

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

## ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра  
на тему: «Проект захищеної IT-інфраструктури  
компанії на базі рішень Microsoft Active Directory»

Виконав студент 4-го курсу групи КІ-19-1

спеціальності 123 «Комп'ютерна інженерія»

 Дмитро Добровольський

Керівник, професор кафедри КІ та КБ, д.т.н., доцент

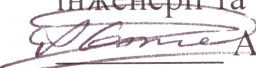
 Володимир Воротніков

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

 Андрій Єфіменко

Житомир – 2023

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  
1 березня 2023 р.

### ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Добровольський Дмитро Вадимович

Тема роботи: «Проект захищеної IT-інфраструктури компанії на базі рішень Microsoft Active Directory»

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 16 червня 2023 р.

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

Віртуальні приватні мережі, забезпечення захисту мережі за допомогою мережевих технологій та засобів Active Directory/

Обладнання та програмне забезпечення:

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

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

| Розділ | Консультант  | Підпис, дата   |                  |
|--------|--------------|----------------|------------------|
|        |              | Завдання видав | Завдання прийняв |
| 1      | Головня О.С. | 20.02.23       | 20.02.23         |
| 2      | Головня О.С. | 20.02.23       | 20.02.23         |
| 3      | Головня О.С. | 20.02.23       | 20.02.23         |

Студент  Дмитро Добровольський  
Керівник  Володимир Воротніков

### Календарний план

| № з/п | Назви етапів випускної кваліфікаційної роботи                                   | Термін виконання етапів роботи | Примітка |
|-------|---------------------------------------------------------------------------------|--------------------------------|----------|
| 1     | Постановка завдання                                                             | 20.02.2023 – 02.04.2023        |          |
| 2     | Написання вступної частини кваліфікаційної роботи                               | 02.04.2023 – 05.04.2023        |          |
| 3     | Аналіз основних теоретичних відомостей мережевих технологій та Active Directory | 05.04.2023 – 15.04.2023        |          |
| 4     | Проектування топології захищеної корпоративної мережі                           | 15.04.2023 – 21.04.2023        |          |
| 5     | Вибір технологій та використання                                                | 21.04.2023 – 25.04.2023        |          |
| 6     | Створення та налаштування мережі в емуляторі GNS3                               | 25.04.2023 – 01.05.2023        |          |
| 7     | Налаштування домену Active Directory                                            | 01.05.2023 – 11.05.2023        |          |
| 8     | Проведення додаткових налаштувань мережевих пристроїв                           | 11.05.2023 – 22.05.2023        |          |
| 9     | Написання висновків                                                             | 22.05.2023 – 26.05.2023        |          |
| 10    | Оформлення кваліфікаційної роботи                                               | 26.05.2023 – 01.06.2023        |          |
| 11    | Підготовка презентації до захисту                                               | 01.06.2023 – 18.06.2023        |          |

Студент  Дмитро Добровольський

Керівник  Володимир Воротніков

## АНОТАЦІЯ

Пояснювальна записку містить: 107 сторінки текстової частини, 71 рисунок, 5 таблиці та 28 джерел.

Метою роботи є дослідження можливості створення захищеної корпоративної мережі на базі MS Active Directory, дослідження інструментів захисту вбудованих у AD, створення захищеної мережі, перевірки її на надійність і отримання необхідних знань для розробки і побудови подібних систем у майбутньому.

У роботі розглянуто домен Active Directory як частину сучасної захищеної мережі, його функції для їх використання у мережі. Основні можливі атаки на мережу та засоби захисту від цих атак. В практичній частині була створена мережа з використання домену Active Directory та мережевих технологій. Створена мережа була перевірена на працездатність.

Ключові слова: ВІРТУАЛЬНІ МЕРЕЖІ, GNS3, ACTIVE DIRECTORY, CISCO, СИСТЕМА КОРИСТУВАЧІВ, МОДЕЛЬ ЗАГРОЗ, РОЗМЕЖУВАННЯ ДОСТУПУ, AAA, RADIUS, MICROSOFT, SSH.

КІК.КР.Б – 123 – 04 – ПЗ

|           |      |                     |                                                                                     |          |                                                                                                  |                |      |         |
|-----------|------|---------------------|-------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------|----------------|------|---------|
|           |      |                     |                                                                                     |          | КІК.КР.Б – 123 – 04 – ПЗ                                                                         |                |      |         |
| Змн.      | Арк. | № докум.            | Підпис                                                                              | Дата     | Проект захищеної ІТ-інфра-<br>структури компанії на базі рі-<br>шення Microsoft Active Directory | Лім.           | Арк. | Аркушів |
| Розроб.   |      | Добровольський Д.В. |  | 20.06.23 |                                                                                                  |                |      |         |
| Керівник  |      | Воротніков В.В.     |  | 20.06.23 |                                                                                                  |                | 4    | 114     |
| Реценз.   |      | Єфіменко А.А.       |  | 20.06.23 |                                                                                                  | ФІКТ, Гр. КІ-4 |      |         |
| Н. контр. |      | Воротніков В.В.     |  | 20.06.23 |                                                                                                  |                |      |         |
| Затверд.  |      | Єфіменко А.А.       |  | 20.06.23 |                                                                                                  |                |      |         |

## ANNOTATION

The explanatory note contains: 107 pages of text, 71 figures, 5 tables and 28 sources.

The purpose of the work is to study the possibility of creating a secure corporate network based on MS Active Directory, researching protection tools built into AD, creating a secure network, checking its reliability and obtaining the necessary knowledge for the development and construction of similar systems in the future.

This work examines the Active Directory domain as part of a modern secure network, its functions for their use in the network. The main possible attacks on the network and means of protection against these attacks. In the practical part, a network was created using the Active Directory domain and network technologies. The created network was tested for operability.

Keywords: VIRTUAL NETWORKS, GNS3, ACTIVE DIRECTORY, CISCO, USER SYSTEM, THREAT MODEL, ACCESS DISTRIBUTION, AAA, RADIUS, MICROSOFT, SSH.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 5    |

## ЗМІСТ

|                                                                                                                                 |     |
|---------------------------------------------------------------------------------------------------------------------------------|-----|
| ВСТУП .....                                                                                                                     | 8   |
| РОЗДІЛ 1. ПРИНЦИПИ ПОБУДОВИ ІТ-ІНФРАСТРУКТУР НА БАЗІ<br>СЛУЖБИ КАТАЛОГІВ MICROSOFT ACTIVE DIRECTORY .....                       | 9   |
| 1.1. Загальна характеристика служби каталогів<br>Microsoft Active Directory .....                                               | 9   |
| 1.2. Можливості служби каталогів Active Directory для захисту мережних<br>інфраструктур .....                                   | 13  |
| 1.3. Типові технології та протоколи побудови<br>мережних інфраструктур .....                                                    | 24  |
| 1.4. Аналіз типових атак на мережну інфраструктуру та типові<br>рекомендації щодо їх послаблення.....                           | 36  |
| 1.5. Постановка технічного завдання на розробку проєкту захищеної ІТ-<br>інфраструктури компанії .....                          | 45  |
| РОЗДІЛ 2. ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ<br>КОМПАНІЇ.....                                                             | 47  |
| 2.1. Проєктування топології мережі .....                                                                                        | 47  |
| 2.2. Розробка схеми адресації комунікаційних пристроїв та кінцевих<br>вузлів мережі.....                                        | 49  |
| 2.3. Проєктування схеми користувачів служби каталогів<br>Microsoft Active Directory .....                                       | 50  |
| 2.4. Обґрунтування та вибір мережних технологій та функціоналу<br>Active Directory для побудови ІТ-інфраструктури компанії..... | 53  |
| РОЗДІЛ 3. РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ СЛУЖБИ КАТАЛОГІВ<br>ACTIVE DIRECTORY ДЛЯ ІТ-ІНРАСТРУКТУРИ КОМПАНІЇ.....                   | 62  |
| 3.1. Встановлення та налаштування Microsoft Active Directory серверів....                                                       | 62  |
| 3.2. Налаштування комунікаційних пристроїв мережної інфраструктури .                                                            | 92  |
| 3.3. Налаштування засобів захисту комунікаційних пристроїв мережної<br>інфраструктури .....                                     | 97  |
| ВИСНОВКИ.....                                                                                                                   | 100 |
| СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ .....                                                                                            | 102 |
| ДОДАТКИ.....                                                                                                                    | 106 |

## ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

MS – Microsoft

AD – Active Directory

LDAP – Lightweight Directory Access Protocol

DAI - Dynamic ARP Inspection

DHCP - Dynamic Host Configuration Protocol

OU – Organization Unit

WS – Work Station

MitM - Man-in-the-Middle

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 7    |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

## ВСТУП

**Актуальність теми.** Захищена мережа на базі Active Directory є актуальною і важливою для будь-якої компанії або організації, яка працює з конфіденційною інформацією. Active Directory є службою каталогу для зберігання інформації про користувачів, комп'ютери та інші ресурси в мережі. Вона надає можливість контролювати доступ до ресурсів та надає механізми аутентифікації, авторизації та аудиту доступу до ресурсів. Захищена мережа на базі Active Directory дозволяє забезпечити надійний захист від несанкціонованого доступу до конфіденційної інформації, зменшити ризик витоку даних.

**Метою кваліфікаційної роботи** є дослідження можливості створення захищеної корпоративної мережі на базі MS Active Directory, дослідження інструментів захисту вбудованих у AD, створення захищеної мережі, перевірки її на надійність і отримання необхідних знань для розробки і побудови подібних систем у майбутньому.

Визначена мета обумовлює наступні завдання:

- Дослідити необхідні для побудови мережі технології і розібратися з їх реалізацією.
- Побудувати проект захищеної мережі.
- Налаштувати побудовану мережу.
- Провести перевірку налаштованої мережі на працездатність і захищеність.

**Об'єктом дослідження** є процес побудови проекту захищеної IT-інфраструктури компанії на базі рішень Microsoft Active Directory.

**Предметом дослідження** є Microsoft Active Directory.

У процесі виконання кваліфікаційної роботи було розроблено проект захищеної мережі, була побудована мережа і були проведені налаштування створеної мережі. Створена мережа була протестована на працездатність і захищеність.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 8    |

# РОЗДІЛ 1 ПРИНЦИПИ ПОБУДОВИ ІТ-ІНФРАСТРУКТУР НА БАЗІ СЛУЖБИ КАТАЛОГІВ MICROSOFT ACTIVE DIRECTORY

## 1.1 Загальна характеристика служби каталогів Microsoft Active Directory

Microsoft Active Directory (AD) — це служба каталогів, створена компанією Microsoft, яка використовується організаціями для керування обліковими записами користувачів, комп'ютерами та іншими ресурсами в мережі. Він надає централізовані служби автентифікації та авторизації, а також дозволяє адміністраторам контролювати доступ до мережевих ресурсів і застосовувати політики безпеки.

Active Directory зберігає інформацію про мережеві ресурси, такі як користувачі, групи, комп'ютери, принтери та програми. Він призначений для масштабування та може використовуватися для керування ресурсами в кількох доменах або лісах. Адміністратори можуть використовувати групову політику для централізованого керування налаштуваннями для користувачів і комп'ютерів у мережі, включаючи політики безпеки, налаштування робочого столу та встановлення програмного забезпечення.

Active Directory підтримує кілька протоколів автентифікації, включаючи Kerberos, NTLM і LDAP. Він також надає такі функції, як єдиний вхід (SSO) та інтеграцію з іншими службами Microsoft, такими як Exchange і SharePoint.

Основний функціонал Active Directory включає наступні можливості:

- централізоване управління користувачами та групами: Active Directory дозволяє створювати, редагувати та видаляти облікові записи користувачів, контролювати доступ до ресурсів в залежності від груп, призначати ролі та права доступу;
- управління комп'ютерами: Active Directory дозволяє додавати комп'ютери до домену, управляти настройками комп'ютерів, надавати доступ до ресурсів на основі політик безпеки;

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 9    |

– централізоване зберігання об'єктів: Active Directory забезпечує централізоване зберігання об'єктів (користувачів, груп, комп'ютерів) і їх атрибутів. Це дозволяє спростити управління об'єктами в мережі та забезпечити їх єдність;

– Аутентифікація та авторизація: Active Directory забезпечує механізми аутентифікації користувачів у мережі, а також контроль доступу до ресурсів на основі прав доступу, призначених об'єктам.

– Групове політикування: Active Directory дозволяє налаштовувати групові політики, які контролюють налаштування та поведінку користувачів і комп'ютерів в мережі. Групові політики дозволяють уніфікувати настройки, надати різні рівні доступу та забезпечити безпеку системи.

– Реплікація даних: Active Directory підтримує реплікацію даних між різними контролерами домену. Це забезпечує високу доступність та стійкість каталогу, а також можливість розміщення контролерів домену у різних місцях мережі.

Загалом, Active Directory надає потужні засоби для централізованого управління та контролю ресурсами в мережі Windows, поліпшує безпеку, спрощує адміністрування та підвищує продуктивність користувачів.

Підсумовуючи, можна сказати Active Directory є потужним інструментом для керування мережевими ресурсами та надання централізованих служб автентифікації та авторизації в середовищі Windows. Дані представлені вище, основані на матеріалах представлених по посиланню [\[1\]](#). Далі розберемо основні протоколи, які використовуються у AD.

Протокол Kerberos – протокол автентифікації, що використовується для перевірки посвідчення користувача або вузла мережі. Він був розроблений MIT у 1980-х роках і зараз є широко використовуваним протоколом автентифікації для комп'ютерних мереж.

Kerberos використовує систему на основі квитків для забезпечення автентифікації, який працює на основі представленого алгоритму:

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 10   |

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 із запитом квитка на потрібний ресурс.
3. Сервер Kerberos ідентифікує облікові дані користувача, як-от ім'я користувача та пароль, і створює квиток для надання квитка (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.
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 дійсний.

Kerberos забезпечує високий рівень безпеки, оскільки використовує надійне шифрування для захисту облікових даних користувача та квитків. Він також використовує взаємну автентифікацію, тобто як користувач, так і сервер ресурсів проходять автентифікацію перед наданням доступу. Це допомагає запобігти несанкціонованому доступу до конфіденційних ресурсів у мережевому середовищі. Дані представлені вище, основані на матеріалах представлених по посиланню [\[2\]](#).

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

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 11   |

як наступник протоколу автентифікації LM (LAN Manager), який був менш безпечним.

NTLM використовує механізм виклик-відповідь для автентифікації користувачів і комп'ютерів. Коли користувач входить до системи Windows, система надсилає виклик користувачеві. Пароль користувача використовується для шифрування виклику, а зашифрований результат надсилається назад до системи. Потім система порівнює зашифрований результат із збереженим хешем пароля, щоб підтвердити особу користувача.

NTLM широко використовується в мережах Windows, але він має кілька недоліків безпеки, які були виявлені протягом багатьох років. Наприклад, він може бути вразливим до атак із передачею хешу, коли зломисник може отримати хеш пароля та використати його для автентифікації користувача, не знаючи фактичного пароля. З цієї причини нові протоколи автентифікації, такі як Kerberos і OAuth2, рекомендуються для більш безпечної автентифікації в сучасних середовищах Windows. Представлені дані по протоколу, оснований на матеріалах представлені по посиланню [\[3\]\[4\]](#).

LDAP розшифровується як Lightweight Directory Access Protocol, який є протоколом, який використовується для доступу та керування інформацією каталогу. Каталог — це база даних, яка зберігає інформацію про об'єкти, наприклад користувачів, групи та ресурси, в ієрархічній структурі. LDAP надає спосіб доступу та оновлення цієї інформації через мережу.

LDAP зазвичай використовується в корпоративних середовищах для керування автентифікацією користувачів, авторизацією та доступом до таких ресурсів, як файли, принтери та програми. Він також використовується в Інтернет-службах, таких як електронна пошта та обмін миттєвими повідомленнями, як спосіб пошуку інформації про користувача та інформації про маршрутизацію.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 12   |

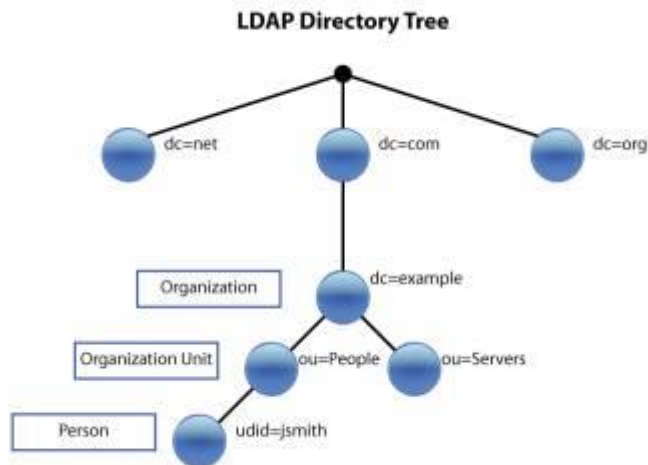


Рисунок 1.1 – LDAP Directory Tree

LDAP працює, надсилаючи запити на сервер каталогів, який потім відповідає із запитуваною інформацією. LDAP використовує ієрархічну структуру під назвою інформаційне дерево каталогу (DIT) для організації інформації в каталозі. DIT складається із записів, які представляють об’єкти в каталозі, і атрибутів, які описують властивості цих об’єктів.

LDAP — це відкритий стандартний протокол, який широко підтримується серверами каталогів і клієнтськими програмами. Він часто використовується в поєднанні з іншими протоколами, такими як Kerberos і SSL/TLS, для забезпечення безпечної автентифікації та шифрування. Представлені дані по протоколу, основані на матеріалах представлені по посиланню [5].

## 1.2 Можливості служби каталогів Active Directory для захисту мережних інфраструктури

Active Directory – потужний інструмент для керування ресурсами у середовищі Windows. Він має велику кількість служб і функцій, які можна використати у побудові мережі. Розберемо деякі з цих служб.

– **Автентифікація:** Active Directory надає служби автентифікації, які перевіряють ідентичність користувачів і комп’ютерів, які мають доступ до мережі. Це гарантує, що лише авторизовані користувачі мають доступ до мережних ресурсів.

– **Авторизація:** Active Directory також надає служби авторизації, які визначають, до яких ресурсів дозволено отримати доступ користувачам і комп'ютерам. Це допомагає гарантувати, що користувачі мають доступ лише до тих ресурсів, які їм потрібні для виконання своєї роботи, і що вони не можуть отримати доступ до ресурсів, до яких вони не повинні мати доступу.

– **Групова політика:** Групова політика Active Directory надає спосіб налаштувати параметри безпеки та застосувати їх до всіх комп'ютерів у мережі. Це може допомогти переконатися, що на всіх комп'ютерах налаштовано однакові параметри безпеки, що може допомогти запобігти вразливостям.

– **Служби сертифікації Active Directory (AD CS):** AD CS надає служби керування сертифікатами, які дозволяють видавати цифрові сертифікати та керувати ними. Це може допомогти захистити мережевий зв'язок, увімкнувши шифрування та перевіряючи особу користувачів і пристроїв.

– **Система доменних імен (DNS):** Active Directory також надає служби DNS, які дозволяють керувати системою доменних імен у вашій мережі. Це може допомогти переконатися, що ваші мережеві ресурси правильно визначено та доступ до них мають авторизовані користувачі.

– **Lightweight Directory Access Protocol (LDAP):** Active Directory також підтримує LDAP, який є стандартним протоколом, який використовується для доступу до служб каталогу. LDAP дозволяє отримувати доступ і змінювати дані каталогу, які можна використовувати для керування обліковими записами користувачів, обліковими записами комп'ютерів та іншими мережевими ресурсами.

– **Аудит безпеки:** Active Directory надає послуги аудиту безпеки, які дозволяють відстежувати та контролювати дії користувачів. Це може допомогти виявити та запобігти несанкціонованому доступу до мережі.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 14   |

Використання цих служби та функції, включених Active Directory, є необхідним для створення безпечної мережі, яка захищена від широкого спектру загроз. Однак важливо зазначити, що безпека — це безперервний процес, і мережу потрібно постійно оцінювати та покращувати стан безпеки мережі. Дані представлені вище, основані на матеріалах представлених по посиланню [\[1\]](#).

Для організації захисту мережевих пристроїв, такої можна використати Active Directory, а саме вбудований RADIUS клієнт, який є частиною протоколу AAA, для розуміння розберемо данні протоколи.

**Authentication, Authorization, and Accounting (AAA)** є трьома основними компонентами безпечної мережевої системи.

**Authentication (Автентифікація)** означає процес перевірки особи користувача, пристрою або програми, які намагаються отримати доступ до мережевого ресурсу. Цього можна досягти за допомогою різних методів, таких як паролі, біометрична автентифікація або цифрові сертифікати.

**Authorization (Авторизація)** передбачає визначення рівня доступу або дозволів, які повинен мати користувач, пристрій або програма після їх автентифікації. Це включає вказівку, до яких ресурсів вони можуть отримати доступ і які дії вони можуть виконувати.

**Accounting (Облік)** - це процес відстеження та моніторингу дій автентифікованих користувачів, пристроїв або програм у мережі. Це включає реєстрацію їхніх дій, наприклад, коли вони отримували доступ до ресурсу та які зміни вони в ньому вносили, з метою аудиту та виставлення рахунків.

Разом ці три компоненти забезпечують комплексну структуру безпеки, яка гарантує, що лише авторизовані користувачі можуть отримати доступ до мережевих ресурсів, якщо вони мають відповідний рівень доступу, а також що їх діяльність контролюється та відстежується з метою безпеки. Представлені дані по протоколу AAA, основані на матеріалах представлених по посиланню [\[6\]](#).

Серед доступних AAA протоколів для віддаленого підключення вибраний протокол RADIUS.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В      |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 15   |

**RADIUS** (Remote Authentication Dial-In User Service) — це мережевий протокол, який використовується для централізованого керування автентифікацією, авторизацією та обліковим записом (AAA) у мережі. Він зазвичай використовується в корпоративних мережах, інтернет-провайдерах і телекомунікаційних мережах для забезпечення єдиної точки автентифікації та авторизації для віддалених користувачів.

Коли користувач намагається отримати доступ до мережевого ресурсу, наприклад підключення до мережі Wi-Fi, RADIUS автентифікує облікові дані користувача, такі як ім'я користувача та пароль, у центральній базі даних автентифікації, такій як Active Directory. Після автентифікації користувача RADIUS визначає його рівень доступу до мережевих ресурсів на основі політик авторизації, налаштованих у центральній базі даних.

RADIUS також надає облікову інформацію про використання мережі, реєструючи дії користувача, такі як час підключення та передані дані, для цілей виставлення рахунків і аудиту.

RADIUS працює з використанням архітектури клієнт/сервер. Клієнт RADIUS зазвичай розташований на мережевому пристрої, наприклад бездротовій точці доступу або шлюзі VPN, до якого отримує доступ користувач. Сервер RADIUS відповідає за автентифікацію та авторизацію користувача, а також за підтримку центральної бази даних автентифікації.

Загалом RADIUS забезпечує безпечний та ефективний спосіб керування віддаленим доступом до мережі, дозволяючи організаціям легко керувати та контролювати доступ до своїх мережевих ресурсів. Представлені дані по протоколу RADIUS, основані на матеріалах представлені по посиланню [\[6\]](#).

Одним з важливих елементів служби Active Directory є Служба спільного принтера, відома також як Служби друку та документів. Служби друку та документів у Active Directory — це набір функцій і функціональних можливостей, які надає Microsoft Active Directory для керування та керування службами друку та документів у мережевому середовищі. Служби друку та документів в Active

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 16   |

Directory пропонують різноманітні можливості для оптимізації та вдосконалення процесу друку та керування документами в організації. Деякі ключові компоненти та функції служб друку та документів в Active Directory включають.

- Сервер друку: Active Directory можна налаштувати як сервер друку, що забезпечує централізоване керування принтерами та чергами друку в мережі. Сервери друку обробляють завдання друку, керують драйвером принтера та спільним доступом до принтера.

- Керування принтером: Active Directory надає інструменти для керування принтерами, наприклад створення об'єктів принтера, налаштування параметрів принтера, налаштування прав доступу та моніторинг використання принтера. Ці завдання керування можна виконувати за допомогою консолі користувачів і комп'ютерів Active Directory або інших засобів керування.

- Керування чергою друку: Active Directory дозволяє адміністраторам керувати чергами друку, які представляють зони очікування для завдань друку. Вони дозволяють установлювати пріоритети, планувати та контролювати завдання друку. Адміністратори можуть контролювати доступ до черг друку та налаштовувати такі параметри, як пріоритет завдань, обмеження кількості сторінок і параметри часу очікування.

- Керування драйвером принтера: Active Directory пропонує можливості керування драйверами, дозволяючи адміністраторам встановлювати, оновлювати та розповсюджувати драйвери принтера в мережі. Це спрощує процес розгортання принтерів на клієнтських комп'ютерах і забезпечує сумісність між принтерами та клієнтськими операційними системами.

- Інтеграція групової політики: Active Directory інтегрується з груповою політикою, функцією, яка забезпечує централізоване налаштування та керування параметрами користувача та комп'ютера. Групову політику можна використовувати для розгортання з'єднань принтера з окремими користувачами чи групами, керування налаштуваннями друку та застосування політик, пов'язаних із друком.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 17   |

– Служби Active Directory Lightweight Directory (AD LDS): AD LDS — це функція, яка надає полегшену версію Active Directory, придатну для сценаріїв, коли потрібна окрема служба каталогів. AD LDS можна використовувати для керування інформацією, пов’язаною з друком, незалежно від основного середовища Active Directory.

– Безпека та контроль доступу: Active Directory забезпечує безпеку та контроль доступу для принтерів і пов’язаних із друком ресурсів. Адміністратори можуть визначати дозволи та права доступу для користувачів і груп, гарантуючи, що лише авторизовані особи можуть друкувати, керувати принтерами або змінювати параметри принтера.

Використовуючи служби друку та документів в Active Directory, організації можуть оптимізувати свою інфраструктуру друку, спростити завдання адміністрування та підвищити безпеку та контроль над ресурсами друку. Це допомагає оптимізувати процеси друку, зменшити витрати та підвищити загальну ефективність керування службами, пов’язаними з документами, у мережевому середовищі. На основі даних представлених по посиланню [\[10\]](#).

Також для підвищення ефективності і зручності користування службою каталогів Active Directory можна використати Служби віддаленого робочого стола. Служби віддаленого робочого стола (RDS) — це компонент Microsoft Windows Server, який дозволяє користувачам отримувати доступ до віддалених робочих столів і програм з будь-якого місця за допомогою мережевого підключення. Active Directory (AD) — це служба каталогів Microsoft, яка забезпечує централізовану автентифікацію, авторизацію та керування мережевими ресурсами.

Що стосується RDS в Active Directory, слід розуміти кілька важливих моментів:

– інтеграція з Active Directory: RDS можна інтегрувати з Active Directory, щоб використовувати можливості керування користувачами та гру-

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 18   |

пами. Ця інтеграція дозволяє адміністраторам керувати дозволами RDS і доступом на основі облікових записів і груп користувачів Active Directory. Використовуючи Active Directory, ви можете застосовувати політики безпеки, призначати дозволи та централізовано керувати доступом користувачів до ресурсів RDS;

- автентифікація та авторизація: Active Directory відіграє вирішальну роль у автентифікації та авторизації користувачів для сеансів віддаленого робочого столу. Коли користувач намагається підключитися до середовища RDS, Active Directory перевіряє його облікові дані та визначає, чи має він необхідні дозволи для доступу до запитуваних ресурсів. Це гарантує, що лише авторизовані користувачі можуть підключатися до віддалених робочих столів і програм;

- керування груповою політикою: Групову політику Active Directory можна використовувати для керування різними параметрами та конфігураціями в розгортанні RDS і їх застосування. Групова політика дозволяє адміністраторам визначати політики, які контролюють доступ користувачів, налаштування безпеки, конфігурації програм тощо. Ці політики можуть бути націлені на певні групи користувачів Active Directory або організаційні підрозділи (OU), забезпечуючи детальний контроль над налаштуваннями RDS;

- керування профілями користувачів: Active Directory також може брати участь у керуванні профілями користувачів у середовищі RDS. У профілях користувачів зберігаються налаштування та конфігурації для користувачів, а за допомогою профілів користувачів Active Directory або переміщуваних профілів користувачі можуть мати узгоджені параметри робочого стола та програми в різних сеансах RDS. Active Directory можна налаштувати для централізованого зберігання цих профілів, дозволяючи користувачам отримувати доступ до своїх персональних налаштувань з будь-якого сеансу RDS;

- єдиний вхід (SSO): інтеграція Active Directory забезпечує можливість єдиного входу в середовищі RDS. Користувачі, які вже пройшли автентифікацію в домені Active Directory, можуть безперешкодно отримувати доступ до

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 19   |

ресурсів RDS без необхідності надання окремих облікових даних. Це покращує взаємодію з користувачем і спрощує процес входу, оскільки користувачі можуть використовувати наявні облікові дані домену для доступу до віддалених робочих столів і програм.

Завдяки інтеграції RDS з Active Directory організації можуть використовувати централізоване керування користувачами, покращену безпеку, узгоджені профілі користувачів і спрощене адміністрування, які надає Active Directory. Він забезпечує ефективне розгортання та керування службами віддаленого робочого столу та додатків, одночасно використовуючи надійні функції Active Directory для автентифікації, авторизації, застосування політики та керування профілями користувачів.

Важливим елементом у контролі за використанням обсягу дискового простору є квота. Квота — це механізм, який використовується для обмеження або розподілу ресурсів у різних обчислювальних контекстах. У контексті файлових систем і сховищ квота встановлює обмеження на обсяг дискового простору або кількість файлів, які може використовувати користувач або група користувачів. Квоти зазвичай використовуються для забезпечення справедливих розподілу ресурсів, запобігання надмірному споживанню ресурсів і ефективного управління ємністю зберігання.

Квоти можуть бути реалізовані як на рівні файлової системи, так і на рівні програми. На рівні файлової системи квоти зазвичай застосовуються операційною системою або програмним забезпеченням файлової системи. Вони часто використовуються в багатокористувацьких середовищах, таких як корпоративні мережі, де кілька користувачів спільно використовують ресурси зберігання.

Деякі ключові аспекти та особливості квот включають.

1) Типи квот. Існує два основних типи квот:

а) Жорстка квота: цей тип встановлює суворі обмеження, що не дозволяє користувачам перевищувати виділену квоту. Після досягнення ліміту користувачі не можуть створювати або додавати файли.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 20   |

б) М'яка квота: м'які квоти забезпечують більш м'який підхід. Користувачам дозволено тимчасово перевищувати свою квоту, але вони можуть отримувати попередження або сповіщення, коли вони наближаються або перевищують ліміт.

2) Керування квотами: квотами можуть керувати системні адміністратори, які визначають і призначають квоти окремим користувачам, групам або каталогам. Адміністратори можуть установлювати конкретні обмеження, контролювати використання та коригувати квоти за потреби.

3) Звітування та сповіщення: системи квот часто включають можливості звітування, що дозволяє адміністраторам створювати звіти про використання та ідентифікувати користувачів, які наближаються до своїх лімітів. Сповіщення можна налаштувати для сповіщення користувачів і адміністраторів, коли вони досягають певного порогу або перевищують свої квоти.

4) Звільнення від квот: у деяких випадках адміністраторам може знадобитися звільнити певних користувачів або каталоги від обмежень квот. Це можна зробити, щоб задовольнити певні вимоги або привілейованих користувачів, яким потрібні додаткові ресурси.

5) Застосування квот: квоти зазвичай застосовуються на рівні файлової системи, де операційна система відстежує та забезпечує використання ресурсів. Коли користувач намагається перевищити свою квоту, файлова система може запобігти подальшому зберіганню або створенню файлів, доки використання не буде приведено в межах виділених обмежень.

Квоти надають засоби управління та контролю за розподілом ресурсів у системах зберігання, забезпечуючи справедливе використання та запобігаючи зловживанню ресурсами. Вони особливо корисні в спільному середовищі, де кільком користувачам або групам потрібен доступ до обмежених ресурсів зберігання.

Безпека у мережі це важливо, але в ситуації коли трапилася втрата даних, з будь-яких причин, важливою буде налаштована реплікація даних.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 21   |

Реплікація Active Directory — це процес синхронізації інформації каталогу між контролерами домену (DC) у середовищі Windows Server. Реплікація гарантує, що зміни, внесені до бази даних Active Directory на одному DC, поширюються на інші DC, зберігаючи узгодженість і забезпечуючи відмово стійкість.

1) Топологія реплікації: Active Directory використовує модель реплікації з кількома майстрами, де кожен контролер домену може приймати й обробляти оновлення. Топологія реплікації визначає з'єднання та шляхи для реплікації в межах домену або між кількома доменами. За замовчуванням реплікація виконується за моделлю «концентратор і спиця», де PDC діє як центральний концентратор, а інші DC підключаються до нього.

2) Партнери реплікації: контролери домену встановлюють партнерство реплікації з іншими DC. Кожен DC підтримує список партнерів реплікації, відомий як «список партнерів реплікації». Список партнерів зберігається в реєстрі та визначає DC, з яких конкретний DC отримує оновлення та яким надсилає оновлення.

3) Протоколи реплікації: реплікація Active Directory використовує два протоколи для зв'язку між контролерами домену:

a) Remote Procedure Call (RPC): це основний протокол реплікації, який використовується в Active Directory. Реплікація на основі RPC працює на інтерфейсі віддаленого виклику процедури служби реплікації каталогів (DRS) і працює через TCP/IP.

b) Простий протокол передачі пошти (SMTP): реплікація SMTP використовується в сценаріях, коли DC не може безпосередньо підключитися до іншого DC через мережеві обмеження або коли реплікація повинна відбуватися через повільне або ненадійне з'єднання. У таких випадках оновлення упаковуються як повідомлення електронної пошти та надсилаються через SMTP.

4) Процес реплікації. Реплікація Active Directory виконується за багатостадійним процесом:

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 22   |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

а) Ініціація реплікації: процес реплікації починається, коли DC виявляє, що до бази даних Active Directory внесені зміни. DC, що діє як джерело змін, називається «початковим» або «записуваним» DC.

б) Сповіщення про оновлення: Початковий DC повідомляє своїх партнерів реплікації про зміни. Це сповіщення запускає процес реплікації на партнерських DC.

в) Цикл реплікації: під час циклу реплікації DC порівнюють атрибути та об'єкти у своїх відповідних базах даних і обмінюються змінами. Процес передбачає стиснення, шифрування та спеціальні протоколи реплікації для передачі оновлень.

г) Оновлення програми: після отримання змін одержувач DC застосовує оновлення до своєї локальної бази даних, гарантуючи, що інформація каталогу залишається узгодженою.

5) Розклад реплікації: реплікація Active Directory відбувається періодично на основі попередньо визначеного розкладу реплікації. За замовчуванням інтервал реплікації становить 15 секунд для внутрішньосайтової реплікації та 180 хвилин для міжсайтової реплікації. Однак ці значення можна налаштувати відповідно до конкретних вимог.

Реплікація Active Directory відіграє важливу роль у забезпеченні узгодженості даних, відмово стійкості та високої доступності в середовищі Windows Server. Він забезпечує ефективний доступ до каталогу та підтримує такі функції, як автентифікація, авторизація та керування груповою політикою на кількох контролерах домену. [\[11\]](#)

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 23   |

### 1.3 Типові технології та протоколи побудови мережних інфраструктур

Для побудови мережної інфраструктури компанії та підключення її до мережі Інтернет застосовуються такі технології та протоколи:

- SSH
- NAT
- DHCP
- STP

Для забезпечення захисту IT-інфраструктури доцільно використовувати функції протоколу STP:

- Dynamic ARP Inspection (DAI)
- DHCP Snooping
- PortFast
- Port-security
- BPDUguard

Для реалізація віддаленого підключення до мережевих пристроїв можна використати два протоколи: Telnet та SSH. Але з боку безпеки, доцільно використовувати виключно SSH.

SSH (Secure Shell) — це криптографічний мережевий протокол, який використовується для безпечного віддаленого входу в систему, виконання команд і передачі даних через незахищену мережу. Він забезпечує безпечний спосіб доступу до віддалених систем і керування ними шляхом встановлення зашифрованого з'єднання між клієнтом і сервером.

– Шифрування: SSH використовує різні алгоритми шифрування для забезпечення конфіденційності та цілісності даних, що передаються між клієнтом і сервером. Він шифрує весь зв'язок, включаючи облікові дані автентифікації, термінальні сеанси та передачу файлів.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 24   |

– Автентифікація: SSH підтримує різні методи автентифікації, включаючи автентифікацію на основі пароля, автентифікацію з відкритим ключем та інтерактивну автентифікацію з клавіатури. Автентифікація з відкритим ключем вважається більш безпечною і широко використовується. Це передбачає створення пари ключів, що складається з закритого ключа (зберігається на клієнті) і відкритого ключа (завантажується на сервер).

– Перенаправлення портів: SSH забезпечує безпечне перенаправлення портів, що дозволяє створювати зашифровані тунелі для передачі даних між локальною та віддаленою системами. Ця функція корисна для доступу до служб у віддалених мережах, ніби вони працюють локально.

– Термінальний доступ: SSH забезпечує безпечну емуляцію терміналу, дозволяючи користувачам отримувати віддалений доступ і керувати інтерфейсом командного рядка (CLI) у віддаленій системі. Він підтримує такі функції, як віддалене виконання команд, керування сесіями та термінальне мультиплексування.

– Передача файлів: SSH включає такі утиліти, як Secure Copy (SCP) і Secure File Transfer Protocol (SFTP) для безпечної передачі файлів між локальною та віддаленою системами. Ці інструменти використовують протокол SSH для автентифікації та шифрування, забезпечуючи конфіденційність і цілісність переданих файлів.

– Пересилання X11: SSH також може безпечно пересилати графічні програми X11, дозволяючи користувачам запускати програми на основі графічного інтерфейсу користувача на віддаленій системі та відображати їх на локальній машині.

– Безпека та керування ключами: SSH надає механізми для керування доступом, включаючи керування доступом на основі користувачів, керування доступом на основі хоста та можливість обмежувати дозволи на основі IP-адрес

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 25   |

або діапазонів мережі. Ключі SSH зазвичай використовуються для автентифікації та безпечного керування доступом до віддалених систем.

SSH широко використовується для адміністрування серверів, віддаленого доступу до систем і безпечної передачі файлів. Це стало стандартним методом безпечного доступу та керування віддаленими машинами в різних середовищах, включаючи Unix-подібні системи, дистрибутиви Linux, macOS і Windows за допомогою клієнтів SSH.

На SSH-сервері запускається програма `sshd`, яка забезпечує серверну функціональність SSH. Вона приймає з'єднання від SSH-клієнтів і дозволяє їм виконувати різні дії на віддаленій системі. На SSH-клієнті запускається програма `ssh`, яка встановлює з'єднання з віддаленим сервером, аутентифікується на ньому і дозволяє користувачеві працювати з віддаленим хостом через SSH-з'єднання.

Для виконання різних операцій за допомогою протоколу SSH використовуються спеціальні команди з різними опціями. Ці команди можуть варіюватися в залежності від операційної системи та оболонки SSH-клієнта. Команди можуть бути виконані з командного рядка на UNIX-подібних системах або через графічний інтерфейс SSH-клієнта.

Отже, SSH дозволяє безпечно виконувати різні дії на віддалених системах, забезпечуючи конфіденційність та цілісність передачі даних. Він є стандартним інструментом для віддаленого доступу та управління віддаленими машинами в різних середовищах, включаючи UNIX-подібні системи, дистрибутиви Linux, macOS та Windows з використанням SSH-клієнтів. На основі даних представлених по посиланню [\[14\]](#).

Для реалізації підключення локальної мережі до мережі доцільно і необхідно використовувати протокол NAT. NAT означає трансляцію мережевих адрес. Це протокол, який використовується в комп'ютерних мережах для перетворення приватних IP-адрес у локальній мережі в публічні IP-адреси, які можна використовувати в Інтернеті та навпаки. NAT дозволяє кільком пристроям у приватній мережі спільно використовувати одну публічну IP-адресу.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 26   |

Основною метою NAT є збереження адресного простору IPv4. З вичерпанням доступних адрес IPv4 NAT став широко поширеним рішенням для розширення можливостей використання обмеженого пулу адрес IPv4.

Два основних типи NAT:

– статичний NAT: у статичному NAT створюється однозначне зіставлення між приватною IP-адресою та публічною IP-адресою. Це зіставлення налаштовується вручну та залишається незмінним, якщо його не змінить адміністратор. Статичний NAT часто використовується, коли пристрій у приватній мережі потребує надання послуг, доступних через Інтернет, наприклад веб-серверів або серверів електронної пошти;

– динамічний NAT: динамічний NAT призначає загальнодоступні IP-адреси з пулу доступних адрес за принципом «першим прийшов, першим обслужено». Коли пристрій із приватної мережі ініціює вихідне підключення до Інтернету, йому призначається тимчасова публічна IP-адреса з пулу. Це тимчасове призначення звільняється, коли сеанс закривається. Динамічний NAT дозволяє багатьом пристроям спільно використовувати обмежену кількість публічних IP-адрес.

NAT працює на мережевому рівні (рівні 3) стека протоколів TCP/IP і зазвичай реалізується в маршрутизаторах або брандмауерах. Це допомагає підвищити безпеку мережі, приховуючи внутрішні IP-адреси пристроїв за однією загальнодоступною IP-адресою, ускладнюючи зовнішнім особам прямий доступ до пристроїв у приватній мережі.

Важливо зазначити, що NAT в основному використовується з адресами IPv4. З впровадженням IPv6, який забезпечує набагато більший адресний простір, потреба в NAT зменшується. Однак NAT все ще можна використовувати в мережах IPv6 для певних цілей, наприклад для перенумерації мережі або полегшення зв'язку між мережами IPv6 і IPv4. На основі даних представлених по посиланню [\[13\]](#).

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 27   |

Для реалізації захисту мережевої інфраструктури від створення петель (від створення широкомовного шторму) доцільно використати протокол STP.

STP (Spanning Tree Protocol) — це мережевий протокол, який використовується для запобігання петлям у мережах Ethernet. Він визначається стандартом IEEE 802.1D. Метою STP є створення безпетлевої логічної топології в мережі шляхом вибіркового блокування певних надлишкових зв'язків.

Основні поняття протоколу STP:

- Bridge ID: кожен мережевий міст (комутатор), що бере участь у STP, має унікальний Bridge ID. Bridge ID – це комбінація значення пріоритету та MAC-адреси. Міст із найнижчим ідентифікатором мосту обирається кореневим мостом;

- корінний міст: Корінний міст є центральною точкою охоплюючого дерева. Усі інші мости в мережі визначають свої шляхи до кореневого мосту. Кореневий міст відповідає за підтримку топології охоплюючого дерева;

- вартість шляху: кожен міст розраховує вартість шляху для кожного зі своїх портів на основі швидкості з'єднання. Високошвидкісні зв'язки мають нижчу вартість. Вартість шляху використовується для визначення найкращого шляху для досягнення кореневого мосту;

- блоки даних протоколу мосту (BPDU): мости обмінюються повідомленнями BPDU для обміну інформацією про топологію мережі. BPDU містять таку інформацію, як ідентифікатор мосту, вартість шляху та статус порту. Мости використовують BPDU для вибору кореневого мосту та визначення портів пересилання;

- ролі портів: кожному порту мосту призначається роль на основі його стану в охоплюючому дереві. Три ролі порту: кореневий (root port), призначений (designated port) і заблокований (blocked port);

- а) кореневий порт (root port): кореневий порт — це порт на неко-реновому мосту, який має найнижчу вартість шляху для досягнення кореневого мосту;

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 28   |

б) визначений порт (designated port): призначені порти – це порти на кожному сегменті, які мають найнижчу вартість шляху для досягнення кореневого мосту. Вони спрямовують транспорт до кореневого мосту;

с) заблокований порт (blocked port): заблоковані порти – це надлишкові порти, які перебувають у стані блокування, щоб запобігти петлям. Ці порти не пересилають трафік.

– топологія охоплюючого дерева: мости використовують інформацію з BPDU для створення топології охоплюючого дерева. Топологія складається з кореневого мосту, призначених портів і заблокованих портів. Spanning Tree гарантує відсутність петель у мережі.

STP працює шляхом постійного моніторингу мережі та адаптації до змін. У разі збою з'єднання або додавання нового моста STP перераховує топологію охоплюючого дерева, щоб забезпечити роботу без циклів.

Варто зазначити, що існують варіації STP, такі як протокол швидкого зв'язуючого дерева (RSTP) і протокол кількох зв'язуючих дерев (MSTP), які забезпечують швидшу конвергенцію та підтримку кількох зв'язуючих дерев відповідно. На основі даних представлених по посиланню [\[12\]](#).

Протокол STP має достатню кількість функцій для боротьби і з атаками ззовні. Будь-то атаки на протокол ARP, протокол DHCP чи підміна MAC-адрес.

Для захисту від нападу на протокол ARP використовується функція Dynamic ARP Inspection. Dynamic ARP Inspection (DAI) є функцією, яка використовується для захисту від атак ARP-отрута (ARP poisoning) в мережах Ethernet. Вона дозволяє вам контролювати інспектувати ARP-пакети, які проходять через комутатори в мережі, та блокувати недовірені ARP-відповіді або ARP-запити.

Основна ідея застосування DAI полягає в тому, щоб виконати перевірку відповідності між IP-адресами і MAC-адресами в ARP-таблиці, яка знаходиться на комутаторі. Коли відбувається ARP-запит або ARP-відповідь, комутатор пе-

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 29   |

ревіряє, чи відповідає відповідна IP-адреса MAC-адресі, вказаному в ARP-таблиці. Якщо виявляється незбіг або відсутність запису, пакет блокується, що допомагає запобігти ARP-отруті.

Налаштування DAI може залежати від використовуваного мережевого обладнання, але основні кроки налаштування зазвичай включають наступні етапи:

1. Включення DAI на комутаторі: Зазвичай це робиться за допомогою команди або налаштуванням веб-інтерфейсу комутатора. Переконайтеся, що ваш комутатор підтримує функцію DAI та її включено.

2. Вказання довірених портів: Ви можете вказати порти, на яких очікується надійний трафік ARP, такі як порти, підключені до серверів або довірених мережевих пристроїв.

3. Визначення DHCP-сервера: Встановіть IP-адресу DHCP-сервера для довірених портів, щоб дозволити легітимний трафік ARP, пов'язаний з процесом отримання IP-адреси від DHCP-сервера.

4. Активація DAI на портах: Включіть DAI на всіх портах, на яких очікується ARP-трафік. Це вимагає перевірки ARP-пакетів, які надходять через ці порти.

5. Налаштування статичних або динамічних ARP-записів: Ви можете налаштувати статичні або динамічні ARP-записи на комутаторі для визначення дозволених IP-адрес і відповідних MAC-адрес.

6. Моніторинг і аналіз: Після встановлення DAI варто моніторити журнали подій або інші інструменти для виявлення можливих атак ARP-отрута або проблем з ARP-трафіком. [\[25\]](#)

Для захисту від нападу на протокол DHCP використовується функція DHCP Snooping. DHCP Snooping (Dynamic Host Configuration Protocol Snooping) — це функція безпеки, яка зазвичай реалізується в мережевих комутаторах для пом'якшення атак, пов'язаних з DHCP. Це допомагає захистити мережу від неавторизованих серверів DHCP і запобігає доступу зловмисних пристроїв до мережі.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 30   |

Протокол DHCP відповідає за призначення IP-адрес та інших параметрів мережевої конфігурації пристроям у мережі. Зазвичай, коли пристрій запитує IP-адресу, він транслює в мережу повідомлення про виявлення DHCP, і будь-який сервер DHCP може відповісти на запит. Однак цим можуть скористатися зломисники, які встановлюють фальшиві DHCP-сервери для розповсюдження неправильної або зломисної інформації про конфігурацію IP на пристрої, які нічого не підозрюють.

Функція DHCP Snooping перевіряє повідомлення DHCP, якими обмінюються клієнти та сервери в мережі. Ось як це зазвичай працює:

- довірені та ненадійні порти: DHCP Snooping класифікує порти комутатора на дві категорії: надійні та ненадійні. Довірені порти зазвичай підключаються до законних серверів DHCP, тоді як ненадійні порти підключаються до пристроїв кінцевого користувача. За замовчуванням усі порти є ненадійними, доки явно не налаштовано інакше;

- база даних зв'язування DHCP Snooping: комутатор підтримує базу даних зв'язування DHCP Snooping, у якій записуються зв'язки між MAC-адресами пристроїв, призначеними їм IP-адресами, інформацією про оренду та портами комутатора, через які вони підключені. Ця база даних динамічно створюється на основі повідомлень DHCP, які спостерігаються комутатором;

- DHCP Discover і DHCP Offer коли ненадійний порт отримує повідомлення DHCP Discover від пристрою, комутатор перехоплює його та позначає порт як ненадійний. Потім комутатор пересилає повідомлення DHCP Discover з усіх довірених портів. Коли законний сервер DHCP отримує повідомлення DHCP Discover, він відповідає DHCP Offer, яка містить доступну IP-адресу для клієнта;

- DHCP Request і DHCP Acknowledge: комутатор перехоплює повідомлення DHCP Offer і перевіряє, чи воно надійшло з довіреного порту. Якщо це так, комутатор оновлює свою базу даних прив'язки DHCP Snooping Binding, використовуючи зв'язок між MAC-адресою клієнта, призначеною IP-адресою та

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 31   |

портом комутатора. Потім комутатор пересилає повідомлення пропозицію DHCP назад запитуючому клієнту. Клієнт відповідає повідомленням DHCP Request, вказуючи на те, що він приймає запропоновану IP-адресу. Комутатор перехоплює повідомлення запиту DHCP і відповідно оновлює свою базу даних прив'язки. Нарешті, повідомлення про підтвердження DHCP від сервера DHCP пересилається клієнту;

– фільтрування DHCP Snooping: DHCP Snooping також виконує додаткові перевірки, щоб відфільтрувати неавторизовані повідомлення DHCP. Наприклад, він видаляє повідомлення DHCP, які надходять на ненадійні порти або мають невідповідні прив'язки MAC-IP до його бази даних. Це допомагає запобігти підробленим або зловмисним повідомленням DHCP від компрометації мережі.

Впровадивши DHCP Snooping, мережеві адміністратори можуть запобігти роботі неавторизованих DHCP-серверів у мережі та переконатися, що лише законним DHCP-серверам дозволено надавати клієнтам інформацію про конфігурацію IP. Це підвищує безпеку мережі, зменшуючи ризик конфліктів IP-адрес, викрадення IP-адреси та інших атак, пов'язаних із DHCP. [\[26\]](#)

Для прискорення роботи комутаторів можна використати функцію PortFast. Функція PortFast є однією з можливостей, яку можна використовувати на комутаторах для прискорення процесу встановлення з'єднання на портах. Вона вперше з'явилася у протоколі Spanning Tree Protocol (STP) і була розроблена для уникнення петель в мережі.

Зазвичай, коли комутатор виявляє, що порт активний, він застосовує протокол Spanning Tree Protocol для перевірки, чи не виникнуть петлі в мережі через цей порт. Цей процес може зайняти кілька секунд, протягом яких порт перебуває в стані "Blocking" або "Listening" перед тим, як перейти в стан "Learning" і "Forwarding", коли вже можна передавати дані.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 32   |

Однак, у деяких випадках, наприклад, коли ви підключаєте пристрій, який не виробляє петлі, до порту комутатора, може бути необхідно прискорити процес встановлення з'єднання. Саме для цього і використовується функція "spanning-tree portfast".

Коли на порту вмикається функція "spanning-tree portfast", комутатор припускає, що до цього порту підключений пристрій, який не виробляє петлі, і автоматично переводить порт у стан "Forwarding", минувши стани "Blocking", "Listening" і "Learning". Це дозволяє пристрою, підключеному до порта, негайно встановити з'єднання і почати передавати дані.

Важливо відмітити, що використання "spanning-tree portfast" може бути небезпечним, якщо до порту підключена мережева петля, оскільки це може призвести до нежиттєздатної станції або петельного шторму в мережі. Тому слід бути дуже обережним при використанні цієї функції і впевнитися, що до порту підключений тільки один пристрій без можливості створення петлі.

У новіших версіях протоколу Spanning Tree Protocol (RSTP або MSTP) функціональність "spanning-tree portfast" може бути розширена і покращена. Так, можуть бути використані, наприклад, режими "rapid spanning-tree portfast" або "edge port", які ще більше прискорюють процес встановлення з'єднання і забезпечують більшу надійність в умовах зміни топології мережі.

Загалом, функція "spanning-tree portfast" дозволяє прискорити процес встановлення з'єднання на портах комутатора, але її слід використовувати з обережністю і враховувати особливості конкретної мережі та підключених пристроїв. [\[24\]](#)

Для забезпечення захисту від несанкціонованому підключенню пристроїв до мережі можна використати функцію Port-security. Функція Port-security на комутаторах Cisco надає можливість налаштувати безпеку порту (port security) на конкретному порту комутатора. Ця функція дозволяє обмежити кількість MAC-адрес, які можуть бути вивчені на даному порту, і пов'язати ці MAC-адреси з інтерфейсом.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 33   |

Основна мета безпеки порту полягає у запобіганні несанкціонованому підключенню пристроїв до мережі. Якщо порт виявляє MAC-адрес, який не належить до дозволених, можна налаштувати різні дії, наприклад, вимкнути порт, зробити запис у журнал подій або відправити сповіщення адміністратору.

Основні параметри, які можна налаштувати з використанням "switchport port-security", включають:

- Максимальна кількість безпечних MAC-адрес на порту: За допомогою команди "switchport port-security maximum <кількість>" можна обмежити максимальну кількість безпечних MAC-адрес, які можуть бути вивчені на порту.

- Дія при порушенні безпеки порту: За допомогою команди "switchport port-security violation {shutdown | restrict | protect}" можна встановити дію, яка відбудеться, якщо виявлено порушення безпеки порту. Наприклад, порт може бути вимкнено (shutdown), обмежено (restrict) або захищено (protect).

- Таймер старіння безпечних MAC-адрес: За допомогою команди "switchport port-security aging {time | static}" можна встановити таймер старіння безпечних MAC-адрес на порту. Це вказує, як довго MAC-адрес залишатиметься безпечним на порту після того, як він не був виявлений.

Це лише кілька прикладів параметрів, які можна налаштувати з використанням "switchport port-security". Реальний набір параметрів може різнитися залежно від моделі комутатора і версії IOS.

Зауважте, що використання безпеки порту має сенс лише в умовах, коли ви маєте потребу в контролі доступу до мережі на рівні фізичного порту комутатора. В більш складних мережах можуть використовуватися інші методи інтегрованої безпеки, такі як 802.1X або брандмауери. [\[15\]](#)

Для захисту від утворення випадкових (чи не випадкових) петель у мережі можна використати функцію BPDUguard. Функція BPDUguard є частиною про-

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 34   |

токолу Spanning Tree Protocol (STP) і використовується в мережних комутаторах для попередження петель (loops) у мережі. BPDU (Bridge Protocol Data Units) є повідомленнями, які комутатори використовують для обміну даними про STP.

Коли функція "spanning-tree bpduguard enable" активована на порту комутатора, вона вимикає порт, якщо він отримує BPDU від іншого комутатора. Це робиться для того, щоб запобігти виникненню петель в мережі через неправильне підключення комутаторів або недоуправління STP.

Основна ідея застосування "spanning-tree bpduguard enable" полягає в тому, що порт, на якому відбувається отримання BPDU, найімовірніше підключений до іншого комутатора. Це може стати наслідком помилкового підключення або наміреного втручання в мережу. У будь-якому разі, активація bpduguard на цьому порті призводить до його вимикання для запобігання можливих проблем, пов'язаних з петлями.

Коли порт комутатора переведено в стан вимкнено (errdisabled) через виявлення BPDU, адміністратор мережі повинен розібратися в причинах і виправити проблему перед активацією порту знову. Це може включати перевірку правильності підключення комутаторів, перевірку конфігурації STP і виконання необхідних коригуючих дій.

Застосування "spanning-tree bpduguard enable" є корисним для захисту мережі від петель і неправильних підключень комутаторів, але важливо правильно налаштувати і керувати протоколом STP в мережі, щоб уникнути непередбачуваних проблем зі з'єднанням. [\[27,28\]](#)

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 35   |

## 1.4 Аналіз типових атак на мережну інфраструктуру та типові рекомендації щодо їх послаблення

На даний момент є багато відомих способів атаки на мережну інфраструктуру, атаки на протоколи ARP, DHCP та інші. Тому потрібно проаналізувати можливі атаки на мережу і сформувані типові рекомендації щодо їх послаблення. Почнемо з формування списку можливих атак на мережну інфраструктуру.

- ARP Poisoning
- DHCP spoofing
- DNS spoofing
- Brute Force Attack
- Man-in-the-Middle attack

Атакою направленою на протокол ARP є ARP poisoning. ARP poisoning, також відоме як ARP spoofing, — це тип мережевої атаки, коли зломисник надсилає фальсифіковані повідомлення протоколу розпізнавання адрес (ARP) через локальну мережу (LAN). Метою отруєння ARP є пов'язування MAC-адреси (Media Access Control) зломисника з IP-адресою іншого мережевого пристрою, наприклад маршрутизатора або комп'ютера жертви. Таким чином зломисник може перехоплювати, змінювати або перенаправляти мережевий трафік між цільовими пристроями.

Існує кілька профілактичних заходів для захисту від атак ARP spoofing.

1. Використовуйте інструменти виявлення підробки ARP: розгортання інструментів виявлення ARP може допомогти виявити будь-які підозрілі або неавторизовані зміни в кеші ARP. Ці інструменти можуть сповіщати мережевих адміністраторів про виявлення підробки ARP, дозволяючи їм вжити відповідних заходів.

2. Впроваджуйте безпечні мережеві протоколи: щоб зменшити ризик отруєння ARP, рекомендується використовувати безпечні мережеві протоколи,

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 36   |

такі як Secure Sockets Layer (SSL) або Transport Layer Security (TLS). Ці протоколи шифрують мережевий трафік, що ускладнює зломисникам перехоплення чи маніпулювання даними.

3. Увімкнути port security: більшість мережевих комутаторів пропонують функції безпеки портів, які можна увімкнути, щоб обмежити кількість MAC-адрес, дозволених на певному порту. Встановивши відповідний ліміт, ви можете запобігти підключенню зломисниками несанкціонованих пристроїв до мережі.

4. Використовуйте статичні записи таблиці ARP: налаштування статичних записів таблиці ARP вручну може забезпечити додатковий рівень захисту від атак ARP spoofing. Явно вказуючи MAC-адресу, пов'язану з кожною IP-адресою, ви гарантуєте, що система спілкується лише з призначеними пристроями.

5. Запровадження сегментації мережі: поділ вашої мережі на менші сегменти або VLAN (віртуальні локальні мережі) може допомогти стримати вплив атак ARP spoofing. Якщо зломиснику вдасться отруїти кеш ARP в одному сегменті, йому буде важче вплинути на пристрої в інших сегментах.

6. Використовуйте системи виявлення вторгнень у мережу (NIDS): розгортання NIDS може допомогти виявити й попередити вас про потенційні атаки ARP spoofing. Ці системи аналізують шаблони мережевого трафіку та можуть ідентифікувати аномалії, що вказують на спроби отруєння ARP.

7. Регулярно оновлюйте та виправляйте системи. Підтримуйте актуальні операційні системи, мережеві пристрої та програмне забезпечення безпеки вкрай важливо. Виробники часто випускають патчі безпеки та оновлення для усунення вразливостей, які зломисники можуть використовувати для підробки ARP або інших атак.

8. Навчайте користувачів: проводите регулярні навчальні сеанси з питань безпеки, щоб навчити користувачів ризикам, пов'язаним із підробкою ARP, а також тому, як виявляти підозрілу мережеву активність і повідомляти

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 37   |

про неї. Заохочуйте користувачів перевіряти автентичність мережевих пристроїв перед підключенням до них.

9. Використовуйте надійну мережеву автентифікацію: впровадження надійних механізмів автентифікації, наприклад використання WPA2-Enterprise або WPA3 для мереж Wi-Fi, може запобігти підключенню неавторизованих пристроїв до вашої мережі. Ці протоколи вимагають від користувачів надання індивідуальних облікових даних, що ускладнює зловмисникам підробку ARP.

10. Увімкніть функції безпеки портів на комутаторах: багато мережевих комутаторів пропонують такі функції, як Dynamic ARP Inspection (DAI) або IP Source Guard, які можуть перевіряти пакети ARP перед їх пересиланням. Ці функції допомагають гарантувати, що дозволені лише дійсні пакети ARP, запобігаючи успішному виконанню атак ARP spoofing.

11. Запровадження моніторингу та журналювання мережі: регулярно відстежуйте мережевий трафік і ведіть докладні журнали активності ARP. Інструменти моніторингу та аналіз журналів можуть допомогти вам виявити та дослідити будь-яку незвичайну або підозрілу поведінку ARP, дозволяючи вжити негайних заходів.

12. Використовуйте шифрування та автентифікацію на вищих рівнях мережі: окрім захисту нижчих рівнів мережі, впровадження шифрування та автентифікації на вищих рівнях, наприклад використання HTTPS для веб-трафіку та цифрових сертифікатів для автентифікації пристрою, додає ще один рівень захисту від атак ARP spoofing.

13. Увімкнути захищений протокол розпізнавання адрес (ARPsec): ARPsec — це розширення традиційного протоколу ARP, яке додає функції безпеки. Він забезпечує перевірку цілісності та автентичності повідомлень ARP, що ускладнює зловмисникам підробку пакетів ARP.

14. Запровадження контролю доступу до мережі: рішення контролю доступу до мережі (NAC) можуть застосовувати політики, щоб гарантувати, що лише авторизованим і сумісним пристроям дозволено підключатися до вашої мережі. Системи NAC можуть виконувати перевірку працездатності пристроїв

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 38   |

перед наданням їм доступу до мережі, зменшуючи ризик підробки ARP неавторизованими пристроями.

15. Регулярно відстежуйте та оновлюйте мережеві пристрої: постійно оновлюйте маршрутизатори, комутатори та інші мережеві пристрої за допомогою останніх оновлень мікропрограми або програмного забезпечення, наданих виробниками. Ці оновлення часто включають виправлення безпеки, які усувають уразливості, які можуть бути використані для атак ARP spoofing.

Пам'ятайте, що впровадження кількох рівнів безпеки та застосування підходу до поглибленого захисту може значно посилити стійкість вашої мережі проти атак ARP spoofing. Регулярні перевірки безпеки, тестування на проникнення та отримання інформації про нові загрози безпеці також допоможуть вам бути на крок попереду потенційних злоумисників. [\[16,17\]](#)

Атакою направленою на протокол DHCP є атака DHCP spoofing. DHCP spoofing — це тип мережевої атаки, коли злоумисник видає себе за сервер DHCP (Dynamic Host Configuration Protocol) у локальній мережі. DHCP — це протокол, який використовується для призначення IP-адрес і параметрів мережевої конфігурації пристроям у мережі.

У типовій атаці DHCP spoofing злоумисник надсилає фальшиві повідомлення DHCP у мережу, пропонуючи IP-адреси та інформацію про конфігурацію мережі нічого не підозрюючим пристроям. Таким чином злоумисник може перехоплювати мережевий трафік, перенаправляти його у свою власну систему та потенційно здійснювати різні злоумисні дії, такі як підслуховування, захоплення сесії або запуск подальших атак.

Ось спрощене пояснення того, як працює DHCP spoofing:

- виявлення DHCP: коли пристрій приєднується до мережі, він транслює повідомлення виявлення DHCP із запитом IP-адреси;
- підроблений DHCP-сервер: злоумисник встановлює підроблений DHCP-сервер у мережі або зламає існуючий DHCP-сервер;

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 39   |

- шахрайська пропозиція DHCP: зломисник відповідає на повідомлення про виявлення DHCP, надсилаючи DHCP Offer на запитуючий пристрій, пропонуючи IP-адресу та інші параметри конфігурації мережі;
- конфігурація пристрою: нічого не підозрюючий пристрій отримує фальшивий DHCP Offer і приймає її, припускаючи, що це законна відповідь від сервера DHCP;
- перенаправлення мережевого трафіку: тепер зломисник контролює IP-адресу пристрою та конфігурацію мережі. Вони можуть перенаправляти мережевий трафік на свою власну систему, діючи як людина посередині, перехоплюючи зв'язок між пристроєм та іншими системами в мережі.

Щоб захиститися від атак DHCP spoofing, адміністратори мережі можуть застосувати такі заходи:

1. DHCP Snooping: увімкніть DHCP Snooping на мережевих комутаторах, щоб перевіряти повідомлення DHCP і переконатися, що лише авторизовані сервери DHCP можуть надавати IP-адреси.
2. Автентифікація DHCP-сервера: налаштуйте автентифікацію DHCP-сервера за допомогою таких механізмів, як DHCPv4-Shield або DHCPv6-Shield, які дозволяють лише надійним серверам відповідати на запити DHCP.
3. Безпека порту: застосуйте функції безпеки порту, такі як прив'язка MAC-адреси або обмеження кількості запитів DHCP на порт, щоб обмежити підключення неавторизованих пристроїв до мережі.
4. Моніторинг мережі. Регулярно перевіряйте мережевий трафік на наявність ненормальної поведінки DHCP або неавторизованих серверів DHCP.
5. Сегментація VLAN: реалізуйте VLAN (віртуальні локальні мережі), щоб розділити мережевий трафік і запобігти впливу фальшивих серверів DHCP на всю мережу.

Впроваджуючи ці заходи безпеки, організації можуть значно знизити ризик атак підробки DHCP і підвищити загальну безпеку своєї мережевої інфраструктури. [\[18,19\]](#)

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 40   |

Атакою направленою на протокол DNS є атака DNS spoofing. DNS spoofing – це тип кібератаки, коли зловмисник маніпулює системою доменних імен (DNS), щоб переспрямувати мережевий трафік до зловмисного пункту призначення. DNS відповідає за переклад зрозумілих для людини доменних імен (наприклад, example.com) в IP-адреси (наприклад, 192.0.2.1), які комп'ютери використовують для обміну даними через Інтернет.

Під час атаки DNS spoofing зловмисник надсилає підроблені відповіді DNS на цільовий комп'ютер або мережу, змушуючи його повірити, що IP-адреса, пов'язана з певним доменним іменем, змінилася. У результаті, коли користувачі намагаються отримати доступ до законного веб-сайту, їхні запити пере-направляються на шкідливий веб-сайт, контрольований зловмисником, без їх відома.

Підробка DNS може використовуватися для різних зловмисних цілей, наприклад:

- фішинг: зловмисник може перенаправляти користувачів на підроблені веб-сайти, схожі на законні, щоб викрасти конфіденційну інформацію, як-от імена користувачів, паролі або фінансові дані;
- атаки «людина посередині» (MITM): контролюючи відповіді DNS, зловмисник може перехоплювати мережевий трафік між двома сторонами, дозволяючи їм підслуховувати, змінювати або впроваджувати шкідливий вміст у спілкування;
- відмова в обслуговуванні (DoS): DNS spoofing можна використовувати для перенаправлення законного трафіку на цільовий сервер, переповнюючи його потоком запитів і викликаючи стан відмови в обслуговуванні.

Щоб зменшити ризик підробки DNS, можна вжити різноманітних заходів, наприклад:

- DNSSEC (розширення безпеки системи доменних імен): DNSSEC — це розширення безпеки DNS, яке забезпечує автентифікацію та цілісність відповідей DNS, що ускладнює зловмисникам підробку даних DNS;

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В      |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 41   |

- суворі методи безпеки мережі: використання брандмауерів, систем виявлення вторгнень та інших заходів безпеки може допомогти виявити та запобігти спробам підробки DNS;
- регулярні оновлення програмного забезпечення: Оновлення програмного забезпечення DNS і мережевих пристроїв допомагає захистити від відомих вразливостей, якими можуть скористатися зловмисники;
- моніторинг DNS і виявлення аномалій: моніторинг моделей трафіку DNS і виявлення будь-яких незвичних або підозрілих дій може допомогти виявити потенційні спроби підробки.

Важливо залишатися пильними та проявляти обережність під час перегляду веб-сторінок, особливо під час введення конфіденційної інформації або доступу до веб-сайтів, які потребують автентифікації. [\[20,21\]](#)

Також є вірогідність використання Brute Force Attack для отримання доступу до мережі. Атака грубою силою (Brute Force Attack) — це метод, який використовують зловмисники для отримання неавторизованого доступу до системи або зашифрованих даних шляхом систематичного випробовування всіх можливих комбінацій паролів або ключів шифрування, доки не буде знайдено правильний. Це простий і вичерпний підхід, який покладається на обчислювальну потужність зловмисника та час, необхідний для випробування кожної можливості.

Процес зазвичай включає автоматизоване програмне забезпечення або сценарії, які швидко генерують і тестують численні комбінації. Атаки грубою силою можуть бути застосовані до різних механізмів безпеки, включаючи облікові записи, захищені паролем, алгоритми шифрування або криптографічні ключі.

Ефективність атаки грубої сили залежить від таких факторів, як складність і довжина пароля або ключа шифрування, обчислювальної потужності, до-

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 42   |

ступної зловмиснику, і заходів безпеки, які застосовуються для виявлення та запобігання таким атакам. Надійніші паролі або довші ключі шифрування з великим простором пошуку значно ускладнюють підбір і забирають багато часу.

Щоб захиститися від атак грубої сили, системні адміністратори можуть застосувати кілька заходів.

- Застосовуйте надійні паролі: заохочуйте користувачів вибирати складні паролі, які містять комбінацію літер (як великих, так і малих), цифр і спеціальних символів. Крім того, дотримуйтеся вимог до довжини пароля.

- Політика блокування облікових записів: реалізуйте механізми, які блокують облікові записи користувачів після певної кількості невдалих спроб входу, запобігаючи подальшим спробам грубої сили.

- Обмеження швидкості: реалізуйте механізми обмеження швидкості, які обмежують кількість спроб входу в одиницю часу, ускладнюючи зловмисникам автоматизацію спроб грубої сили.

- Двофакторна автентифікація (2FA): вимагайте від користувачів надання другої форми автентифікації, наприклад унікального коду, надісланого на їх мобільний пристрій, на додаток до пароля. Це додає додатковий рівень безпеки, роблячи атаки грубою силою більш складними.

- Системи виявлення вторгнень (IDS): розгорніть інструменти IDS, які можуть виявляти та сповіщати адміністраторів про численні невдалі спроби входу або підозрілу активність, що дозволяє своєчасно реагувати.

- Тести Captcha або виклик-відповідь: впровадження Captcha або механізмів виклик-відповідь може відрізнити користувачів-людей від автоматизованих сценаріїв, таким чином запобігаючи або сповільнюючи атаки грубої сили.

Впроваджуючи ці профілактичні заходи, організації можуть значно знизити ризик успішних атак грубої сили (Brute Force) та підвищити загальну безпеку своїх систем. [\[22\]](#)

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 43   |

Не варто виключати ймовірність перехоплення зв'язку між сторонами, така атака має назву Man-in-the-Middle. Man-in-the-Middle (MitM) відноситься до типу кібератаки, коли зловмисник перехоплює та потенційно змінює зв'язок між двома сторонами без їх відома. Зловмисник займає позицію між відправником і одержувачем, дозволяючи їм підслуховувати спілкування та потенційно маніпулювати даними, що передаються.

Спрощене пояснення того, як працює атака Man-in-the-Middle.

- Початкове спілкування: допустимо, Аліса хоче поспілкуватися з Бобом. Зазвичай дані Аліси надходять безпосередньо до Боба.
- Перехоплення зловмисника: зловмисник, Єва, стає між Алісою та Бобом. Дані Аліси перехоплює Єва, яка тепер контролює канал зв'язку.
- Видача себе за іншу особу: Єва може видати себе за Алісу для Боба, а Боб за Алісу, змушуючи їх повірити, що вони спілкуються безпосередньо один з одним. Цього можна досягти за допомогою різних методів, таких як підробка цифрових сертифікатів або маніпулювання параметрами мережі.
- Моніторинг і зміна: Єва може стежити за спілкуванням між Алісою та Бобом, перехоплювати повідомлення, читати їхній вміст і, можливо, змінювати дані, що передаються.
- Передача повідомлень: Єва передає повідомлення між Алісою та Бобом, створюючи враження, ніби вони спілкуються один з одним напряму. Це дозволяє Єві контролювати потік інформації, потенційно вводячи шкідливий вміст або змінюючи повідомлення.
- Необізнаність: Аліса та Боб зазвичай не знають, що їх спілкування зламано. Вони вірять, що безпечно спілкуються один з одним, тоді як насправді їхні повідомлення перехоплюються та маніпулюються Євою.

Атаки Man-in-the-Middle можуть відбуватися в різних контекстах, зокрема через незахищені мережі Wi-Fi, скомпрометовану мережеву інфраструктуру або через шкідливе програмне забезпечення, встановлене на пристроях

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 44   |

жертв. Наслідки можуть бути серйозними: від крадіжки конфіденційної інформації (наприклад, облікових даних або фінансових даних) до неавторизованого доступу до систем або подальшого використання.

Щоб зменшити ризик атак типу «людина посередині», важливо використовувати безпечні канали зв'язку, наприклад зашифровані протоколи (наприклад, HTTPS), і переконатися, що пристрої та програмне забезпечення регулярно оновлюються останніми виправленнями безпеки. Крім того, користувачам слід бути обережними, підключаючись до загальнодоступних мереж Wi-Fi, і розглянути можливість використання віртуальних приватних мереж (VPN) для додаткового рівня безпеки. [\[23\]](#)

## **1.5 Постановка технічного завдання на розробку проекту захищеної IT-інфраструктури компанії**

### **1. Огляд проекту**

Мета проекту - розробити захищену IT-інфраструктуру компанії на базі рішень Microsoft Active Directory. Проект має на меті забезпечити безпеку та стійкість роботи компанії та її клієнтів, зменшити ризики витоку конфіденційної інформації та відновити доступ до даних у разі непередбачуваних ситуацій.

### **2. Вимоги до системи**

#### **2.1 Функціональні вимоги**

- Забезпечення автентифікації користувачів у системі
- Забезпечення авторизації користувачів у системі
- Захист конфіденційної інформації
- Моніторинг доступу до системи
- Забезпечення резервного копіювання даних
- Відновлення доступу до даних у разі непередбачуваних ситуацій

#### **2.2 Нефункціональні вимоги**

- Безпека: система повинна бути забезпечена високим рівнем безпеки, забезпечити захист конфіденційної інформації, мінімізувати

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 45   |

ризика витоку інформації, відновлювати доступ до даних у разі витоку інформації

- Доступність: система повинна бути доступною в будь-який момент часу, забезпечити безперебійну роботу системи, відновлювати доступ до даних у разі виникнення технічних проблем
- Швидкодія: система повинна бути швидкою та ефективною, забезпечити максимальну продуктивність та швидкість роботи системи
- Масштабованість: система повинна бути готовою до масштабування, забезпечити зручну інтеграцію з новими технологіями та засобами забезпечення безпеки.

### 3. Архітектура системи

Система буде базуватися на рішеннях Microsoft Active Directory. В реалізації дозволяється використання будь-яких додаткових технологій для підвищення надійності системи.

**Висновки:** у першому розділі були проведені теоретичні дослідження необхідних для побудови мережі технологій, згідно теми дипломної роботи було сформовано технічне завдання, яке формує необхідні вимоги для майбутньої мережі.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 46   |

## РОЗДІЛ 2 ПРОЕКТУВАННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ КОМПАНІЇ

### 2.1 Проектування топології мережі

Для ІТ-інфраструктури компанії була розроблена топологія захищеної мережі, при проектуванні зверталася увага на наступні моменти:

- Розробка ведеться локальної мережі
- Необхідне з'єднання з мережею інтернет
- Мережа має бути масштабованою, підтримувати підключення нових пристроїв
- Мережа має підтримувати великий обсяг обладнання, немає прив'язки до конкретного виробника

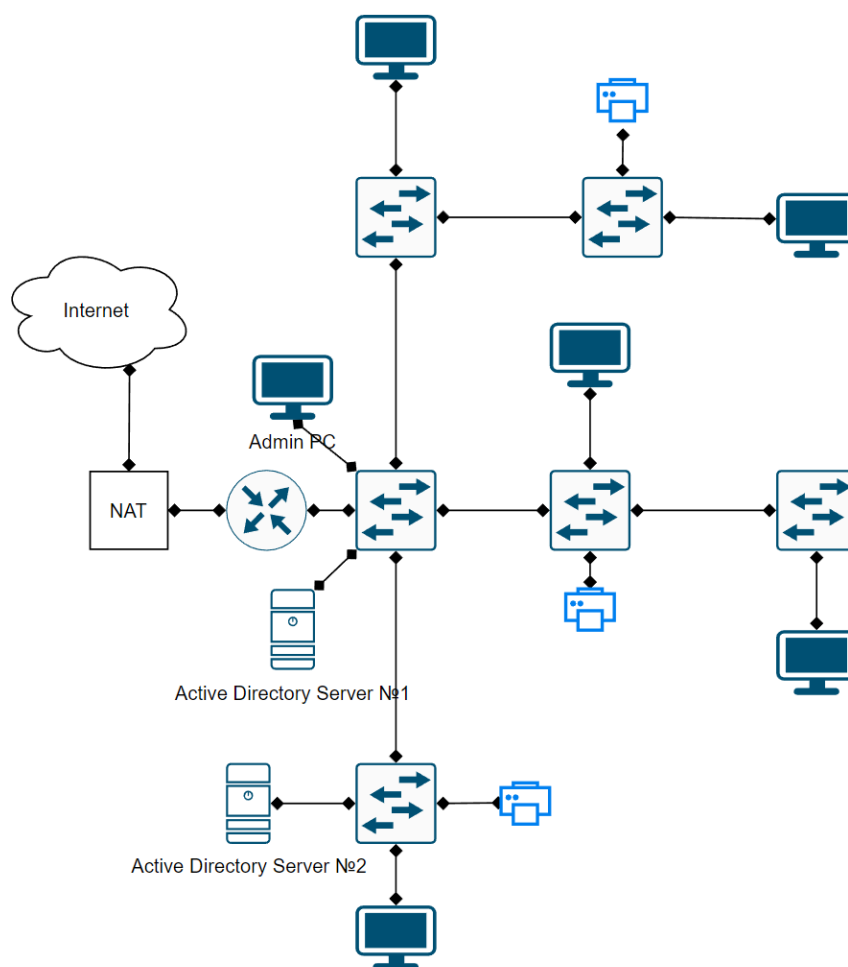


Рисунок 2.1 – Загальна топологія мережі

Спроектowana мережа представлена на рисунку 2.1. Дана мережа складається з 1 маршрутизатора, 6 комутаторів з можливістю розширення, 2 серверів і довільної кількості кінцевих пристроїв, наявність певної кількості кінцевих пристроїв на топології мережі не говорить за їх реальну кількість. Кінцева створена мережа представлена у додатку [A].

З'єднання між пристроями виконано за допомогою виті пари Gigabit Ethernet та виті пари Fast Ethernet (в теорії, на практиці в GNS3 доступний тільки Ethernet, дане уточнення актуально для всіх з'єднань Gigabit Ethernet та Fast Ethernet).

Особливістю з'єднань комутаційного обладнання є те, що для забезпечення високої продуктивності роботи мережі використовуються високошвидкісні лінії зв'язку Gigabit Ethernet та Fast Ethernet. Кінцеві вузли під'єднанні до комутаційного обладнання за допомогою ліній Fast Ethernet на витій парі.

Отримання адрес для кінцевих вузлів передбачено протоколом DHCP. Для мережевих пристроїв, серверів і мережевих принтерів передбачено використання статично визначених адрес. Передбачено виконання віддаленого підключення до мережевих пристроїв за допомогою протоколу SSH. Для виконання авторизації на мережевих пристроях використовуються протокол RADIUS, що є складовою Active Directory, для виконання підключення буде визначений локальний користувач, у разі недоступності RADIUS серверу, в основному підключення буде виконуватися за допомогою створено користувача-адміністратора на сервері AD.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 48   |

## 2.2 Розробка схеми адресації комунікаційних пристроїв та кінцевих вузлів мережі

Як наведено вище, для більшості пристроїв IP адреса буде призначатися автоматично, але все рівно мережа має велику кількість пристроїв, які потребують статично призначені IP адреси. Розрахунки приведені нижче:

Таблиця 2.1 – Інформація про мережу

| Призначення                         | IP-адреса                   |
|-------------------------------------|-----------------------------|
| Мережева адреса:                    | 192.168.0.0                 |
| Використовуваний діапазон IP адрес: | 192.168.0.1 - 192.168.0.254 |
| Широкомовна адреса:                 | 192.168.0.255               |
| Загальна кількість хостів:          | 256                         |
| Кількість доступних хостів:         | 254                         |
| Маска підмережі:                    | 255.255.255.0               |
| Обернена маска:                     | 0.0.0.255                   |
| Шлюз по замовчуванню                | 192.168.0.1                 |
| Діапазон адрес комутаторів          | 192.168.0.2-192.168.0.7     |
| Діапазон адрес серверів             | 192.168.0.8-192.168.0.9     |
| Вільний діапазон IP адрес           | 192.168.0.10-192.168.0.99   |
| Діапазон адрес робочих станцій      | DHCP                        |

У таблиці 2.1 проведений розподіл IP адрес для усіх мережевих пристроїв, адреса шлюзу за замовчуванням є адреса маршрутизатору, адреси серверів є адреси DNS серверів, вільний діапазон виділений для налаштування статичних IP адрес, усі інші IP адреси виділені під протокол DHCP.

Таблиця 2.2 – Параметри IP-адресації мережі

| Мережа/<br>Пристрій   | Інтерфейс/Мереж-<br>ний адаптер/Шлюз | IP-адреса   | Маска         | /   |
|-----------------------|--------------------------------------|-------------|---------------|-----|
| Dob.net               |                                      | 192.168.0.0 | 255.255.255.0 | /24 |
| LAN_A                 |                                      | 10.1.1.0    | 255.255.255.0 | /24 |
| Маршрутиза-<br>тор R1 | Інтерфейс E0/0                       | DHCP        |               |     |
|                       | Інтерфейс E0/1                       | 10.1.1.254  | 255.255.255.0 | /24 |
| Маршрутиза-<br>тор R2 | Інтерфейс E0/0                       | 10.1.1.1    | 255.255.255.0 | /24 |
|                       | Інтерфейс E0/1                       | 192.168.0.1 | 255.255.255.0 | /24 |
| Комутатор<br>SW1      | Інтерфейс Vlan 1                     | 192.168.0.2 | 255.255.255.0 | /24 |
|                       | Шлюз за замовчу-<br>ванням           | 192.168.0.1 | -             | -   |

| Мережа/<br>Пристрій | Інтерфейс/Мереж-<br>ний адаптер/Шлюз | ІР-адреса    | Маска         | /   |
|---------------------|--------------------------------------|--------------|---------------|-----|
| Комутатор<br>SW2    | Інтерфейс Vlan 1                     | 192.168.0.3  | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           |              |               |     |
| Комутатор<br>SW3    | Інтерфейс Vlan 1                     | 192.168.0.4  | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           | 192.168.0.1  | -             | -   |
| Комутатор<br>SW4    | Інтерфейс Vlan 1                     | 192.168.0.5  | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           | 192.168.0.1  | -             | -   |
| Комутатор<br>SW5    | Інтерфейс Vlan 1                     | 192.168.0.6  | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           | 192.168.0.1  | -             | -   |
| Комутатор<br>SW6    | Інтерфейс Vlan 1                     | 192.168.0.7  | 255.255.255.0 | /24 |
|                     | Шлюз за замовчу-<br>ванням           | 192.168.0.1  | -             | -   |
| DomainServer-1      | Інтерфейс E0/0                       | 192.168.0.8  | 255.255.255.0 | /24 |
| DomainServer-2      | Інтерфейс E0/0                       | 192.168.0.9  | 255.255.255.0 | /24 |
| AdminPC             | Інтерфейс E0/0                       | 192.168.0.25 | 255.255.255.0 | /24 |

В таблицю адресації внесені лише статичні ІР адреси, усі робочі станції отримують адресу за допомогою DHCP.

### 2.3 Проектування схеми користувачів служби каталогів Microsoft Active Directory

Для коректної роботи системи існує необхідність створення користувачів і розмежування прав для цих користувачів. При розробці системи користувачів потрібно враховувати, що організація має 3 окремих департаментів, працівники яких не має доступу до іншого департаменту. Врахувати, що мережа має бути адміністрована, тому необхідно створити аккаунти адміністраторів з різним рівнем доступу і привілегій. Також необхідно врахувати, що організація має керівний склад, як для департаментів, так і над системою департаментів.

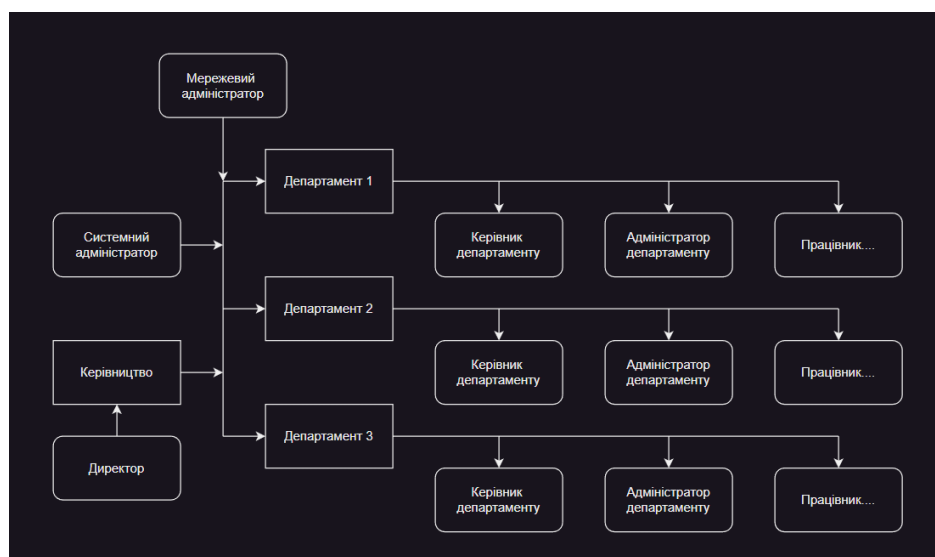


Рисунок 2.2 – Структура організації

Організація має 3 департаменти і керівництво у вигляді директора і заступників директора, заступники директора є керівниками відділів. Також є склад адміністраторів різних рівнів, адміністратор може бути один або декілька, але адміністрування буде виконуватися за допомогою облікових записів адміністраторів різних рівнів доступу. Використання різних записів адміністраторів допоможе ефективно поділити зону обов'язків адміністраторів і підвищити рівень безпеки мережі. В разі втрати облікового запису адміністратора або його взлому злоумисник буде мати обмежену кількість можливостей, і це дозволить оперативно зреагувати на дану ситуацію і провести оперативні дії. Повна система користувачів представлена у додатку [Б].

Таблиця 2.3 – Розмежування прав адміністраторів

|                     | Адміністратор департаменту | Мережевий адміністратор | Системний адміністратор |
|---------------------|----------------------------|-------------------------|-------------------------|
| Власний департамент | +                          | -                       | +                       |
| Інший департамент   | -                          | -                       | +                       |
| Мережеві пристрої   | -                          | +                       | -                       |
| Керівництво         | -                          | -                       | +                       |

У мережі є лише один адміністратор з повним доступом до мережі і з максимальними повноваженнями. До цього облікового запису використовуються особливі вимоги до безпеки, одна з них: пароль з більшою кількістю символів і

використання різних символів, що значно підвищить час на підбор пароллю і використання спроб на введення пароллю, що зробить підбор пароллю майже неможливим. Адміністратор департаменту має повний доступ до робочих станцій свого департаменту. Мережевий адміністратор має доступ лише до мережевих пристроїв і має можливість підключення до них через SSHv2.0. Повна система розмежування доступу представлена у додатку [В].

Таблиця 2.4 – Розмежування доступу користувачів

|                          | Власний<br>департамент | Інший<br>департамент | Керівництво |
|--------------------------|------------------------|----------------------|-------------|
| Працівник                | +                      | -                    | -           |
| Керівник<br>департаменту | +                      | -                    | -           |
| Директор                 | +                      | +                    | +           |

Таблиця не повна, тому вважаю що необхідні додаткові пояснення. Працівник має доступу лише до своєї робочої станції, за замовчуванням, і не має доступу до інших навіть у своєму департаменті. Керівник департаменту має доступ до всіх робочих станцій свого департаменту. Директор має повний доступ до робочих станцій свого департаменту. У мережі реалізовано використання служби віддаленого робочого столу, тому важливо зауважити, керівники департаменту також входять до керівництва, тому за потреби директор, в процесі роботи, зможе отримати доступ до всіх робочих станцій, звісно якщо вони увімкнуті.

## 2.4 Обґрунтування та вибір мережних технологій та функціоналу Active Directory для побудови IT-інфраструктури компанії

Для створення захищеної корпоративної мережі недостатньо лише налаштувати IP-адресацію. Для комфортної і безпечної роботи мережі необхідно реалізувати мережеві технології і відповідний функціонал AD.

Для створення мережі будуть використані відповідний функціонал контролера домену:

- Служба віддаленого робочого столу
- Служба спільного принтеру
- DNS сервер
- Використання квот
- Використання групових політик
- Налаштування RADIUS-серверу
- Реплікацію даних

Для підвищення ефективності робочого процесу буде реалізовано службу віддаленого доступу до різних вузлів у мережі. Говорячи про MS Active Directory, буде використана служба RDS, а для мережевих пристроїв протокол SSHv2.

Для підвищення зручності друкування та економії ресурсів буде реалізовано службу спільного принтеру. Встановлення спільного принтеру значно підвищить якість роботи так як встановлення і налаштування драйверів. У мережі буде реалізовано 3 принтери, 3 з яких однакові і іншої моделі. Кожен департамент матиме свій принтер і директор матиме свій принтер. Кожен департамент матиме доступ лише до свого принтеру і директор матиме доступ лише до свого принтера. Такі обмеження передбачають неприємні ситуації в майбутньому.

Використання DNS серверу підвищить рівень зручності використання та адміністрування мережі. Контролер домену має свій DNS сервер. Його можна використати для спрощення роботи у мережі. А саме звільнити від необхідності

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 53   |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

запам'ятовувати IP-адресу пристрою, а використовувати його назву або кодове ім'я.

DNS-запити будуть налаштовані для мережевих пристроїв, таким чином підвищиться зручність адміністрування мережевих пристроїв.

Для ефективного використання об'єму накопичувача буде використаний механізм квотування. Квотування буде налаштовано лише для одного департаменту. Даний департамент буде працювати лише з текстовими файлами, тому великий об'єм пам'яті не є необхідністю, а налаштоване квотування дасть можливість ефективно розподілити місце між усіма користувачами на робочій станції.

Квотування буде налаштовано для третього департаменту. Кожен користувач матиме 10 Gb для себе. Цього об'єму досить для виконання текстової роботи. Це обмеження буде використано для усі співробітників департаменту, окрім керівника та адміністратора.

Головним інструментом для створення та застосування обмежень у доменні Active Directory виступають групові політики, тому їх використання є необхідним для обмеження та розподілення доступу до різних організаційних одиниць. Групові політики є основною для більшості функціоналу MS Active Directory. Реалізація віддаленого підключення, квотування, можливістю авторизації все налаштовується за допомогою групових політик.

Для домену будуть створені декілька групових політик, одна з них глобальна. Глобальна групова політика буде регулювати базові процеси, буде встановлювати мінімальну кількість символів в паролі. Також будуть налаштовані додаткові групові політики для кожного департаменту. Вони будуть надавати різний рівень доступу для користувачів, обмежувати доступ до інших департаментів, обмежувати доступ до робочих станцій керівників відділів та адміністраторів.

Для стабільної роботи мережі необхідно замислитися: "Що буде, якщо один з контролерів домену вийде з ладу?", якщо він один то робота цілої орга-

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 54   |

нізації зупиниться, тому необхідно створити ще один контролер домену та налаштувати реплікацію даних між ними. Після цього, коли один з контролерів домену вийде з ладу, то мережа може продовжити роботу.

Для безпечної створення мережі необхідно використати відповідні мережеві технології, ці технології повинні забезпечити безперебійну роботу мережі і надати необхідний рівень захисту.

У мережі будуть використані такі технології:

- DHCP
- NAT
- NTP
- SYSLOG
- STP

На сьогоднішній день кожна локальна мережа не є закритою, вона має підключення до мережі Інтернет, тому існує необхідність налаштування підключення до інтернету. Створена мережа реалізована у GNS3 – це накладає деякі особливості в реалізації, тому уявляємо, що мережа підключена до комутатора провайдера і отримує адресу через DHCP. За допомогою цієї адреси можливе підключення до мережі інтернет, але тільки з одного пристрою, тому необхідна реалізація NAT, а саме динамічний NAT. Використання динамічного NAT, обумовлено простотою налаштування, налаштувати статичний NAT для усіх вузлів не проста задача.



Рисунок 2.3 – Реалізація протоколу NAT

Для реалізації підключення за допомогою NAT буде використано 2 маршрутизатори, маршрутизатор R1 отримає адресу за допомогою протоколу DHCP і даний інтерфейс є NAT outside, а інтерфейс підключений до маршрутизатору R2 має NAT inside.

У мережі повинна бути реалізована динамічна роздача IP-адрес за допомогою протоколу DHCP. Це значно спростить користування мережею і дозволить зручно підключати нові пристрої до мережі. Для даної мережі є, як мінімум, дві можливі реалізації використання протоколу DHCP, можливо роздавати IP-адреси з маршрутизатору або з контролеру домену. Буде використаний перший варіант реалізації, роздачою IP-адрес буде займатися маршрутизатор R2. Таким чином розподіли інфраструктуру на мережеву ( маршрутизатори, комутатори) та домену ( контролери домену, робочі станції та принтери).

Для забезпечення безперервної роботи мережі існує суттєва необхідність в логуванні подій. Збереження записів о подіях, які відбуваються у мережі є важливим для підтримання працездатності мережі. Саме записи допоможуть адміністратору мережі дізнатися про помилки, які трапилися у мережі, бо перший крок у вирішенні проблеми це знайти проблему. Для роботи протоколу SYSLOG спочатку потрібно налаштувати протокол NTP. Протокол NTP відповідає за отримання точного часу. Мати точний час на мережевих пристроях є дуже важливо, бо логи прив'язуються до часу, що дозволяє ефективно працювати з ними. Без налаштованого протоколу NTP кожний пристрій може мати свій системний час і незрозуміло коли трапилися події і чи мають вони зв'язок. Також не зрозуміло коли саме трапилася подія, але це визначити легше. Без запису точного часу події майже неможливо зрозуміти, що трапилося у мережі. Тому протокол NTP обов'язковий для налагодження у мережі де використовується протокол SYSLOG.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 56   |

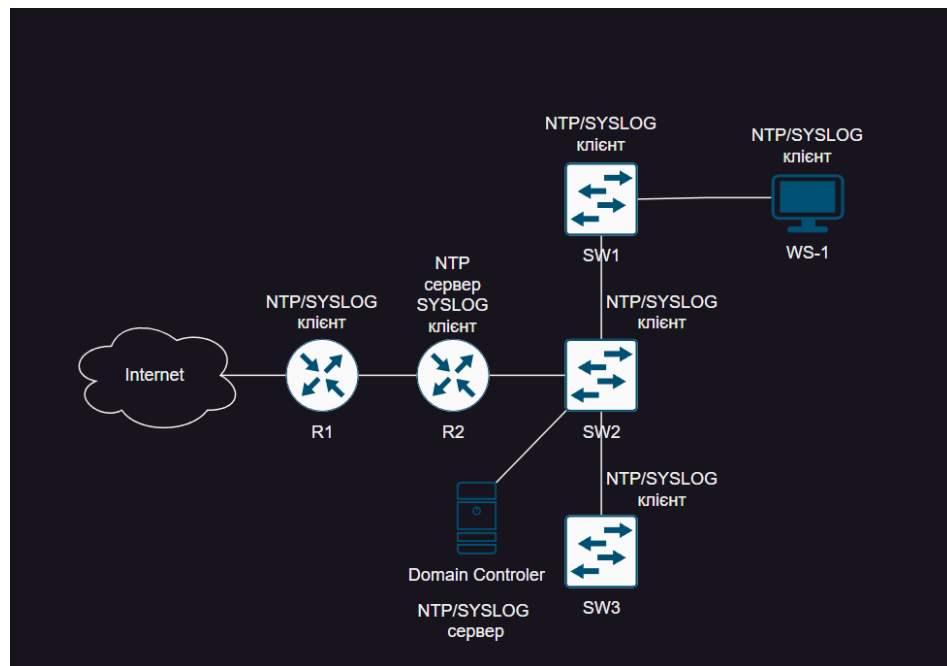


Рисунок 2.4 – Реалізація протоколів NTP та SYSLOG

Реалізовані ці протоколи у мережі будуть таким чином: маршрутизатор R1 буде виступати SYSLOG сервером у локальній мережі, а точний час він буде отримувати з мережі Інтернет. Також у мережі є другий NTP сервер, цим сервером виступає контролер домену. Він отримує точний час з мережі Інтернет і оновлює час на усіх робочих станціях у мережі, звідси якщо ця робоча станція є частиною домену.

SYSLOG сервером виступає контролер домену. Він буде автоматично отримувати усі SYSLOG повідомлення з мережі. SYSLOG клієнтами будуть виступати усі мережеві пристрої і також робочі станції. Отримання логів з робочих станцій зможе підвищити рівень безпеки у мережі, якщо зломисник отримає доступ до робочої станції і видалить запису з аудиту, то без доступу до контролеру він не зможе повністю стерти сліди у мережі. Для реалізації SYSLOG будуть використані сторонні програмні застосунки.

Для утримання достатнього рівня безпеки IT-інфраструктури компанії потрібно продумати реалізацію захисту. Для реалізації захисту від загроз спочатку потрібно осмислити їх і зрозуміти шляхи порушення безпеки. Потрібно створити діаграму загроз для явного усвідомлення всіх можливих шляхів порушення безпеки у мережі.

Модель загроз корпоративної мережної інфраструктури на базі Active Directory зазвичай включає такі елементи:

1) Зовнішні загрози:

a) Вторгнення зломисників: Зломисники можуть намагатися проникнути в мережу, використовуючи різні методи, такі як фішинг, використання вразливостей програмного забезпечення тощо.

b) Denial-of-service (DoS) атаки: Зломисники можуть намагатися перевантажити сервери інфраструктури, заважаючи користувачам отримувати доступ до ресурсів.

c) Атаки на службу керування доступом: Цільові атаки на протоколи та механізми керування доступом можуть дозволити зломисникам отримати несанкціонований доступ до активів мережі.

2) Внутрішні загрози:

a) Виток інформації: Працівники, навмисно чи ненавмисно, можуть витікати чутливу інформацію поза межі мережі, порушуючи безпеку даних.

b) Недостатній контроль доступу: Слабка аутентифікація, недостатньо обмежені права доступу або відсутність політик безпеки можуть призвести до несанкціонованого доступу працівників до ресурсів.

3) Внутрішні загрози зловживання довіри:

a) Користувачі з підвищеними привілеями: Адміністратори або інші працівники з підвищеними привілеями можуть зловживати своїм статусом та отримувати несанкціонований доступ до конфіденційної інформації або ресурсів.

b) Слабкі паролі: Використання слабких паролів або паролів, яких можна легко підібрати, працівниками може відкрити доступ для несанкціонованих осіб.

4) Втрати даних:

a) Випадкова втрата даних: Технічні проблеми, такі як відмова обладнання або помилкові дії користувачів, можуть призвести до випадкової втрати даних.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 58   |

б) Збитки внаслідок зловмисницької діяльності: Цільові атаки зловмисників можуть призвести до втрати даних або вимагання викупу за доступ до них.

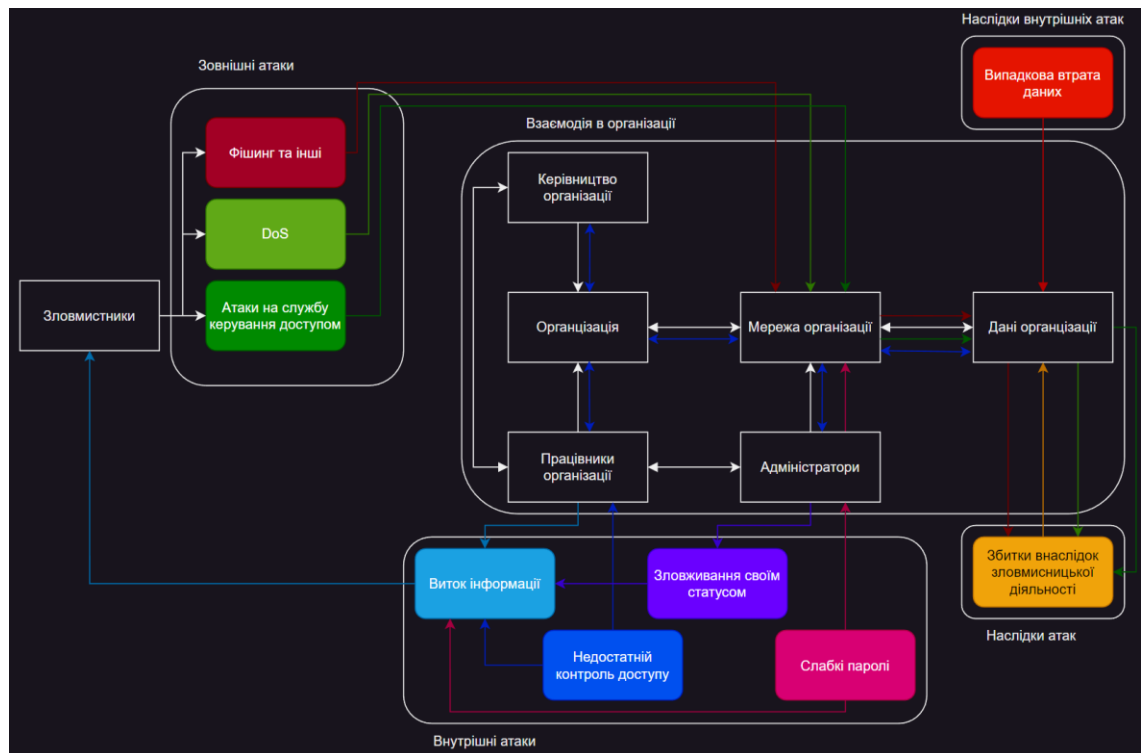


Рисунок 2.5 – Діаграма загроз

На основі вище описаних технологій необхідно реалізувати ефективний захист для мережевих пристроїв мережі. Для захисту мережевих пристроїв будуть використаний протокол SSHv2, списки доступу ACL, створений механізм аутентифікації (використання RADIUS), створений механізм авторизації (будуть різні права доступу для користувачів), використання протоколу STP. Також будуть відключені на пристроях усі порти які не використовуються. Для комутаторів буде налаштовано Port Security, BPDU Guard та PortFast.

Для уникнення створення у мережі широкомовного шторму буде використаний протокол STP. Для налаштування цього протоколу будуть використані його функції PortFast, Port Security, Dynamic ARP Inspection та BPDU Guard та використання DHCP Snooping. Всі ці функції будуть налаштовані для захисту мережі, як від створення раптових петель, так і від ціленаправленої атаки.

Для підвищення швидкодії мережі використаємо функцію PortFast. Данна функція налаштовується на портах комутатора, які ведуть до кінцевих пристроях. При підключенні пристрою до порту з налаштованою функцією PortFast, порт минує проміжні стадії і одразу переходить до стану forwarding.

Для захисту мережі від широкомовного шторму і різних атак використовуються функції Port Security, Dynamic ARP Inspection, BPDU Guard та DHCP Snooping. Port Security запам'ятовує MAC-адресу, тому його можна використати для фіксації MAC-адресу порта комутатора, і якщо зловмисник спробує замінити комутатор то в нього це не вийде.

Функції Dynamic ARP Inspection, BPDU Guard та DHCP Snooping забезпечують захист від різних типів атак на мережу.

Налаштування функції Dynamic ARP Inspection. Налаштовується на портах, які йдуть до надійних пристроїв. Надійними пристроями можуть бути: сервери або довірені мережеві пристрої. Поділяє порти на довірені та недовірені. Протидії атака типу ARP-poisoning (ARP-spoofing).

Для захисту від атак на протокол DHCP використаємо функцію DHCP Snooping. Вказуємо комутатору на до якого підключений справжній DHCP-сервер і комутатор мережі. Таким чином ми дозволяємо DHCP-відповіді тільки для цих портів і забороняємо для інших.

В мережі авторизований сервер лише один, тому команда для його налаштування буде виглядати так:

```
sw2(config)# dhcp-snooping authorized-server 192.168.0.1
```

Функція BPDU Guard використовується для попередження петель у мережі. Дана функція налаштовується на портах комутатора, які ведуть до кінцевих пристроїв. При налаштуванні даної функції, якщо комутатор отримує BPDU-повідомлення на порт де налаштований BPDU Guard, то даний порт блокується.

Також будуть виконанні додаткові налаштування для забезпечення безпеки. Для профілактики мережі будуть відключені порти мережевих пристроїв, які не використовуються.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 60   |

**Висновки:** у другому розділі був розроблений проект самої комунікаційної мережі, на базі розглянутих технологій і протоколів описаних у першому розділі. Була розроблена топологічна структура мережі, був проведений опис створеної мережі: кількість і тип комунікаційних вузлів та протоколи, які будуть використовуватися. Була створена схема адресації мережі, схема була створена з метою забезпечення роботи мережі і економного використання IP адрес. Були розібрані функції домену Active Directory і мережевих пристроїв, які будуть використані при створенні мережі. Була створена система користувачів організації. На основі розглянутих у першому розділі атак і методів їх захисту була створена діаграма загроз. На основі створеної діаграми загроз і системи користувачів було створено розмежування доступу у мережі. Також були розібрані технології захисту мережевих пристроїв і особливості їх реалізації.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 61   |

## РОЗДІЛ 3 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ СЛУЖБИ КАТАЛОГІВ ACTIVE DIRECTORY ДЛЯ IT-ІНФРАСТРУКТУРИ КОМПА- НІЇ

### 3.1 Встановлення та налаштування Microsoft Active Directory серверів

Для початку роботи з AD сервером необхідно його встановити, тому почнемо з встановлення AD серверу. Встановлення серверу подібно до встановлення звичайної ОС Windows, розберемо лише основні моменти.

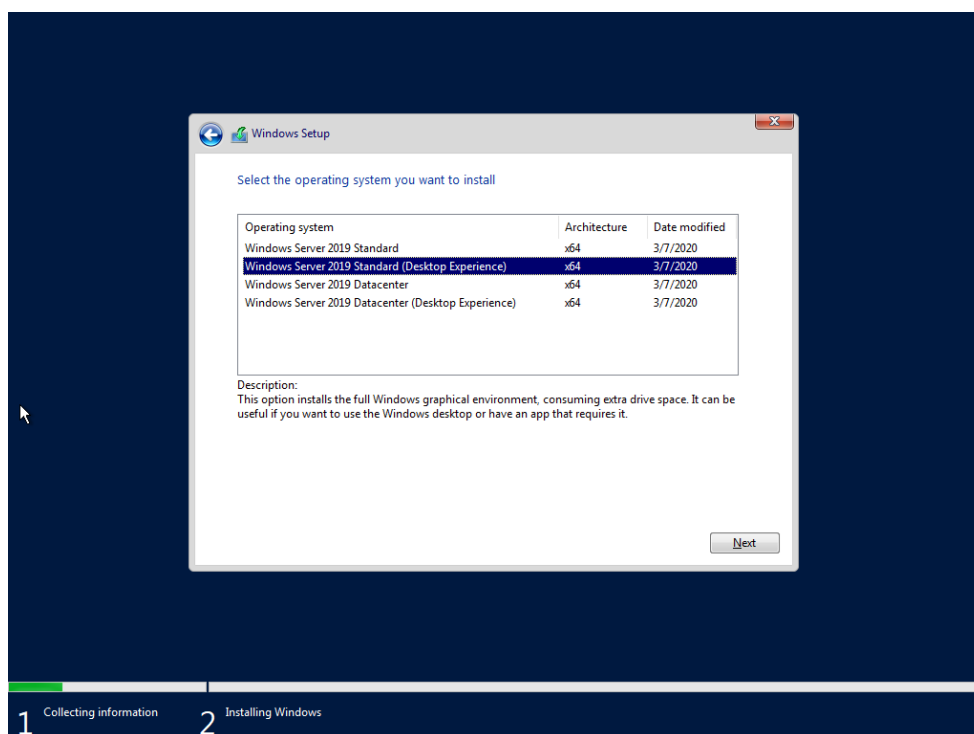


Рисунок 3.1 – Вибір ОС для встановлення

Важливим моментом є вибір ОС для встановлення, важливо розуміти чим відрізняються запропоновані для встановлення ОС, нам необхідні ОС Windows Server 2019 Standard. Windows Server 2019 Standard і Windows Server 2019 Standard (Desktop Experience) відрізняються наявністю графічного інтерфейсу, відсутність графічного інтерфейсу може бути перевагою за обмежених ресурсів для серверу, у нашому випадку ресурсів для серверу достатньо і наявність графічного інтерфейсу набагато спростую роботу з сервером, тому встановлюємо Windows Server 2019 Standard (Desktop Experience).

Далі вибираємо тип встановлення Custom: Install Windows only (advanced).

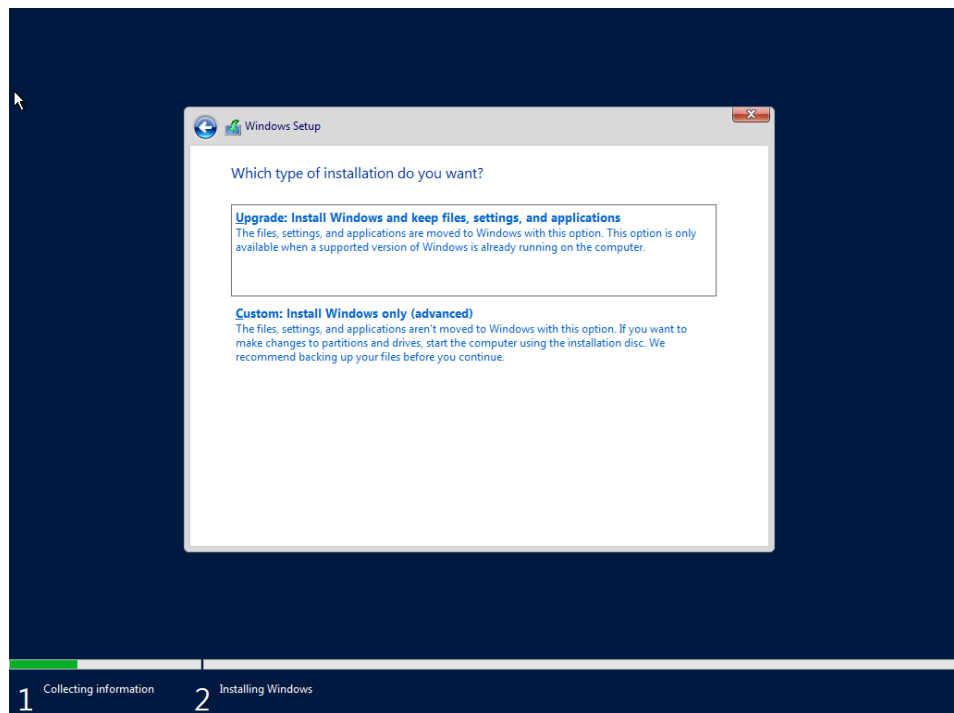


Рисунок 3.2 – Вибір типу встановлення

Далі переходимо до розбиття диску, у даному розділі можна керувати доступним місцем на диску, формувати диск і розбивати його на томи. У нашому випадку створюю один великий том на весь вільний простір.

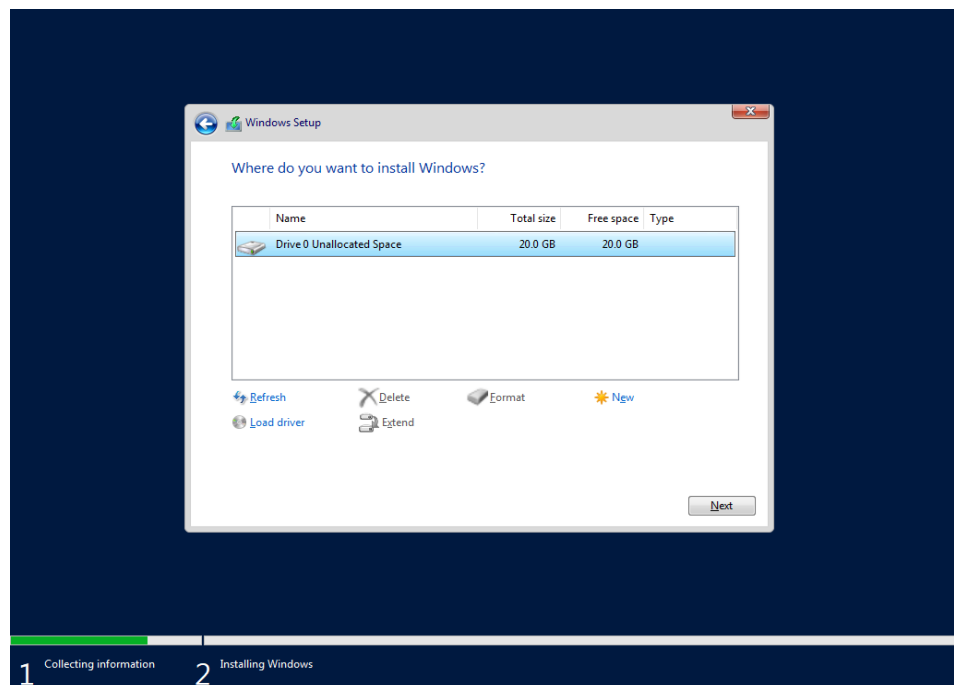


Рисунок 3.3 – Розбиття диску

Далі чекаємо встановлення серверу і можемо переходити до налаштувань самого Active Directory серверу.

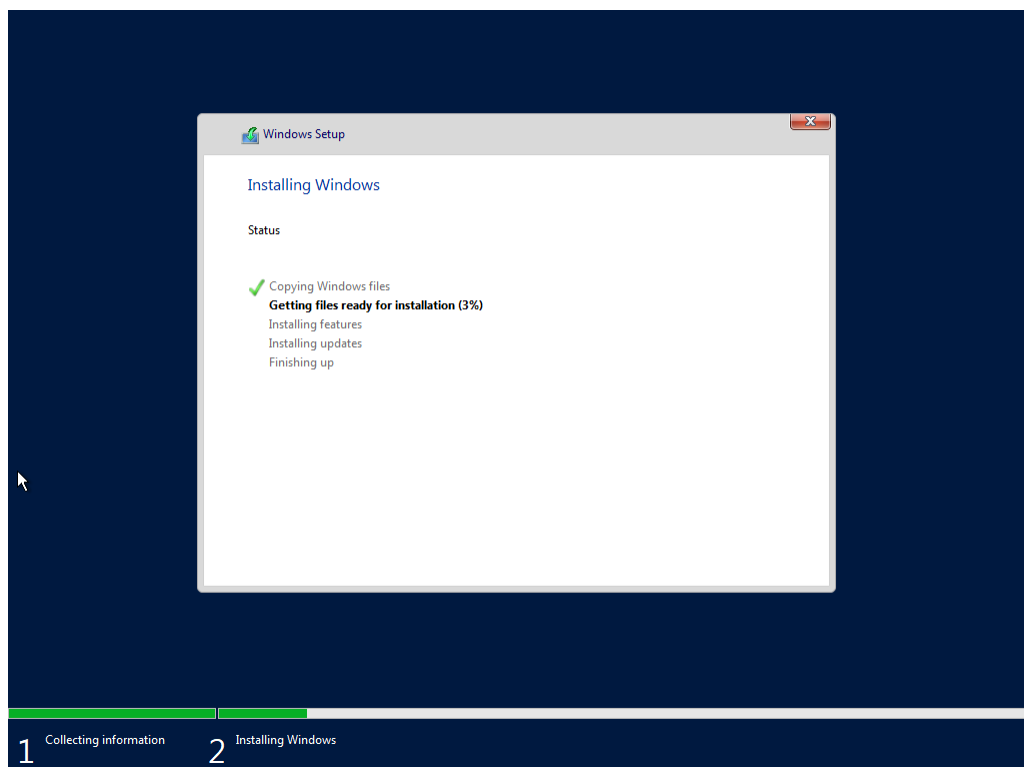


Рисунок 3.4 – Процес встановлення AD серверу

Перед розгортання серверу як контролер домену необхідно провести базові налаштування системи:

- налаштування IP адресації (сервер має мати статичну адресу)
- налаштувати назву серверу (за потреби)
- налаштування часу (часового поясу)

Після проведення базових налаштувань можна розгортати сам контролер домену, необхідні для роботи домену модулі будемо додавати по мірі їх встановлення, тому для початку встановлюємо лише Active Directory Domain Services.

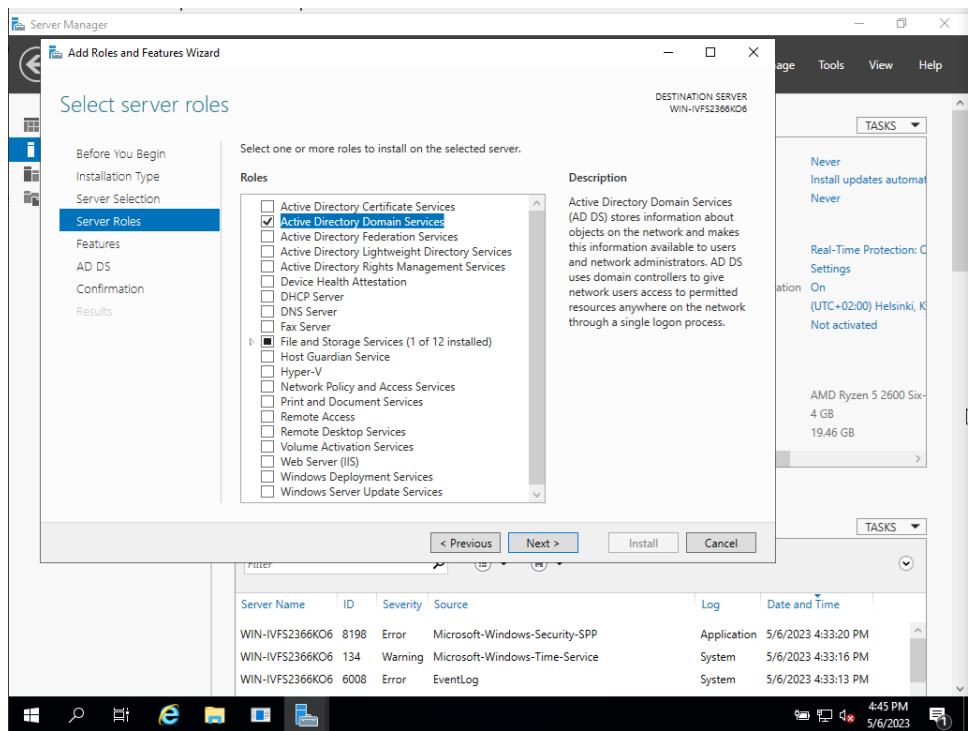


Рисунок 3.5 – Вибір модулів для встановлення

Після встановлення модуля розгортаємо цей сервер як контролер домену, вибираємо відповідний пункт і вводимо назву домену.

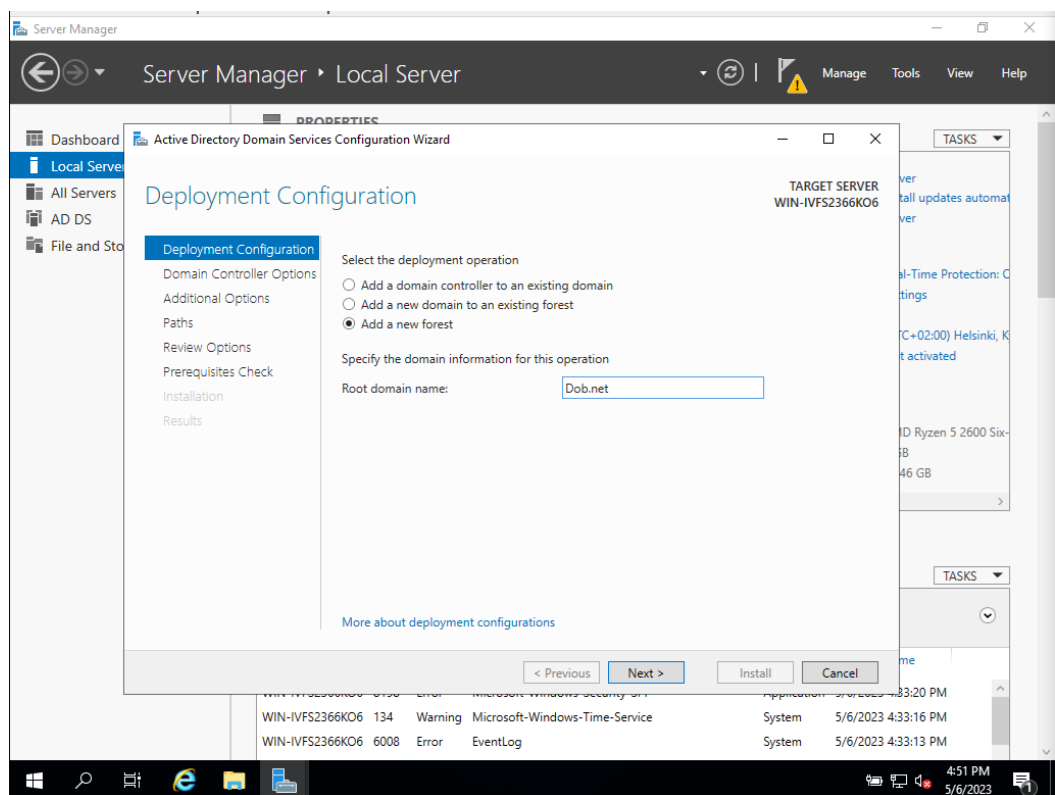


Рисунок 3.6 – Розгортання серверу як контролер домену

Задаємо пароль і вибираємо функціональний рівень контролеру домену.

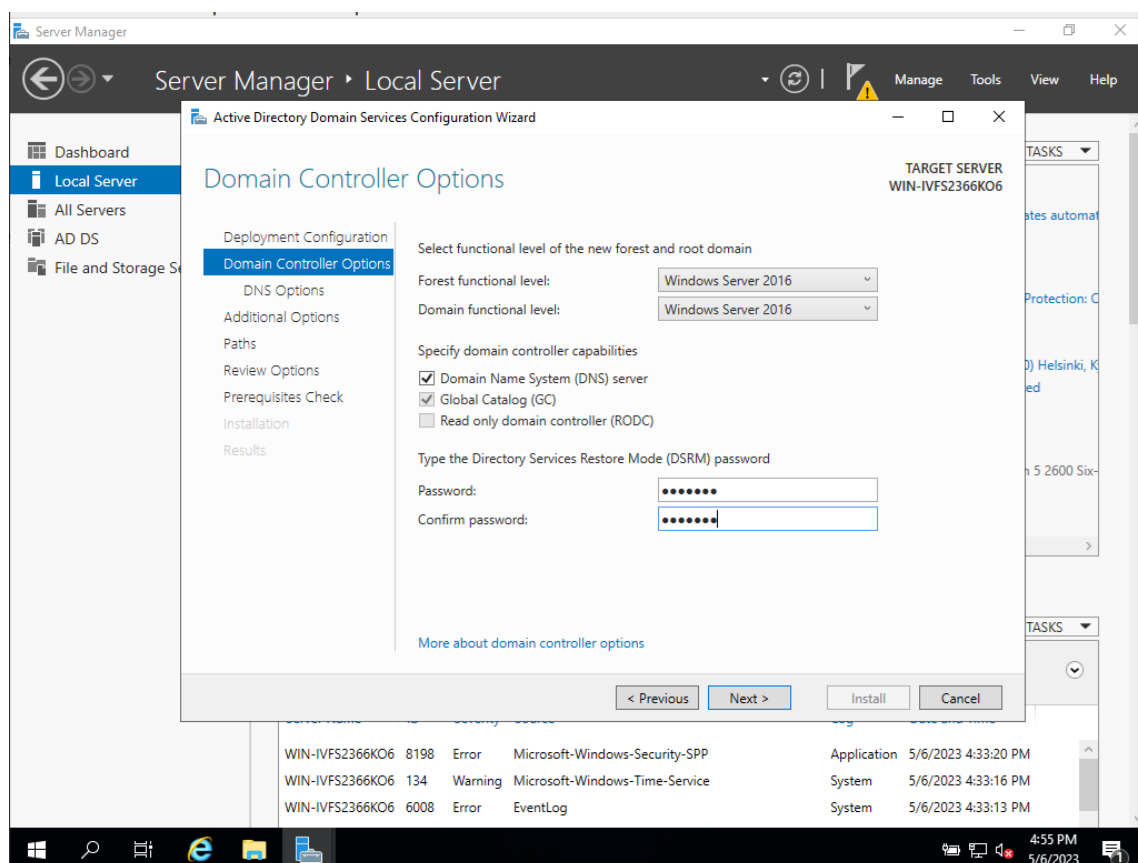


Рисунок 3.7 – Вибір функціонального рівня та задання паролю

Після встановлення Windows серверу і розгортання його як контролеру домену можна переходити до його налаштування, почнемо з створення структури користувачів.

На основі описаної вище структури користувачів необхідно відтворити цю структуру у контролері домену. Почнемо з створення OU адміністраторів і в цій OU створимо групи для адміністраторів різних областей повноважень.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 66   |

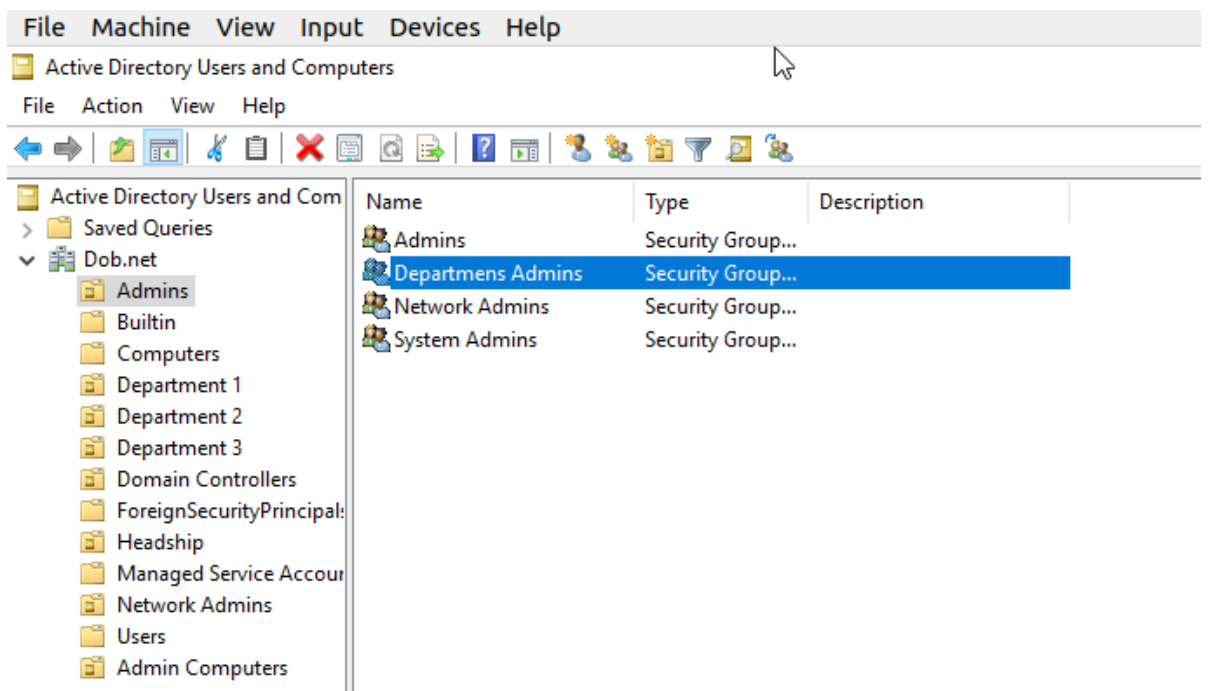


Рисунок 3.8 – Створені групи користувачів

Створена загальна група адміністраторів «Admins» у якій зібрані усі інші групи адміністраторів. Створені групи адміністраторів різних рівнів повноважень. Далі створимо OU для першого департаменту.

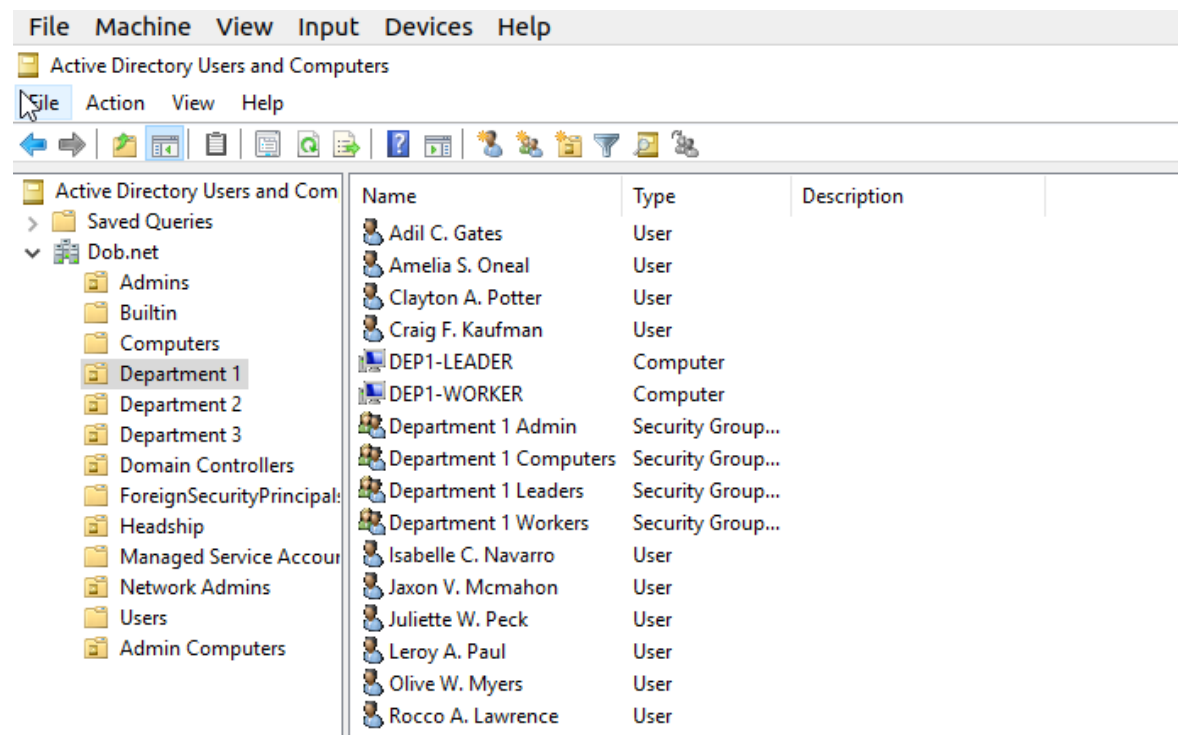


Рисунок 3.9 – Створений перший департамент

В цій OU знаходяться усі користувачі, які працюють у першому департаменті, групи та комп'ютери. Створені групи для користувачів, група для адміністратора і голови департаменту, та група для комп'ютерів, які використовуються у цьому департаменті. Також створена OU для комп'ютерів адміністраторів, які не є частиною департаментів.

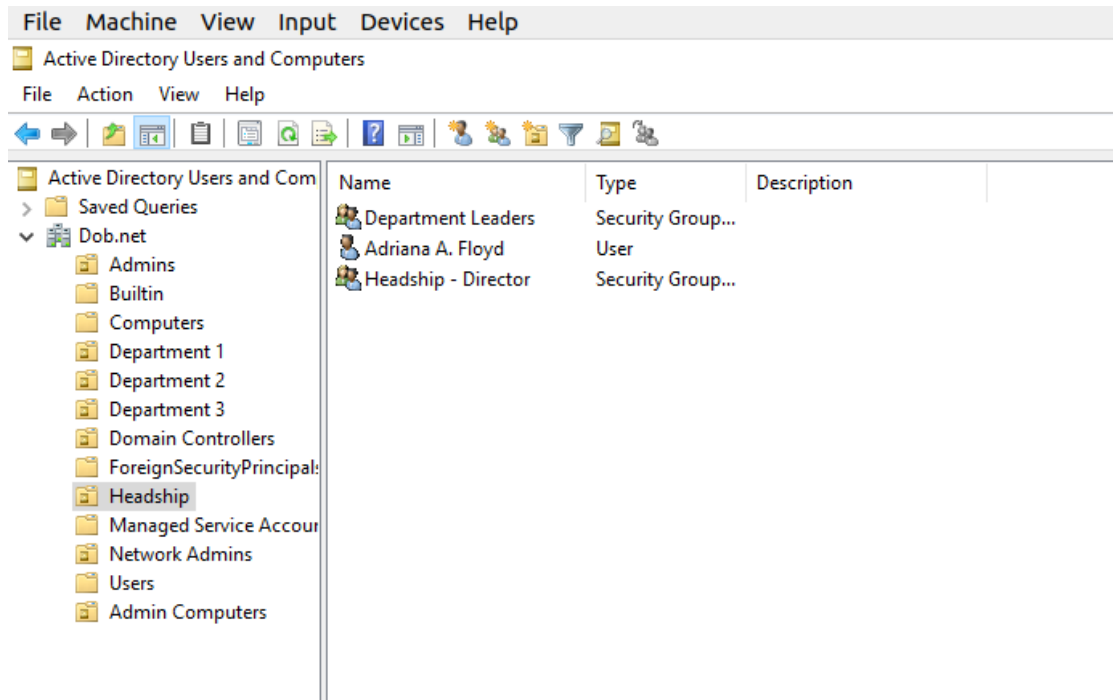


Рисунок 3.10 – Створений департамент керівництва

Для керівництва організації створена окрема OU, у якій знаходяться обліковий запис директора, група директора і група для заступників директора - «Department Leaders».

Після створення структури користувачів можна переходити до створення і налаштування групових політик.

Для підвищення рівня безпеки мережі необхідно обмежити список користувачів, які мають можливість додавати нові робочі станції до домену. Для цього скористаємося раніше створеною групою „Admins“, у якій знаходяться усі адміністратори мережі. Далі налаштуємо групову політику за замовчуванням, дозволимо додавання нових робочих станцій лише користувачам, які пройшли перевірку, а саме користувачі групи „Admins“.

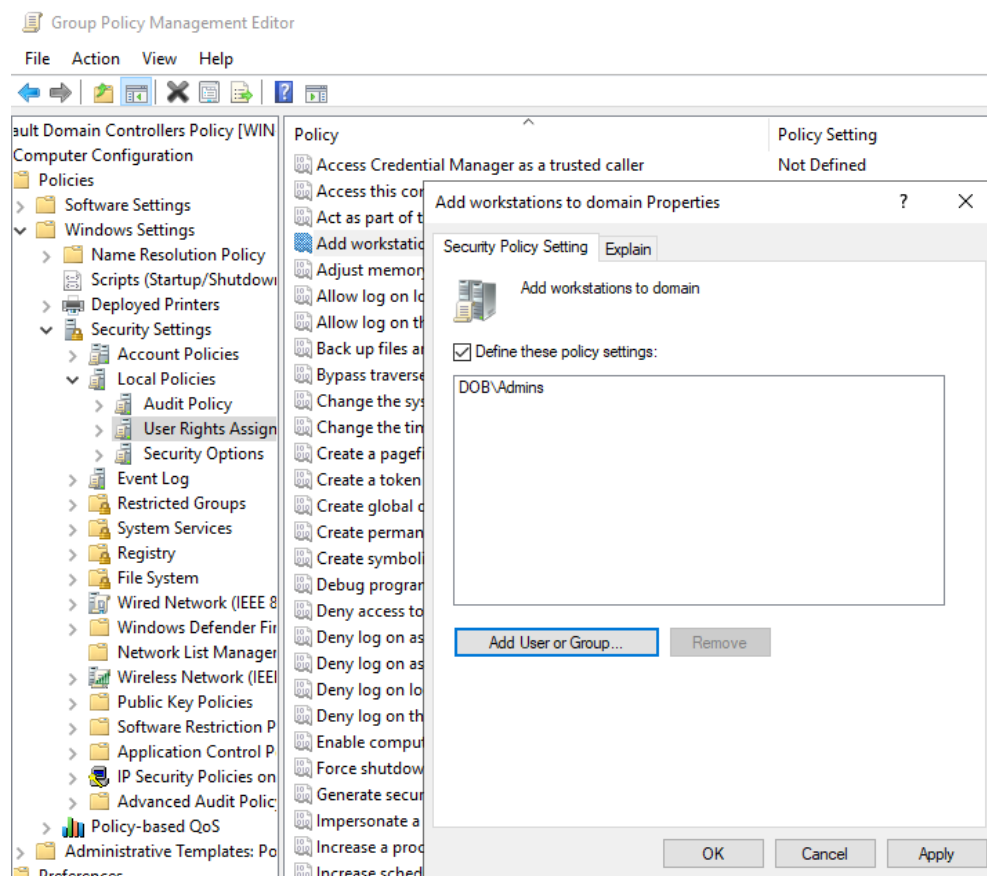


Рисунок 3.11 – Обмеження можливості додавання робочих станцій до домену

Далі можна перейти к налаштуванню розмежування доступу до робочих станцій домену за допомогою групових політик. За замовчуванням усі користувачі мають доступ до будь-якого комп'ютера мережі, це є недопустимим з питань безпеки. Тому необхідно розмежити доступ так, як написано у другому розділі. Для цього створим нову групову політику, вкажимо, що цілі для неї комп'ютери групи «Department 1 Computers» і дозволимо вхід лише працівникам цього департаменту.

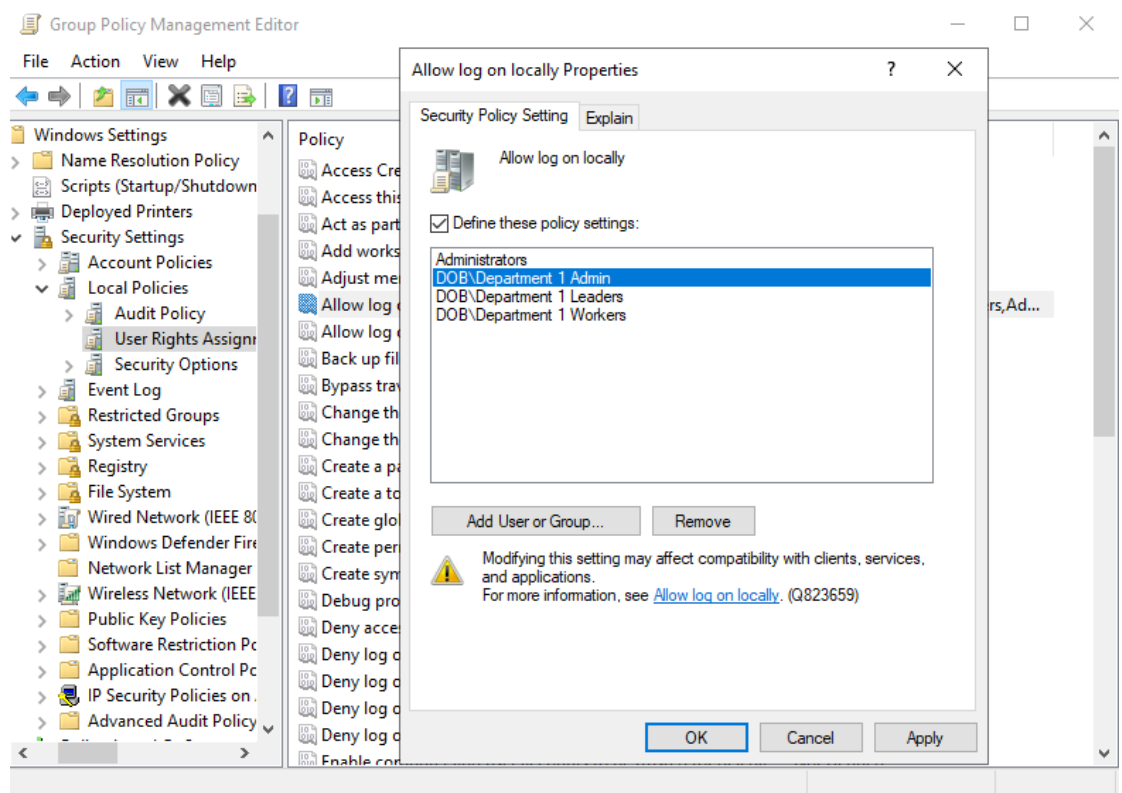


Рисунок 3.12 – Створення групової політики для обмеження доступу до департаменту

Далі необхідно надати права адміністратора для певних користувачів домену, для цього скористаємося груповою політикою. Створимо нову групову політику для першого департаменту і надаємо повноваження адміністраторів групі «Department 1 Admin». Створюю подібні групові політики для кожного департаменту.

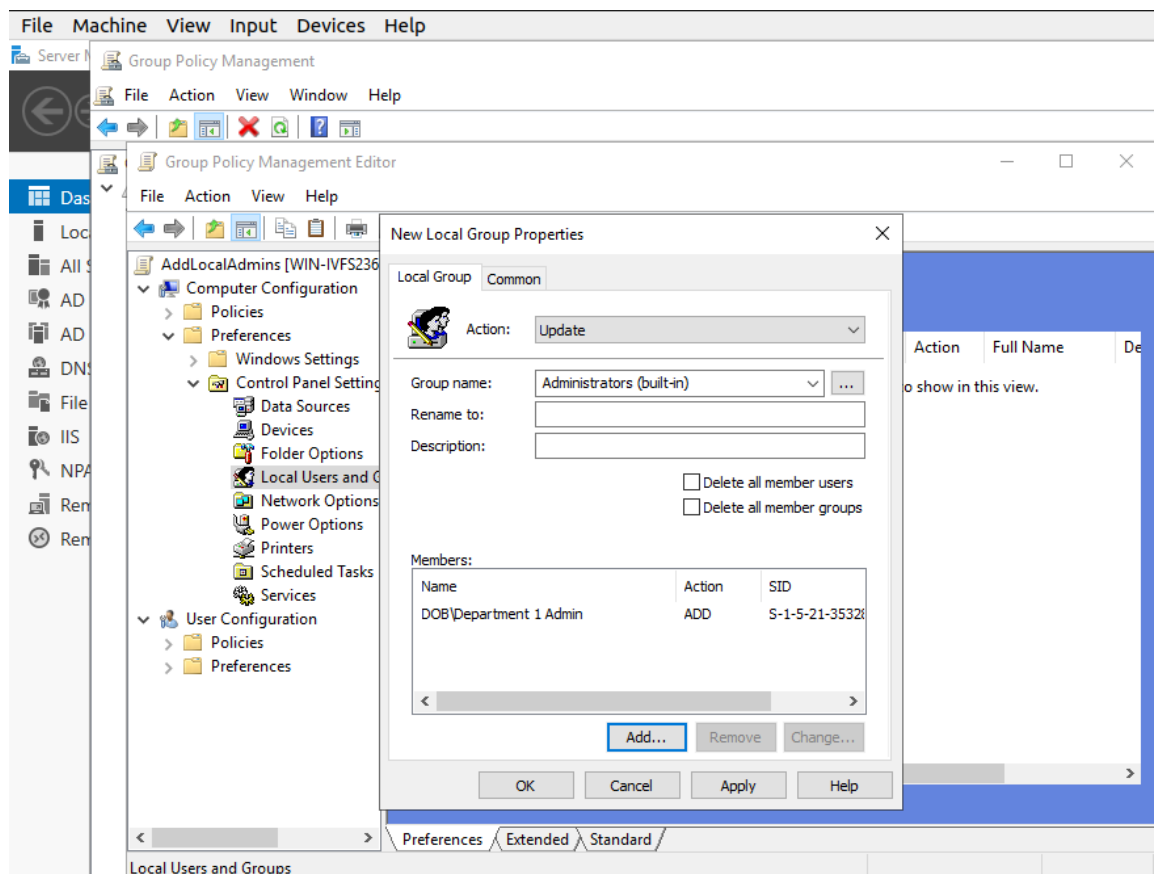


Рисунок 3.13 – Створення політики для назначення адміністраторів робочих станцій

За створеною структурою домену всі робочі станції знаходяться у певних організаційних одиницях, тому для підвищення безпеки можна заборонити авторизацію користувачам домену на робочих станціях, які знаходяться в OU за замовчуванням «Computers». Таким чином рівень безпеки у мережі буде підвищено. Для цього дозволимо авторизацію лише на робочих станціях, які входять до групи «Computers». В цій групі нема контролерів домену, бо додати неавторизований контролер домену складніше, і якщо злоумисник може це зробити то він вже має достатній рівень доступу.

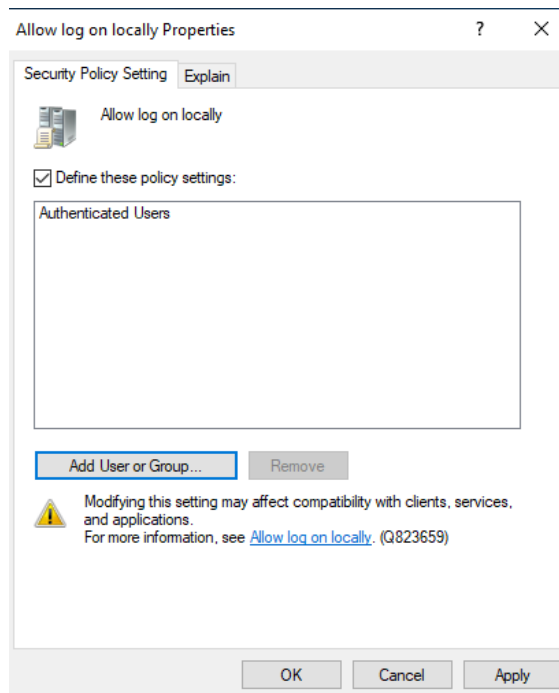


Рисунок 3.14 – Створення політики для авторизації лише на легальних робочих станціях

Також необхідно заборонити користувачам, окрім спеціальних адміністраторів, доступ до контролерів домену. Це також підвищить рівень безпеки у мережі, зловмисник не зможе легко отримати доступ до контролеру домену.

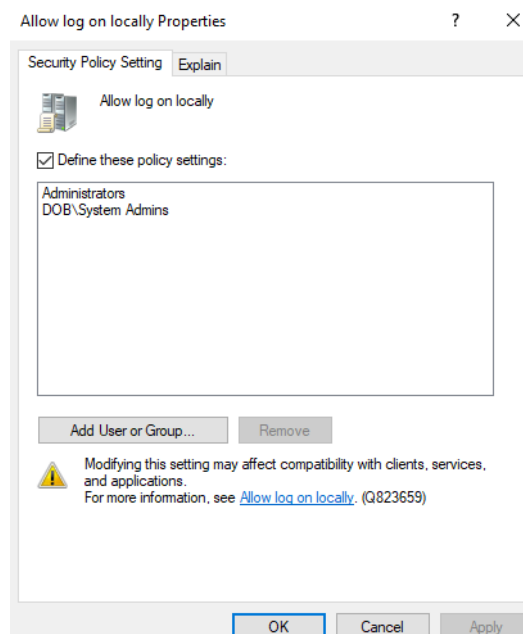


Рисунок 3.15 – Обмеження доступу до контролерів домену

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 72   |

Таким чином, отримати доступ до контролерів домену можуть лише певні адміністратори. Також обмежую доступ до робочої станції системного адміністратора, доступ до цієї робочої станції має лише системний адміністратор.

Після створення і налаштування основних групових політик можна переходити до налаштування квотування. Переходимо до налаштування квот для першого департаменту. Згідно з даними, описаними вище, налаштуємо квоти для користувачів у 10 Гб. Для налаштування квоти використаємо групові політики. Створимо групову політику для першого департаменту.

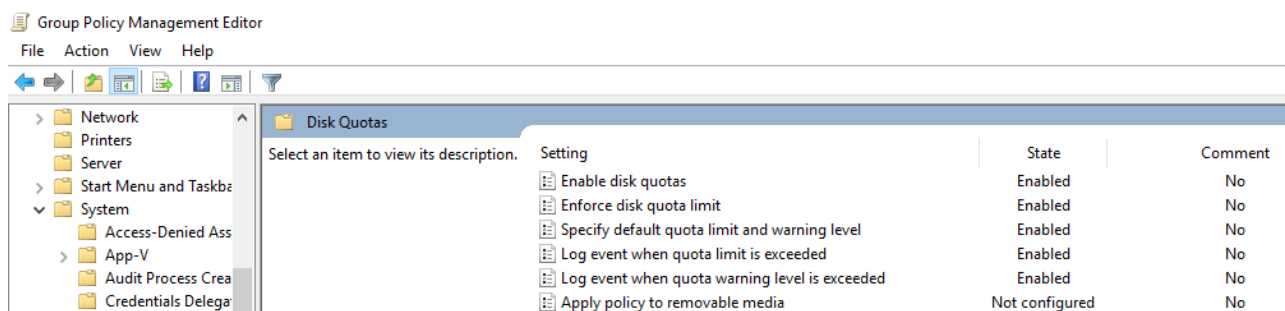


Рисунок 3.16 – Налаштовані дискові квоти для першого департаменту

Після налаштування дискових квот звичайні користувачі будуть мати 10 Гб на власні дані і отримувати повідомлення при 9 Гб занятого місця.

Загальна структура створених групових політик:

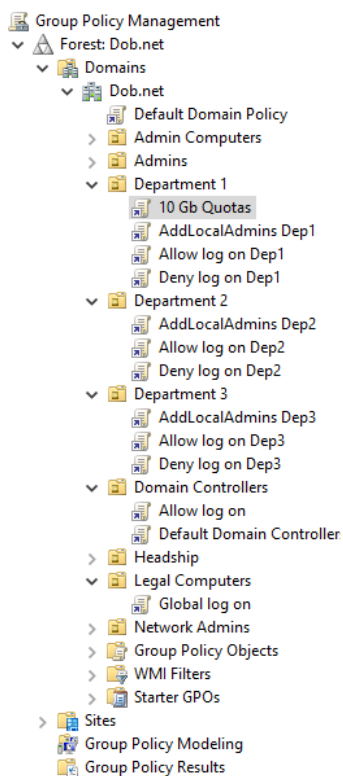


Рисунок 3.17 – Створені групові політики

Після завершення налаштування групових політик можна переходити до налаштування DNS серверу. Налаштовую DNS-записи для мережевих пристроїв. Створюю записи для кожного мережевого пристрою. Таким чином, підвищим зручність користування мережею.

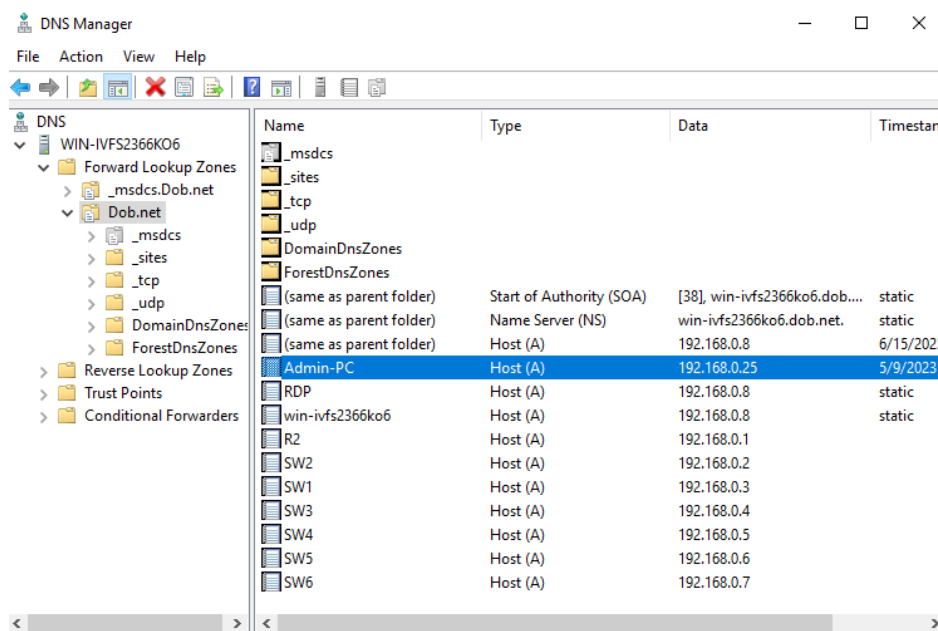


Рисунок 3.18 – Створені DNS-записи для мережевих пристроїв

Створивши структуру користувачів, маючи налаштоване розмежування доступу і налаштований DNS сервер, переходимо до налаштування вбудованого в Active Directory RADIUS сервера.

Почнемо з встановлення нових модулів, необхідних для роботи RADIUS серверу. Для роботи нам необхідно встановити:

- Active Directory Certificate Services
- Network Policy and Access Services
- Remote Access

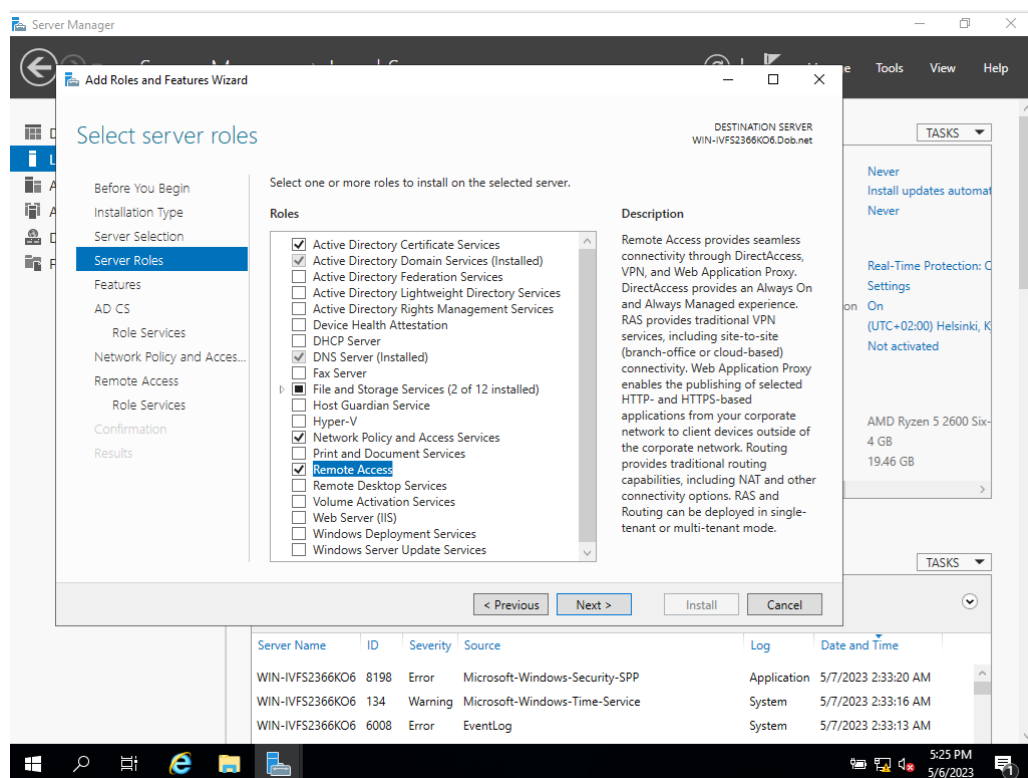


Рисунок 3.19 – Встановлення необхідних модулів

Далі переходимо до налаштування Брандмауера Windows, нам необхідно відкрити порт який використовує RADIUS.

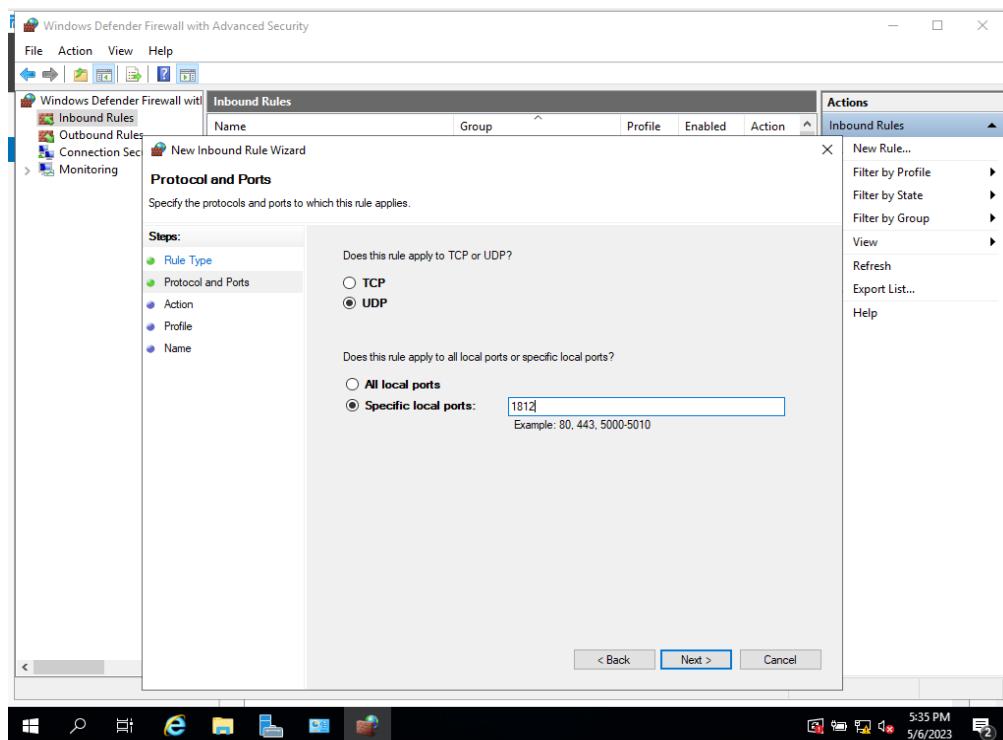


Рисунок 3.20 – Відкриття порту

Далі переходимо до налаштування Active Directory Certificate Services, а саме створення нового частного ключа, він нам знадобиться для підтримання відповідного рівня безпеки.

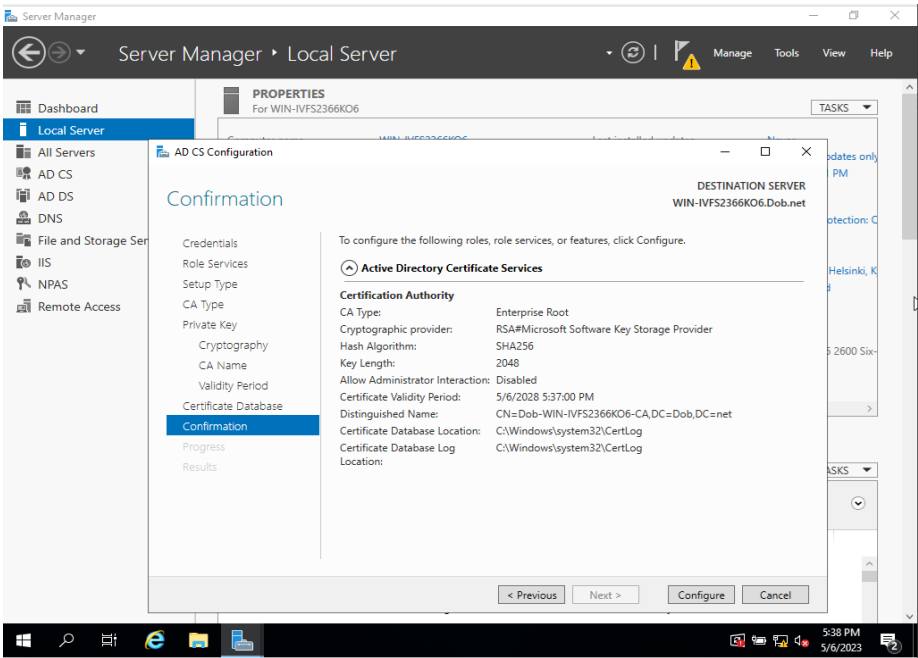


Рисунок 3.21 – Налаштування Active Directory Certificate Services

Далі переходимо до налаштувань Network Policy Server.

Додаю нового RADIUS-клієнта.

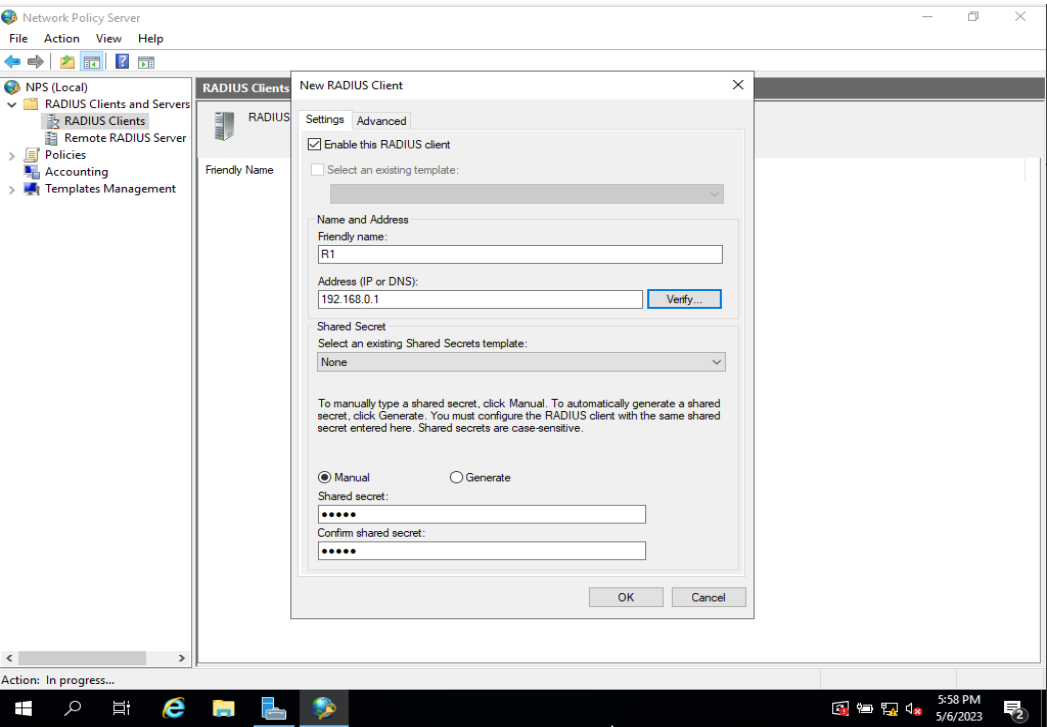


Рисунок 3.22 – Додавання RADIUS-клієнта

Основні функції контролеру домену налаштовані, переходимо до додавання робочих станцій до домену.

Додаємо нову робочу станцію до домену, для цього переходимо у властивості ПК > Налаштування імені комп'ютера, домену та робочої групи > Змінити налаштування.

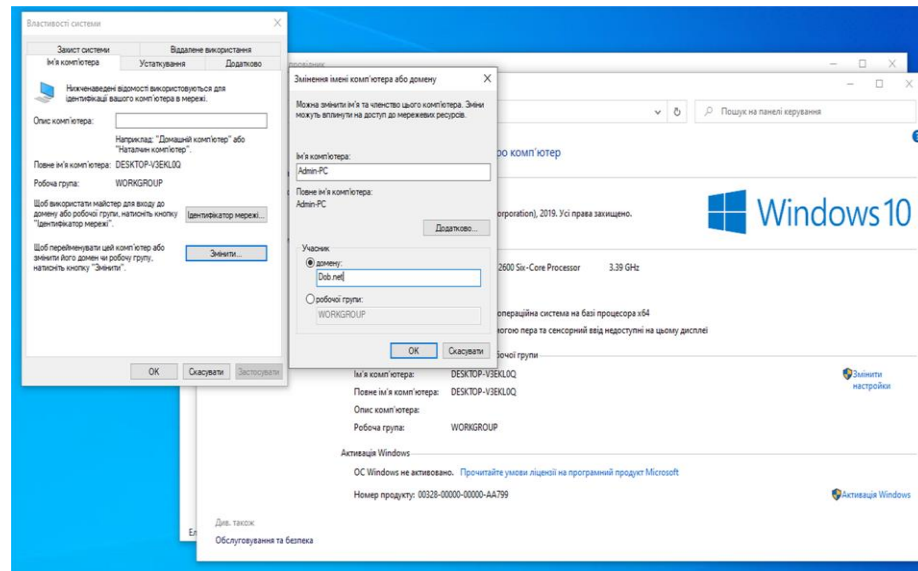


Рисунок 3.23 – Додавання робочої станції до домену

За необхідності змінюємо ім'я робочої станції та вводимо назву домену, після введення паролю користувача адміністратора приєднуємося до домену.

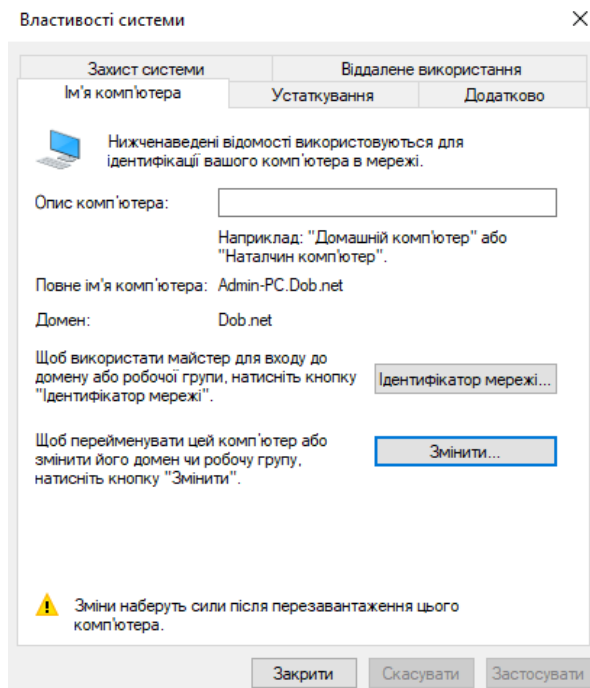


Рисунок 3.24 – Успішне приєднання до домену

Переходим до налаштування системи логування подій у мережі.

На жаль Active Directory сервер немає вбудованого SYSLOG серверу, тому необхідно використати зовнішнє ПО. Для логування подій буде використано SolarWinds Kiwi Syslog Server.

Почнемо з встановлення серверу на контролері домену:

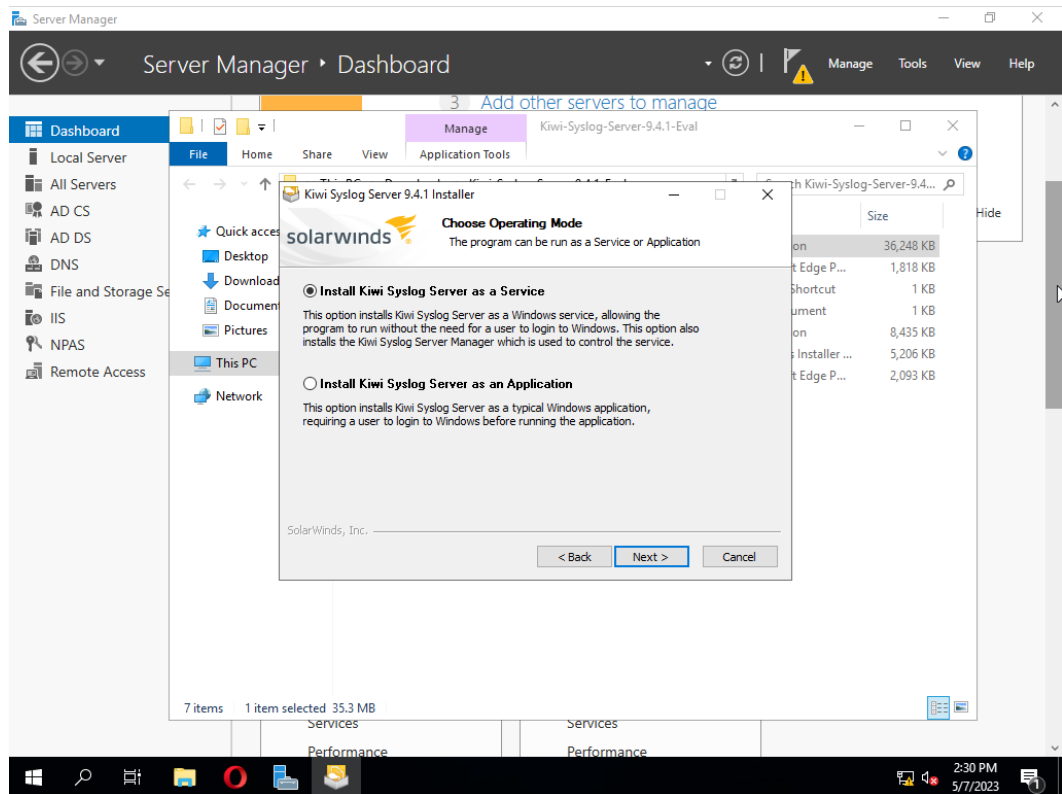


Рисунок 3.25 – Встановлення Syslog серверу

Встановлюємо сервер як сервіс, що дає можливість йому працювати навіть без авторизації користувача у систему. За необхідності можна встановити Kiwi Syslog Web Access для можливості керування сервером через веб інтерфейс.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В      |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 78   |

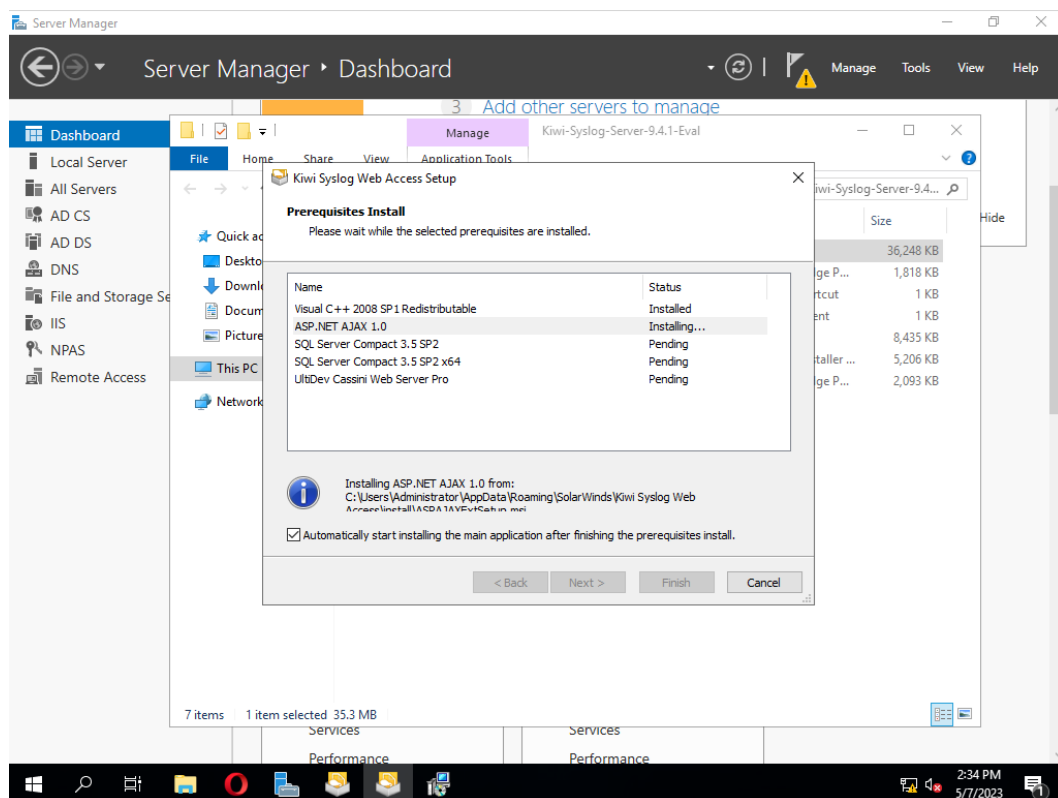


Рисунок 3.26 – Встановлення Kiwi Syslog Web Access

Далі встановимо SolarWinds Log Forwarder для отримання логів вже з Windows хостів.



Рисунок 3.27 – Встановлення SolarWinds Log Forwarder

Далі налаштуємо підключення до Syslog серверу

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 79   |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

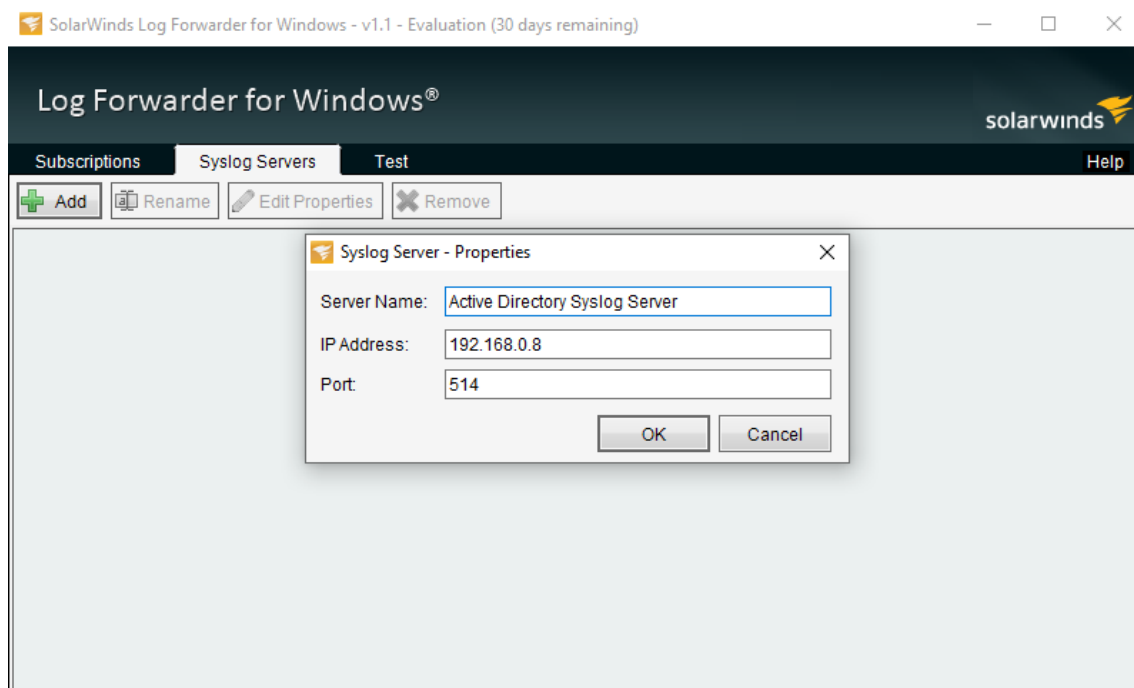


Рисунок 3.28 – Підключення до Syslog серверу  
Налаштовуємо повідомлення, які будемо отримувати

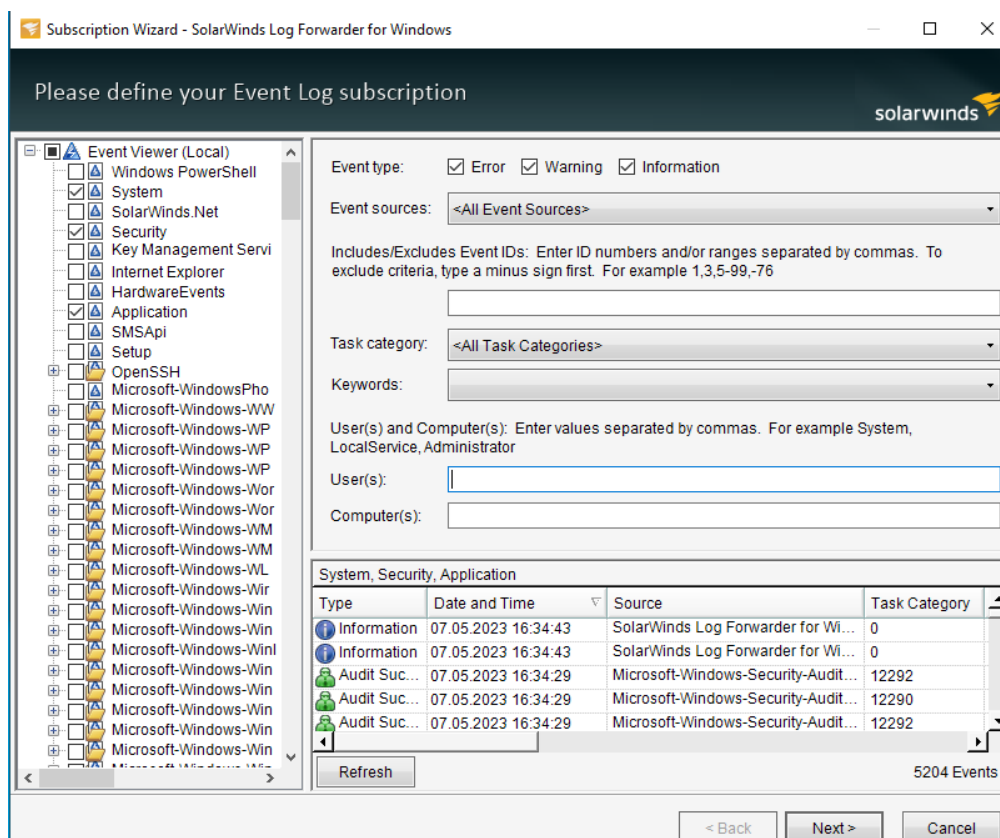
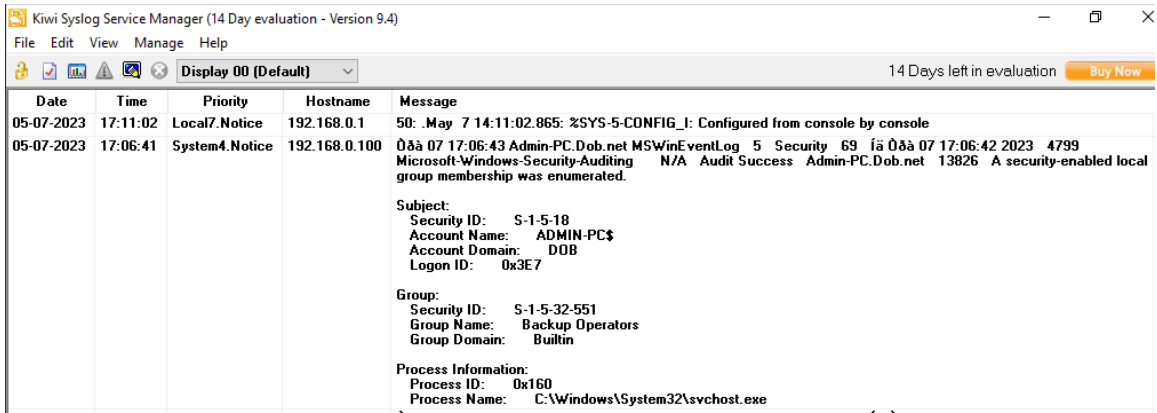


Рисунок 3.29 – Вибір типу подій для моніторингу

Після проведення налаштувань Syslog сервер почне отримувати повідомлення і від мережевих пристроїв, і в робочих станцій. Повідомлення можна переглянути на сервері:



The screenshot shows the Kiwi Syslog Service Manager interface. It has a menu bar (File, Edit, View, Manage, Help) and a toolbar. A dropdown menu is set to 'Display 00 (Default)'. A status bar at the top right indicates '14 Days left in evaluation' and a 'Buy Now' button. The main area contains a table of received messages:

| Date       | Time     | Priority      | Hostname      | Message                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|----------|---------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 05-07-2023 | 17:11:02 | Local7.Notic  | 192.168.0.1   | 50: May 7 14:11:02.865: %SYS-5-CONFIG_I: Configured from console by console                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 05-07-2023 | 17:06:41 | System4.Notic | 192.168.0.100 | 05:07 17:06:43 Admin-PC.Dob.net MSWinEventLog 5 Security 69 05:07 17:06:42 2023 4799 Microsoft-Windows-Security-Auditing N/A Audit Success Admin-PC.Dob.net 13826 A security-enabled local group membership was enumerated.<br><br>Subject:<br>Security ID: S-1-5-18<br>Account Name: ADMIN-PC\$<br>Account Domain: DOB<br>Logon ID: 0x3E7<br><br>Group:<br>Security ID: S-1-5-32-551<br>Group Name: Backup Operators<br>Group Domain: BuiltIn<br><br>Process Information:<br>Process ID: 0x160<br>Process Name: C:\Windows\System32\svchost.exe |

Рисунок 3.30 – Отримані Syslog повідомлення

Перейдемо до встановлення служб віддаленого доступу. Почнемо з встановлення Remote Desktop Services (RDS). Вибираємо Remote Desktop Services Installation.

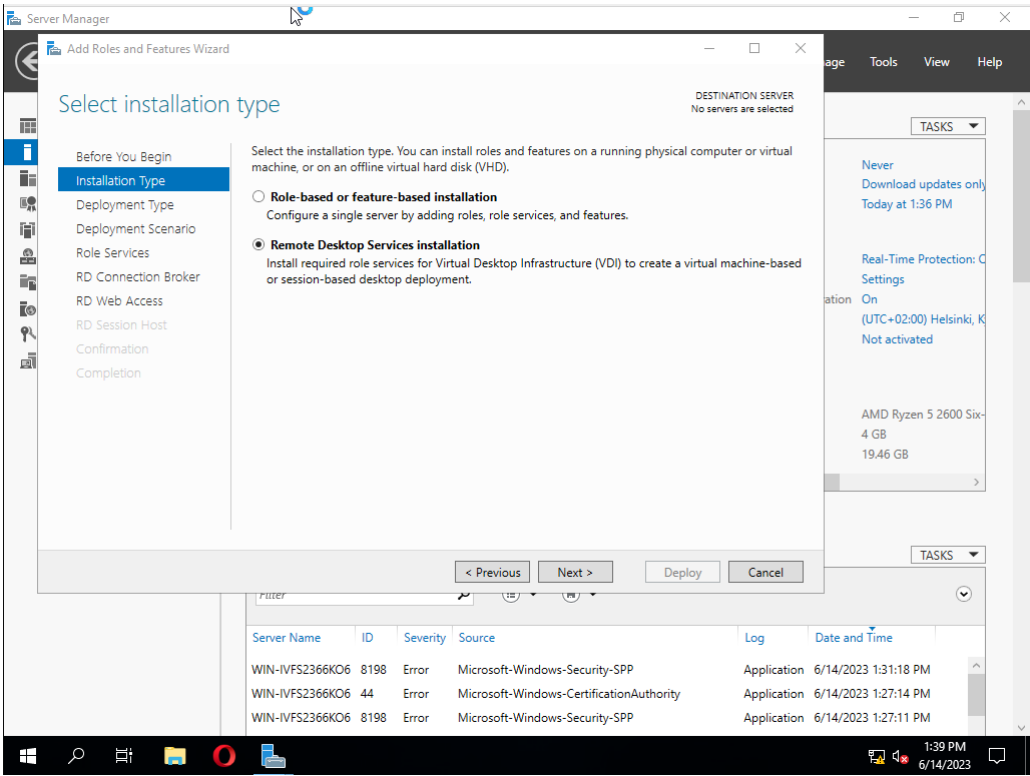


Рисунок 3.31 – Remote Desktop Services Installation

Далі вибираємо Session-based desktop deployment.

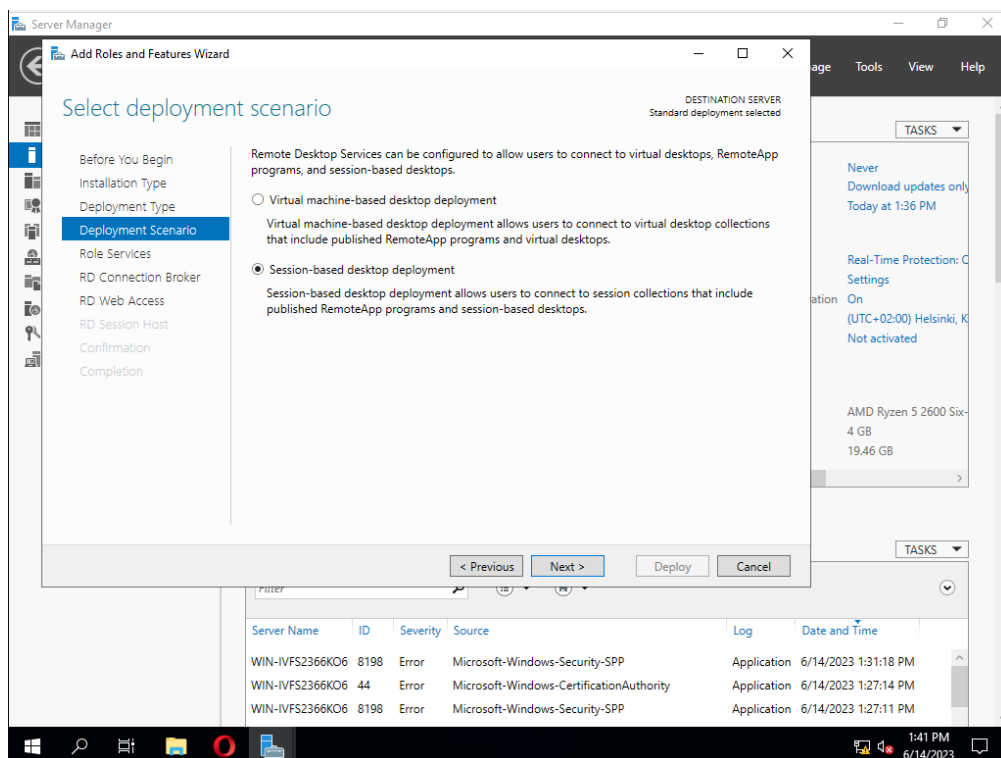


Рисунок 3.32 – Вибір Session-based desktop deployment

Вибираємо поточний контролер домену для встановлення і ставимо галочку на встановлення RD Web Access.

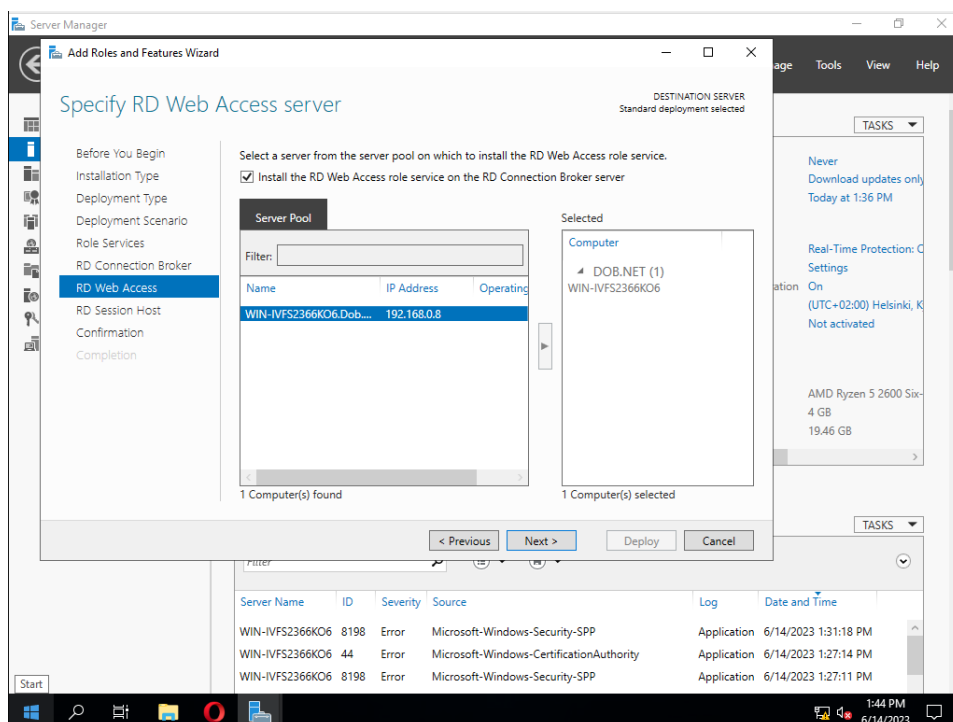


Рисунок 3.33 – Вибір контролеру домену для встановлення

На всіх трьох етапах (RD Connection Broker, RD Web Access, RD Session Host) вибираємо поточний контролер домену для встановлення.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 82   |

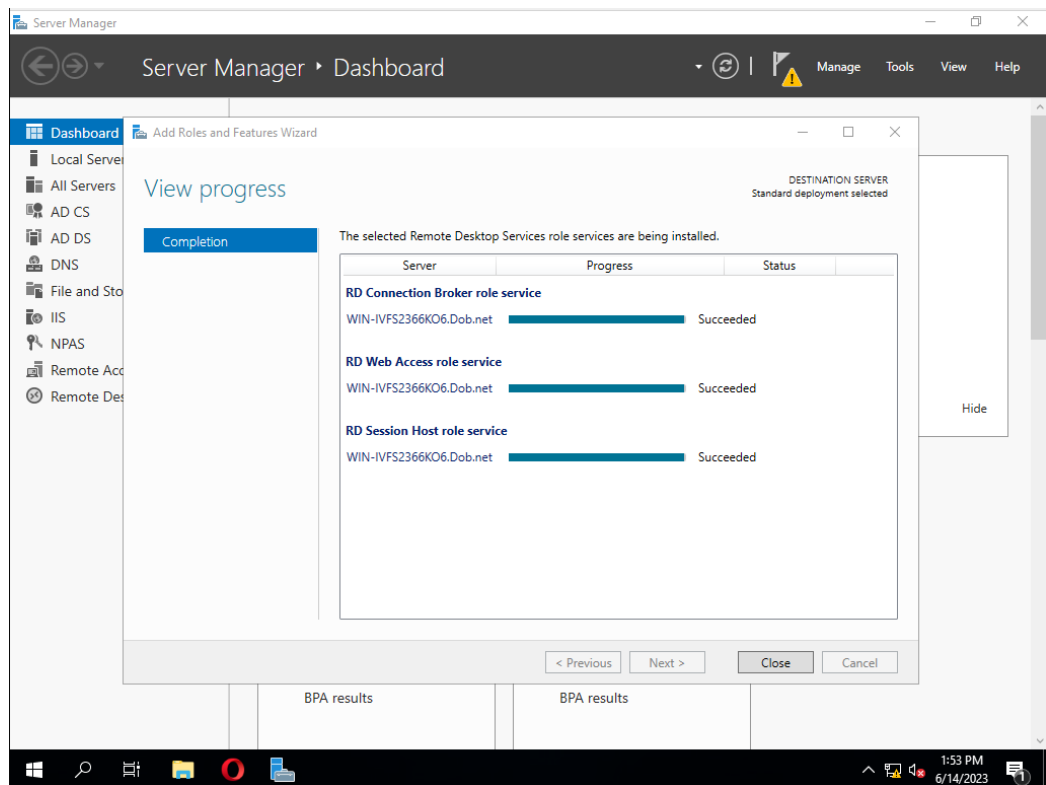


Рисунок 3.34 – Процес встановлення сервісів

Після завершення встановлення RDS можна переходити до налаштування служби. Обираю у ролі серверу ліцензій перший контролер домену.

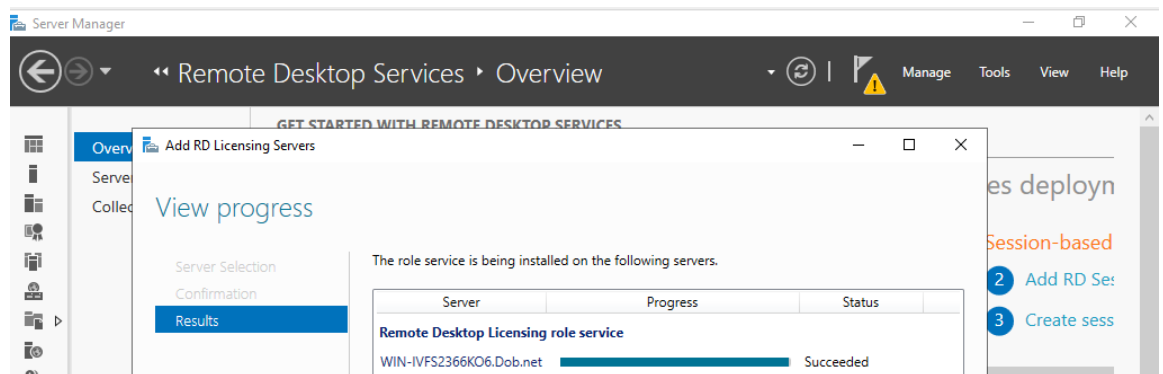


Рисунок 3.35 – Встановлення ролі серверу ліцензій для першого контролеру

Після встановлення серверу ліцензій перевіряю чи дозволено приєднання через служби віддаленого робочого столу. Для цього додаю користувачів яким дозволено користуватися сервісами віддаленого доступу.

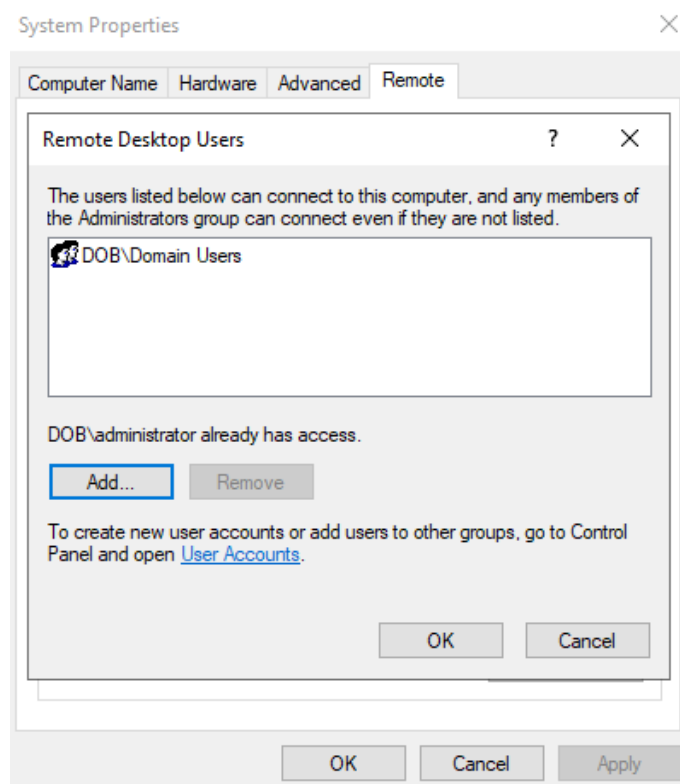


Рисунок 3.36 – Додаю користувачів до групи віддаленого доступу

Перейдемо до налаштування RD Licensing. Ліцензування буде здійснюватися у режимі Per User.

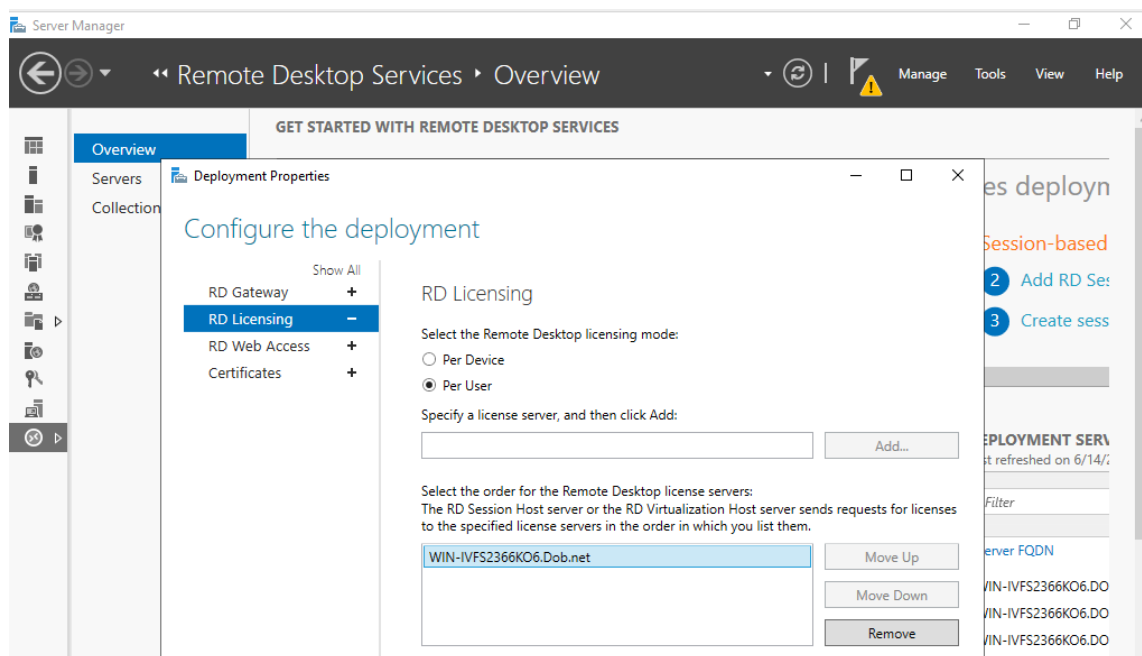


Рисунок 3.37 – Вибираю режим ліцензування

Після цього можна переходити до створення самопідписаного сертифікату. Сертифікат необхідний для підтримання необхідного рівня безпеки при

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 84   |

використання служби віддаленого робочого столу. Для створення цього сертифікату використовуємо PowerShell. Створюю сертифікат і задаю пароль для нього.

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

PS C:\Users\Administrator> New-SelfSignedCertificate -CertStoreLocation cert:\localmachine\my -dnsname "RDP"

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\my

Thumbprint                               Subject
-----
B8D793420B68D3A18044CDCADCCFCE391D1E415  CN=RDP

PS C:\Users\Administrator> $pwd = ConvertTo-SecureString -String "D12345d" -Force -AsPlainText
PS C:\Users\Administrator>
```

Рисунок 3.38 – Створення сертифікату

Далі необхідно вивантажити створений сертифікат у вигляді файлу.

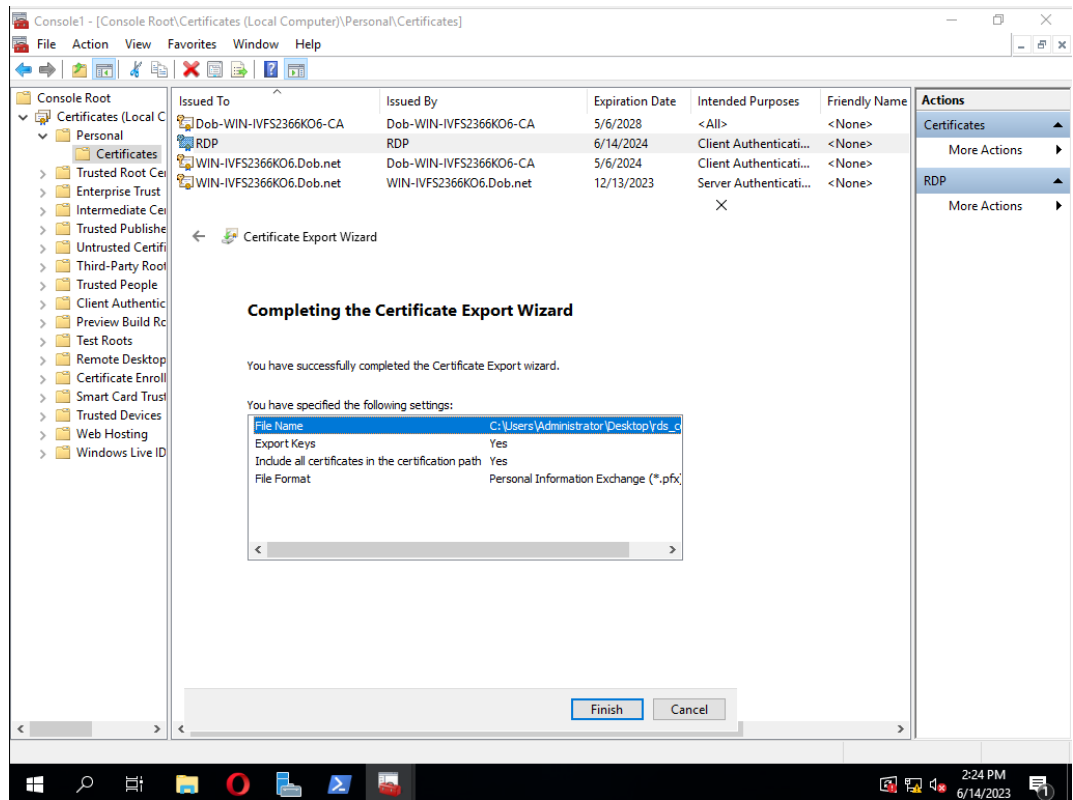


Рисунок 3.39 – Експорт сертифікату

Після експорту сертифікату можна продовжити налаштування ліцензування. Використаємо цей сертифікат для 3 ролей (RD Connection Broker — Enable Single Sign On \ Publishing, RD Web Access).

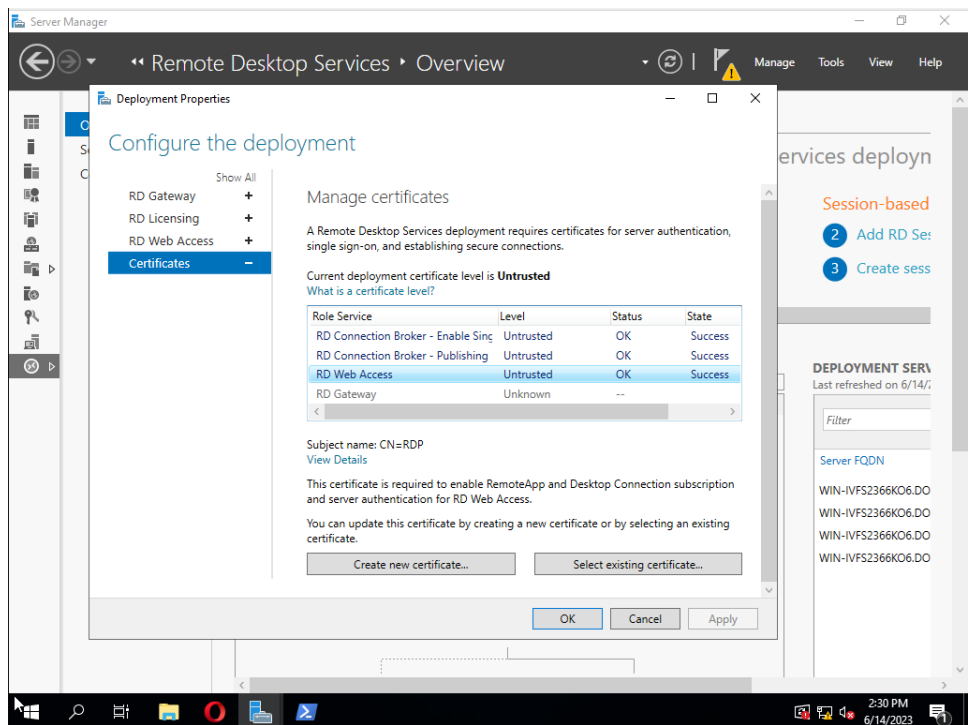


Рисунок 3.40 – Використання сертифікату

Далі додаю DNS-запит для доступу до служби віддаленого робочого столу. Використання доменного ім'я зробить використання служб віддаленого доступу зручнішим.

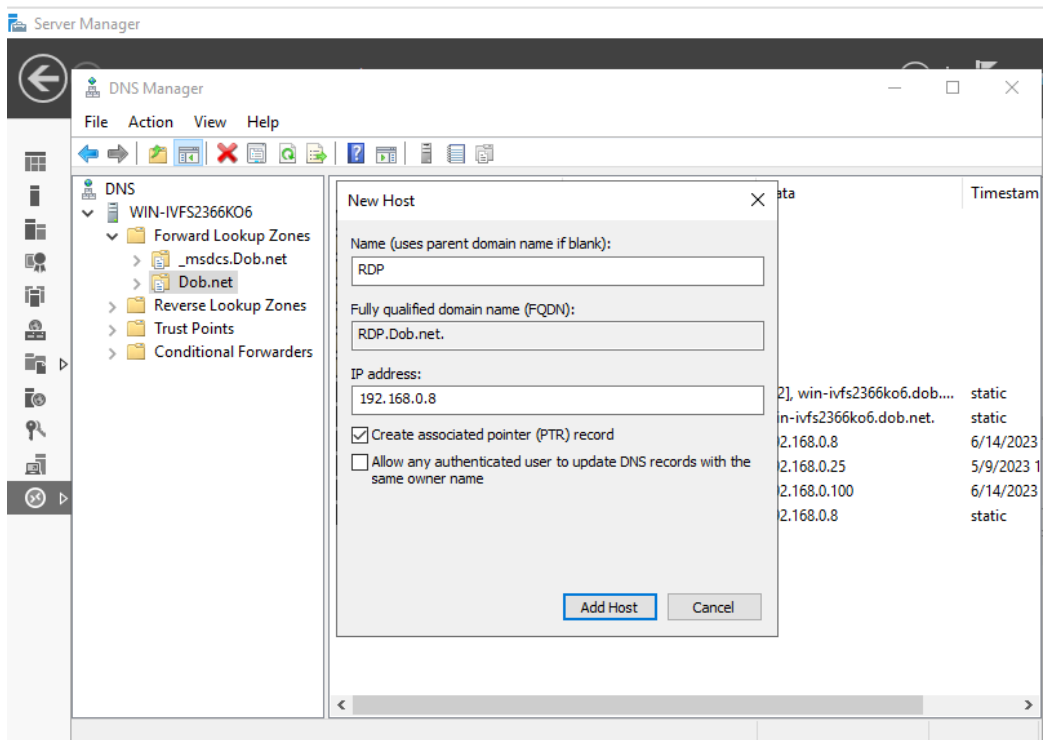


Рисунок 3.41 – Створення DNS-запису для RDP

Після перевірки працездатності серверу можна переходити до створення колекції програм для використання. Спочатку створюю колекцію.

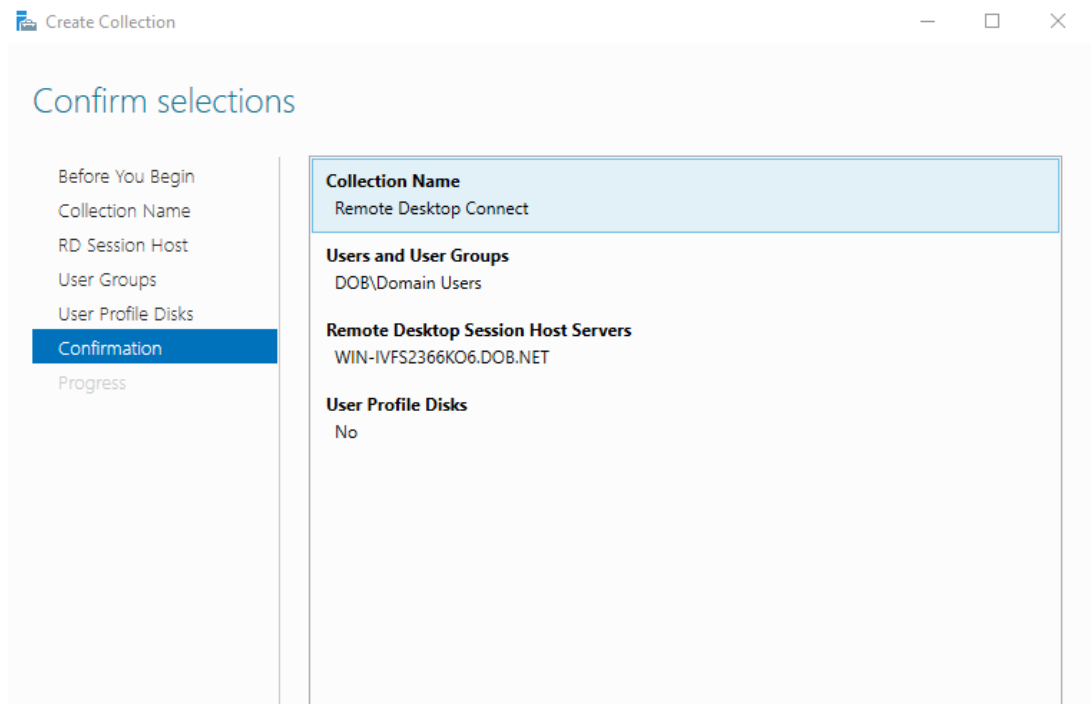


Рисунок 3.42 – Створення колекції

Потім додаю програми для віддаленого використання, додаю програму для віддаленого підключення.

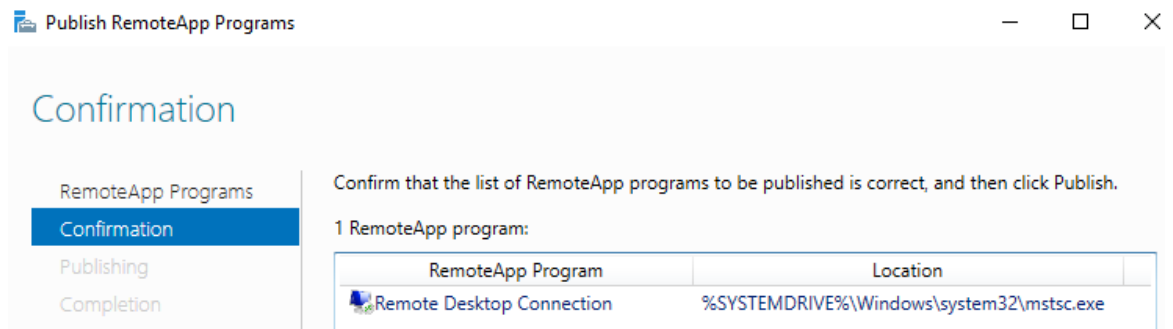


Рисунок 3.43 – Додавання програм для колекції

Далі налаштуємо ще одну функцію для підвищення комфорту користування ІТ інфраструктурою компанії.

Для керування спільними принтерами в Active Directory встановимо роль Print and Document Services. Ця служба дозволить користувачам домену використовувати спільні принтери.

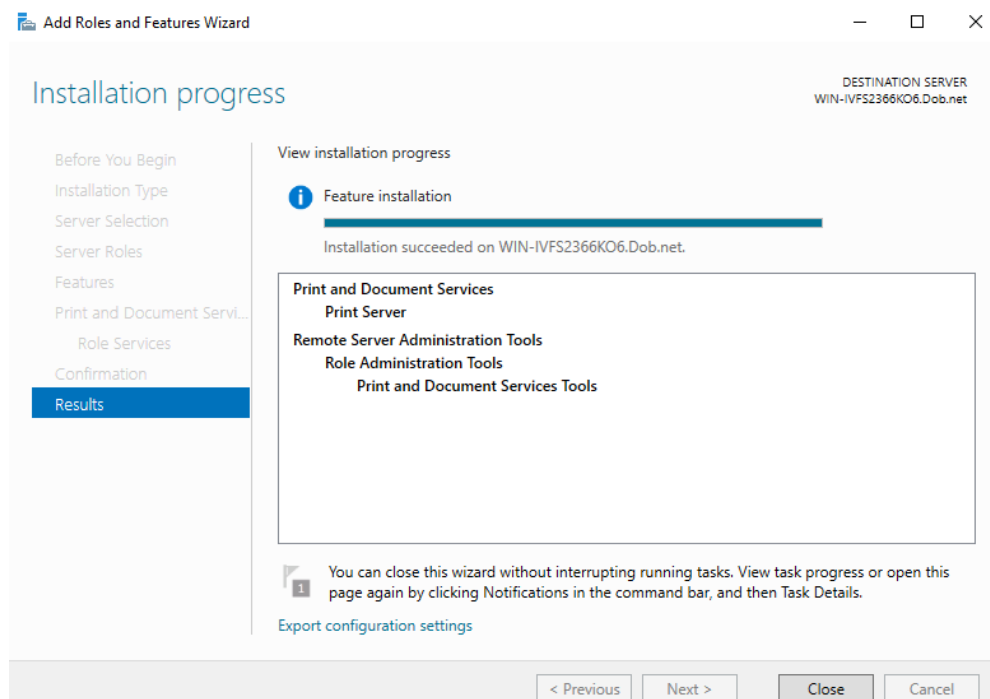


Рисунок 3.44 – Встановлення серверу друку

Після встановлення серверу можна переходити до його налаштування. Переходимо до оснащення Print Management і бачимо встановленні у системі принтери. Бачимо 4 принтери від компанії HP, ці принтери необхідно поділити між департаментами. Важливо пам'ятати, що працівники департаментів не повинні мати доступ до принтерів інших департаментів.

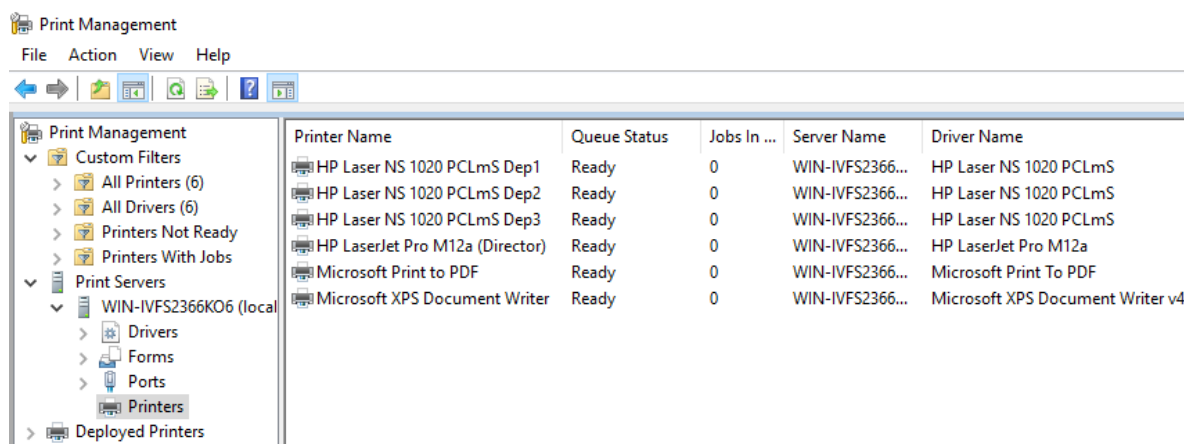


Рисунок 3.45 – Головне вікно оснащення Print Management

Для розмежування доступу до департаментів необхідно використати групові політики, використаємо вже створену політику прив'язану до відповідного департаменту.

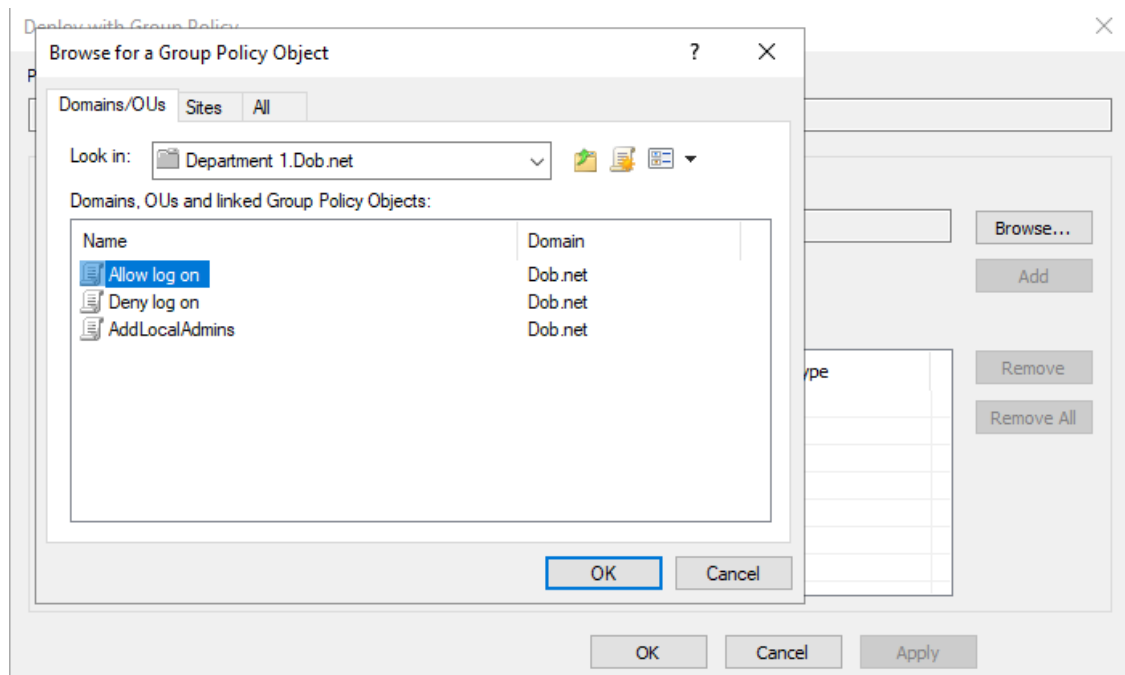


Рисунок 3.46 – Вибір групової політики для обмеження доступу до принтеру

Після налаштування принтера, переходимо до робочої станції першого департаменту, спробуємо додати налаштований принтер. Переходимо до встановлення принтеру, спробуємо його знайти в мережі.

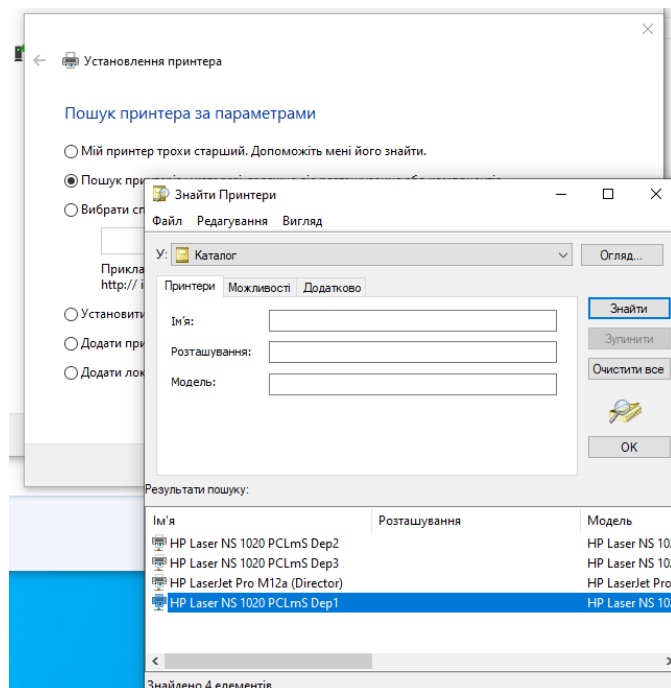


Рисунок 3.47 – Налаштований принтер у мережі

Після того як знайшли принтер можна переходити до налаштування драйверу. Вибираємо принтер і надаємо дозвіл на встановлення драйверу.

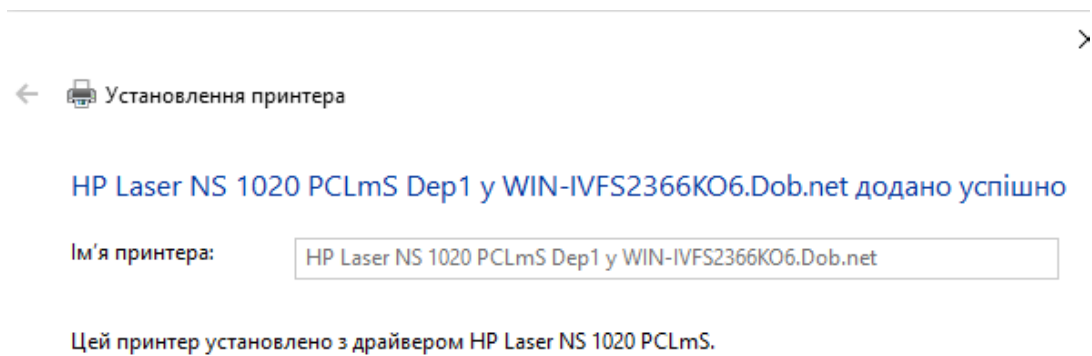


Рисунок 3.48 – Встановлення принтера

Після встановлення принтеру можна перевірити його працездатність, для цього роздрукуємо пробну сторінку.

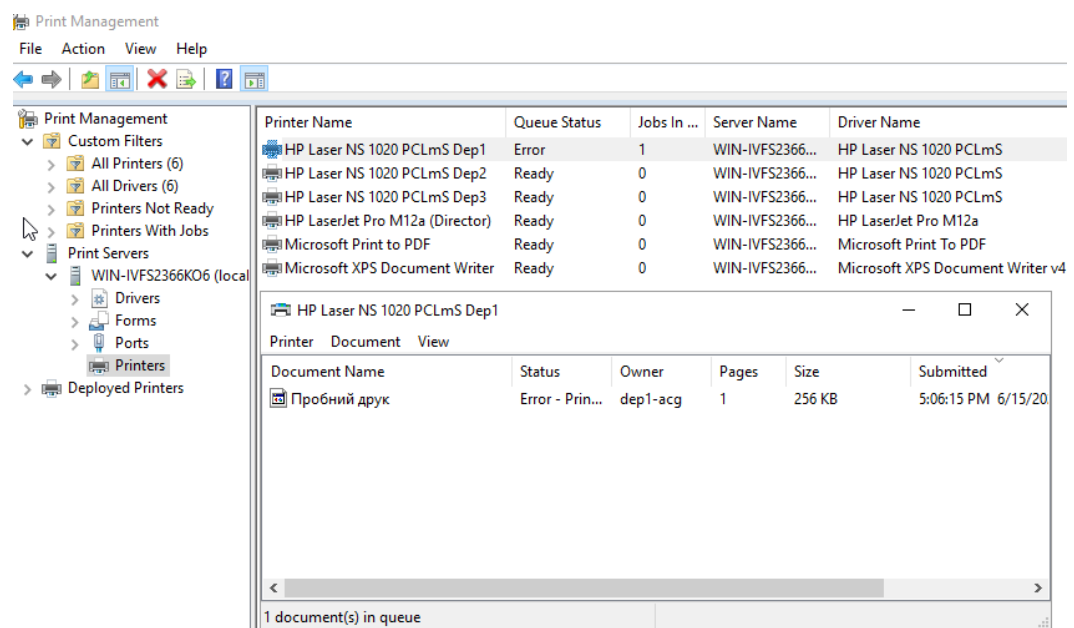


Рисунок 3.49 – Черга друку принтера

Можна побачити, що все працює правильно і сторінка надійшла на друк. Але через те, що принтер віртуальний, виникла помилка.

Після налаштування більшості функцій контролеру домену, переходи до додавання ще одного контролеру домену і налаштування реплікації даних

Почнемо з приєднання нового контролеру домену. Для цього встановимо новий Windows Server. Процес встановлення описувати не буду, він описаний вище. Далі розгортаю сервер як контролер домену, після додаю контролер до домену організації.

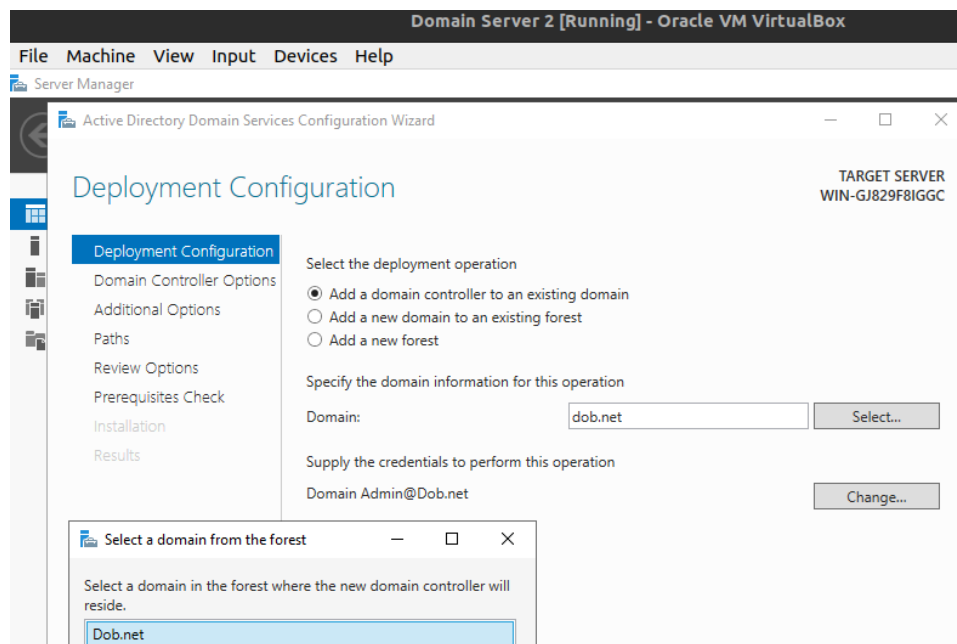


Рисунок 3.50 – Додавання контролеру до домену  
Розгортаємо новий контролер як Read Only (RODC).

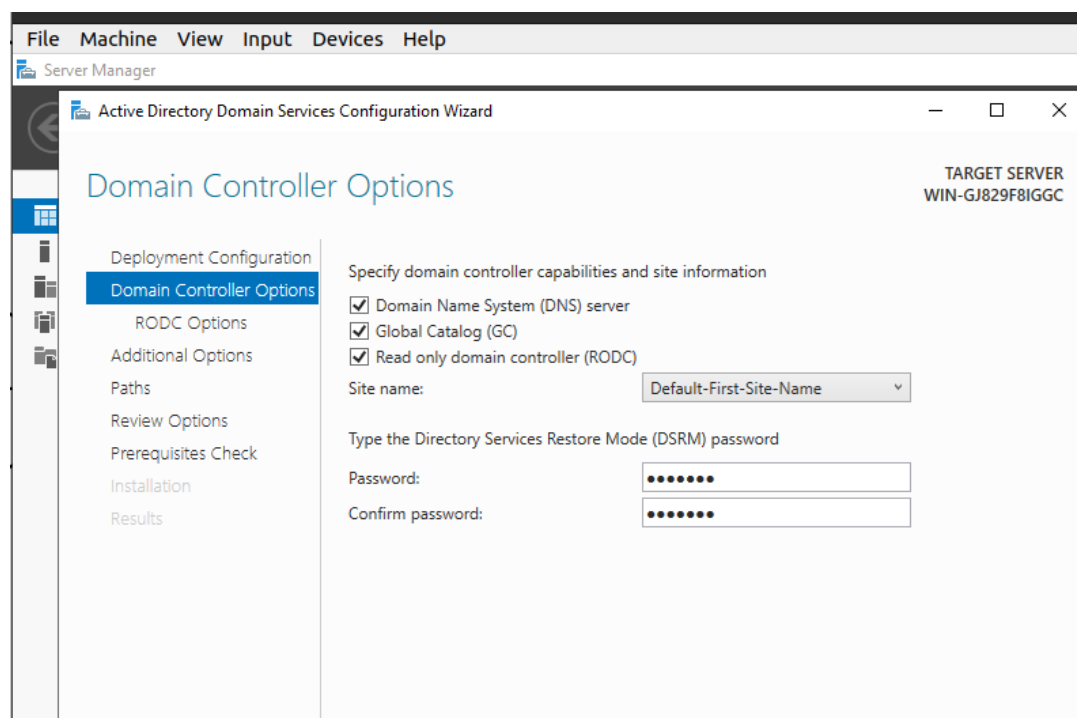


Рисунок 3.51 – Розгортання контролеру як Read Only  
Потім налаштовуємо реплікацію з першого контролеру домену.

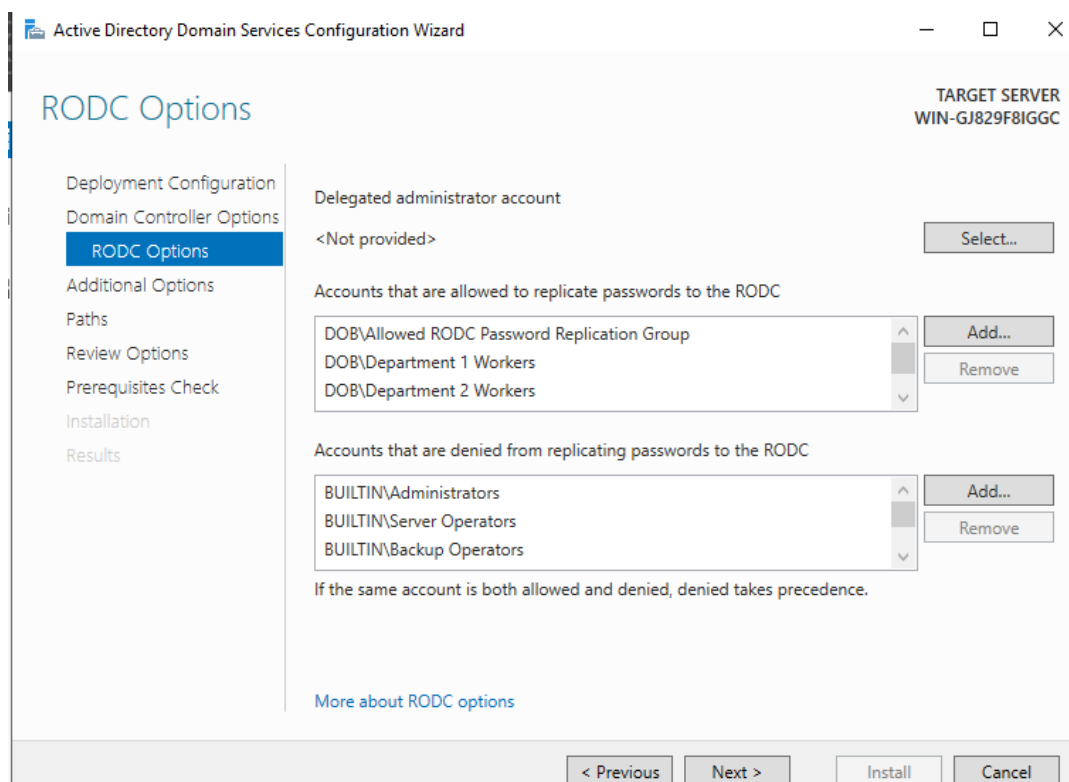


Рисунок 3.52 – Налаштування груп користувачів для реплікації

### 3.2 Налаштування комунікаційних пристроїв мережної інфраструктури

В налаштуванні комунікаційних пристроїв мережної інфраструктури почне з налаштування доступу до мережі Інтернет (звісно після налаштування IP-адресації), для цього використаємо технологію NAT.

У наш час кожна мережа має мати можливість у виходу у Інтернет, тому є необхідність у налаштуванні зв'язку, для цього буде використано NAT Overflow.

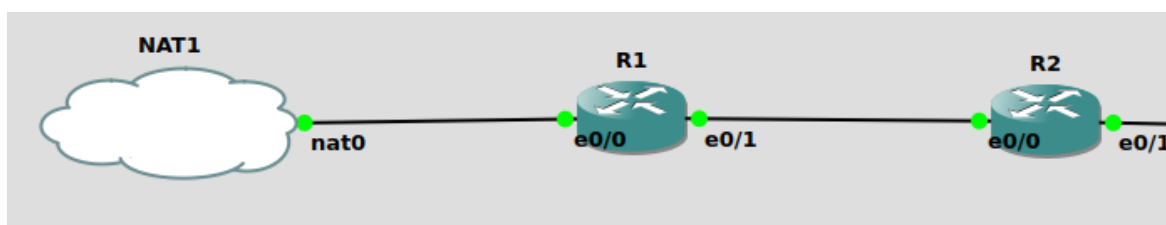


Рисунок 3.53 – Налаштування NAT

Для реалізації налаштувань було використано 2 маршрутизатори Cisco і були введені такі налаштування:

R1

```
int e0/0
ip nat outside
```

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 92   |

```

exit
int e0/1
ip nat inside
exit
ip nat inside source list 1 interface e0/0 overload
access-list 1 permit any
int e0/0
ip address dhcp
no sh
int e0/1
ip address 10.1.1.254 255.255.255.0
no sh
ex
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
default-information originate
end

```

- R2

```

int e0/0
ip address 10.1.1.1 255.255.255.0
no sh
exit
ip route 0.0.0.0 0.0.0.0 10.1.1.254
ip domain-lookup
ip name-server 8.8.8.8 8.8.4.4
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.255 area 0
default-information originate
end

```

Після проведення відповідних налаштувань мережа має вихід у Інтернет.

Для підвищення рівня безпеки у мережі необхідна можливість логування подій та перегляду логованих подій. Для цього спочатку необхідно налаштувати протокол NTP. Основним NTP сервером виступає контролер домену, він отримує адресу з мережі Інтернет. Далі він передає час на маршрутизатор R1, а сам маршрутизатор передає NTP на інші мережеві пристрої.

```

R2
(2)T4, DEVELOPMENT TEST SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Thu 08-Oct-15 21:21 by prod_rel_team
*Jun 16 11:49:48.876: %SSH-5-ENABLED: SSH 2.0 has been enabled
*Jun 16 11:49:48.883: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Jun 16 11:49:48.883: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
Jun 16 11:50:28.894: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.254 on Ethernet0/0 fr
om LOADING to FULL, Loading Done
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#service timestamps log datetime msec
R2(config)#service timestamps debug datetime msec
R2(config)#clock timezone UTC +2
R2(config)#clock summer-time CEST recurring
R2(config)#ntp authentication-key 1 md5 pass1
R2(config)#ntp trusted-key 1
%NTP trusted-key is invalid : key already configured
R2(config)#ntp authenticate
R2(config)#ntp master 15
R2(config)#ntp server 0.ua.pool.ntp.org
Translating "0.ua.pool.ntp.org"...domain server (8.8.8.8) [OK]
R2(config)#

```

Рисунок 3.54 – Налаштування NTP серверу

```

SW2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW2(config)#service timestamps log datetime msec
SW2(config)#service timestamps debug datetime msec
SW2(config)#clock timezone UTC +2
SW2(config)#clock summer-time CEST recurring
SW2(config)#ntp authentication-key 1 md5 pass1
SW2(config)#ntp trusted-key 1
%NTP trusted-key is invalid : key already configured
SW2(config)#ntp authenticate
SW2(config)#ntp server 192.168.0.1

```

Рисунок 3.55 – Налаштування NTP клієнта

Після налаштування NTP можна переходити до налаштування SYSLOG, основні налаштування серверу описані вище, налаштування зі сторони мережних пристроїв представлені в основному налаштування IP адреси серверу.

```

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#logging on
R2(config)#logging 192.168.0.8
R2(config)#logging buffered 64000
R2(config)#logging userinfo

```

Рисунок 3.56 – Налаштування протоколу Syslog

Для забезпечення можливості комфортного адміністрування необхідно забезпечити можливість віддаленого підключення до мережних пристроїв. Підключення до пристроїв здійснюється за допомогою протоколу SSHv2, а для підвищення рівня безпеки будуть використані ACL, які обмежують можливість віддаленого підключення з невірних хостів.

```

R2
R2(config)#ip domain-name DIP.net
R2(config)#crypto key generate rsa general-keys modulus 1040
The name for the keys will be: R2.DIP.net

% The key modulus size is 1040 bits
% Generating 1040 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

R2(config)#line vty 0 4
R2(config-line)#login local
R2(config-line)#transport input ssh
R2(config-line)#logging synchronous
R2(config-line)#exit
R2(config)#access-list 12 permit host 192.168.0.25
R2(config)#line vty 0 4
R2(config-line)#access-class 12 in
R2(config-line)#exit
.May 7 13:48:51.278: %SSH-5-ENABLED: SSH 1.99 has been enabled
R2(config-line)#exit
R2(config)#ip ssh version 2

```

Рисунок 3.57 – Налаштування SSH/ACL

Дані налаштування забезпечать підключення лише з конкретного хоста і лише за протоколом SSHv2. Далі необхідно перевірити можливість підключення

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 94   |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

за протоколом SSH. Спочатку перевірю можливість підключення з авторизованого хоста.

```

OpenSSH SSH client
PS C:\Users\Administrator> ssh admin@192.168.0.1
Password:
R2#show run
Building configuration...

Current configuration : 2699 bytes
!
! Last configuration change at 16:32:19 CEST Sun May 7 2023
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R2
!
boot-start-marker
boot-end-marker
!
!
logging userinfo
logging buffered 64000
!
no aaa new-model
clock timezone UTC 2 0
clock summer-time CEST recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip icmp rate-limit unreachable
!
!

```

Рисунок 3.58 – Підключення з авторизованого хоста

Підключення за допомогою SSH пройшло успішно. Далі перевірю можливість підключення не з авторизованого хоста.

```

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\administrator> ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
PS C:\Users\administrator> ssh admin@192.168.0.1
ssh: connect to host 192.168.0.1 port 22: Connection refused
PS C:\Users\administrator>

```

Рисунок 3.59 – Підключення з не авторизованого хоста

Підключення не вдалося, тобто налаштування правильні.

Після налаштування віддаленого підключення до мережевих пристроїв за допомогою SSHv2, переходимо до налаштування RADIUS.

Для централізації авторизації і підвищення рівня безпеки існує необхідність у реалізації можливості підключення за допомогою протоколу AAA, у нашому випадку RADIUS. Для цього буде використаний вбудований у Active Directory модуль Network Policy Center який має вбудований RADIUS сервер.

Налаштовуємо підключення за допомогою RADIUS-серверу. Раніше ми налаштували вже RADIUS-сервер. Тепер налаштуємо RADIUS-клієнти.

```

Escape character is '^]'.

SW1(config)#
SW1#
Jun 18 15:00:47.692: %SYS-5-CONFIG_I: Configured from console by console
SW1#
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#enable secret D12345d
SW1(config)#aaa new-model
SW1(config)#aaa authentication login default group radius local
SW1(config)#aaa authorization exec default group radius if-authenticated
SW1(config)#radius-server host 192.168.0.8 key D12345d
SW1(config)#service password-encryption
  
```

Рисунок 3.60 – Налаштування RADIUS-клієнта

Для роботи клієнту налаштуємо IP серверу та ключ, також створюємо локального користувача, який буде використовуватися для авторизації якщо RADIUS сервер не доступний, для цього налаштуємо пріоритет авторизації спочатку RADIUS, якщо сервер відсутній то за допомогою локального користувача.

Перевіряємо можливість підключення за допомогою RADIUS.

```

OpenSSH SSH client

PS C:\Users\MNA> ssh SW1
The authenticity of host 'sw1 (192.168.0.3)' can't be established.
RSA key fingerprint is SHA256:NxCz1Y7uXHPHqyTlaJWVgL/1GK4WBChT19ruw4BG04k.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'sw1,192.168.0.3' (RSA) to the list of known hosts.
Password:

SW1>en
Password:
% Access denied

SW1>en
Password:
SW1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#
  
```

Рисунок 3.61 – Перевірка можливості підключення

Підключення з використання RADIUS та SSH можливе, Користувач, як і планувалося має повноваження 15 рівня.

```
SW1(config)#
Jun 18 15:02:37.100: %SYS-5-PRIV_AUTH_FAIL: Authentication to privilege level 15
failed by dob\mna on vty0 (192.168.0.25)
SW1(config)#
Jun 18 15:02:44.403: %SYS-5-PRIV_AUTH_PASS: Privilege level set to 15 by dob\mna
on vty0 (192.168.0.25)
```

Рисунок 3.62 – Повідомлення про аутентифікацію на комутаторі

### 3.3. Налаштування засобів захисту комунікаційних пристроїв мережної інфраструктури

Одним з головних проблем у забезпеченні безпеки мережі були можливі атаки на протоколи DHCP та ARP. Щоб зробити мережу більш безпечною, необхідно налаштувати функцію DHCP Snooping та DAI на комутаторах. Цей метод захисту дозволяє контролювати повідомлення без прямого впливу на трафік користувачів або інші протоколи. Щоб правильно налаштувати функцію, потрібно визначити надійні порти, які підключені до комутаторів або DHCP-серверів, і ненадійні порти, які підключені до клієнтів.

Налаштовуємо функції Port Security, BPDU Guard, DHCP Snooping і PortFast на комутаторах, почне налаштування мережі з комутатора SW2.

Налаштовуємо функції захисту для комутатора SW2. Почнемо з налаштувань для мережевих пристроїв.

Глобальні налаштування:

SW2(config)#ip dhcp snooping

SW2(config)#ip arp inspection vlan 1

Налаштування для мережевих пристроїв та серверів:

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 97   |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

```

SW2
Fri Jun 16 2023]]
Jun 16 13:30:04.894: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/1
, vlan 1.([0800.27ef.f2e9/192.168.0.25/0800.2725.1d8b/192.168.0.8/16:30:04 CEST
Fri Jun 16 2023]]
Jun 16 13:30:05.898: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Et0/2
, vlan 1.([0800.2725.1d8b/192.168.0.8/0800.27ef.f2e9/192.168.0.25/16:30:05 CEST
Fri Jun 16 2023]]
SW2(config)#int range e0/0, e0/3, e1/0-1
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport port-security
SW2(config-if-range)#switchport port-security maximum 1
SW2(config-if-range)#switchport port-security mac-address sticky
SW2(config-if-range)#ip arp inspection trust
SW2(config-if-range)#ip dhcp snooping limit rate 256
SW2(config-if-range)#ip dhcp snooping trust
SW2(config-if-range)#ex
SW2(config)#int e0/2
SW2(config-if)#switchport mode access
SW2(config-if)#switchport port-security
SW2(config-if)#switchport port-security maximum 1
SW2(config-if)#switchport port-security mac-address sticky
SW2(config-if)#ip arp inspection trust
SW2(config-if)#ex
SW2(config)#

```

Рисунок 3.63 – Налаштування протоколу STP для мережевих пристроїв та серверів на комутаторів

Налаштування протоколу STP для робочих станцій:

```

SW2(config)#int range e0/1, e1/2
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport port-security
SW2(config-if-range)#switchport port-security maximum 3
SW2(config-if-range)#switchport port-security mac-address sticky
SW2(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 2 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW2(config-if-range)#spanning-tree bpduguard enable
SW2(config-if-range)#

```

Рисунок 3.64 – Налаштування протоколу STP для робочих станцій

Налаштування протоколу STP для портів, що не використовується:

```

SW2(config)#int range e2/0-3, e3/0-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport port-security
SW2(config-if-range)#switchport port-security maximum 3
SW2(config-if-range)#switchport port-security mac-address sticky
SW2(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 8 interfaces due to the range command
but will only have effect when the interfaces are in a non-trunking mode.
SW2(config-if-range)#spanning-tree bpduguard enable
SW2(config-if-range)#switchport access vlan 99
% Access VLAN does not exist. Creating vlan 99
SW2(config-if-range)#sh
SW2(config-if-range)#

```

Рисунок 3.65 – Налаштування захисту для портів, що не використовуються

**Висновки:** у третьому розділі була створена мережа і наведені основний лістинг команд для налагодження відповідних протоколів для мережевих пристроїв у створеній мережі. Був встановлений Microsoft Server 2019, який був розгорнутий як контролер домену. На контролері домену був розгорнутий RADIUS сервер, був встановлений NTP і Syslog сервери. Було налаштоване логування подій як і для мережевих пристроїв, так і для робочих станцій. Був налаштований серверу друку. Для мережевих пристроїв були налаштовані відповідні функції безпеки. Створена мережа протестована на коректність налаштувань.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 99   |

## ВИСНОВКИ

При виконанні дипломного проекту був проведений аналіз теми дипломного проекту, був проведений розгляд технології MS Active Directory, був реалізований Active Directory сервер на базі віртуальної машини Windows, підбрані відповідні технології та протоколи для реалізації мережі на базі теми курсового проекту, була створена і налаштована сама мережа, був наведений опис усіх підмереж створеної мережі.

У першому розділі були проведені теоретичні дослідження необхідних для побудови мережі технологій, згідно теми дипломної роботи було сформовано технічне завдання, яке формує необхідні вимоги для майбутньої мережі.

У другому розділі був розроблений проект самої комунікаційної мережі, на базі розглянутих технологій і протоколів описаних у першому розділі. Була розроблена топологічна структура мережі, був проведений опис створеної мережі: кількість і тип комунікаційних вузлів та протоколи, які будуть використовуватися. Була створена схема адресації мережі, схема була створена з метою забезпечення роботи мережі і економного використання IP адрес. Були розібрані функції домену Active Directory і мережевих пристроїв, які будуть використані при створенні мережі. Була створена система користувачів організації. На основі розглянутих у першому розділі атак і методів їх захисту була створена діаграма загроз. На основі створеної діаграми загроз і системи користувачів було створено розмежування доступу у мережі. Також були розібрані технології захисту мережевих пристроїв і особливості їх реалізації.

У третьому розділі була створена мережа і наведені основний лістинг команд для налагодження відповідних протоколів для мережевих пристроїв у створеній мережі. Був встановлений Microsoft Server 2019, який був розгорнутий як контролер домену. На контролері домену був розгорнутий RADIUS сервер, був встановлений NTP і Syslog сервери. Було налаштоване логування подій як і для мережевих пристроїв, так і для робочих станцій. Був налаштований серверу друку. Для мережевих пристроїв були налаштовані відповідні функції безпеки. Створена мережа протестована на коректність налаштувань.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 100  |

На мою думку, робота має велику доцільність та практичну цінність, оскільки в ході її виконання були отримані навички створення захищених корпоративних мереж. Створена мережа не є навчальною і підходить для реальної роботи. Мережа має великий функціонал і достатній рівень захисту. Звісно мережа створена у емуляторі GNS3, тому її використовувати її у реальному житті не вийде, але навички і знання отримані при створенні мережі мають реальну практичну цінність.

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 101  |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Active Directory Domain Services Overview [Електронний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> – 17.08.2022. – Загол. з екрану.
2. Kerberos Authentication Overview [Електронний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/ru-ru/windows-server/security/kerberos/kerberos-authentication-overview> – 21.12.2022. – Загол. з екрану.
3. NTLM user authentication [Електронний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/ntlm-user-authentication> – 23.02.2023. – Загол. з екрану.
4. NTLM [Електронний ресурс] / Fandom. – <https://microsoft.fandom.com/ru/wiki/NTLM> – 23.02.2023. – Загол. з екрану – 23.02.2021. – Загол. з екрану
5. Basic LDAP Concepts [Електронний ресурс] / LDAP. – <https://ldap.com/basic-ldap-concepts/> – 11.08.2021. – Загол. з екрану
6. Computer Network | AAA (Authentication, Authorization and Accounting) [Електронний ресурс] / LDAP. – <https://www.geeksforgeeks.org/computer-network-aaa-authentication-authorization-and-accounting/> – 21.08.2022. – Загол. з екрану
7. What is the RADIUS Protocol? [Електронний ресурс] / jumpcloud. – <https://jumpcloud.com/blog/what-is-the-radius-protocol> – 23.02.2022. – Загол. з екрану
8. STP [Електронний ресурс] / gitbook. – <https://linkmeup.gitbook.io/sdsm/4.-stp/01-stp> – 23.02.2020. – Загол. з екрану
9. Access Control List [Електронний ресурс] / gitbook. – <https://linkmeup.gitbook.io/sdsm/5.-acl-i-nat/00-access-control-list> – 23.06.2021. – Загол. з екрану
10. Print and Document Services Overview [Електронний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/en-us/previous-versions/windows/it->

|      |      |                     |        |      |                                 |      |
|------|------|---------------------|--------|------|---------------------------------|------|
|      |      | Добровольський Д.В. |        |      | <i>КІК.КР.Б – 123 – 04 – ПЗ</i> | Арк. |
|      |      | Воротніков В.В.     |        |      |                                 |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                                 | 102  |

[pro/windows-server-2012-r2-and-2012/hh831468\(v=ws.11\)](https://pro/windows-server-2012-r2-and-2012/hh831468(v=ws.11)) – 15.04.2017. – Загол. з екрану

11. Active Directory Replication Concepts [Електронний ресурс] / Microsoft Learn. – <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/replication/active-directory-replication-concepts> – 29.06.2021 – Загол. з екрану

12. STP - Spanning Tree Protocol Explained With Examples [Електронний ресурс] / ComputerNetworkingNotes – <https://www.computernetworkingnotes.com/ccna-study-guide/stp-spanning-tree-protocol-explained-with-examples.html> – 09.08.2019 – Загол. з екрану

13. Network Address Translation Definition | How NAT Works [Електронний ресурс] / CompTIA – <https://www.comptia.org/content/guides/what-is-network-address-translation#:~:text=What%20Is%20NAT%3F,as%20do%20most%20home%20router> s. – 21.12.2020. – Загол. з екрану.

14. How Does SSH Protocol Work? [Електронний ресурс] / N-able – <https://www.n-able.com/blog/ssh-network-protocol-overview> – 08.08.2019 – Загол. з екрану

15. Port Security [Електронний ресурс] / Study-CCNA – <https://study-ccna.com/port-security/> – 18.03.2018 – Загол. з екрану

16. ARP Poisoning: What it is & How to Prevent ARP Spoofing Attacks [Електронний ресурс] / Varonis – <https://www.varonis.com/blog/arp-poisoning> – 04.08.2022 – Загол. з екрану

17. ARP Spoofing: What Is the Aim of an ARP Spoofing Attack? [Електронний ресурс] / PowerdMarc – <https://powerdmarc.com/what-is-arp-spoofing-attack/> – 04.08.2022 – Загол. з екрану

18. The Ultimate Guide to DHCP Spoofing and Starvation [Електронний ресурс] / PivIT Global – Attacks <https://info.pivitglobal.com/resources/dhcp-spoofing-and-starvation-attacks> – 26.05.2022 – Загол. з екрану

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 103  |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

19. DHCP Attacks + WPAD [Електронний ресурс] / ProSec Networks – <https://www.prosec-networks.com/en/blog/dhcp-attacks-wpad/> – 16.08.2021 – Загол. з екрану

20. What Is DNS Spoofing? [Електронний ресурс] / ProofPoint [https://www.proofpoint.com/us/threat-reference/dns-spoofing#:~:text=DNS%20\(Domain%20Name%20Service\)%20spoofing,malicious%20website%20under%20attacker%20control](https://www.proofpoint.com/us/threat-reference/dns-spoofing#:~:text=DNS%20(Domain%20Name%20Service)%20spoofing,malicious%20website%20under%20attacker%20control) – 16.02.2022 – Загол. з екрану

21. What Is DNS Spoofing? [Електронний ресурс] / PowerdMarc – <https://powerdmarc.com/what-is-dns-spoofing/> – 26.05.2022 – Загол. з екрану

22. What Is a Brute Force Attack? [Електронний ресурс] / Fortinet – <https://www.fortinet.com/resources/cyberglossary/brute-force-attack#:~:text=A%20brute%20force%20attack%20is,and%20organizations%27%20systems%20and%20networks>. – 13.02.2022 – Загол. з екрану

23. Man in the middle (MITM) attack [Електронний ресурс] / Fortinet – <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/> – 03.02.2023 – Загол. з екрану

24. Configuring Spanning Tree PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast, and Loop Guard attack [Електронний ресурс] / Fortinet – [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp\\_enha.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html) – 06.05.2007 – Загол. з екрану

25. Understanding and Configuring Dynamic ARP Inspection [Електронний ресурс] / Cisco – <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dynarp.html> – 16.06.2020 – Загол. з екрану

26. Configuring DHCP Snooping [Електронний ресурс] / Cisco – <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SXF/native/configuration/guide/swcg/snoodhcp.pdf> – 09.02.2017 – Загол. з екрану

27. Advanced STP Tuning [Електронний ресурс] / Cisco Press – <https://www.ciscopress.com/articles/article.asp?p=2995351&seqNum=3#:~:text=BPDU%20guard%20is%20a%20safety,is%20added%20to%20a%20topology>. – 11.01.2020 – Загол. з екрану

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 104  |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

28. What is BPDU Guard and How to Configure BPDU Guard? [Електронний ресурс] / GeeksForGeeks – <https://www.geeksforgeeks.org/what-is-bpdu-guard-and-how-to-configure-bpdu-guard/> – 27.12.2021 – Загол. з екрану

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          | 105  |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          |      |

# ДОДАТКИ

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В      |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 106  |

Детальна схема створеної мережі

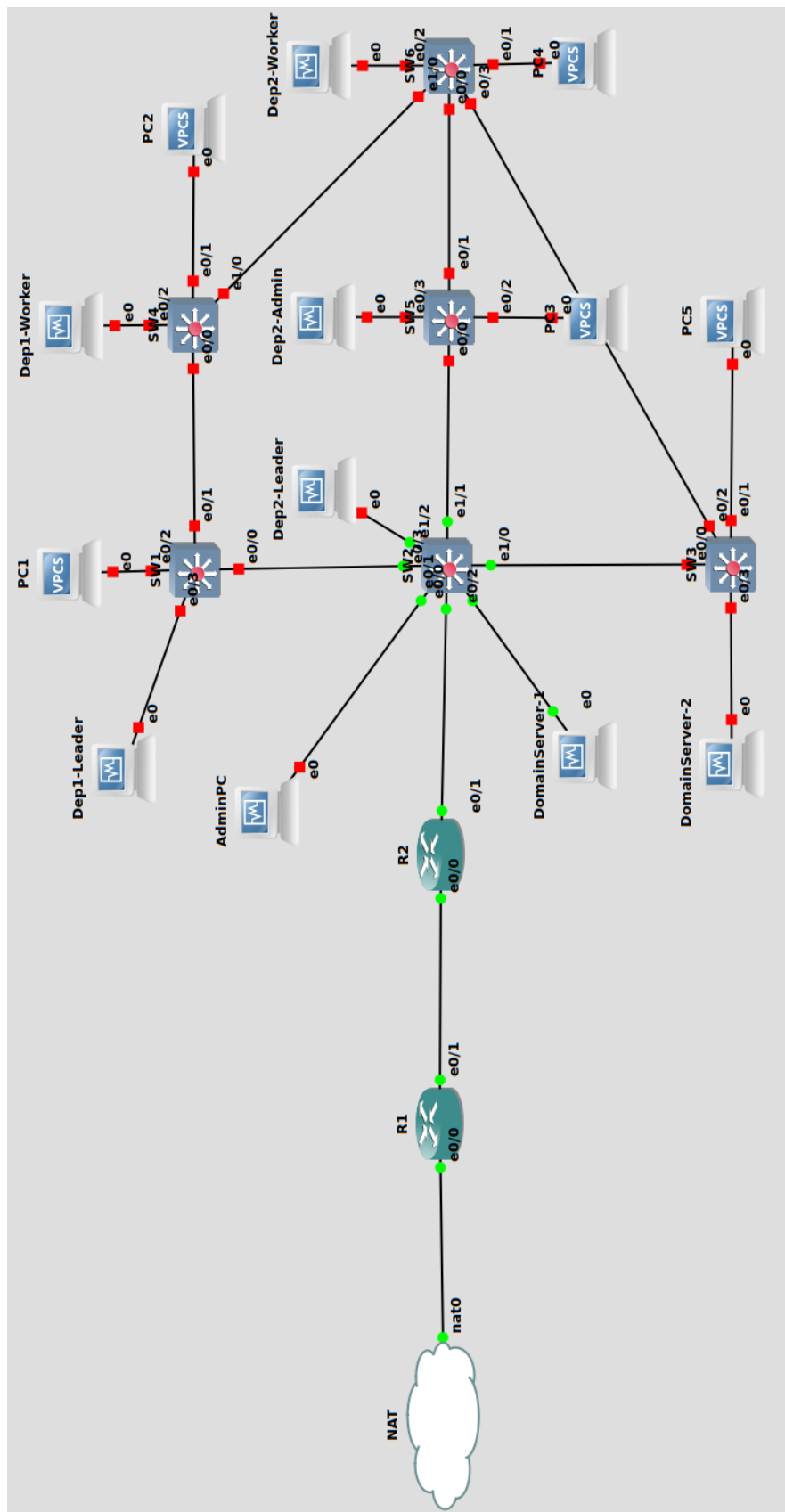


Рисунок А.1 – Детальна схема створеної мережі

Створена система користувачів

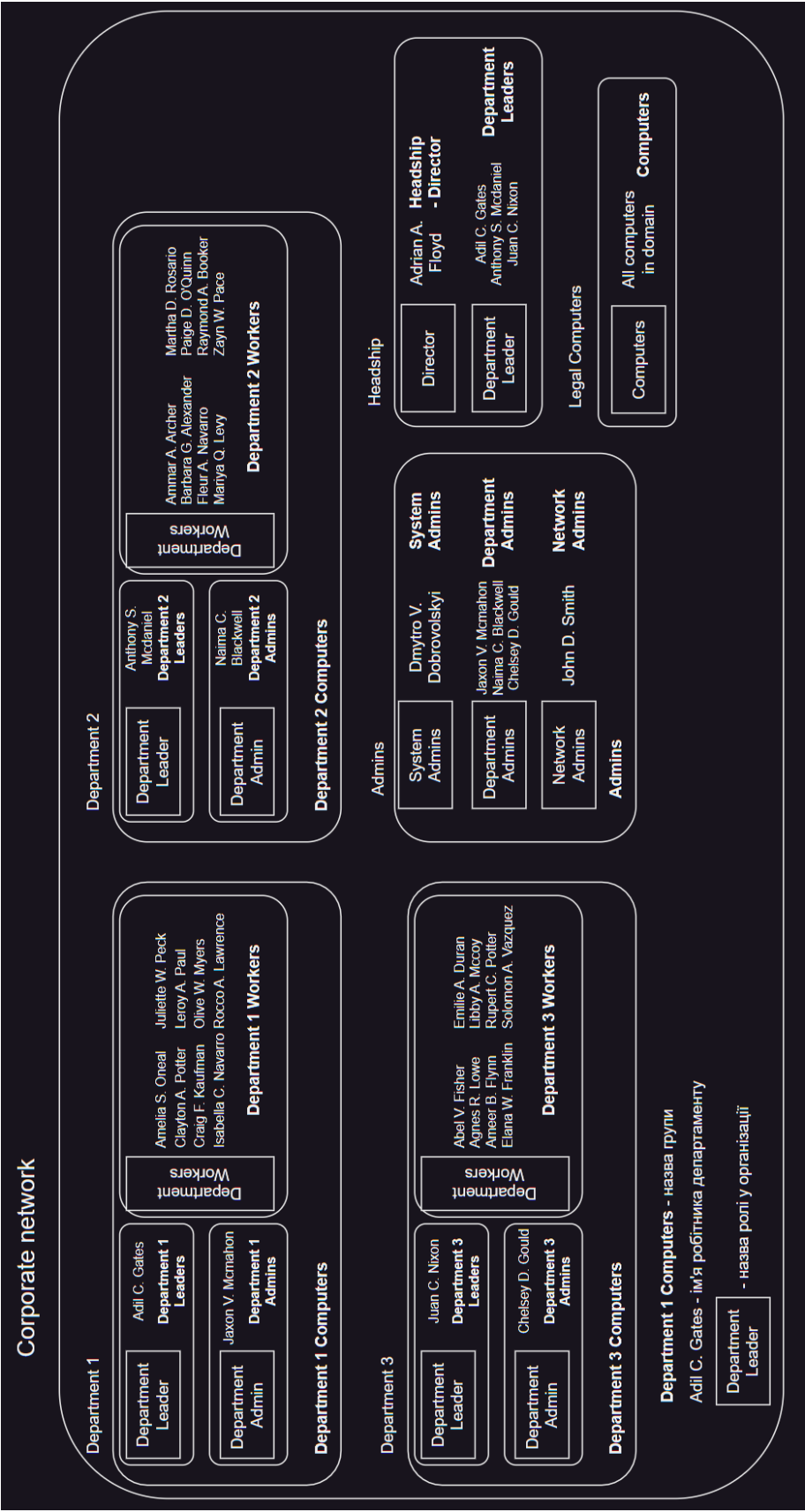


Рисунок Б.1 – Створена система користувачів

## Розмежування доступу

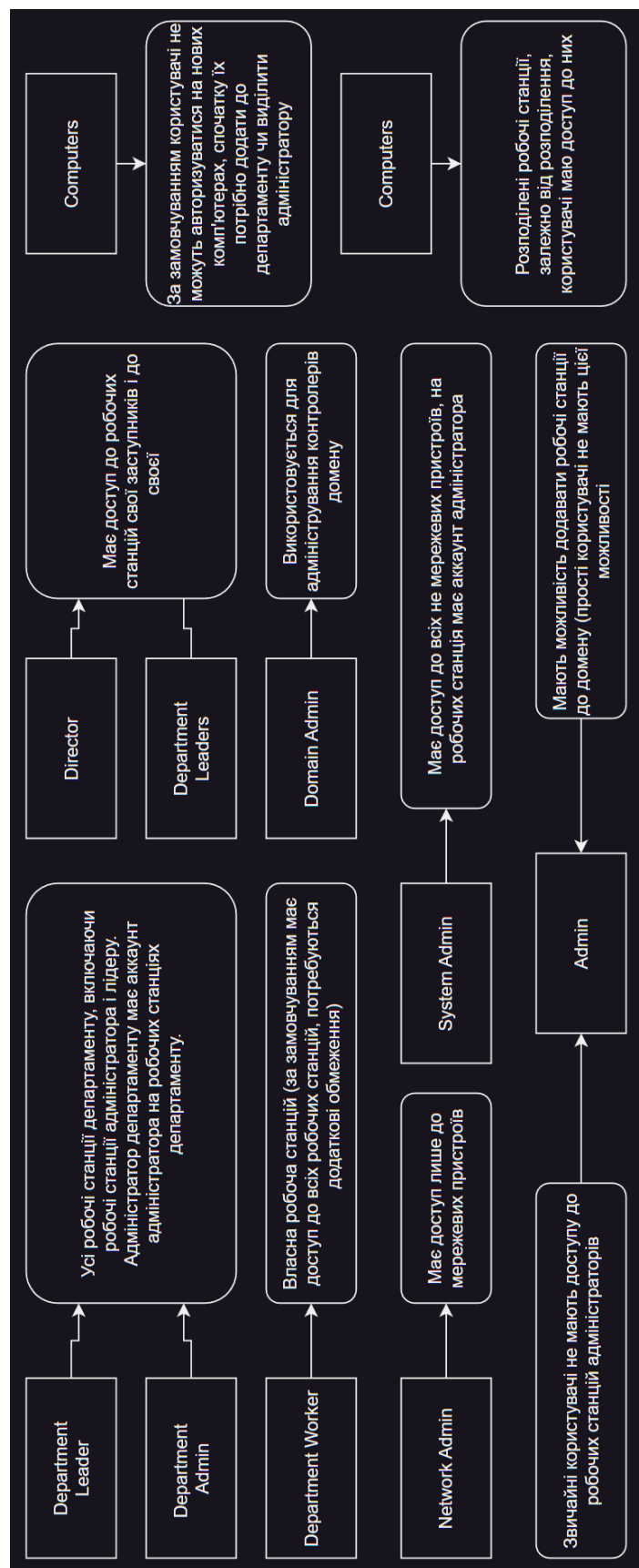


Рисунок В.1 – Розмежування доступу

|      |      |                     |        |      |
|------|------|---------------------|--------|------|
|      |      | Добровольський Д.В. |        |      |
|      |      | Воротніков В.В.     |        |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |

## Параметри інтерфейсів пристроїв

| Пристрій | Інтерфейс | Підключення до пристрою | Підключення до інтерфейсу |
|----------|-----------|-------------------------|---------------------------|
| NAT      | nat0      | R1                      | E0/0                      |
| R1       | E0/0      | NAT                     | nat0                      |
|          | E0/1      | R2                      | E0/0                      |
| R2       | E0/0      | R1                      | E0/1                      |
|          | E0/1      | SW2                     | E0/0                      |
| SW2      | E0/0      | R2                      | E0/1                      |
|          | E0/1      | AdminPC                 | E0                        |
|          | E0/2      | DomainServer-1          | E0                        |
|          | E0/3      | SW1                     | E0/0                      |
|          | E1/0      | SW3                     | E0/0                      |
|          | E1/1      | SW5                     | E0/0                      |
|          | E1/2      | Dep2-Leader             | E0                        |
| SW1      | E0/0      | SW2                     | E0                        |
|          | E0/1      | SW4                     | E0/0                      |
|          | E0/2      | WS-1                    | E0                        |
|          | E0/3      | Dep1-Leader             | E0                        |
| SW4      | E0/0      | SW1                     | E0/1                      |
|          | E0/1      | WS-2                    | E0                        |
|          | E0/2      | Dep1-Worker             | E0                        |
|          | E1/0      | SW6                     | E1/0                      |
| SW5      | E0/0      | SW2                     | E1/1                      |
|          | E0/1      | SW6                     | E0/0                      |
|          | E0/2      | WS-3                    | E0                        |
|          | E0/3      | Dep2-Admin              | E0                        |
| SW6      | E0/0      | SW5                     | E0/1                      |

|                |      |                |      |
|----------------|------|----------------|------|
|                | E0/1 | WS-4           | E0   |
|                | E0/2 | Dep2-Worker    | E0   |
|                | E0/3 | SW3            | E0/2 |
|                | E1/0 | SW4            | E1/0 |
| SW3            | E0/0 | SW2            | E1/0 |
|                | E0/1 | WS-5           | E0   |
|                | E0/2 | SW6            | E0/3 |
|                | E0/3 | DomainServer-2 | E0   |
| AdminPC        | E0   | SW2            | E0/1 |
| DomainServer-1 | E0   | SW2            | E0/2 |
| DomainServer-2 | E0   | SW3            | E0/3 |
| WS-1           | E0   | SW1            | E0/2 |
| WS-2           | E0   | SW4            | E0/1 |
| WS-3           | E0   | SW5            | E0/2 |
| WS-4           | E0   | SW6            | E0/1 |
| WS-5           | E0   | SW3            | E0/1 |
| Dep1-Leader    | E0   | SW1            | E0/3 |
| Dep1- Worker   | E0   | SW4            | E0/2 |
| Dep2-Leader    | E0   | SW2            | E1/2 |
| Dep2-Admin     | E0   | SW5            | E0/3 |
| Dep2-Worker    | E0   | SW6            | E0/2 |

## Параметри конфігурації мережевих пристроїв

## Параметри конфігурації маршрутизатора R1

```

R1#show run
Building configuration...
Current configuration : 2474 bytes
! Last configuration change at 17:46:00 CEST
Fri Jun 16 2023
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
boot-start-marker
boot-end-marker
security passwords min-length 1
logging userinfo
logging buffered 64000
no aaa new-model
clock timezone UTC 2
clock summer-time CEST recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip source-route
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
ip domain name Dob.net
no ipv6 traffic interface-statistics
no ipv6 cef
multilink bundle-name authenticated
username admin privilege 15 secret 5
$1$9WDS$wPe0S9Bsj8KZy2jGC6W5r.
redundancy
ip tcp synwait-time 5
ip ssh version 2
interface Ethernet0/0
ip address dhcp
ip nat outside
ip virtual-reassembly
interface Ethernet0/1
ip address 10.1.1.254 255.255.255.0
ip nat inside
ip virtual-reassembly
...
router ospf 1
log-adjacency-changes

```

```

network 10.1.1.0 0.0.0.255 area 0
default-information originate
ip forward-protocol nd
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0
overload
logging 192.168.0.8
access-list 1 permit any
access-list 12 permit 192.168.0.25
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
access-class 12 in
logging synchronous
login local
transport input ssh
exception data-corruption buffer truncate
end

```

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 112  |

## Параметри конфігурації маршрутизатора R2

```

R2#show run
Building configuration...
Current configuration : 2561 bytes
! No configuration change since last restart
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R2
boot-start-marker
boot-end-marker
enable secret 5
$1$TtBs$gXeVNSl1LmUD9B5vFlnxj.
aaa new-model
aaa authentication login default group radius
local
aaa authorization exec default group radius if-
authenticated
aaa session-id common
clock timezone UTC 2 0
clock summer-time CEST recurring
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip icmp rate-limit unreachable
ip dhcp excluded-address 192.168.0.1
192.168.0.99
ip dhcp pool LAN_A
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 192.168.0.8 8.8.8.8
ip domain name Dob.net
ip name-server 8.8.8.8
ip name-server 8.8.4.4
ip cef
no ipv6 cef
multilink bundle-name authenticated
username admin privilege 15 secret 5
$1$FFJA$kJQZJxIgR5pJXoFKYZ9IO0
redundancy
ip tcp synwait-time 5
ip ssh version 2
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
interface Ethernet0/1
ip address 192.168.0.1 255.255.255.0
...
router ospf 1
network 10.1.1.0 0.0.0.255 area 0
network 192.168.0.0 0.0.0.255 area 0
default-information originate
ip forward-protocol nd
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.1.254
access-list 12 permit 192.168.0.25
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
access-class 12 in
logging synchronous
login local
transport input ssh
ntp authentication-key 1 md5 051B071C321D
7
ntp authenticate
ntp trusted-key 1
ntp master 15
ntp server 192.168.0.8
ntp server 0.ua.pool.ntp.org
end

```

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 113  |

## Параметри конфігурації комутатора SW2

```
SW2#show run
Building configuration...
Current configuration : 4900 bytes
! Last configuration change at 17:47:23 CEST
Fri Jun 16 2023
! NVRAM config last updated at 17:04:39
CEST Fri Jun 16 2023
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
hostname SW2
boot-start-marker
boot-end-marker
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging userinfo
logging buffered 64000
logging console discriminator EXCESS
username admin privilege 15 secret 5
$1$swEE$m9HhiBSkblGTZEcr92MZW1
aaa new-model
aaa authentication login default group radius
local
aaa authorization exec default group radius if-
authenticated
aaa session-id common
clock timezone UTC 2 0
clock summer-time CEST recurring
ip arp inspection vlan 1
no ip icmp rate-limit unreachable
ip dhcp snooping
no ip domain-lookup
ip domain-name Dob.net
ip name-server 192.168.0.8
ip name-server 8.8.8.8
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 mode access
switchport port-security
ip arp inspection trust
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet0/1
```

```
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.27ef.f2e9
switchport port-security
ip arp inspection trust
spanning-tree portfast edge
spanning-tree bpduguard enable
interface Ethernet0/2
switchport mode access
switchport port-security mac-address sticky
switchport port-security mac-address sticky
0800.2725.1d8b
switchport port-security
ip arp inspection trust
interface Ethernet0/3
switchport mode access
ip arp inspection trust
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet1/0
switchport mode access
ip arp inspection trust
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet1/1
switchport mode access
ip arp inspection trust
ip dhcp snooping limit rate 256
ip dhcp snooping trust
interface Ethernet1/2
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
interface Ethernet2/0
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
switchport port-security mac-address sticky
switchport port-security
shutdown
spanning-tree portfast edge
spanning-tree bpduguard enable
interface Ethernet2/1
switchport access vlan 99
switchport mode access
switchport port-security maximum 3
```

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | KIK.KP.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 114  |

```

switchport port-security mac-address sticky
switchport port-security
shutdown
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
shutdown
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
shutdown
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
shutdown
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
shutdown
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
shutdown
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
shutdown
spanning-tree portfast edge
spanning-tree bpduguard enable
interface Vlan1
ip address 192.168.0.2 255.255.255.0
ip default-gateway 192.168.0.1
ip forward-protocol nd
no ip http server
no ip http secure-server
ip ssh version 2
logging host 192.168.0.8
access-list 12 permit 192.168.0.25
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
access-class 12 in
logging synchronous
login local
transport input ssh
ntp authentication-key 1 md5 140713181F55 7
ntp authenticate
ntp trusted-key 1
ntp server 192.168.0.1
en

```

|      |      |                     |        |      |                          |      |
|------|------|---------------------|--------|------|--------------------------|------|
|      |      | Добровольський Д.В. |        |      | КІК.КР.Б – 123 – 04 – ПЗ | Арк. |
|      |      | Воротніков В.В.     |        |      |                          |      |
| Змн. | Арк. | № докум.            | Підпис | Дата |                          | 115  |