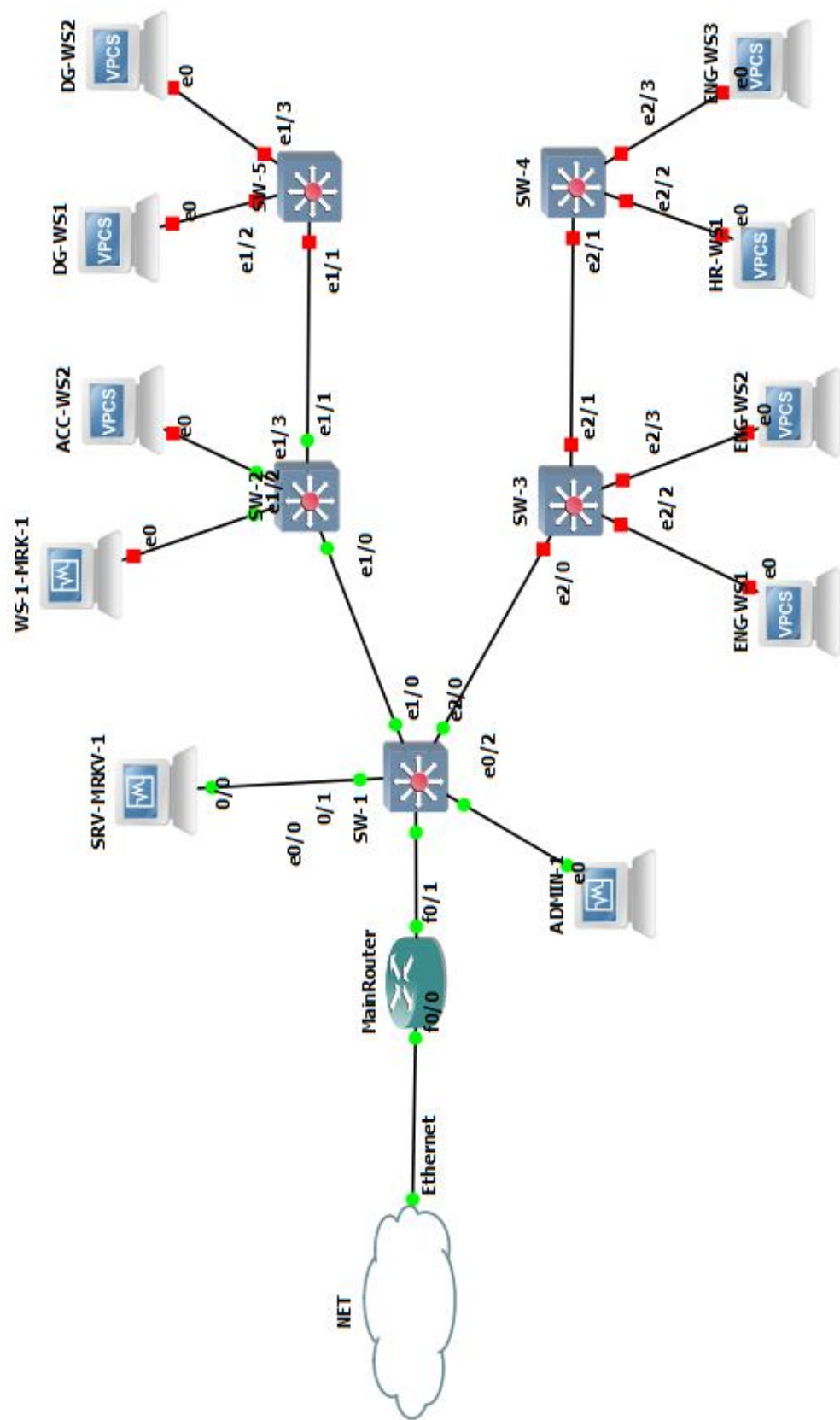
23.New-ADOrganizationalUnit: [Електронний ресурс] / Microsoft – [https://learn.microsoft.com/en-us/powershell/module/activedirectory/new-  
adorganizationalunit?view=windowsserver2022-ps](https://learn.microsoft.com/en-us/powershell/module/activedirectory/new-adorganizationalunit?view=windowsserver2022-ps) – Загол. з екрану.

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 61   |

# ДОДАТКИ

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркесв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 62   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

Загальна схема мережі.



## Лістинг конфігурації мережевих пристроїв

**Router CONF:**

```

MainRouter#show run
Building configuration...
Current configuration : 1089 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname MainRouter
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
!
ip cef
ip name-server 8.8.8.8
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 205.8.15.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
no ip http server
ip forward-protocol nd
!
ip nat inside source list 1 interface FastEthernet0/0 overload
!

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            |      |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            | 64   |

```

access-list 1 permit 0.0.0.0 255.255.255.0
access-list 1 permit 205.0.0.0 0.255.255.255
no cdp log mismatch duplex
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

SW-1:  
Building configuration...

Current configuration : 4876 bytes

```

! Last configuration change at 20:12:25 UTC Sun Jun 16 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname IOU1
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркеев Б.В. |        |      | ККИКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 65   |

```

vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport mode access
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.272f.68f3
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/2
switchport mode access
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0800.2772.7e75
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet0/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/0
switchport mode access
switchport port-security mac-address sticky
switchport port-security mac-address sticky aabb.cc00.0201
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet1/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 66   |

```

spanning-tree bpduguard enable
!
interface Ethernet1/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet2/0
switchport mode access
switchport port-security mac-address sticky
switchport port-security mac-address sticky aabb.cc00.0402
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
ip dhcp snooping limit rate 256
ip dhcp snooping trust
!
interface Ethernet2/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet2/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet2/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 67   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Vlan1
ip address 205.8.15.4 255.255.255.0
!
ip default-gateway 205.8.15.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 68   |

```

line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
!
End

SW-2:
SW-2#show run
Building configuration...

Current configuration : 4739 bytes
!
! Last configuration change at 20:18:26 UTC Sun Jun 16 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-2
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 69   |

```

interface Ethernet0/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet0/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet0/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet0/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet1/0
switchport mode access
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet1/1
switchport mode access
switchport port-security mac-address sticky
switchport port-security mac-address sticky aabb.cc00.0311
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet1/2

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 70   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet1/3
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet2/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet2/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet2/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet2/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/0

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 71   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Ethernet3/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
spanning-tree portfast edge
spanning-tree bpduguard enable
!
interface Vlan1
ip address 205.8.15.5 255.255.255.0
!
ip default-gateway 205.8.15.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 72   |

```

privilege level 15
logging synchronous
line vty 0 4
login
!
End
SW-5:
SW-5#show run
Building configuration...

Current configuration : 4087 bytes
!
! Last configuration change at 20:49:03 UTC Sun Jun 16 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-5
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.Б. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 73   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/0
!
interface Ethernet1/1
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet1/2
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 74   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

ip dhcp snooping trust
!
interface Ethernet1/3
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet2/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet2/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet2/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet2/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 75   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

ip dhcp snooping trust
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 205.8.15.6 255.255.255.0
!
ip default-gateway 205.8.15.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
End

```

SW-3:  
Building configuration...

Current configuration : 4387 bytes  
!  
! Last configuration change at 20:25:56 UTC Sun Jun 16 2024  
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
service compress-config  
!  
hostname SW-3  
!  
boot-start-marker  
boot-end-marker  
!

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 76   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip tcp synwait-time 5
!
interface Ethernet0/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 77   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

interface Ethernet0/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 78   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet2/0
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet2/1
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security mac-address sticky aabb.cc00.0512
switchport port-security mac-address sticky aabb.cc80.0500
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet2/2
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet2/3
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 205.8.15.7 255.255.255.0
!
ip default-gateway 205.8.15.1
ip forward-protocol nd
!
no ip http server

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 79   |

```

no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
End

```

SW-4:  
Building configuration...

```

Current configuration : 4475 bytes
!
! Last configuration change at 20:27:29 UTC Sun Jun 16 2024
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname SW-4
!
boot-start-marker
boot-end-marker
!
logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
!
no aaa new-model
!
no ip icmp rate-limit unreachable
!
no ip domain-lookup
ip cef
no ipv6 cef
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 80   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

ip tcp synwait-time 5
!
interface Ethernet0/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet0/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            | 81   |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            |      |

```

ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/2
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet1/3
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet2/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
ip dhcp snooping trust
!
interface Ethernet2/1
switchport mode access
switchport port-security maximum 3

```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            |      |
| Змн. | Арк. | № док.м.    | Підпис | Дата |                            | 82   |

```

switchport port-security mac-address sticky
switchport port-security mac-address sticky aabb.cc00.0412
switchport port-security mac-address sticky aabb.cc80.0400
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
interface Ethernet2/2
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
interface Ethernet2/3
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
ip arp inspection trust
ip dhcp snooping trust
!
interface Ethernet3/0
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
ip address 205.8.15.8 255.255.255.0
!
ip default-gateway 205.8.15.1
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
login
!
end

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 83   |

## Лістинг створених та використаних скриптів

**INST\_FOREST.ps1**

```

# import modules
Import-Module ServerManager
Import-Module ActiveDirectory

# params
$computerName = "SRV-MRKV"
$taskName = "Continue_ADDS_Installation"

Rename-Computer -NewName $computerName -Force

# 2nd script
$continueScript = '@'
# import modules
Import-Module ServerManager
Import-Module ActiveDirectory
Import-Module ADDSDeployment

$domainName = "corpmarkeiev.net"
$netbiosName = "CORPMARKEIEV"
$computerName = "SRV-MRKV"

Write-Output "Продовження налаштувань після перезавантаження..."

# ADWS check
$adwsService = Get-Service -Name ADWS -ErrorAction SilentlyContinue
if ($null -eq $adwsService) {
    Write-Output "ADWS service not found. Ensure that AD DS role is installed and ADWS is running."
    exit
} elseif ($adwsService.Status -ne 'Running') {
    Write-Output "Starting ADWS service..."
    Start-Service -Name ADWS
}

# AD DS role install
Add-WindowsFeature -Name AD-Domain-Services -IncludeAllSubFeature -IncludeManagementTools

# main install proccess
Install-ADDSForest `
    -CreateDnsDelegation:$false `
    -DatabasePath "C:\Windows\NTDS" `
    -DomainMode "WinThreshold" `
    -DomainName "corpmarkeiev.net" `
    -DomainNetbiosName "CORPMARKEIEV" `
    -ForestMode "WinThreshold" `
    -InstallDns:$true `
    -LogPath "C:\Windows\NTDS" `

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 84   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```
-SysvolPath "C:\Windows\SYSVOL" `
-SafeModeAdministratorPassword (ConvertTo-SecureString -AsPlainText "B1234567m" -Force) `
-Force:$true
```

```
# delete task after all
```

```
Unregister-ScheduledTask -TaskName "Continue_ADDS_Installation" -Confirm:$false
```

```
# res
```

```
Write-Output "Контролер перейменовано на: $computerName"
```

```
Write-Output "Встановлено роль головного контролера домену"
```

```
Write-Output "Назва домену: $domainName"
```

```
Write-Output "NetBIOS ім'я домену: $netbiosName"
```

```
Write-Output "Рівень функціональності домену: Windows Server 2016"
```

```
Write-Output "Рівень функціональності лісу: Windows Server 2016"
```

```
Write-Output "Встановлено DNS сервер"
```

```
Write-Output "Шляхи до бази даних NTDS: C:\Windows\NTDS"
```

```
Write-Output "Шляхи до журналу NTDS: C:\Windows\NTDS"
```

```
Write-Output "Шляхи до SYSVOL: C:\Windows\SYSVOL"
```

```
'@
```

```
# write to file
```

```
$continueScriptPath = "C:\scripts\FOREST_INST_Continue.ps1"
```

```
$continueScript | Out-File -FilePath $continueScriptPath -Encoding UTF8
```

```
# schedule task
```

```
$action = New-ScheduledTaskAction -Execute 'powershell.exe' -Argument "-File
```

```
$continueScriptPath"
```

```
$trigger = New-ScheduledTaskTrigger -AtStartup
```

```
$settings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries -
StartWhenAvailable
```

```
$principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType ServiceAccount -
RunLevel Highest
```

```
Register-ScheduledTask -Action $action -Trigger $trigger -Settings $settings -Principal $principal -
TaskName $taskName
```

```
# END RELOAD
```

```
Write-Output "Renaming computer to $computerName. Rebooting to apply changes in 120 sec..."
```

```
Start-Sleep -Seconds 120
```

```
Restart-Computer -Force
```

```
FOREST_INST_CONTINUE.ps1
```

```
Import-Module ServerManager
```

```
Import-Module ActiveDirectory
```

```
Import-Module ADDSDeployment
```

```
$domainName = "corpmarkeiev.net"
```

```
$netbiosName = "CORPMARKEIEV"
```

```
$computerName = "SRV-MRKV"
```

```
Write-Output "Продовження налаштувань після перезавантаження..."
```

```
#ADWS check $adwsService = Get-Service -Name ADWS -ErrorAction SilentlyContinue
```

```
if ($null -eq $adwsService) {
```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 85   |

```

Write-Output "ADWS service not found. Ensure that AD DS role is installed and ADWS is
running."
exit
} elseif ($adwsService.Status -ne 'Running') {
    Write-Output "Starting ADWS service..."
    Start-Service -Name ADWS
}
# AD DS role
Add-WindowsFeature -Name AD-Domain-Services -IncludeAllSubFeature -IncludeManagementTools
# install new forest
Install-ADDSForest `
    -CreateDnsDelegation:$false `
    -DatabasePath "C:\Windows\NTDS" `
    -DomainMode "WinThreshold" `
    -DomainName "corpmarkeiev.net" `
    -DomainNetbiosName "CORPMARKEIEV" `
    -ForestMode "WinThreshold" `
    -InstallDns:$true `
    -LogPath "C:\Windows\NTDS" `
    -SysvolPath "C:\Windows\SYSVOL" `
    -SafeModeAdministratorPassword (ConvertTo-SecureString -AsPlainText "B1234567m" -Force) `
    -Force:$true

# delete task after all
Unregister-ScheduledTask -TaskName "Continue_ADDS_Installation" -Confirm:$false

# res
Write-Output "Контролер перейменовано на: $computerName"
Write-Output "Встановлено роль головного контролера домену"
Write-Output "Назва домену: $domainName"
Write-Output "NetBIOS ім'я домену: $netbiosName"
Write-Output "Рівень функціональності домену: Windows Server 2016"
Write-Output "Рівень функціональності лісу: Windows Server 2016"
Write-Output "Встановлено DNS сервер"
Write-Output "Шляхи до бази даних NTDS: C:\Windows\NTDS"
Write-Output "Шляхи до журналу NTDS: C:\Windows\NTDS"
Write-Output "Шляхи до SYSVOL: C:\Windows\SYSVOL"

```

### DHCP\_IP.ps1

```

Write-Host "Налаштування IP-конфігурації контролера та встановлення модуля DHCP з подаль-
шими налаштуваннями" -ForegroundColor White

```

```

Import-Module ServerManager
Import-Module ActiveDirectory

```

```

Install-WindowsFeature -Name DHCP -IncludeManagementTools

```

```

Import-Module DhcpServer

```

```

# params
$dnsdomain = "corpmarkeiev.net"
$newname = "SRV-MRKV"

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 86   |

```
$featureLogPath = "C:\\poshlog\\featurelog.txt"
```

```
#FUNCTION
```

```
if (-not (Test-Path -Path $featureLogPath)) {  
    New-Item $featureLogPath -ItemType File -Force  
}  
$addsTools = "RSAT-AD-Tools"  
Add-WindowsFeature $addsTools  
Get-WindowsFeature | Where-Object {$_.Installed} | Out-File -FilePath $featureLogPath -Append
```

```
# IP CONF
```

```
$ipaddress = "205.8.15.2"  
$ipprefixlen = 24  
$ipgw = "205.8.15.1"  
$ipdns = "205.8.15.2"  
$ipid = (Get-NetAdapter).ifIndex  
$zero = "205.8.15.0"  
$startrange = "205.8.15.8"  
$endrange = "205.8.15.254"  
$mask = "255.255.255.0"
```

```
# Check curr IP
```

```
if (-not (Get-NetIPAddress -IPAddress $ipaddress)) {  
    New-NetIPAddress -IPAddress $ipaddress -PrefixLength $ipprefixlen -InterfaceIndex $ipid  
    Set-DnsClientServerAddress -InterfaceIndex $ipid -ServerAddresses $ipdns  
    Set-NetIPInterface -InterfaceIndex $ipid -InterfaceMetric 1  
}
```

```
# RESULTS
```

```
Write-Host "IP Configuration:" -ForegroundColor Cyan  
Get-NetIPConfiguration
```

```
# DHCP SCOPE
```

```
Add-DhcpServerv4Scope -EndRange $endrange -Name "Main" -StartRange $startrange -SubnetMask  
$mask -State Active -ComputerName $newname  
Set-DhcpServerv4OptionValue -ComputerName $newname -DnsServer $ipdns -DnsDomain  
$dnsdomain -Router $ipgw  
Set-DhcpServerv4OptionValue -ComputerName $newname -ScopeID $zero -DnsServer $ipdns -  
DnsDomain $dnsdomain -Router $ipgw
```

```
# params for dhcp
```

```
$scopeName = "MainScope"  
$scopeId = "205.8.15.0"  
$exclusionStart1 = "205.8.15.1"  
$exclusionEnd1 = "205.8.15.7"
```

```
# valid check
```

```
if (-not ([IPAddress]::TryParse($ipaddress, [ref]$null))) {  
    Write-Host "Invalid IP address. Please enter a valid IP address." -ForegroundColor Red  
    exit  
}
```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.Б. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 87   |

```

}
if (-not ([IPAddress]::TryParse($ipdns, [ref]$null))) {
    Write-Host "Invalid DNS server IP address. Please enter a valid IP address." -ForegroundColor Red
    exit
}
if (-not ([IPAddress]::TryParse($ipgw, [ref]$null))) {
    Write-Host "Invalid router IP address. Please enter a valid IP address." -ForegroundColor Red
    exit
}

# excluded addrs
try {
    Add-DhcpServerv4ExclusionRange -ScopeId $scopeId -StartRange $exclusionStart1 -EndRange
    $exclusionEnd1 -ErrorAction Stop
    Write-Host "Exclusion range successfully added to the DHCP scope." -ForegroundColor Green
} catch {
    Write-Host "Failed to add exclusion range: $_" -ForegroundColor Red
}

# results
Write-Host "Configured DHCP Scope Parameters:" -ForegroundColor Cyan
Write-Host "Scope Name: $scopeName" -ForegroundColor Cyan
Write-Host "Scope ID: $scopeId" -ForegroundColor Cyan
Write-Host "Start Range: $startrange" -ForegroundColor Cyan
Write-Host "End Range: $endrange" -ForegroundColor Cyan
Write-Host "Subnet Mask: $mask" -ForegroundColor Cyan
Write-Host "DNS Server: $ipdns" -ForegroundColor Cyan
Write-Host "DNS Domain: $dnsdomain" -ForegroundColor Cyan
Write-Host "Router (Gateway): $ipgw" -ForegroundColor Cyan
Write-Host "Exclusion Range 1: $exclusionStart1 - $exclusionEnd1" -ForegroundColor Cyan

Write-Output "IP Address: $ipaddress"
Write-Output "Prefix Length: $ipprefixlen"
Write-Output "Gateway: $ipgw"
Write-Output "DNS: $ipdns"
Write-Output "Interface ID: $ipid"
Write-Output "Network Address: $zero"
Write-Output "Start Range: $startrange"
Write-Output "End Range: $endrange"
Write-Output "Subnet Mask: $mask"

```

### OU\_GRP.ps1

Import-Module ActiveDirectory

```

$rootOUs = @(
    "Departments",
    "Company Groups",
    "Company Computers"
)

```

```

$createdRootOUs = @()

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 88   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

foreach ($ou in $rootOUs) {
    New-ADOrganizationalUnit -Name $ou -Path "DC=corpmarkeiev,DC=net"
    $createdRootOUs += "OU=$ou,DC=corpmarkeiev,DC=net"
}

$wsDepartments = @(
    "WS Accountancy Department",
    "WS HR Department",
    "WS Digital Transformation",
    "WS Engineering Department"
)

$createdWSDepartments = @()
foreach ($ou in $wsDepartments) {
    New-ADOrganizationalUnit -Name $ou -Path "OU=Company
Computers,DC=corpmarkeiev,DC=net"
    $createdWSDepartments += "OU=$ou,OU=Company Computers,DC=corpmarkeiev,DC=net"
}

$departments = @(
    "Accountancy Department",
    "HR Department",
    "Digital Transformation",
    "Engineering Department",
    "System Administrators"
)

$createdDepartments = @()
foreach ($ou in $departments) {
    New-ADOrganizationalUnit -Name $ou -Path "OU=Departments,DC=corpmarkeiev,DC=net"
    $createdDepartments += "OU=$ou,OU=Departments,DC=corpmarkeiev,DC=net"
}

$groupList = @(
    "Accountancy Department Users",
    "HR Department Users",
    "Digital Transformation Users",
    "Engineering Department Users",
    "System Administrators"
)

$createdGroups = @()
foreach ($group in $groupList) {
    New-ADGroup -Name $group -GroupCategory Security -GroupScope Global -Path "OU=Company
Groups,DC=corpmarkeiev,DC=net"
    $createdGroups += "CN=$group,OU=Company Groups,DC=corpmarkeiev,DC=net"
}

Write-Output "Total created root OUs: $($createdRootOUs.Count)"
$createdRootOUs | Format-Table -AutoSize
Write-Output "Total created WS departments in Company Computers:
$($createdWSDepartments.Count)"

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 89   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

$createdWSDepartments | Format-Table -AutoSize
Write-Output "Total created departments: $($createdDepartments.Count)"
$createdDepartments | Format-Table -AutoSize
Write-Output "Total created groups: $($createdGroups.Count)"
$createdGroups | Format-Table -AutoSize

```

USERS.ps1

Import-Module ActiveDirectory

```
$csvPath = "C:\scripts\Users.csv"
```

```

if (-Not (Test-Path -Path $csvPath)) {
    Write-Error "CSV file not found at path: $csvPath"
    exit
}

```

```
$ADUsers = Import-Csv $csvPath -Delimiter ";"
```

```

$addedUsersCount = 0
$addedUsersInfo = @()
$ouDistribution = @{}
$groupDistribution = @{}

```

```

foreach ($User in $ADUsers)
{
    # csv params
    $Username = $User.username
    $Password = $User.password
    $Firstname = $User.firstname
    $Lastname = $User.lastname
    $telephone = $User.telephone
    $jobtitle = $User.jobtitle
    $department = $User.department
    $Company = $User.company

    switch ($department) {
        "Accountancy Department" { $ouPath = "OU=Accountancy
Department,OU=Departments,DC=corpmarkeiev,DC=net" }
        "HR Department" { $ouPath = "OU=HR
Department,OU=Departments,DC=corpmarkeiev,DC=net" }
        "Digital Transformation" { $ouPath = "OU=Digital
Transformation,OU=Departments,DC=corpmarkeiev,DC=net" }
        "Engineering Department" { $ouPath = "OU=Engineering
Department,OU=Departments,DC=corpmarkeiev,DC=net" }
        "System Administrators" { $ouPath = "OU=System
Administrators,OU=Departments,DC=corpmarkeiev,DC=net" }
        default { $ouPath = "OU=Departments,DC=corpmarkeiev,DC=net" }
    }
}

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 90   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

# check if user true
if (Get-ADUser -Filter {SamAccountName -eq $Username})
{
    # if user - true, warning
    Write-Warning "A user account with username $Username already exists in Active Directory."
}
else
{
    try {
        # if not -- create new user
        New-ADUser `
        -SamAccountName $Username `
        -UserPrincipalName "$Username@corpmarkeiev.net" `
        -Name "$Firstname $Lastname" `
        -GivenName $Firstname `
        -Surname $Lastname `
        -Enabled $true `
        -DisplayName "$Lastname, $Firstname" `
        -Path $ouPath `
        -Company $Company `
        -OfficePhone $telephone `
        -Title $jobtitle `
        -Department $department `
        -AccountPassword (ConvertTo-SecureString $Password -AsPlainText -Force) `
        -ChangePasswordAtLogon $True

        # add user to his grp
        switch ($department) {
            "Accountancy Department" { $groupName = "Accountancy Department Users" }
            "HR Department" { $groupName = "HR Department Users" }
            "Digital Transformation" { $groupName = "Digital Transformation Users" }
            "Engineering Department" { $groupName = "Engineering Department Users" }
            "System Administrators" { $groupName = "System Administrators" }
            default { $groupName = "" }
        }

        if ($groupName -ne "") {
            Add-ADGroupMember -Identity $groupName -Members $Username
        }

        $addedUsersCount++
        $addedUsersInfo += [PSCustomObject]@{
            Firstname = $Firstname
            Lastname = $Lastname
            Username = $Username
            Department = $department
            Group = $groupName
            OU = $ouPath
        }
    }
}

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 91   |

```

if ($SouDistribution.ContainsKey($SouPath)) {
    $SouDistribution[$SouPath]++
} else {
    $SouDistribution[$SouPath] = 1
}

if ($groupDistribution.ContainsKey($groupName)) {
    $groupDistribution[$groupName]++
} else {
    $groupDistribution[$groupName] = 1
}
}
catch {
    Write-Error "Failed to create user $Username. Error: $_"
}
}
}

```

Write-Output "Total added users: \$addedUsersCount"

\$addedUsersInfo | Format-Table -AutoSize

Write-Output "User distribution by OU:"

\$SouDistribution.GetEnumerator() | Sort-Object Name | Format-Table -Property Name, Value - AutoSize

Write-Output "User distribution by Groups:"

\$groupDistribution.GetEnumerator() | Sort-Object Name | Format-Table -Property Name, Value - AutoSize

# JOBTITLE\_UPDATE\_FIX

# list

```

$usersJobTitles = @{
    "John Doe" = "Accounter"
    "Jane Smith" = "Accounter"
    "Michael Thompson" = "HR Specialist"
    "Sara Brown" = "HR Specialist"
    "Alex Davis" = "Designer"
    "Anna Klein" = "Photograph"
    "Tom Parker" = "Lead engineer"
    "Emma Peterson" = "Engineer"
    "Chris Morris" = "DC Admin"
    "Olivia Nelson" = "System Admin"
}

```

# path to OU

```

$SouPaths = @{
    "John Doe" = "OU=Accountancy Department,OU=Departments,DC=corpmarkeiev,DC=net"
    "Jane Smith" = "OU=Accountancy Department,OU=Departments,DC=corpmarkeiev,DC=net"
    "Michael Thompson" = "OU=HR Department,OU=Departments,DC=corpmarkeiev,DC=net"
}

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 92   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```

"Sara Brown" = "OU=HR Department,OU=Departments,DC=corpmarkeiev,DC=net"
"Alex Davis" = "OU=Digital Transformation,OU=Departments,DC=corpmarkeiev,DC=net"
"Anna Klein" = "OU=Digital Transformation,OU=Departments,DC=corpmarkeiev,DC=net"
"Tom Parker" = "OU=Engineering Department,OU=Departments,DC=corpmarkeiev,DC=net"
"Emma Peterson" = "OU=Engineering Department,OU=Departments,DC=corpmarkeiev,DC=net"
"Chris Morris" = "OU=System Administrators,OU=Departments,DC=corpmarkeiev,DC=net"
"Olivia Nelson" = "OU=System Administrators,OU=Departments,DC=corpmarkeiev,DC=net"
}

# update
foreach ($user in $usersJobTitles.Keys) {
    $jobTitle = $usersJobTitles[$user]
    $ouPath = $ouPaths[$user]

    # Оновлення JobTitle
    Get-ADUser -Filter {Name -eq $user} -SearchBase $ouPath | Set-ADUser -Title $jobTitle

    Write-Output "Оновлено JobTitle для $user до $jobTitle"
}

```

### LOGIN\_GPO.ps1

```

Import-Module ActiveDirectory
Import-Module GroupPolicy

```

Write-Output "Налаштування групових політик для розмежування доступу користувачів до робочих станцій"

```

$domain = "corpmarkeiev.net"
$netbiosDomain = "CORPMARKEIEV"
$companyComputersOU = "OU=Company Computers,DC=corpmarkeiev,DC=net"
$dcOU = "OU=Domain Controllers,DC=corpmarkeiev,DC=net"

```

```

$dcAdmin = "Chris Morris"
$systemAdmin = "Olivia Nelson"

```

```

# get "WS"
$wsOUs = Get-ADOrganizationalUnit -SearchBase $companyComputersOU -Filter {Name -like "WS*"}

```

```

foreach ($ou in $wsOUs) {
    $ouName = $ou.Name
    $ouPath = "OU=$ouName,$companyComputersOU"
    $deptName = $ouName -replace '^WS ', "
    $deptUsersGroup = "$netbiosDomain\" + ($deptName -replace ' ', ") + " Users"
    $gpoName = "$ouName - Restrict Logon"

```

```

    $gpo = New-GPO -Name $gpoName -Comment "Restrict local logon to $deptName users"

```

```

    New-GPLink -Name $gpoName -Target $ouPath -Enforced Yes

```

```

    $deniedUsers = "$netbiosDomain\Domain Users"

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 93   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

```
Set-GPRegistryValue -Name $gpoName -Key  
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName  
"DenyInteractiveLogonRight" -Type MultiString -Value $deniedUsers
```

```
Set-GPRegistryValue -Name $gpoName -Key  
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName  
"SeInteractiveLogonRight" -Type MultiString -Value @("$netbiosDomain\Administrator",  
"$deptUsersGroup", "$netbiosDomain\Olivia Nelson")  
}
```

```
#make crhis domain adm
```

```
Add-ADGroupMember -Identity "Domain Admins" -Members "$netbiosDomain\Chris Morris"
```

```
Add-ADGroupMember -Identity "Administrators" -Members "$netbiosDomain\Chris Morris"
```

```
$dcGpoName = "DC Admin - Allow Logon"
```

```
$dcGpo = New-GPO -Name $dcGpoName -Comment "Allow DC Admin logon"
```

```
New-GPLink -Name $dcGpoName -Target $dcOU -Enforced Yes
```

```
Set-GPRegistryValue -Name $dcGpoName -Key
```

```
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName
```

```
"SeInteractiveLogonRight" -Type MultiString -Value @("$netbiosDomain\Administrator",  
"$netbiosDomain\Chris Morris")
```

```
# Olivia system admin logon
```

```
$workstationsGpoName = "System Admin - Allow Logon"
```

```
$workstationsGpo = New-GPO -Name $workstationsGpoName -Comment "Allow System Admin  
logon"
```

```
New-GPLink -Name $workstationsGpoName -Target $companyComputersOU -Enforced Yes
```

```
Set-GPRegistryValue -Name $workstationsGpoName -Key
```

```
"HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName
```

```
"SeInteractiveLogonRight" -Type MultiString -Value @("$netbiosDomain\Administrator",  
"$netbiosDomain\Olivia Nelson")
```

```
# olivia admin
```

```
Add-ADGroupMember -Identity "Administrators" -Members "$netbiosDomain\Olivia Nelson"
```

```
Write-Output "Налаштування завершено!"
```

```
Write-Output "Olivia Nelson має доступ до усіх робочих станцій домену окрім контролера до-  
мену з правами адміністратора"
```

```
Write-Output "Olivia Nelson додано до групи Administrators"
```

```
Write-Output "Chris Morris має доступ до контролера домену"
```

```
Write-Output "Chris Morris додано до груп Domain Admins та Administrators"
```

```
gpupdate /force
```

**PASS\_LOCK\_PSO.ps1**

```
Import-Module ActiveDirectory
```

```
Write-Host "Configruing PSO for users..."
```

```
$systemAdminsOuPath = "OU=System Administrators,OU=Departments,DC=corpmarkeiev,DC=net"
```

```
$otherUsersOuPath = "OU=Departments,DC=corpmarkeiev,DC=net"
```

```
$systemAdminsPsoName = "PSO for System Administrators"
```

```
$systemAdminsPso = New-ADFineGrainedPasswordPolicy -Name $systemAdminsPsoName `
```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркеєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 94   |

- Precedence 1 `
- PasswordHistoryCount 24 `
- ReversibleEncryptionEnabled \$false `
- ComplexityEnabled \$true `
- MinPasswordLength 12 `
- MinPasswordAge (New-TimeSpan -Days 1) `
- MaxPasswordAge (New-TimeSpan -Days 42) `
- LockoutThreshold 3 `
- LockoutObservationWindow (New-TimeSpan -Minutes 60) `
- LockoutDuration (New-TimeSpan -Minutes 60)

Add-ADFineGrainedPasswordPolicySubject -Identity \$systemAdminsPsoName -Subjects "System Administrators"

```
$systemAdminsPsoDetails = Get-ADFineGrainedPasswordPolicy -Identity $systemAdminsPsoName
Write-Host "Configured PSO for System Administrators:"
Write-Host " - Name: $($systemAdminsPsoDetails.Name)"
Write-Host " - Precedence: $($systemAdminsPsoDetails.Precedence)"
Write-Host " - Password History Count: $($systemAdminsPsoDetails.PasswordHistoryCount)"
Write-Host " - Reversible Encryption Enabled:
$($systemAdminsPsoDetails.ReversibleEncryptionEnabled)"
Write-Host " - Complexity Enabled: $($systemAdminsPsoDetails.ComplexityEnabled)"
Write-Host " - Minimum Password Length: $($systemAdminsPsoDetails.MinPasswordLength)"
Write-Host " - Minimum Password Age: $($systemAdminsPsoDetails.MinPasswordAge)"
Write-Host " - Maximum Password Age: $($systemAdminsPsoDetails.MaxPasswordAge)"
Write-Host " - Lockout Threshold: $($systemAdminsPsoDetails.LockoutThreshold)"
Write-Host " - Lockout Observation Window:
$($systemAdminsPsoDetails.LockoutObservationWindow)"
Write-Host " - Lockout Duration: $($systemAdminsPsoDetails.LockoutDuration)"
$otherUsersPsoName = "PSO for Other Users"
$otherUsersPso = New-ADFineGrainedPasswordPolicy -Name $otherUsersPsoName `
  -Precedence 2 `
  -PasswordHistoryCount 12 `
  -ReversibleEncryptionEnabled $false `
  -ComplexityEnabled $true `
  -MinPasswordLength 8 `
  -MinPasswordAge (New-TimeSpan -Days 1) `
  -MaxPasswordAge (New-TimeSpan -Days 42) `
  -LockoutThreshold 6 `
  -LockoutObservationWindow (New-TimeSpan -Minutes 10) `
  -LockoutDuration (New-TimeSpan -Minutes 10)
```

Add-ADFineGrainedPasswordPolicySubject -Identity \$otherUsersPsoName -Subjects "Accountancy Department Users", "Digital Transformation Users", "Engineering Department Users", "HR Department Users"

```
$otherUsersPsoDetails = Get-ADFineGrainedPasswordPolicy -Identity $otherUsersPsoName
Write-Host "Configured PSO for Other Users:"
Write-Host " - Name: $($otherUsersPsoDetails.Name)"
Write-Host " - Precedence: $($otherUsersPsoDetails.Precedence)"
Write-Host " - Password History Count: $($otherUsersPsoDetails.PasswordHistoryCount)"
```

|      |      |             |        |      |                            |      |
|------|------|-------------|--------|------|----------------------------|------|
|      |      | Маркєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О. |        |      |                            |      |
| Змн. | Арк. | № докум.    | Підпис | Дата |                            | 95   |

Write-Host " - Reversible Encryption Enabled:  
 \$(\$otherUsersPsoDetails.ReversibleEncryptionEnabled)"  
 Write-Host " - Complexity Enabled: \$(\$otherUsersPsoDetails.ComplexityEnabled)"  
 Write-Host " - Minimum Password Length: \$(\$otherUsersPsoDetails.MinPasswordLength)"  
 Write-Host " - Minimum Password Age: \$(\$otherUsersPsoDetails.MinPasswordAge)"  
 Write-Host " - Maximum Password Age: \$(\$otherUsersPsoDetails.MaxPasswordAge)"  
 Write-Host " - Lockout Threshold: \$(\$otherUsersPsoDetails.LockoutThreshold)"  
 Write-Host " - Lockout Observation Window:  
 \$(\$otherUsersPsoDetails.LockoutObservationWindow)"  
 Write-Host " - Lockout Duration: \$(\$otherUsersPsoDetails.LockoutDuration)"

Write-Host "PSO policies configured successfully and linked to specified groups."

Write-Host "Updating Policies..."  
 gpupdate /force

### AUDIT\_GPO.ps1

Import-Module ActiveDirectory  
 Import-Module GroupPolicy

\$gpoName = "Audit Policy Configuration"  
 \$ouPaths = @("OU=Company Computers,DC=corpmarkeiev,DC=net", "OU=Domain  
 Controllers,DC=corpmarkeiev,DC=net")

\$gpo = New-GPO -Name \$gpoName -Comment "Configuring audit policies"

foreach (\$ouPath in \$ouPaths) {  
 New-GPLink -Name \$gpoName -Target \$ouPath -Enforced Yes  
 }

\$auditCategoryPath = "HKLM\SOFTWARE\Policies\Microsoft\Windows\Audit"

\$auditPolicies = @(  
 @{ Name = "Audit Other Logon/Logoff Events"; Key = "AuditOtherLogonEvents"; Value = "3" },  
 @{ Name = "Audit Logon"; Key = "AuditLogon"; Value = "3" },  
 @{ Name = "Audit Computer Account Management"; Key =  
 "AuditComputerAccountManagement"; Value = "3" },  
 @{ Name = "Audit Other Account Management Events"; Key =  
 "AuditOtherAccountManagementEvents"; Value = "3" },  
 @{ Name = "Audit Security Group Management"; Key = "AuditSecurityGroupManagement";  
 Value = "3" },  
 @{ Name = "Audit User Account Management"; Key = "AuditUserAccountManagement"; Value =  
 "3" },  
 @{ Name = "Audit Logoff"; Key = "AuditLogoff"; Value = "3" },  
 @{ Name = "Audit Other Account Logon Events"; Key = "AuditOtherAccountLogonEvents";  
 Value = "3" },  
 @{ Name = "Audit Directory Service Access"; Key = "AuditDirectoryServiceAccess"; Value = "3"  
 },  
 @{ Name = "Audit Active Directory Domain Services Object Changes"; Key =  
 "AuditActiveDirectoryDomainServicesObjectChanges"; Value = "3" },  
 @{ Name = "Audit Account Lockout"; Key = "AuditAccountLockout"; Value = "3" },  
 @{ Name = "Audit Registry"; Key = "AuditRegistry"; Value = "3" },

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 96   |

```

    @{ Name = "Audit Certification Services"; Key = "AuditCertificationServices"; Value = "3" },
    @{ Name = "Audit Policy Change"; Key = "AuditPolicyChange"; Value = "3" }
)

foreach ($policy in $auditPolicies) {
    Set-GPRegistryValue -Name $gpoName -Key "$auditCategoryPath" -ValueName $policy.Key -
Type String -Value $policy.Value
    Write-Host "Configured $($policy.Name) policy."
}

Write-Host "Audit policies configured successfully and linked to specified OUs."

```

## RESTRICTION\_GPO.ps1

```

Write-Host "Застосування політик обмежень для користувачів домену."

if (-not (Get-Module -ListAvailable -Name GroupPolicy)) {
    Write-Error "Модуль GroupPolicy не знайдено. Будь ласка, встановіть його перед запуском скрипта."
    exit
}
Import-Module GroupPolicy

$gpoName = "UserRestrictions"
$ouList = @(
    "OU=WS Accountancy Department,OU=Company Computers,DC=corpmarkeiev,DC=net",
    "OU=WS Digital Transformation,OU=Company Computers,DC=corpmarkeiev,DC=net",
    "OU=WS Engineering Department,OU=Company Computers,DC=corpmarkeiev,DC=net",
    "OU=WS HR Department,OU=Company Computers,DC=corpmarkeiev,DC=net",
    "OU=Accountancy Department,OU=Departments,DC=corpmarkeiev,DC=net",
    "OU=Digital Transformation,OU=Departments,DC=corpmarkeiev,DC=net",
    "OU=Engineering Department,OU=Departments,DC=corpmarkeiev,DC=net",
    "OU=HR Department,OU=Departments,DC=corpmarkeiev,DC=net"
)

$gpo = Get-GPO -Name $gpoName -ErrorAction SilentlyContinue
if (!$gpo) {
    $gpo = New-GPO -Name $gpoName
    Write-Host "Новий GPO створено: $gpoName"
} else {
    Write-Host "GPO вже існує: $gpoName"
}

Write-Host "Налаштування політик обмежень..."

Set-GPRegistryValue -Name $gpoName -Key
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" -ValueName
"NoControlPanel" -Type DWord -Value 1
Write-Host "Доступ до панелі керування заборонено."

Set-GPRegistryValue -Name $gpoName -Key "HKCU\Software\Policies\Microsoft\Windows\System"
-ValueName "DisableCMD" -Type DWord -Value 1

```

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 97   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

Write-Host "Доступ до рядка PowerShell заборонено."

Set-GPRegistryValue -Name \$gpoName -Key  
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" -ValueName  
"DisableRegistryTools" -Type DWord -Value 1

Write-Host "Доступ до налаштувань системи заборонено."

Set-GPRegistryValue -Name \$gpoName -Key  
"HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR" -ValueName "Start" -Type DWord -Value  
4

Write-Host "Підключення USB пристроїв заборонено."

Set-GPRegistryValue -Name \$gpoName -Key  
"HKLM\Software\Policies\Microsoft\Windows\Installer" -ValueName "DisableMSI" -Type DWord -  
Value 1

Write-Host "Встановлення програмного забезпечення заборонено."

Set-GPRegistryValue -Name \$gpoName -Key  
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments" -ValueName  
"SaveZoneInformation" -Type DWord -Value 1

Write-Host "Завантаження з браузера заборонено."

```
foreach ($ou in $ouList) {  
    New-GPLink -Name $gpoName -Target $ou  
    Write-Host "Політика групи застосована до OU: $ou."  
}
```

Write-Host "Політики обмежень для користувачів налаштовано."

## USERS.csv

firstname;lastname;username;department;password;telephone;jobtitle;company;cn  
John;Doe;John.Doe;Accountancy  
Department;Password1;1234567890;Accountant;corpmarkeiev;CN=John Doe,OU=Accountancy  
Department,OU=Branch1,OU=Departments,DC=corpmarkeiev,DC=net  
Jane;Smith;Jane.Smith;Accountancy  
Department;Password2;2345678901;Accountant;corpmarkeiev;CN=Jane Smith,OU=Accountancy  
Department,OU=Branch1,OU=Departments,DC=corpmarkeiev,DC=net  
Michael;Thompson;Michael.Thompson;HR Department;Password3;3456789012;HR  
Specialist;corpmarkeiev;CN=Michael Thompson,OU=HR  
Department,OU=Branch1,OU=Departments,DC=corpmarkeiev,DC=net  
Sara;Brown;Sara.Brown;HR Department;Password4;4567890123;HR  
Specialist;corpmarkeiev;CN=Sara Brown,OU=HR  
Department,OU=Branch1,OU=Departments,DC=corpmarkeiev,DC=net  
Alex;Davis;Alex.Davis;Digital Transformation;Password5;5678901234;Digital  
Analyst;corpmarkeiev;CN=Alex Davis,OU=Digital  
Transformation,OU=Branch2,OU=Departments,DC=corpmarkeiev,DC=net  
Anna;Klein;Anna.Klein;Digital Transformation;Password6;6789012345;Digital  
Analyst;corpmarkeiev;CN=Anna Klein,OU=Digital  
Transformation,OU=Branch2,OU=Departments,DC=corpmarkeiev,DC=net  
Tom;Parker;Tom.Parker;Engineering  
Department;Password7;7890123456;Engineer;corpmarkeiev;CN=Tom Parker,OU=Engineering  
Department,OU=Branch2,OU=Departments,DC=corpmarkeiev,DC=net

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            | 98   |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            |      |

Emma;Peterson;Emma.Peterson;Engineering  
 Department;Password8;8901234567;Engineer;corpmarkeiev;CN=Emma Peterson,OU=Engineering  
 Department,OU=Branch2,OU=Departments,DC=corpmarkeiev,DC=net  
 Chris;Morris;Chris.Morris;System  
 Administrators;Password9;9012345678;SysAdmin;corpmarkeiev;CN=Chris Morris,OU=System  
 Administrators,OU=Departments,DC=corpmarkeiev,DC=net  
 Olivia;Nelson;Olivia.Nelson;System  
 Administrators;Password10;123456789;SysAdmin;corpmarkeiev;CN=Olivia Nelson,OU=System  
 Administrators,OU=Departments,DC=corpmarkeiev,DC=net

|      |      |              |        |      |                            |      |
|------|------|--------------|--------|------|----------------------------|------|
|      |      | Маркєєв Б.В. |        |      | ККІКБ.КР.Б – 123 – 20 – ПЗ | Арк. |
|      |      | Шелуха О.О.  |        |      |                            |      |
| Змн. | Арк. | № докум.     | Підпис | Дата |                            | 99   |