ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ, ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Освітньо-професійна програма Інформаційні управляючі системи та технології
Спеціальність 126 Інформаційні системи та технології
Ступінь вищої освіти Магістр

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ

Завідувач кафедри
_____Юрій УТКІН
«15» грудня 2022 року

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «**Забезпечення цілісності інформаційної системи підприємства на базі служб Active Directory**»

виконав здобувач вищої освіти денної форми навчання

Гуйва Олексій Олександрович

Керівник кваліфікаційної роботи,
професор, д.т.н. Юрій ПОНОЧОВНИЙ

Полтава – 2022 року

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАЧКИ

ПК	–	Персональний комп’ютер;
БД	–	База даних;
DNS	–	Domain Name System
DHCP	–	Dynamic Host Configuration Protocol
ІТ	–	Інформаційні технології;
ІС	–	Інформаційна система;
ПЗ	–	Програмне забезпечення;
СУБД	–	Система управління базами даних;
ТЗ	–	Технічне завдання;
ОС	–	Операційна система.

ВСТУП

Актуальність теми. Модернізація підприємства є невід'ємним процесом для будь якої компанії, деякі підприємства модернізують своє виробництво, деякі продукцію, але інколи компанії забувають про модернізацію програмного або апаратного забезпечення, що може призвести до зупинки організації або втрати конфіденційної інформації. На разі серед підприємств набуває популярність створення власних доменних серверів, так як за допомогою них компанія має змогу покращити інформаційну безпеку на всіх пристроях, які використовуються. Це стосується не тільки персональних комп'ютерів та ноутбуків, в доменний сервер можна вести принтер, сканер та мережеве обладнання. Технологія буда створена в 2000-х роках, але велику популярність набуває саме зараз, так як перші версії служби «Active Directory» були недопрацьовані, система часто видавала збій і була не дуже надійною. З оновленням серверної операційної системи Windows, вона покращувалась, і на сьогодні дозволяє розгортати цілком працездатні та відмовостійкі домені сервери. Методи впровадження служб Active Directory висвітлені в роботах Яцук. П, Морімото.Р, Ноел. М, Кока.Д, Гардін'єр.К.

У досліджені [1] запропоновано дати доступ до створення облікових записів в домені великій групі людей. Проаналізувавши це питання було прийняте рішення зменшити кількість людей, які мають адміністративний доступ до створення або редагування облікових записів в доменному сервері. Адміністративні права повинні мати лише системні адміністратори, за допомогою цього рішення буде зменшено ризики зміни даних та неконтрольованого додавання користувачів на сервер.

В роботі [2] було прийняте рішення розгортання домену на виділеному сервері. Після обговорення було прийнято рішення використовувати віртуальні машини, так як це зменшить кількість економічних ресурсів.

Розгортання доменного серверу для організації ТОВ СМС «Системи модернізації складів» було узгоджено з керівництвом підприємства, що також підкреслює актуальність даного питання.

Мета роботи полягає у створенні повністю працездатного доменного серверу для організації ТОВ СМС «Системи модернізації складів», за допомогою якого компанія покращить безпеку та цілісність інформації.

Завданнями кваліфікаційної роботи є:

- Дослідження сучасних технологій для захисту даних;
- Аналіз можливостей віртуальних машин та служб Active Directory;
- Створення порівняльних таблиць для вибору програмного та апаратного забезпечення;
- Апгрейд сервера та серверного обладнання яке знаходиться на підприємстві;
- Встановлення на сервер підприємства віртуальної машини на якій буде розгорнуто домен;
- Розгортання домених служб Active Directory на сервері та налаштування ролей та компонентів;
- Представлення працездатного сервера керівництву.

Об'єктом дослідження є життєвий цикл доменних серверів у частині етапів аналізу, проектування та адміністрування.

Предмет дослідження – розгортання сервера домену за допомогою служб Active Directory, адміністрування ролей та компонент для забезпечення цілісності інформаційної системи підприємства.

Методи дослідження – проведені в роботі дослідження базуються на методах аналізу та забезпечення інформаційної безпеки підприємства, функціонування служб Active Directory, теорії систем масового обслуговування.

Інформаційна база – Інтернет-ресурси, що місять інформацію про забезпечення інформаційної безпеки підприємства, стандарти з інформаційної безпеки, опис служби Active Directory, віртуальних машин та оновлення апаратної бази серверу.

Елементи наукової новизни полягають у визначенні раціональної конфігурації доменного серверу на основі обґрунтованого вибору служб Active Directory, адміністрування ролей та компонентів, що дозволило забезпечити

заданий рівень цілісності інформаційної системи підприємства.

Практична значущість полягає у реалізації розробленого за допомогою технології ActiveDirectory домену на 200 робочих станцій у повсякденну діяльність ТОВ СМС. Отримані результати можуть буть корисними при підготовці фахівців до процесів створення облікових засобів в службі Active Directory та розгортанні віртуальних машин.

Апробація результатів дослідження відбувалася шляхом оприлюднення доповідей на міжнародній та студентських конференціях, семінарах.

Публікації. За результатами проведеного дослідження опубліковано тези: «Криптографічні алгоритми для захисту інформаційних систем», Матер. VIII Міжнародної конференції «Інтеграція інформаційних систем і інтелектуальних технологій в умовах трансформації інформаційного суспільства», 21-22 жовтня 2021 р., м. Полтава; «Можливості служби ACTIVE DIRECTORY», Матер. науково-практичної конференції за підсумками виробничої практики здобувачів вищої освіти спеціальності «Інформаційні системи та технології», 23 лютого 2022 р. м. Полтава; «Захист облікових записів за допомогою служб ACTIVE DIRECTORY», Матер. щорічної студентської наукової конференції Полтавського державного аграрного університету, 10 листопада 2022 р. м. Полтава.

Структура та обсяг кваліфікаційної роботи логічно пов'язані з задачами досліджень. Робота містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел, додатки. Загальний обсяг текстової частини дипломної роботи складає 75 сторінок формату А4. Вона містить 45 рисунків і 2 таблиці. В роботі використано 53 науково-технічних джерело.

РОЗДІЛ 1
АНАЛІЗ ЗАСТОСУВАННЯ ДОМЕННИХ СЕРВЕРІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВ ТА ВИМОГ ДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Аналіз особливостей використання доменних серверів на прикладі розробок корпорації Microsoft

Доменний сервер – це ієрархічно організоване сховище даних про облікові записи користувачів, дані персональних комп'ютерів та налаштування мережі, яке забезпечує зручний пошук та використання цих даних для автентифікації і не тільки.

Також можна сказати, що служби каталогів корпорації Microsoft у першу чергу призначені для операційних систем Windows Server. За допомогою даних каталогів є можливість об'єднувати різні об'єкти мережі (ноутбуки, принтери, точки доступу та інші сервіси) в одну єдину систему.

Елементи домену Microsoft складається з серверу, контролера домену, домену, дерева домену. Визначення наведені в таблиці 1.1.

Таблиця 1.1 - Поняття які входять в Active Directory

Поняття	Характеристика
Сервер	Персональний комп'ютер або професійний сервер який виконує функції (ролі) в домені.
Домен	Мінімальна структура Active Directory (складається з відділів, персональних комп'ютерів, користувачів).
Дерево домену	Ієрархічна структура домену, яка має один корневий домен.
Контролер домену	Сервер, який зберігає каталоги, та запити користувачів. Також контролер слугує в якості однієї з ролей FSMO.
Ліс доменів	Велика кількість доменів, які знаходяться в різних формах відносин.

Системні адміністратори використовують технологію Active Directory у Windows Server для зберігання та організації об'єктів у мережі в ієрархічну

захищену логічну структуру, наприклад користувачів, комп'ютерів чи інших фізичних ресурсів.

Active Directory об'єкти використовують каталоги для зберігання інформації, всі об'єкти визначені в схемі. Визначення об'єктів містять інформацію, таку як тип даних та синтаксис, яку каталог використовує, щоб гарантувати достовірність зберігання. Жодні дані не можуть бути збережені в каталозі, поки вони не визначені у схемі. Схема за замовчуванням містить усі визначення та опис об'єктів, які необхідні для коректної роботи Active Directory [3].

Важливо при встановлені домену відразу розділити ролі та компоненти (права доступу), а саме права доступу для окремих розділів в дереві домену. Наприклад, для початку потрібно дати повні права доступу для адміністратора системи, так як для додавання будь якої робочої станції або користувача, Active Directory запросить користувача який має права на додавання а бо видалення с домену відповідних елементів. Саме тому на початку потрібно встановити ролі для адміністратора домену.

Коли адміністратор має доступ до каталогу через логічну структуру, яка складається з елементів таких як домен та ліс домену, сам каталог реалізується через фізичну структуру, яка складається з бази даних, яка зберігається на всіх контролерах які знаходяться в лісі домену.

Сховище Active Directory обробляє весь доступ до БД. Сховище даних складається із служб та фізичних файлів, які управляють правами доступу, процесами читання та запису даних усередині бази даних на жорсткому диску кожного контролера [3].

Важливо також робити резервні копії домену (бекап), за допомогою нього буде можливість в будь який момент буде можливість відновити контролер домену на будь якій машині. Для цього буде потрібно лише встановити на окрему машину контролер домену та в розділі налаштувань завантажити зроблений раніше бекап.

Також перед додаванням машини (персонального комп’ютера, ноутбуку) до домену потрібно додати на машину обліковий запис локального адміністратору, так як при необхідності зміни файлів таких як папки Windows або робота з

користувачами, перед зміною або видаленням будь яких даних потрібно буде ввести логін та пароль користувача домену який має на це права доступу, або при необхідності якщо домен буде тимчасово недоступний можна буде використати обліковий запис локального адміністратора який має такі ж самі права доступу. За допомогою цього користувач або адміністратор зможе виконувати зміни на персональному комп'ютері або ноутбуці навіть при вимкненому домені.

1.2 Опис логічної структури доменного сервера на прикладі його реалізації в службах Active Directory

Логічна структура та архітектура сховища Active Directory складається з чотирьох частин :

1. Домен та ліс. Ліс та домен та організаційна одиниця (OU) являють основними елементами логічної структури Active Directory. Ліс виділяє один єдиний каталог та являє собою границю безпеки [3], приклад наведено на рис. 1.1.

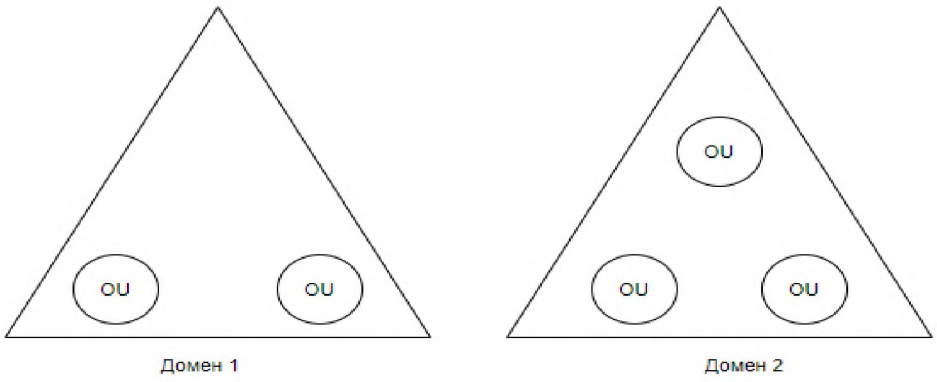

Рисунок 1.1 – Домен та ліс

2. Схема. Схема містить визначення об'єктів, які використовуються при створенні об'єктів, які зберігаються в каталозі [3].

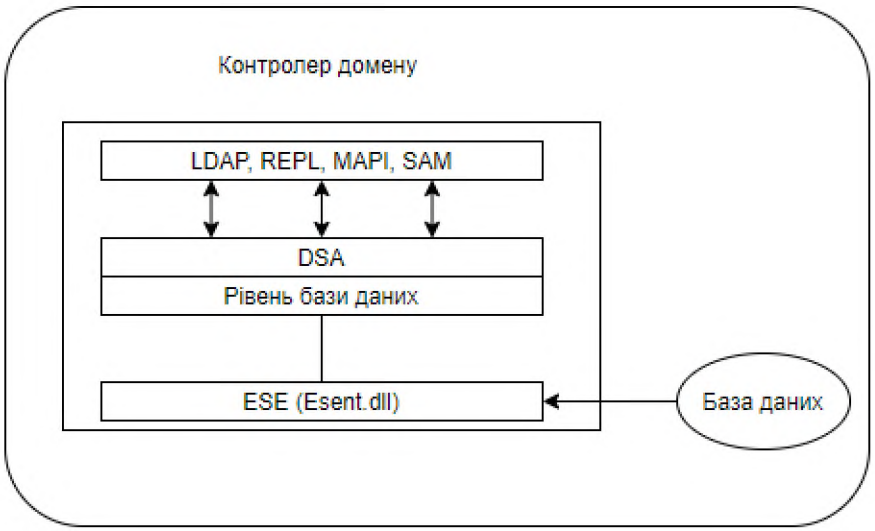

Рисунок 1.2 – Схема контролера домену

3. Сховище даних. Сховище даних - це частина каталогу, яка управляє зберіганням та вилученням даних на кожному контролері домену [3].

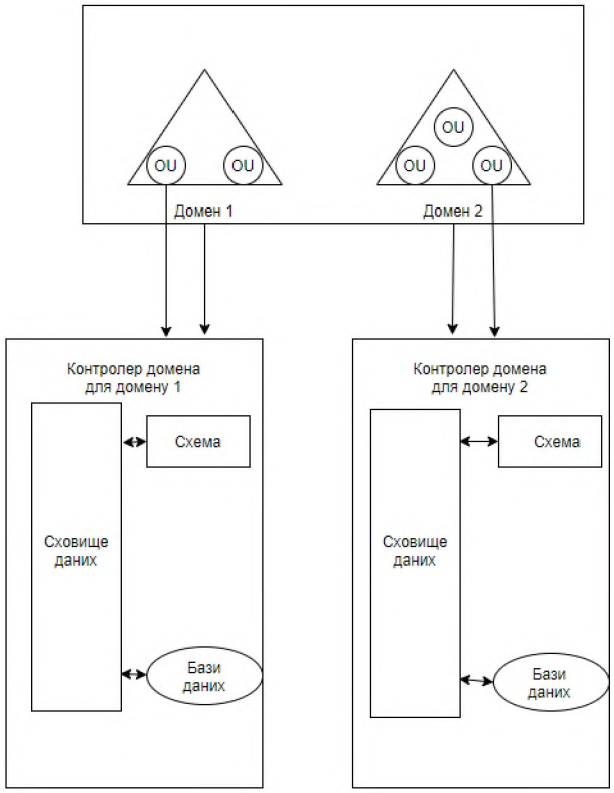

Рисунок 1.3 – Сховище даних домену

1.3 Аналіз засобів забезпечення інформаційної безпеки в доменних серверах

1.3.1 Аналіз вимог до цілісності у системі показників інформаційної безпеки підприємства

Безпека інформації (даних) - це стан захищеності інформації (даних), при якому забезпечуються її (їх) конфіденційність, доступність та цілісність.

Показник захищеності інформації - кількісна або якісна характеристика безпеки інформації, що визначає рівень вимог, що висуваються до конфіденційності, цілісності та доступності цієї інформації та реалізуються при її обробці [38].

Цілісність інформації - це термін в інформатиці та теорії телекомунікацій, який означає, що дані є повними, умови, за яких дані не були змінені в ході будь-яких операцій, що виконуються над ними, чи то передача, зберігання або подання [31].

Теоретично цілісність даних означає коректність даних та його несуперечність. Зазвичай вона включає цілісність зв'язків, яка виключає помилки зв'язків між первинним і вторинним ключем. Наприклад, коли існують дочірні записи-сироти, які мають зв'язку з батьківськими записами [32].

Поняття «цілісність об'єкта» використовується у контексті термінології інформаційної безпеки (об'єктом може бути інформація, спеціалізовані дані, ресурси автоматизованої системи). Зокрема, властивість цілісності інформації (ресурсів автоматизованої системи) є одним із трьох основних критеріїв інформаційної безпеки об'єкта [33].

Цілісність інформації (ресурсів автоматизованої інформаційної системи) - це стан інформації (ресурсів автоматизованої інформаційної системи), у якому її (їх) зміна здійснюється лише навмисно суб'єктами, які мають право [35].

Цілісність інформації - стан інформації, у якому відсутня будь-яке її зміна чи зміна здійснюється лише навмисно суб'єктами, які мають нею право.

Цілісність ресурсів інформаційної системи - стан ресурсів інформаційної системи, у якому їх зміна здійснюється лише навмисно суб'єктами, які мають нею право, у своїй зберігаються їх склад, зміст і організація взаємодії [37].

Методи та способи реалізації вимог, викладених у визначенні терміна, докладно описуються у межах єдиної схеми забезпечення інформаційної безпеки об'єкта (захисту інформації) [37].

Основними методами забезпечення цілісності інформації (даних) під час зберігання в автоматизованих системах є:

- забезпечення відмовостійкості (резервування, дублювання, дзерклювання обладнання та даних, наприклад через використання RAID-масивів);
- забезпечення безпечного відновлення (резервне копіювання та електронне архівування інформації).

1.3.2 Опис довірених відносин у доменному сервері на прикладі ActiveDirectory

Для можливості аутентифікації з використанням облікових записів з кількох доменів необхідно, щоб були довірчі відносини між останніми. При створенні домену в структурі лісу довіра вибудовується автоматично. Але якщо ми хочемо об'єднати два домени різних організацій або які раніше працювали незалежно одна від одної, то необхідно налаштувати довірчі стосунки [5].

Довірені стосунки можуть бути різних типів. Перед налаштуванням потрібно розуміти якій тип потрібен. Є такі типи довірливих відносин :

1. Односторонні або двосторонні. За допомогою цього способу визначається направлення довірених стосунків один до одного. В одно довірених стосунках тільки один домен довіряє другому. Таким чином користувач буде мати змогу на комп’ютері одного домену можна буде авторизуватися з іншим.

При створенні такої довіри потрібно вказати також напрямок (вхідний або вихідний) - він визначає чиї користувачі зможуть проходити автентифікацію на домені якого.

В двосторонніх довірах домени довіряють один одному. За допомогою цього

автентифікацію можна буде робити на будь якій робочій машині та під користувачем з будь якого домену.

2. Зовнішня довіра або довіра лісу. Зовнішнє чи нетранзитивне відношення встановлюється між двома доменами безпосередньо поза лісом. Довіра лісу чи транзитивне відношення пов'язує ліси та їх домени [5].

1.3.3 Аналіз засобів забезпечення безпеки мережі за допомогою технології Active Directory

У міру зростання організації за рахунок збільшення кількості співробітників, необхідних для підтримки повсякденних бізнес-функцій, також збільшується кількість пристроїв, підключених до мережі організації[5].

Навіть якщо компанія невелика їй потрібен спеціаліст який буде контролювати кількість користувачів в мережі та створювати облікові записи, другими словами компанії потрібен спеціаліст який зможе не лише допомагати користувачам з невеликими проблемами зв’язаними з IT технологіями, а й той який зможе забезпечувати безпеку інформації яка зберігається на серверах або жорстких дисках.

Саме тому в багатьох організаціях є посада «Системний адміністратор», саме ця людина буде допомагати організації з вирішенням питань з безперебійною роботою робочих станцій та забезпеченням інформаційної безпеки [5].

Компанія Microsoft в серверних версіях Windows розробила компоненти які допоможуть полегшити роботу системних адміністраторів та збільшити безпеку інформації. В кожній організації є хоча б декілька персональних комп’ютерів, за допомогою яких працює бухгалтерія або інші відділи. Коли на підприємстві декілька ПК або ноутбуків системному адміністратору легко спостерігати за безпекою декількох робочих станцій, але якщо компанія має сто або більше машин (робочих місць де використовують ноутбуки або персональні комп’ютери) важке спостерігати за кількістю облікових засобів та доступу до них. Саме тому багато організацій створюють доменний сервер, саме за допомогою нього є можливість контролювати робочі станції та кількість об’єктів в мережі компанії.

Сервер Windows, на якому інстальовано і налаштовано Active Directory, називається контролер домену, просто тому, що він дозволяє IT-фахівцям контролювати все, що знаходиться в його домені. Це означає, що замість створення облікового запису користувача на кожному комп'ютері в мережі, Active Directory дозволяє створювати обліковий запис користувача на контролері домену, призначати користувачів у групи безпеки і навіть створювати Об'єкт групової політики (Group Policy Object) для призначення політик безпеки користувачам та групам у домені [5].

Коли користувач намагається увійти в домен, хост надсилає ім'я користувача домену та New Technology LAN Manager (NTLM) хеш версії 2, та пароль користувача до контролера домену під час автентифікації. Контролер домену визначить, чи дійсні облікові дані користувача, відповість вузлу в домені та визначить політики безпеки, які застосовуються до користувача. Це означає, що користувач із дійсним обліковим записом може увійти на будь-який пристрій у мережі, якщо це дозволено політикою безпеки, яка застосовується до облікового запису користувача домену [5].

Active Directory дозволяє використовувати такі функції керування та безпеки:

- Керування профілями користувачів на клієнтах та серверах у домені;
- Управління мережевою інформацією та конфігураціями;
- Централізоване управління політиками безпеки для користувачів, груп та пристроїв у домені;
- Конфігурації та політики реєстру клієнтів.

Перелік дозволяє зібрати конфіденційну інформацію про всі об'єкти, користувачів, пристрої та політики у всьому домені Active Directory. Така інформація дасть уявлення про те, як організація використовує Active Directory для керування своїм доменом. Ви також зможете отримати чітке уявлення про те, як використовувати довіру між клієнтами домену, користувачами та контролером домену для компрометації домену Active Directory організації.

Таким чином домена структура дозволяє не лише збільшити безпеку локальної мережі компанії а й полегшити роботи спеціалістів які займаються адмініструванням в компанії [6].

Висновки до розділу 1

В даний момент велика кількість IT компаній задається питанням як покращити цілісність та безпеку інформації на робочих станціях, так як встановлення звичайного паролю як це було раніше вже не є актуальним способом забезпечити захист, так як є велика кількість програм за допомогою яких навіть спеціаліст невеликого рівня буде мати змогу підібрати пароль доступу користувача.

В мережі інтернет є багато рекомендацій як можна покращити безпеку інформації, але велика кількість цих програм працюють на недостатньому рівня. Деякі компаній вирішують повернутись до методів безпеки які використовувались раніше, такі як ключ-карта, за допомогою якої користувач буде отримувати доступ до ПК або ноутбуку, шифрування паролю та багато іншого. Але ключ-карту легко загубити, а в інтернеті є безліч програм дешифраторів. Таким чином компаніям доводиться вигадувати нові методи, щоб забезпечити свою безпеку.

Велика кількість підприємств використовує програмне забезпечення від компанії Microsoft, головне програмне забезпечення від компанії є Windows, саме за допомогою нього користувач може отримати інтерфейс для роботи. Окрім звичайних ОС, компанія виробляє програмне забезпечення для серверів.

Серверна ОС від компанії Microsoft містить велику кількість можливостей для покращення інформаційної безпеки. Саме тому компанія створила служби Active Directory, якщо сервери які використовуються в компанії працюють за допомогою операційної системи Windows Server, адміністратори будуть мати змогу використовувати Active Directory для створення, контролю та захисту облікових записів.

РОЗДІЛ 2
ПОСЛІДОВНІСТЬ РОЗГОРТАННЯ ДОМЕННОГО СЕРВЕРУ ACTIVE DIRECTORY НА ПІДПРИЄМСТВІ

2.1 Опис підприємства ТОВ «СМС» та його вимог щодо наповнення служб доменного серверу

Асоціація «KONSORT» включає в себе низку компаній : ТОВ «CHIORINO», ТОВ «Сучасні миючі системи», ТОВ «Еврогір системз», ТОВ «Ремонт обладнання, складської техніки», ТОВ «Системи модернізації складів», «Speak it!» сучасна школа англійської мови [4].

«KONSORT» - це новий етап розвитку компанії «СМС», яка пройшла шлях від ремонту першої рокли до побудови великого заводу з виробництва складського обладнання і техніки. Ми вже давно вийшли за рамки «складів» і виготовляємо обладнання для автоматизації виробництва (B2B) в таких основних сферах: логістична, промислова, аграрна, екологічна. Ми поступово стали лідером ринку та продовжуємо розвиток - постійно в пошуку нових ідей для росту [4].

«KONSORT» допомагає компаніям та організаціям в оновлені приладів на складах і не тільки. Компанія виготовляє велику кількість обладнання яке використовується в різних сферах : в будівництві, виробництві будь якої продукції, транспортуванні та багото чого іншого.

Організація знаходиться за адресою : Світла вулиця, 1а, Щербані, Полтавська область, 38750 [4].

Компанія бере відповідальність за свою продукцію та за бізнеси, які нам довіряють – тому і після реалізації проектів ми підтримуємо зв'язок з клієнтами, обслуговуємо всю техніку та обладнання і надаємо консультації. У разі необхідності термінового ремонту електро і гідравлічної техніки – існує бригада оперативного реагування та наші сервісні служби по всій території України. Вони швидко та якісно проведуть всі ремонтні роботи, щоб Ваш бізнес продовжував свою діяльність без зупинок і втрат [4].

LEAN-технології у виробництві та професіоналізм працівників у синергії здатні дати високу якість за помірну ціну. Почуємо вашу проблему, розробимо під неї рішення, щоб максимально автоматизувати ваші бізнес-процеси. Повний цикл виготовлення рішення — від розробки, проектування, виробництва і монтажу до подальшого навчання персоналу і технічного обслуговування обладнання. Досвід успішних рішень задач у сферах логістики, промисловості, аграрному секторі та екології [4].

ТОВ СМС «Системи модернізації складів» - технологічний партнер для підприємців. Для тих, хто кожного дня придумує, створює, тестує, перероблює, запускає і знову придумує. Компанія допомагає прокачати власну справу та вивести її на новий рівень ефективності. Створює обладнання для автоматизації виробництва й логістики: рольганги, калібратори, конвеєри, лінії для транспортування, сортування та переробки.

Також сама компанія постійно модернізує своє виробництво та офіс. Модернізація підприємства являє собою : купівлю нових лазерних станків для роботи з металом, використання при виробництві власного програмного забезпечення, встановлення плазмових телевізорів та поставлення задач та перегляду виконання.

Офіс також не стоїть на місці : постійне оновлення програмного та апаратного забезпечення, розділення мережі Wi-Fi та Ethernet, постійний абгрейт серверів та серверного обладнання. В зв’язку з цими факторами не дивно, що компанія вирішили покращити свою безпеку, а саме підготувати доменний сервер (Active Directory), за допомогою чого на підприємстві буде проводитись облік записів користувачів та персональних комп’ютерів і ноутбуків.

На зорі комп'ютеризації все управління користувачами зводилося до адміністрування єдиного сервера. Згодом ситуація стала змінюватися, по-перше, підприємства набували дедалі більше серверів, по-друге, питанням безпеки стало приділятися дедалі більше уваги, що вимагало більшого контролю кожної дії користувача (як наслідок, введення суворої автентифікації кожному за значимого системи дії).

Згодом це призвело до того, що адміністратор змушений був створювати обліковий запис користувача на кожному сервері в мережі підприємства, а також на кожній робочій станції, якою має право користуватися співробітник. Користувач, своєю чергою, мав постійно надавати аутентифікуючу інформацію (кожному сервісу корпоративної мережі).

Враховуючи те, що на разі відбувається раптове вимкнення світла, керівництво вирішило придбати додаткові батареї до блока безперебійного живлення та знайти генератор для забезпечення офісу та заводу світлом, так як після встановлення домену, для нормальної роботи ПК або ноутбуку потрібно постійне підключення до сервера.

Перед встановленням Active Directory, потрібно обрати де саме це буде реалізовуватись. Розгорнути доменний сервер можна як на персональному комп'ютері так і на спеціалізованому сервері. Керівництвом було прийняте рішення провести порівняльну характеристику всіх можливих варіантів розгортання доменної структури. Апаратне забезпечення на якому буде встановлена домена структура повинне відповідати таким критеріям:

- Можливість майбутнього апгрейду;
- Стабільність постійної роботи;
- Ціна;
- Відмовостійкість [6].

Таким чином для розгортання Active Directory можна використати :

1. Персональний комп'ютер. Встановивши серверну версію Windows є можливість розгорнути домен на персональному ПК, але таке рішення не саме найкраще, так як ПК непризначений до постійної роботи як професійні сервери, також в майбутньому можуть виникнути питання з апгрейду, так як материнські плати які встановлені в звичайному ПК не розраховані на велику кількість оперативної пам'яті або хороший серверний процесор як у професійних серверах. Єдиний плюс розгортання домену на персональному комп'ютері це ціна, в інших випадках не варто економити, краще купити професійне обладнання.

2. Професійний сервер. Звісно великим недоліком професійних серверів

є їх ціна, але в нього також є велика кількість плюсів. Професійний сервер розрахований на постійну роботу як кажуть 24 на 7. Залізо яке встановлене з заводу дозволяє встановлювати майже будь яке програмне забезпечення без апгрейду. Додавання оперативної пам'яті або жорстких дисків відбувається майже так само як і в звичайному персональному комп'ютері.

3. Оренда віртуального сервера. Такий метод компанії використовують для збільшення безпеки від зовнішніх факторів таких як : проникнення в серверну зловмисника який зможе отримати змогу нашкодити серверу або заволодіти інформацією яка знаходиться на ньому. Але, такий метод також не з дешевих, окрім того не потрібно забувати про можливість злому користувача та багато інших факторів.

4. Встановлення на вже функціонуючий сервер віртуальних машини. Завдяки цьому методу компанія має змогу постійно спостерігати за сервером та самостійно робити потрібні оновлення, також цей метод є тим самим середнім між купівлею власного сервера та використанням персонального комп'ютера. Для вдосконалення цього метода в життя потрібно лише зробити невеликий апгрейд сервера, наприклад: додати оперативної пам'яті, встановити додаткові жорсткі диски для нового програмного забезпечення і звісно провести діагностику обладнання [6].

Після отримання порівняльної характеристики керівництво прийняло рішення розгортання Active Directory вже на функціонуючому сервері після його апгрейду. Після отримання відповідних компонентів був зроблений апгрейд сервера :

1. Оперативна пам'ять – на сервері було встановлено 64 гігабайт (DDR4), після оновлення стало 128 гігабайт (DDR4);

2. Жорсткі диски – на сервері було два жорстких диски кожен по 1 терабайту, було додатково встановлено ще два жорсткі диски по 1 терабайту кожен;

3. Мережеві карти – було додано 2 карти, в кінченому результаті стало 6 мережевих карт;

4. Діагностика встановлених компонентів, перевірка охолодження та

заміна термопасти;

5. Очистка за допомогою компресора та спиртової суміші.

Провівши необхідні процедури з сервером потрібно було обрати віртуальну машину яка буде встановлена для Active Directory [7]. Для вирішення цього питання було прийняте рішення зробити порівняльну характеристику популярних віртуальних машин за допомогою порівняльної таблиці. В табл. 2.1 наведений приклад.

Таблиця 2.1 – Порівняльна характеристика віртуальних машин

	Hyper-V	VMware Server	VirtualBox	DOSBox	OpenVZ
Процесор який встановлений на місці розгортання	Intel x86-64 AMD64	Intel x86, AMD64	Intel x86, AMD64	Intel x86	Intel x86, AMD64, IA-64
Підтримка операційної системи	Будь яка	Будь яка	Будь яка	Linux	Linux
Швидкість роботи ОС в порівнянні з вже встановленою на місці розгортання	Дуже велика	Велика	Велика	Низька	Низька
Принцип дії	Апаратна візуалізація	Віртуалізація x86	Динамічна віртуалізація	Віртуалізація x86	Віртуалізація x86
Ліцензія	Доступна	Доступна	Платна	Платна	Платна
Операційна система машини носія	Будь яка	Будь яка	Будь яка	Будь яка	Будь яка

Переглянувши порівняльну таблицю стало зрозуміло, що кращим варіантом для підприємства є віртуальна машина Hyper-V, так як вона є безкоштовною та представленою на серверних версіях Windows Server, також швидкість роботи операційної системи в порівнянні зі встановленою в неї найбільша, що також зіграло важливу роль у виборі саме її [7].

Після проведення порівняння та апгрейду можна розпочинати процес встановлення та налаштування серверу.

2.2 Етапи розгортання Active Directory на підприємстві

Для початку потрібно встановити віртуальну машину, на яку в свою чергу поставити операційну систему Windows Server 2016.

Для активування віртуальної машини потрібно відкрити PowerShell, та прописати в консолі : Enable-WindowsOptionalFeature -Online -FeatureName Microsoft-Hyper-V -All (потрібно відкрити консоль від імені адміністратора), далі система завантажить додаткові файли для віртуальної машини, після завершення встановлення потрібно виконати перезавантаження ПК [8].

Після перезавантаження потрібно встановити серверну на віртуальну машину Windows Server 2016, після чого можна розпочинати встановлення Active Directory:

1. Відкриваємо диспетчер серверів та обираємо пункт «Add roles and features», таким чином додаються ролі та функції на віртуальний сервер.
2. В якості типу встановлення потрібно вказати «Role-based or feature-based installation», встановлення на основі ролів та функцій.

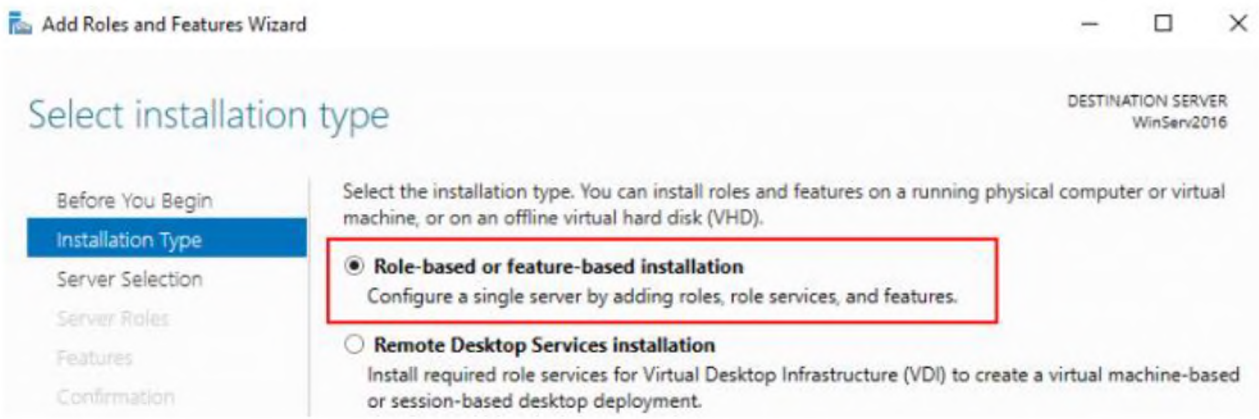

Рисунок 2.1 – Встановлення ролей та компонентів

3. В списку потрібно обрати сервер на який потрібно встановлювати налаштування.
4. Далі потртібно обирати служби «Active Directory Domain Services»,

домені служби.

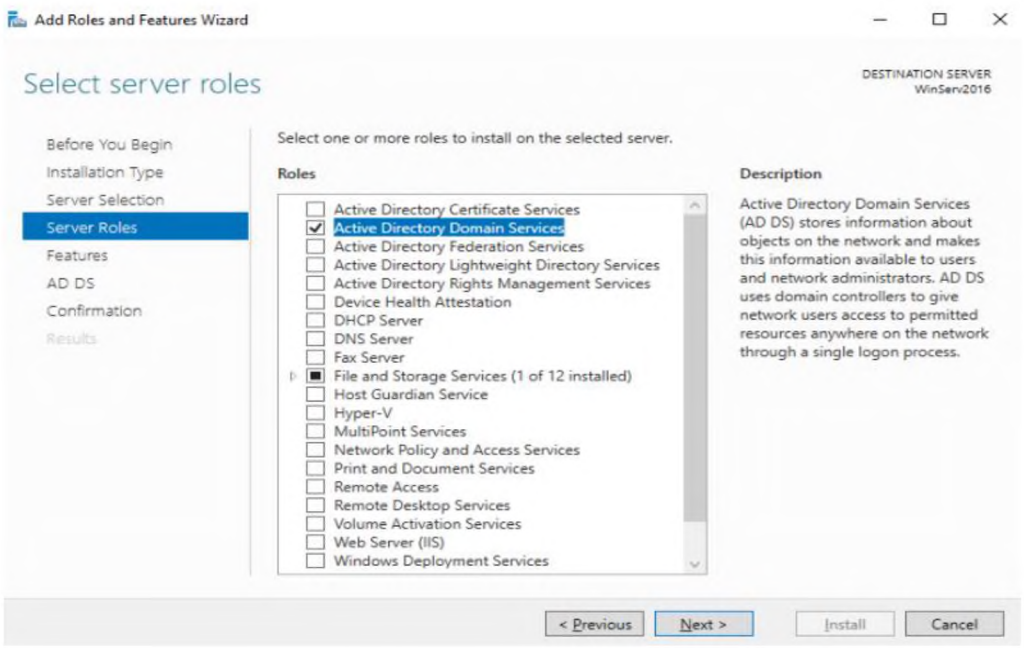

Рисунок 2.2 – Вибір доменних служб

5. Наступним кроком будуть вказані компоненти сервера.

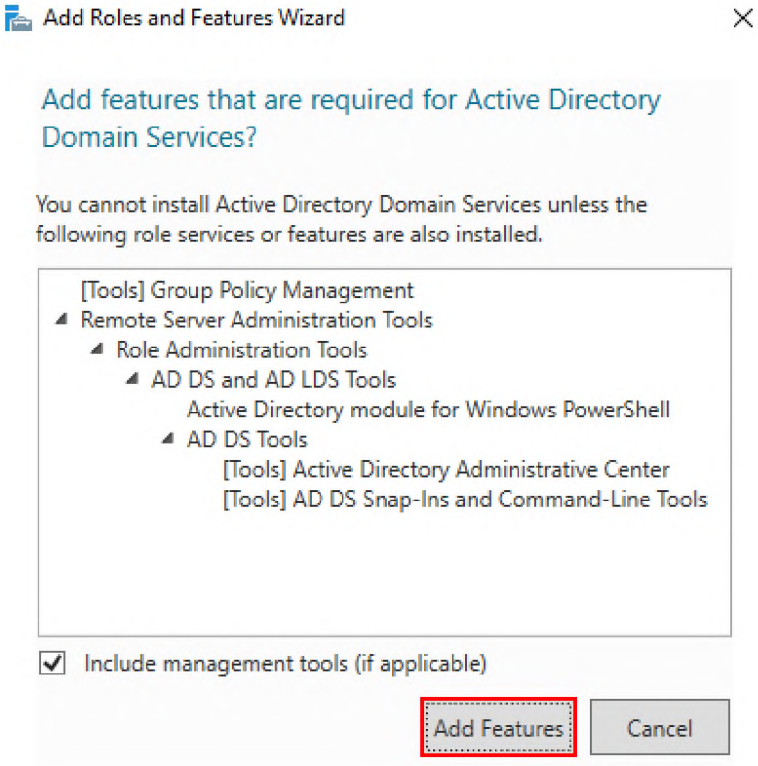

Рисунок 2.3 – Компоненти сервера

6. Останнім кроком перевіряємо всі відмічені компоненти та даємо згоду на встановлення.

Виповнивши всі кроки наведені вище, не може сказати, що роботу зроблено, так як потрібно налаштувати Active Directory, для цього потрібно виконати наступні кроки [9] :

1. В пошуковій строчці потрібно зробити запит «dcpromo», та відкрити утиліту
2. У вікні натискаємо «ОК».

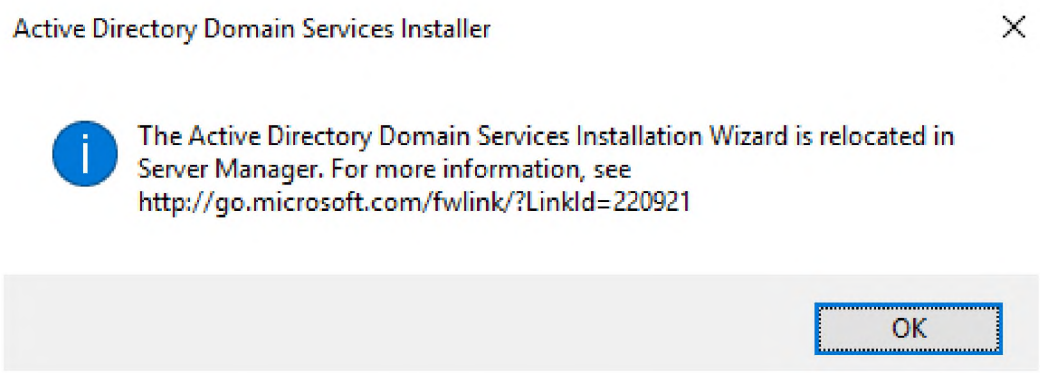

Рисунок 2.4 – Встановлення домену

3. Після встановлення домену потрібно перейти до диспетчера серверів та відкрити вкладку AD DS.
4. В горизонтальному меню потрібно натиснути на знак оклику пля чого обрати «Promote this server to a domain controller», за допомогою цієї дії ми підвищуємо роль сервера до рівня контролера.

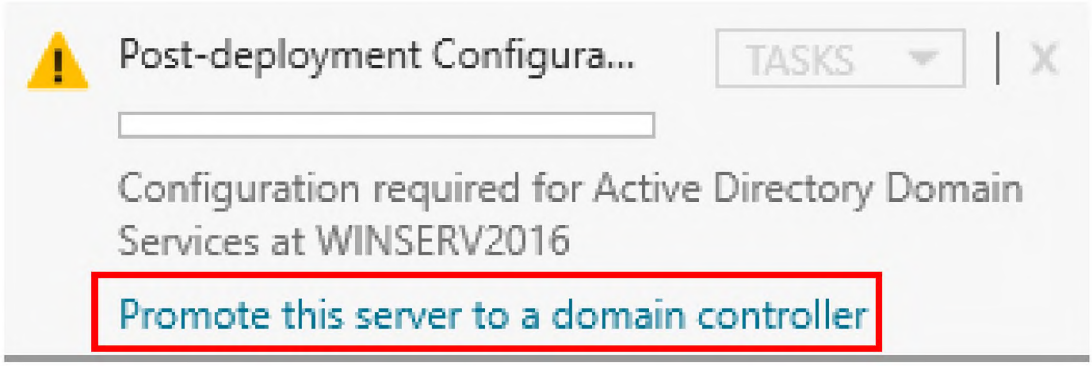

Рисунок 2.5 – Підвищення рівня сервера

5. Далі обираємо доменне ім'я, важливо що ім'я не може бути однокомпонентним. Для компанії СМС «Системи модернізації складів» домен виглядає так «cmc.holding».

6. У вкладці Domain Controller Options, потрібно ввести та підтвердити пароль для режиму відновлення служб та каталогів.

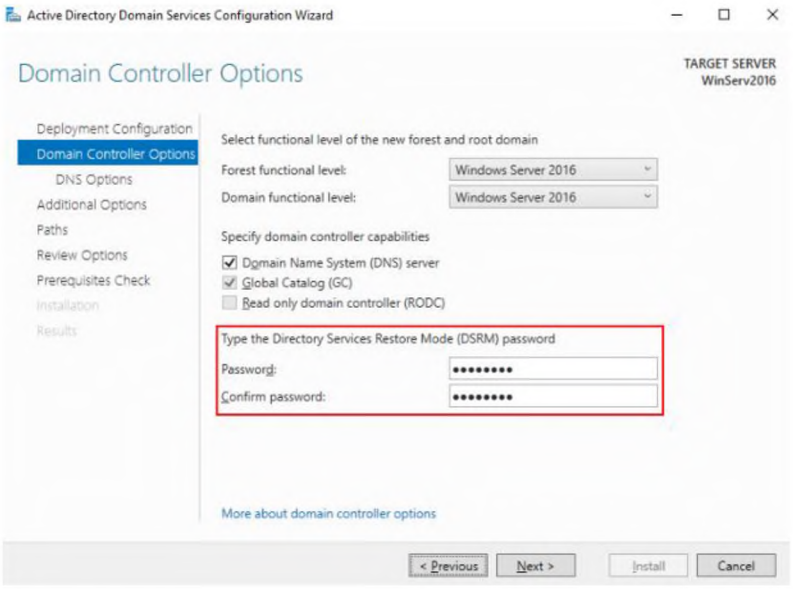

Рисунок 2.6 – Безпека та відновлення доменної структури

7. Вказуємо ім'я для домену.

8. Вказуємо шлях до бази даних AD DS. На цьому кроці важливо пам'ятати, що краще всього шлях залишати за замовченням.

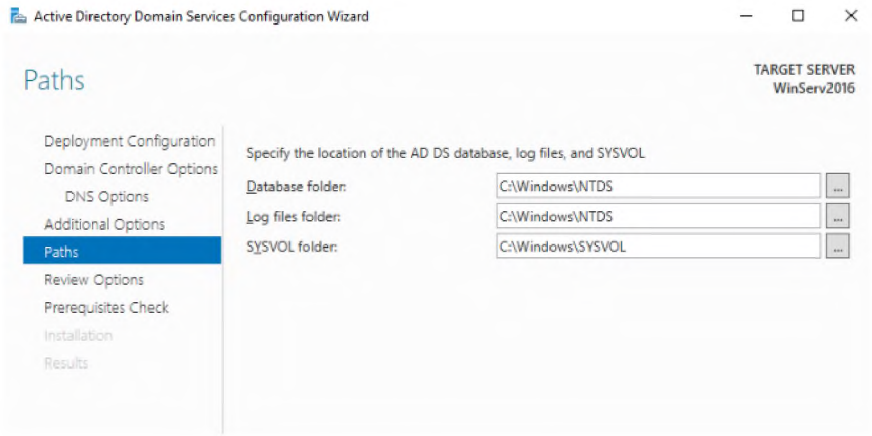

Рисунок 2.7 – Шлях до бази даних

9. Потрібно перевірити встановлені параметри та перейти до наступного кроку.

10. Після закінчення перевірки попередніх вимог, натискаємо на встановити.

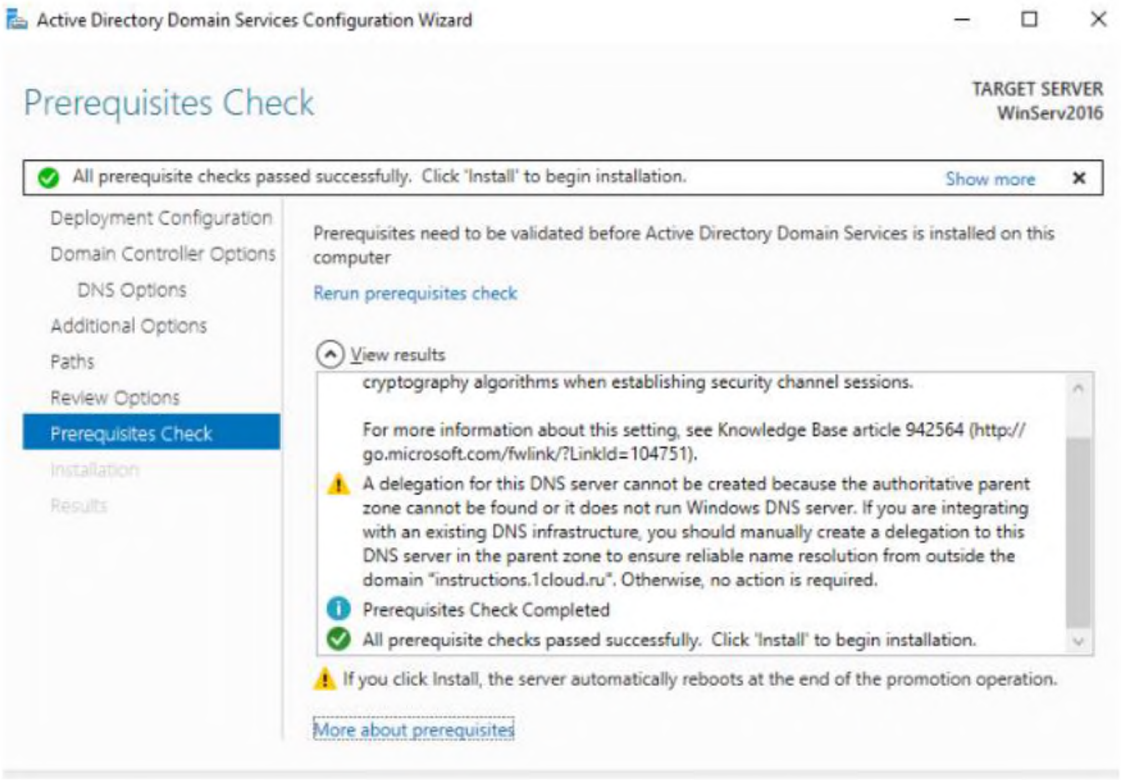

Рисунок 2.8 – Закінчення перевірки необхідних вимог

11. Після перезавантаження Active Directory буде встановлена на сервер.

Встановивши Active Directory, нею не можна відразу користуватись, так як вона не налаштована. Для підключення користувачів потрібно зробити налаштування DHCP-сервера [10].

Налаштування DHCP-сервера складається з двох частин :

- Авторизація DHCP-сервера в домені AD. Не кожен DHCP-сервер може роздавати мережеві налаштування в домені AD лише авторизовані. Це зроблено з метою безпеки, щоб інші DHCP-сервери не могли "підсунути" неправильні налаштування комп'ютерів у домені;

- Налаштування нової DHCP-області. Це вже безпосередньо налаштування самого DHCP-сервера, в ході якого визначаються які налаштування мережі будуть видаватися комп'ютерам в сегменті мережі.

Отже потрібно розпочати з Авторизація DHCP-сервера, для того щоб зробити авторизацію потрібно повернутися до диспетчера серверів. Відкривши вкладку DHCP потрібно обрати пункт «Налаштувати».

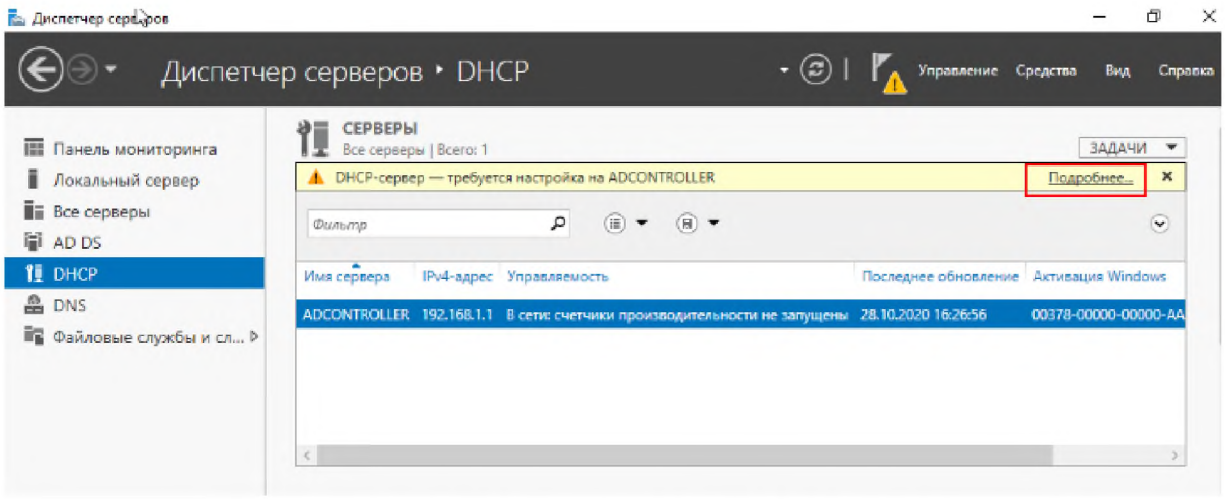

Рисунок 2.9 – Налаштування DHCP-сервера

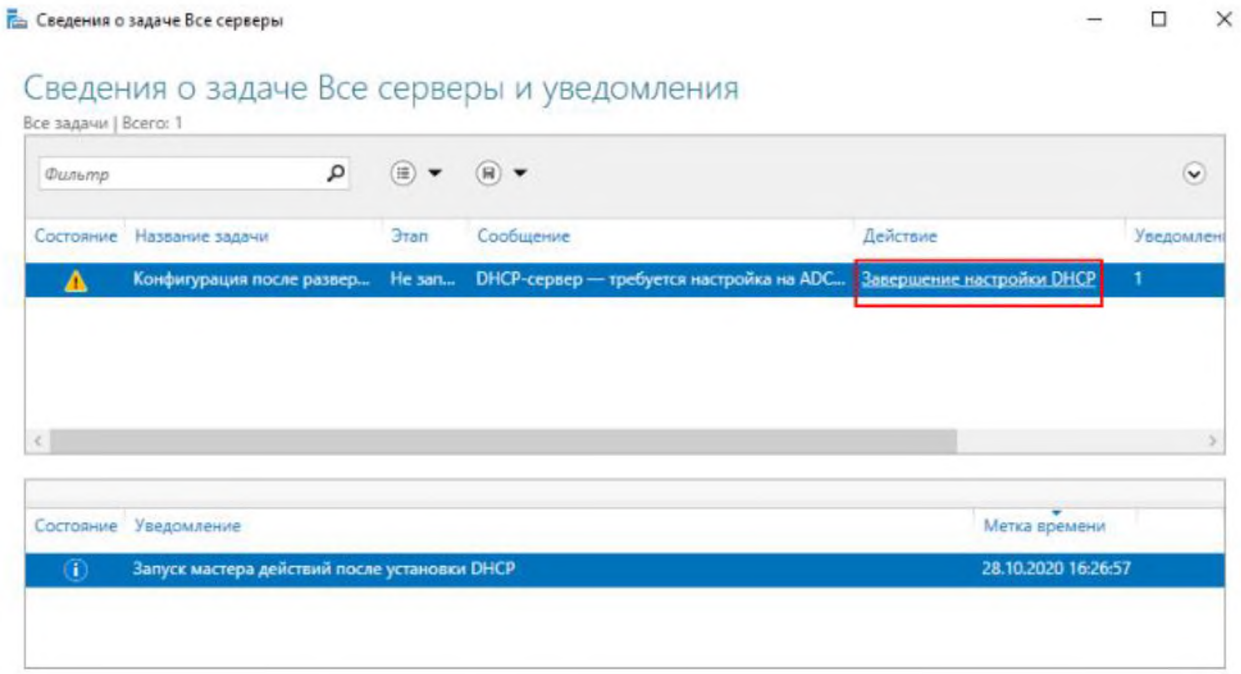

Рисунок 2.10 – Налаштування серверу

У відкритому вікні майстра налаштувань DHCP переходимо до вікна авторизації.

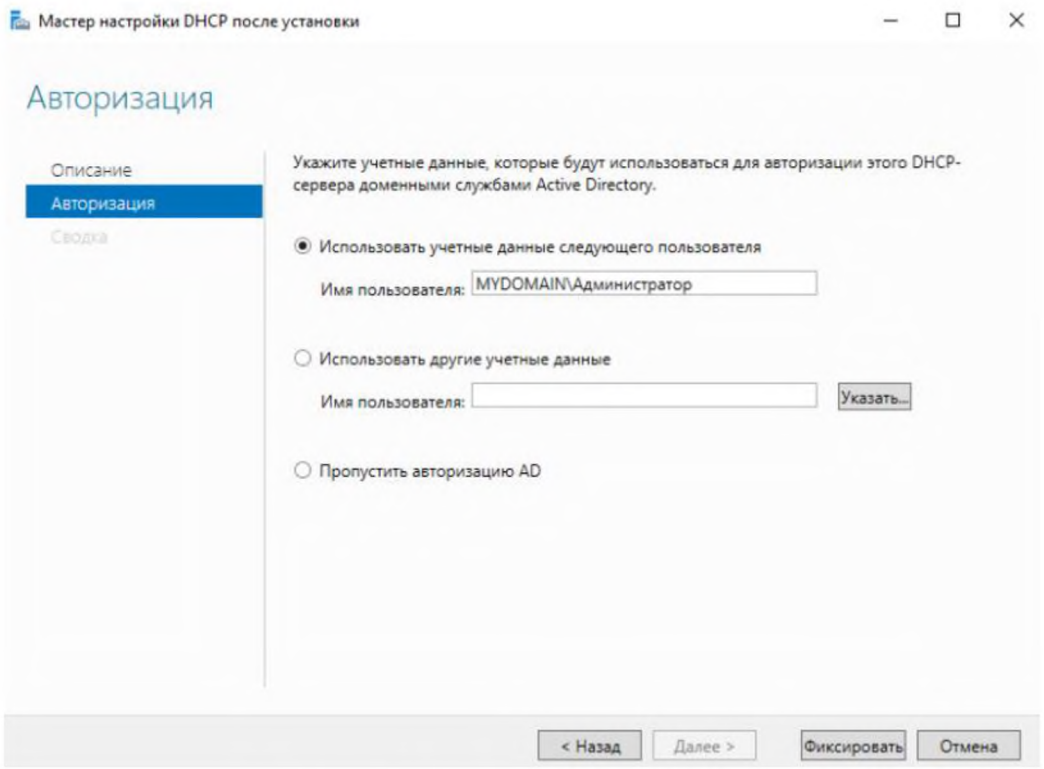

Рисунок 2.11 – Авторизація

На вибір можна обрати декілька варіантів:

- Використати облікові дані адміністратора (за замовчуванням);
- Використовувати облікові дані іншого користувача;
- Пропустити авторизацію AD.

За умовчанням авторизувати DHCP-сервер у домені можуть лише члени групи EnterpriseAdmins, куди якраз і входить користувач MYDOMAIN\Адміністратор. Таким чином обираємо варіант за замовчуванням та переходимо до вікна «Зведення» на якому натискаємо «Далі», та закінчуємо налаштування DHCP сервера [11].

Тепер потрібно зробити налаштування нової DHCP області, якою будемо користуватись.

В диспетчері серверів переходимо до вкладки «DHCP»

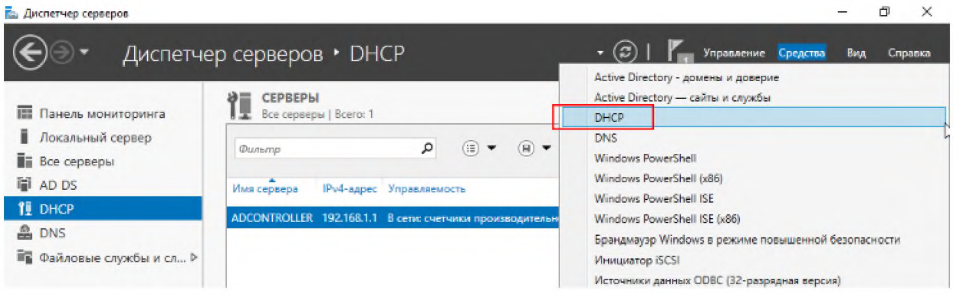

Рисунок 2.12 – Налаштування DHCP

У вікні з налаштуваннями DHCP потрібно клацнути правою кнопкою мишки на IPv4 і потім на пункт меню "Створити область". Після цього відкриється майстер створення нової сфери.

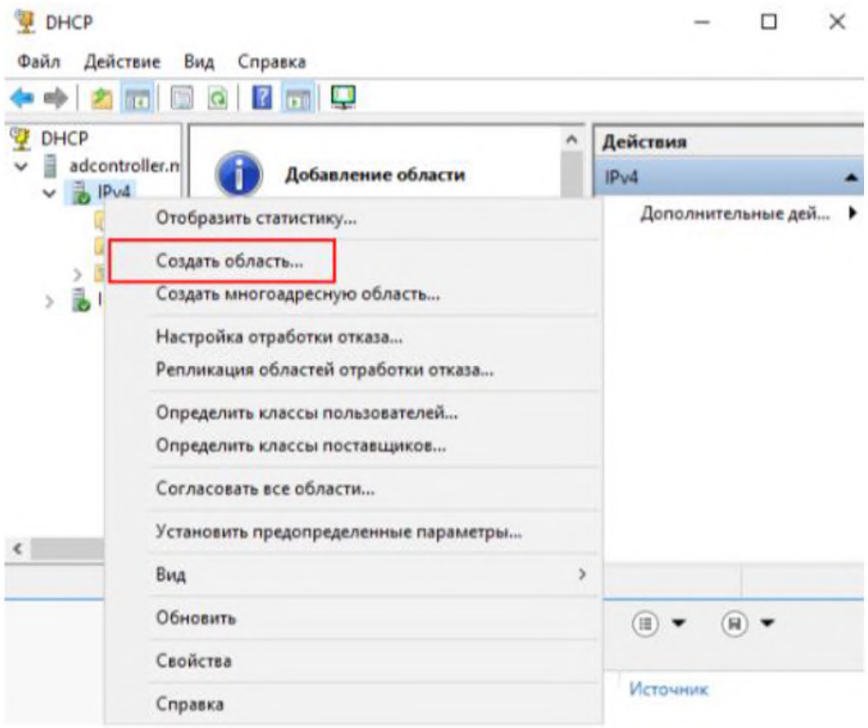

Рисунок 2.13 – Створення області

Під поняттям область DHCP розуміється певний діапазон IP-адрес, які може видавати DHCP-сервер іншим комп'ютерам у мережі. Кожна область крім діапазону IP-адрес також містить інші мережеві налаштування [12].

У наступному вікні потрібно обрати діапазон IP адрес які будуть видаватись користувачам в домені. Назву пишемо DHCP-область SCOPE1 та переходимо до наступного вікна. У наступному вікні обираємо діапазон адрес які будуть

зарезервовані, в нашому випадку : 192.168.0.1/24, та діапазон адрес які будуть видаватись користувачам 192.168.0.25/254, (192.168.1.255 - це зарезервована широкомовна адреса, її видавати теж не можна) [12].

Не обов'язково видавати так багато IP адрес, в залежності від кількості робочих місць які будуть підключатись до серверу і потрібно ставити відповідний діапазон, але не потрібно забувати, що кількість робочих місць з часом буде змінюватись, тому потрібно вказувати більше IP адрес чим потрібно.

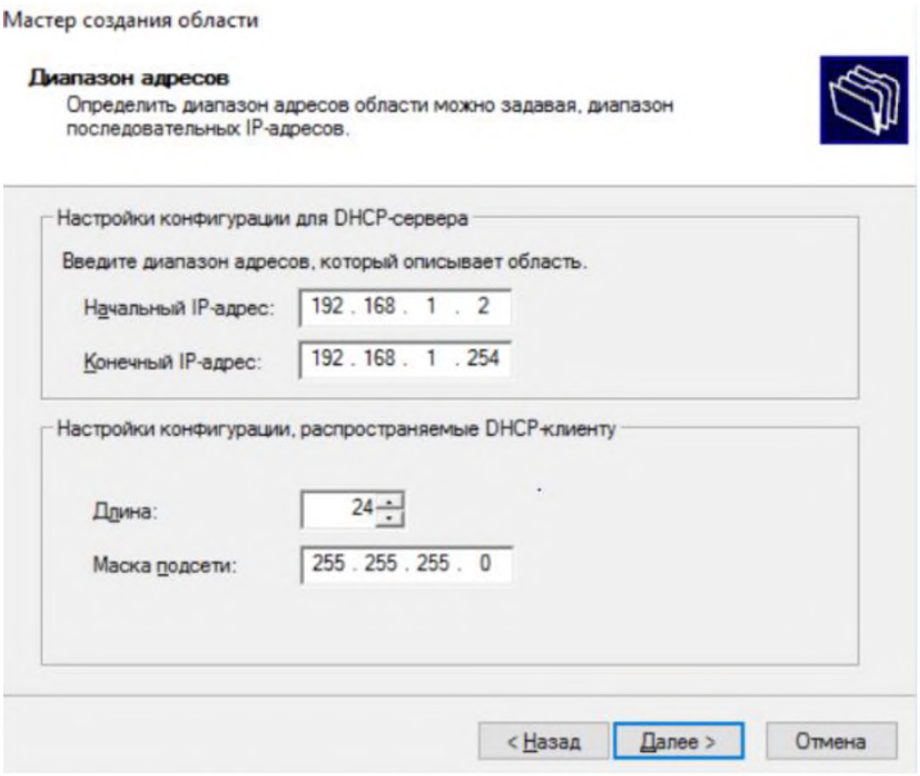

Рисунок 2.14 – Створення області IP адрес

Налаштувавши діапазон адрес потрібно перейти до наступного вікна «Термін тривалості оренди адрес». Протокол DHCP передбачає виділення адрес лише на певний час, після чого комп'ютери повинні продовжувати оренду. Тут можна налаштувати цей час (за замовчуванням – 8 днів). У випадку з компанією СМС потрібно виставити більший термін оренди, так як працівники можуть бути у відряджені досить довго, після чого їх IP адрес може бути присвоєний іншому робочому місцю [12].

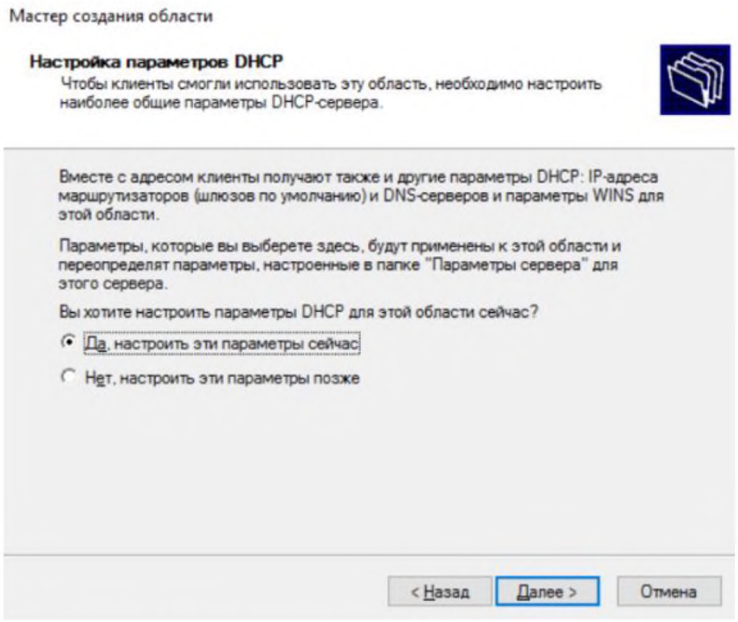

Рисунок 2.15 – Налаштування оренди IP адрес

Перше мережне налаштування для клієнтів - це шлюз за замовчуванням. У стенді з двох віртуальних машин це налаштування в принципі не потрібне. Але можна уявити, що windows_server відіграватиме роль шлюзу у зовнішню мережу, і додати адресу 192.168.1.1 як шлюз за замовчуванням [13]. Далі йде налаштування DNS. Тут можна встановити ім'я батьківського домену та адреси DNS-серверів. DNS сервер - це IP-адреси серверів, куди слід звертатися клієнтам за допомогою DNS-імен. Зараз у цьому списку фігурує та сама адреса, що ми додали як шлюз за замовчуванням. На цьому етапі налаштування DNS та DHCP закінчено [13].

Налаштування DNS. Налаштування системи доменних імен можна зробити в налаштуванні серверу за допомогою диспетчера серверів.

1. Відкриваємо диспетчер серверів та обираємо засоби та DNS

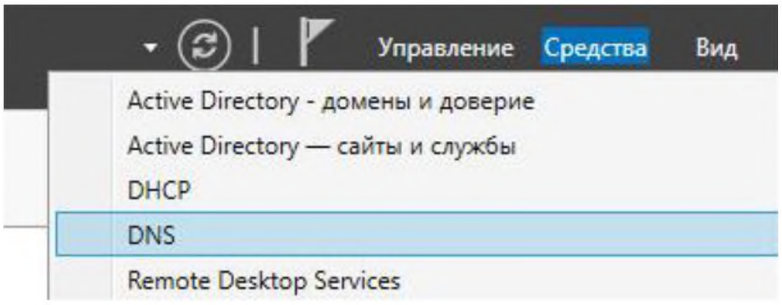

Рисунок 2.16 – Налаштування DNS за допомогою диспетчер серверів

2. У вікні вибираємо потрібний сервер, якщо їх кілька - розкриваємо його - натискаємо правою кнопкою миші по Сервери умовного пересилання - Створити сервер умовного пересилання:

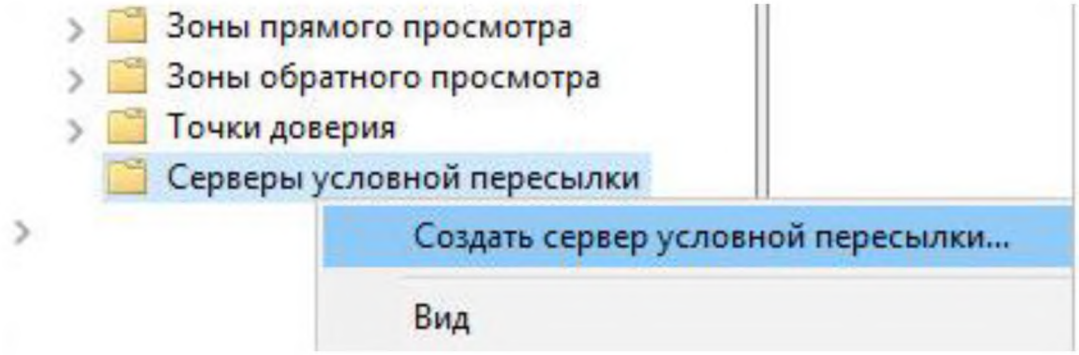

Рисунок 2.17 – Створення сервера умовного пересилання

3. У DNS-домен пишемо другий домен (наприклад konsort.holding), потім задаємо його IP-адресу, ставимо галочку Зберігати умовний сервер пересилки в Active Directory і реплікувати її наступним чином - вибираємо Всі DNS-сервери в цьому домені [14].

4. Після створення серверу умовного пересилання потрібно відкрити PowerShell, та вести команду : «nslookup secondary.local». Після спрацювання команди відповідь повинна бути такою :

- Server: localhost;
- Address: 192.0.0.1;
- Non-authoritative answer;
- Name: konsort.holding;
- Address: 192.168.10.10.

Після внесення всіх необхідних налаштувань з DNS, можна розпочинати створення довірливих відносин між доменами. Для цього потрібно знову повернутися до диспетчера серверів та зробити такі налаштування:

1. У створеному домені konsort.holding потрібно відкрити засоби Active Directory, після чого обрати домени та довіра.

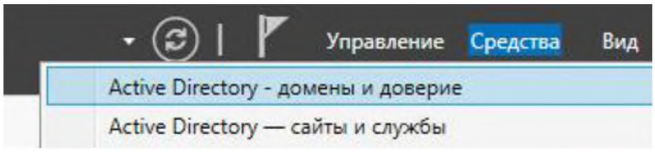

Рисунок 2.18 – Створення довірливих відносин в домені konsort.holding

2. У відкритому вікні натискаємо правою кнопкою на домен konsort.holding та обираємо налаштування.

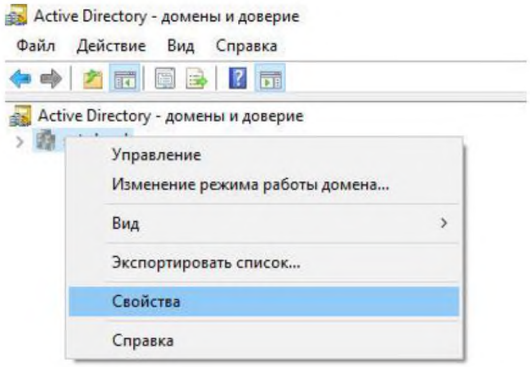

Рисунок 2.19 - Налаштування домену konsort.holding

3. Обираємо пункт Відносини та довіра та обираємо створити довірливі відносини.

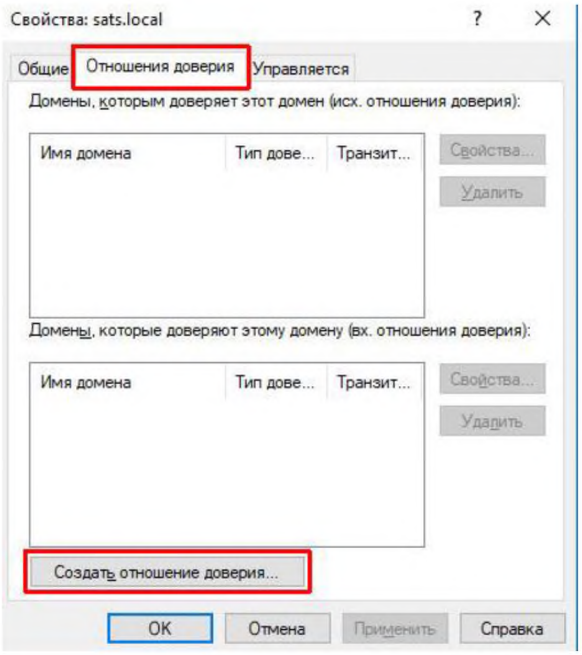

Рисунок 2.20 – Довірливі відносини

4. У відкритому вікні водимо ім’я другого домену та йдемо далі.

5. В типі довіри потрібно обрати Довірені ліси

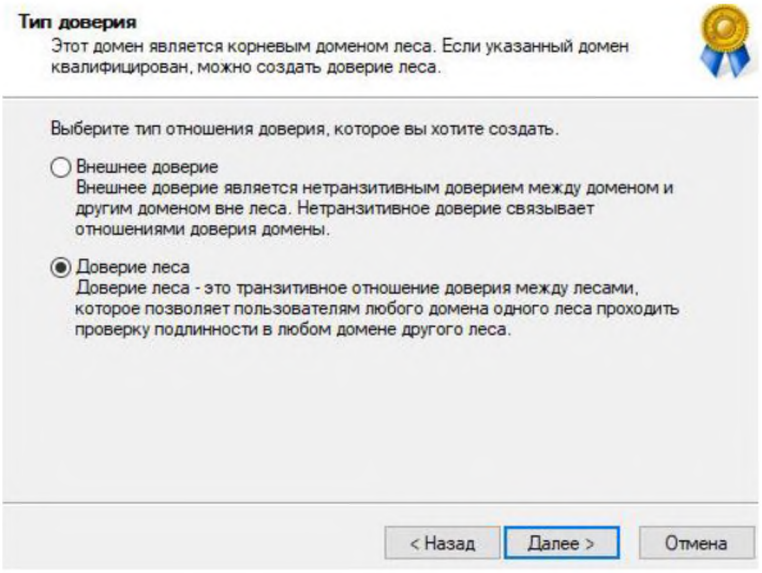

Рисунок 2.21 – Тип довіри

6. В наступному вікні «Направлення відносин та довіри» обираємо двостороннє.

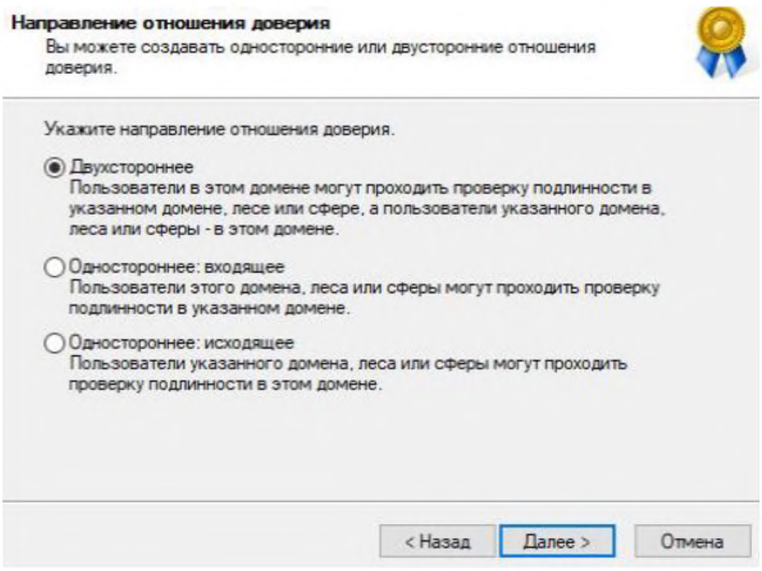

Рисунок 2.22 – Направлення відносин та довіри

7. У наступному вікні вибираємо, на якому з доменів ми застосовуємо налаштування - якщо у нас є права адміністратора для обох доменів, то вибираємо

для цього домену:

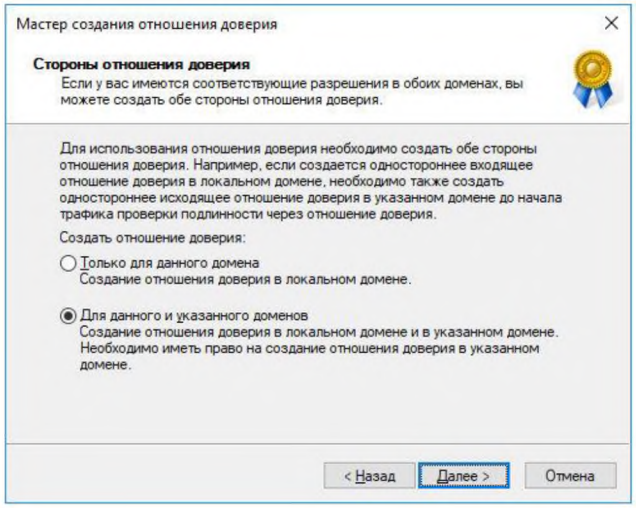

Рисунок 2.23 – Сторони відносин в довірі

8. На наступному етапі система зв'яжеться з другим контролером домену, і якщо він доступний, запросить логін та пароль від користувача з правами адміністратора. Після чого водимо дані користувача та натискаємо Далі.

Потім потрібно обрати «Рівень автентифікації вихідної довіри» - якщо обидва домени належать організації, краще вибрати Перевірка автентичності в лісі, щоб надати доступ до всіх ресурсів.

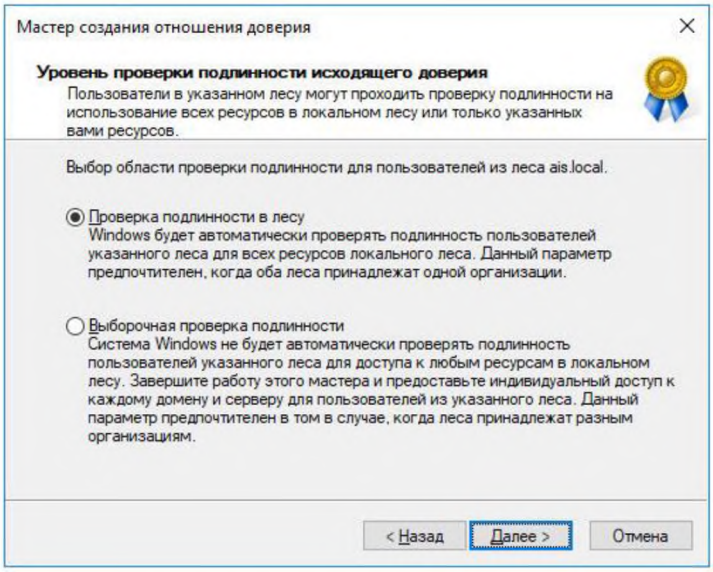

Рисунок 2.24 – Рівень перевірки автентичності довіри

9. В останньому вікні потрібно обрати створити довірливі відносини та натиснути далі. Після чого довірливі відносини будуть створені.

Довірливі відносини потрібні для компаній і організацій де використовують два домена. Наприклад якщо в однієї компанії є декілька дочірніх фірм які працюють в одному офісі, тоді за допомогою довірливих відносин є можливість об'єднати всі домени в одну структура яка дозволить полегшити адміністрування домену [14].

2.3 Алгоритм підключення робочих місць до доменного серверу

Для підключення робочих місць до домену потрібно мати власного користувача який має права адміністратора в домені. [14]:

1. Обрати власний домен в нашому випадку cmc.holding та відкрити його.

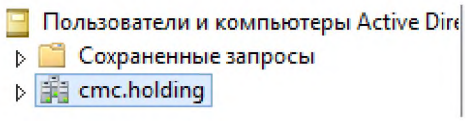

Рисунок 2.25 – Вибір домену

2. Перейти в вкладку «users».

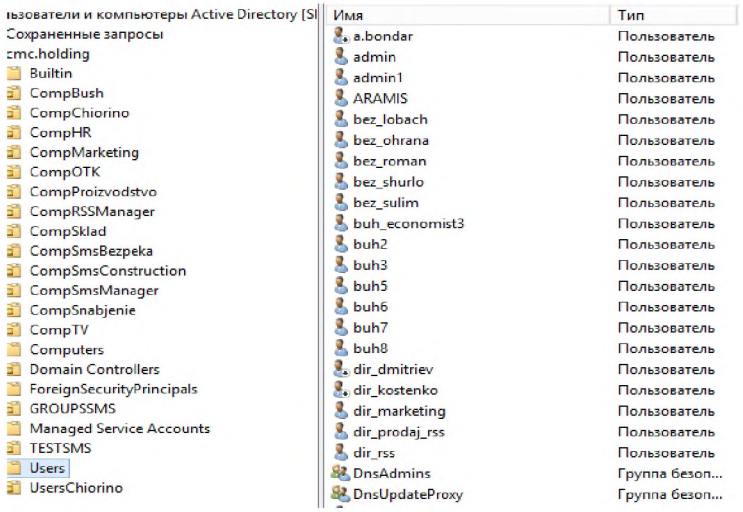

Рисунок 2.26 – Налаштування «users»

3. Правою кнопкою миші натиснути на вільному місці, після чого обрати створити користувача.

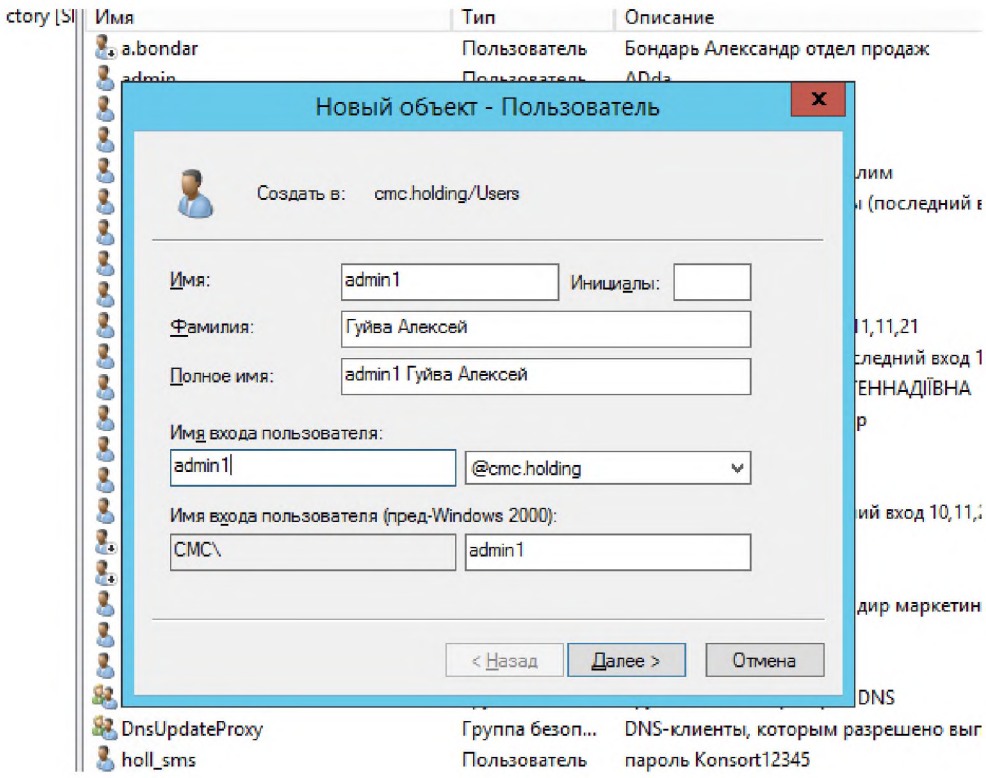

Рисунок 2.27 – Створення користувача в домені

4. Заповнюємо необхідні поля інформацією та натискаємо «Далі», після чого користувач з’явиться у вкладці «users».

Далі для додавання персонального комп’ютера або ноутбуку потрібно змінити мережеві налаштування. В першу чергу потрібно зайти в панель задач, після чого обрати мережа та інтернет, далі переходимо до «Ethernet» та в «Параметри адаптеру» обираємо нашу мережеву карту, після чого натискаємо «Властивості» «протокол IP v4» та робимо зміни [15].

Обираємо використовувати наступний DNS сервер, та у вікні «Бажаний DNS сервер» потрібно прописати IP-адресу сервера домену, в нашому випадку 192.168.0.200, а в вікні «Альтернативний DNS сервер» потрібно прописати 8.8.8.8 (IP адресу сайту google). Саме за допомогою цього параметру ми маємо змогу під’єднати комп’ютер або ноутбук до домену (Рисунок 2.3.4)

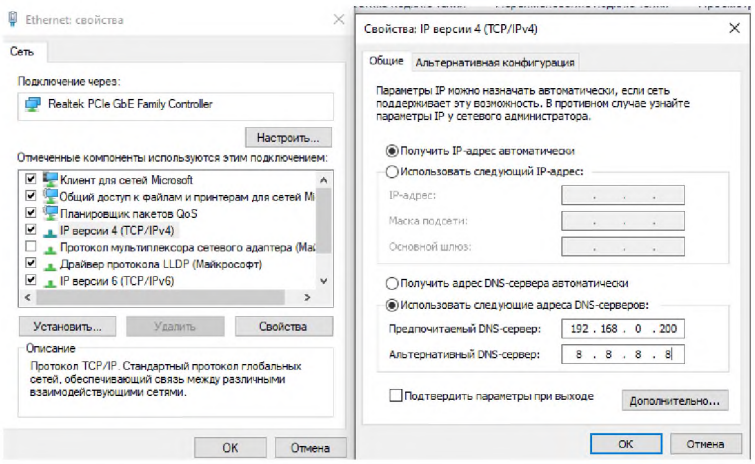

Рисунок 2.28 – Налаштування мережевої карти

Для додавання машини до домену потрібно виконати такі дії :

1. Відкриваємо командний рядок від адміністратора, та прописуємо команду sysdm.cpl.

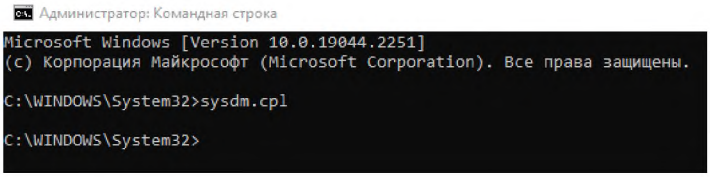

Рисунок 2.29 – Командний рядок під керівництвом адміністратора

2. В налаштуваннях системи потрібно перейти в вкладку «Змінити».

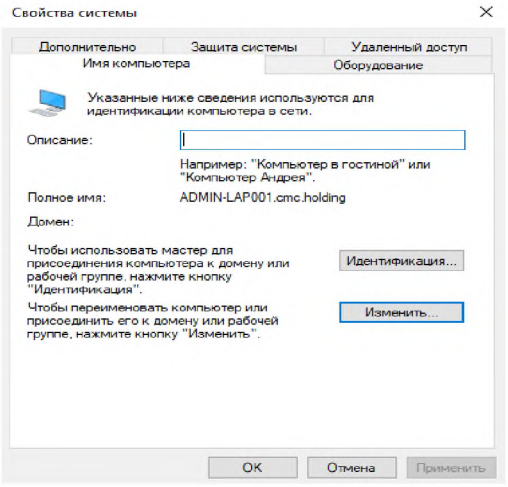

Рисунок 2.30 – Властивості системи

3. Вводимо ім’я комп’ютера яке буде відображатись в домені, та переходимо з «Робочої групи» в «Домен» в нашому випадку домен «cmc.holding».

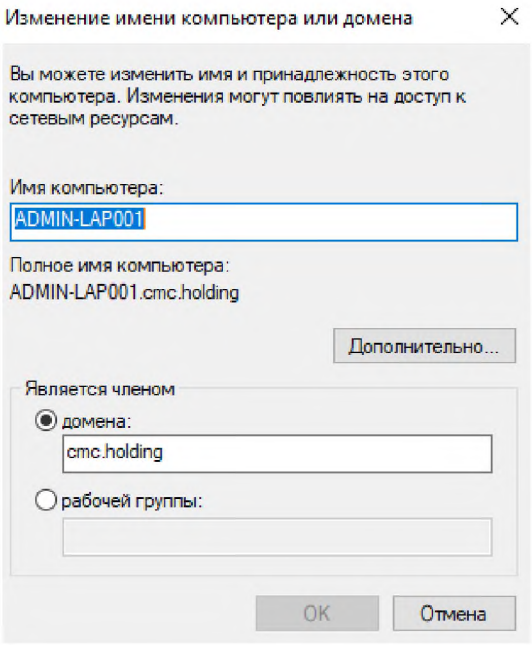

Рисунок 2.31 – Зміна імені ПК та внесення в домен

4. Після внесення змін виникне вікно в якому буде написано «Для додавання машини в домен потрібно володіти користувачем з правами адміністратора», у вікні вводимо логін та пароль користувача та натискаємо «ОК» [16].

5. При появі вікна «пристрій успішно додано в домен» потрібно виконати перезавантаження робочого місця.

6. Після перезавантаження ПК, перед входом в обліковий запис потрібно виконати «Вхід за допомогою іншого облікового запису», після чого ввести : логін (ім’я облікового запису який створений в домені), перед тим як написати ім’я потрібно відзначити, що ми входимо саме в наш домен, а саме логін повинен писатись саме так (CMC\admin1), та вводимо пароль доступу.

Після виконання цих дій можна сказати, що користувач і його пристрій знаходяться в домені [16].

Висновки до розділу 2

За допомогою розгорнутого серверу Active Directory, працівники компанії можуть бут спокійними, так як проникнути до їхнього ПК або ноутбуку стало не так і легко, для входу в систему доведеться знати користувача який зареєстрований в домені та підібрати до нього пароль.

Також впровадження доменної структури дозволить системним адміністраторам мати доступ до будь якого робочого місця, для подальшої роботи з системою. Доступ до серверу обмежений, за для забезпечення безпеки.

Використовуючи сервер домену є можливість слідкувати за оборотом техніки на підприємстві, за допомогою цього бухгалтерський облік техніки можна проводити набагато простіше. Якщо на підприємство купується техніка (персональний комп'ютер або ноутбук), в першу чергу системні адміністратори роблять потрібні налаштування та вносять техніку в домен, після чого техніка отримує відповідне ім'я в мережі та власного користувача.

Основним бажанням компанії яка користується комп'ютерною технікою – це безпека техніки та інформації яка знаходиться на ній, саме тому зараз компанії не жалкують кошти на впровадження новітніх технологій по забезпеченню цілісності та інформаційної безпеки підприємства. Проаналізувавши інформацію в мережі інтернет можна сказати, що розгортання доменного серверу повинно бути обов'язковим для компаній, в яких робочих місць де використовуються ПК або ноутбуки більше 50.

РОЗДІЛ 3
ЗАСОБИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА ТА ОЦІНКА ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ЇЇ МОДЕРНІЗАЦІЇ

Основними методами забезпечення цілісності інформації (даних) під час зберігання в автоматизованих системах є:

- забезпечення відмовостійкості (резервування, дублювання, дзеркалювання обладнання та даних, наприклад через використання RAID-масивів);
- забезпечення безпечного відновлення (резервне копіювання та електронне архівування інформації).

3.1 Алгоритм адміністрування прав користувачів для забезпечення цілісності інформаційної системи підприємства

Окрім розгортання домену потрібно зробити його налаштування. Домену структуру встановлюють не тільки для того, щоб слідкувати за кількість облікових записів, ай для доступу до окремих блоків даних. Частіше за все підприємства беруть на роботу людей с великим досвідом в своїй сфері, бухгалтерський облік, конструкторські програми, безпека підприємства, но не завжди ці люди повністю розуміють, що в декілька натисків мишкою в системних файлах операційної системи можуть зробити великі проблеми [17].

Майстер додавання ролей та компонентів

Переходимо до панелі моніторингу та натискаємо на пункт "Додати ролі та компоненти", після чого повинне відкритися вікно «майстер додавання ролей та

компонентів» [18]. У першому вікні натискаємо далі повинен відкритись єкран "Вибір типу установки".

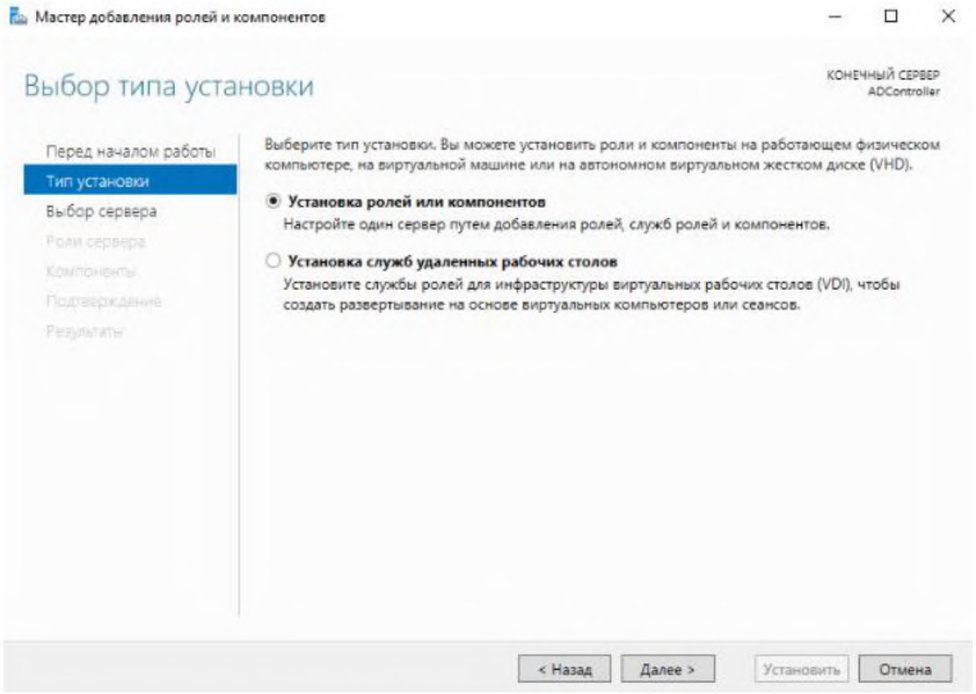

Рисунок 2.32 – Додавання ролей та компонентів

Залишаємо значення за встановленням та натискаємо «далі». У виборі сервера потрібно обрати наш сервер та натиснути кнопку «Далі».

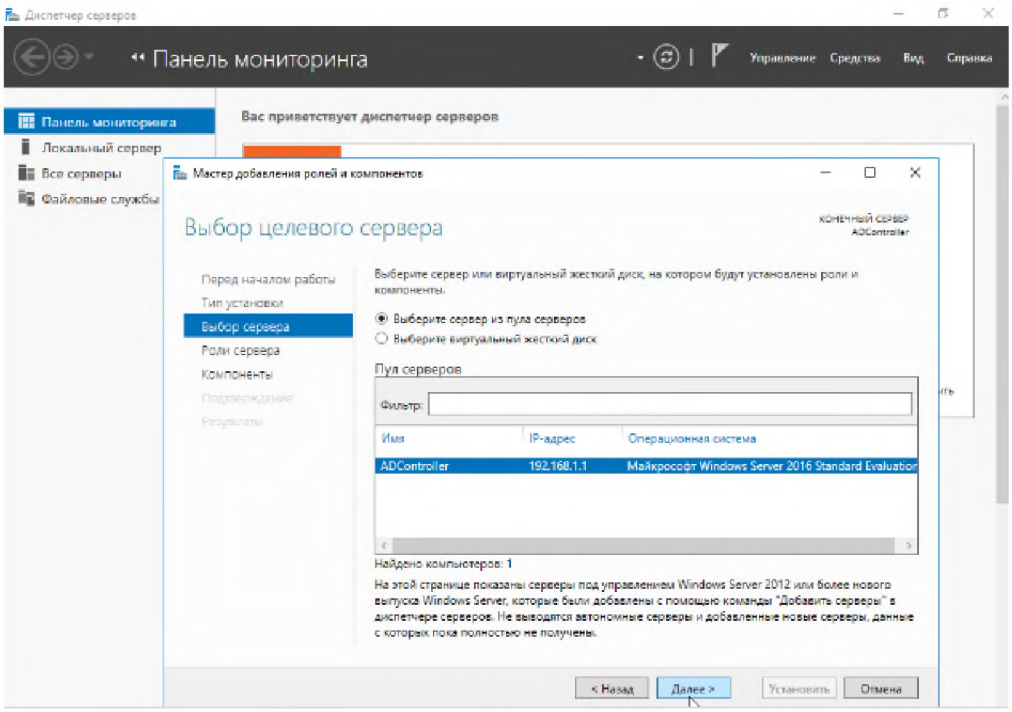

Рисунок 2.33 – Вибір серверу

Майстер додавання ролей дозволяє встановлювати роль не тільки на поточну машину, але взагалі на будь-який доданий сервер і навіть на віртуальний жорсткий диск [19].

У вікні «Ролі серверу» обираємо ролі які потрібні для наших цілей, а саме :

- DHCP-server;
- DNS-server;
- Домені служби Active Directory.

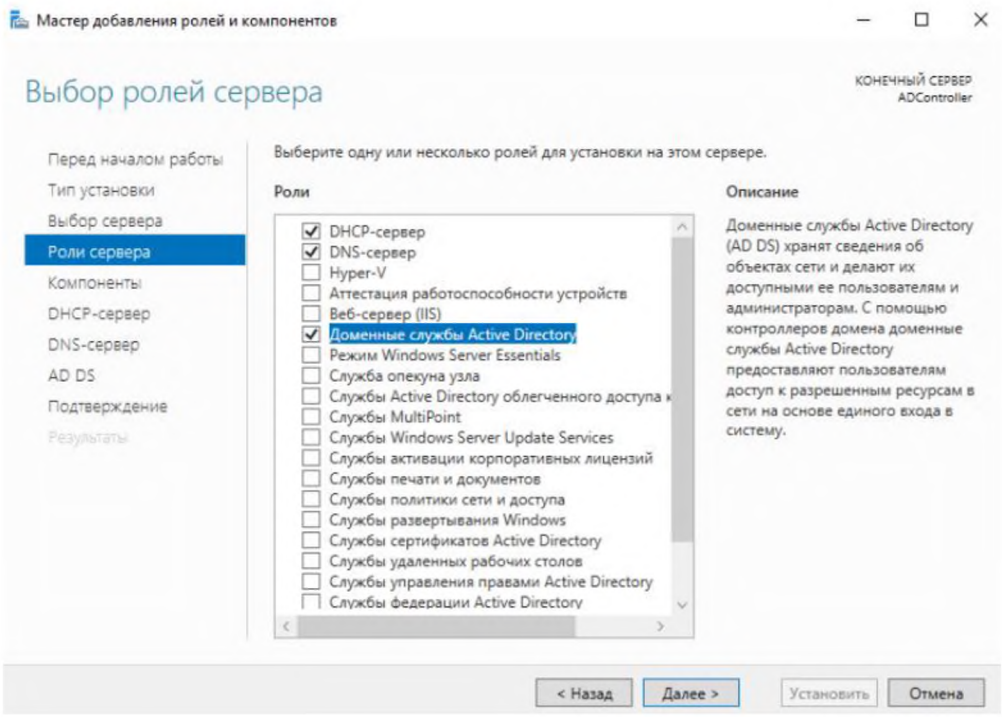

Рисунок 2.34 – Додавання ролей на сервер

Наступним кроком потрібно додати компоненти сервера:

- Середа AD DS та AD LDS;
- Модулі Active Directory для Windows PowerShell;
- Середа AD DS;
- Центр адміністрування Active Directory;
- Оснастка для командної строки AD DS [20].

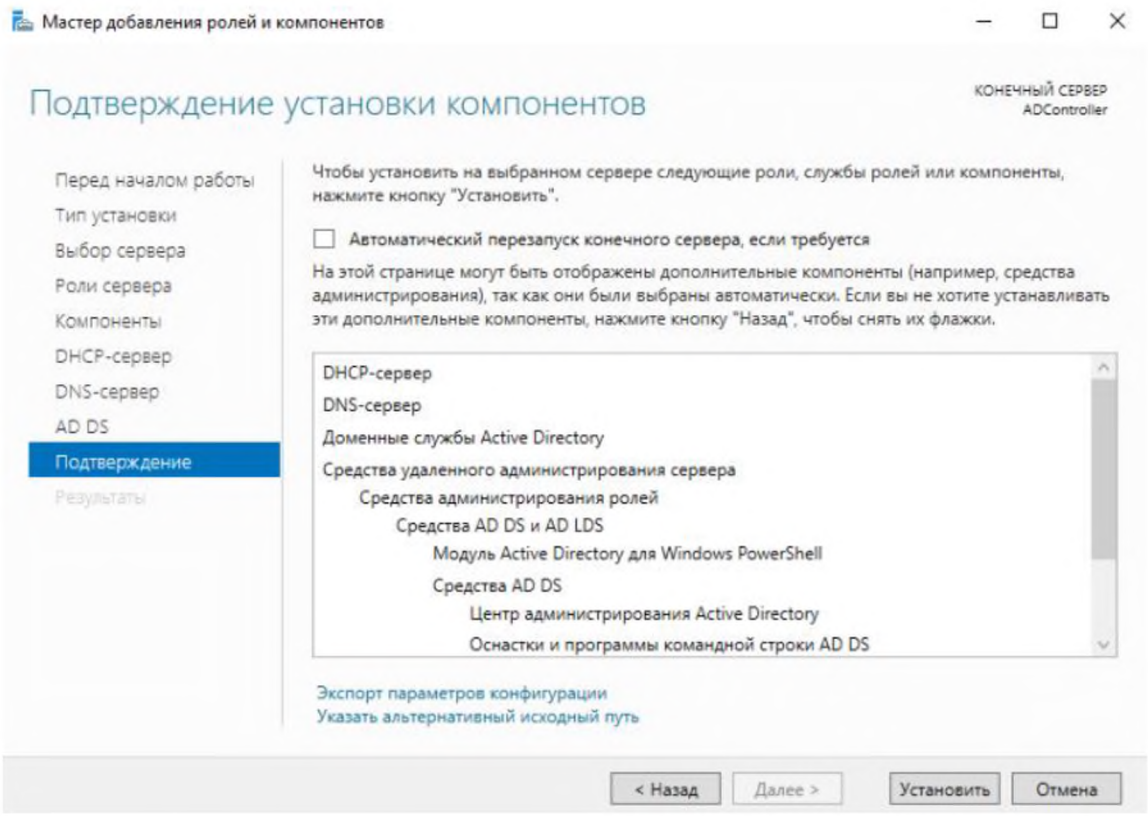

Рисунок 2.35 – Компоненти які будуть додані до сервера

Після перевірки ролей та компонентів потрібно натиснути на «Встановити», наступним кроком потрібно підвисити роль сервера до контролеру домену, після чого робимо перезавантаження сервера [21].

3.2 Резервне копіювання (Backup) серверних налаштувань та програмних засобів

Резервне копіювання (backup) - процес створення копії даних. Необхідний відновлення даних в оригінальному чи новому місці розташування. Часто потреба копіювання виникає у разі пошкодження чи руйнування даних. Зробити резервне копіювання даних на сервері можна за допомогою диспетчера серверів [22].

Резервне копіювання серверів та серверного обладнання є обов'язковим для будь якої організації, так як ніхто не застрахований від втрати інформації.

За допомогою резервного копіювання системний адміністратор буде мати змогу як відновити сервер так і інформацію яка зберігалась на ньому. Резервне копіювання є обов'язковим для сервера на якому зберігається програма для бухгалтерського обліку наприклад: 1С, медок, арт звіт про. Та багато інших. Окрім цього якщо на підприємстві використовується управляючий роутер за допомогою якого побудована мережа компанії, на ньому також потрібно постійно робити резервні копії, для можливості швидкого віднолення робото здатності мережі [24].

Windows Server Backup - вбудований компонент операційної системи Windows, що дозволяє створювати резервні копії системи та працювати з ними. Якщо компанія використовує серверну Windows з резервним копіюванням не повинно виникнути проблем, так як не потрібно знаходити та підбирати програмне забезпечення за допомогою якого потрібно робити Backup, а враховуючи те, що деякі програми для резервного копіювання є платними за допомого Server Backup компанія також економить свої кошти [24].

Встановлення резервного копіювання даних за допомогою Windows Server Backup, виконується за допомогою таких кроків:

1. Відкриваємо вікно управління сервером та натискаємо на пункт «Add roles and features».
2. В якості типу потрібно вказати «Role-based or feature-based installation» (Встановлення на основі ролей або функцій).

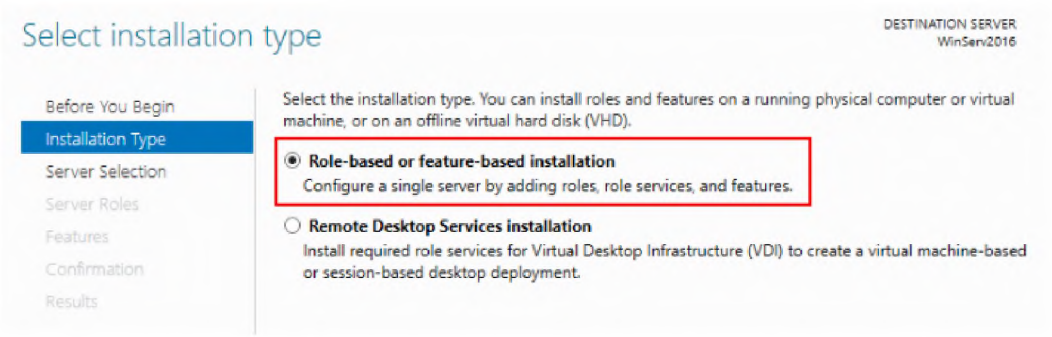

Рисунок 2.36 – Встановлення ролей та функцій для Backup

3. Обираємо наш сервер для встановлення ролей та функцій.
4. У списку функцій потрібно відмітити «Windows Server Backup».

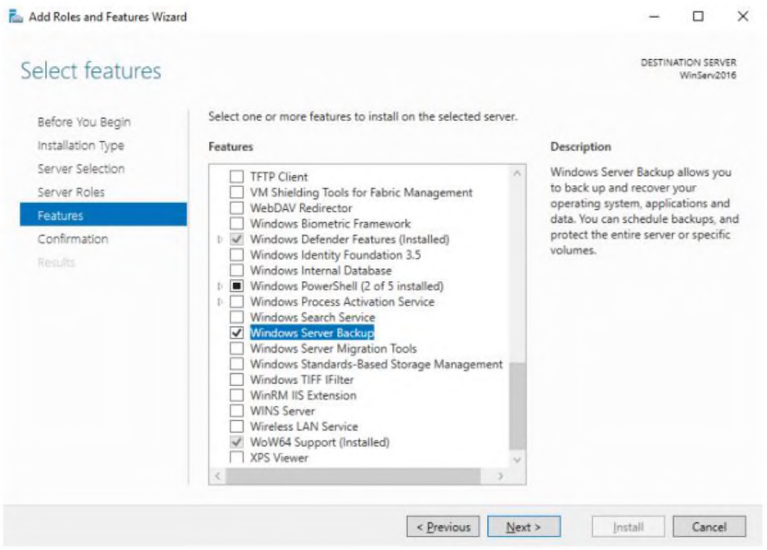

Рисунок 2.37 – Вибір ролей та функцій

5. Для встановлення натискаємо кнопку «Далі».
6. Виконавши ці дії ми встановили функції та ролі для резервного копіювання на наш сервер.

Встановивши ролі та компоненти потрібно зробити налаштування серверу, за допомогою яких буде робитись резервне копіювання [25]. Щоб відкрити систему архівації Windows, потрібно зайти у «Диспетчер серверів», у верхньому правому куті обираємо «Tools» і натискаємо «Windows Server Backup». Знайти ці компонент можна також на панелі керування в розділі Адміністрація.

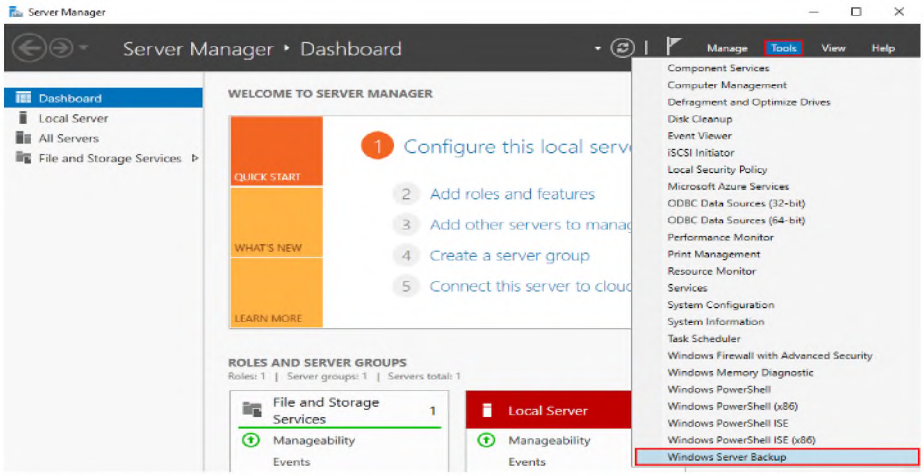

Рисунок 2.38 – Налаштування «Windows Server Backup»

У вікні в меню зліва обираємо Local Server [26]. У горизонтальному меню праворуч з'явиться вертикальне меню, в якому можна налаштувати розклад резервного копіювання, одноразове створення копії та відновлення.

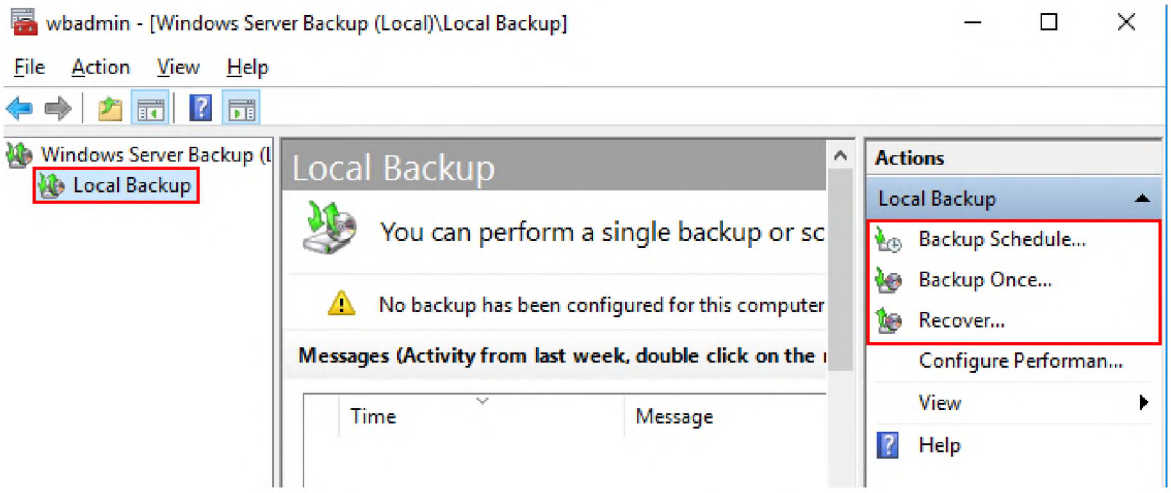

Рисунок 2.39 – Розклад резервного копіювання

Щоб налаштувати розклад, потрібно натиснути на кнопку «Backup Schedule». За допомогою цих ролей є змога створити резервні копії як всієї системи так і окремих компоненті. Для наших цілей краще всього зробити резервне копіювання всієї системи. Для цього потрібно відмітити Full Server.

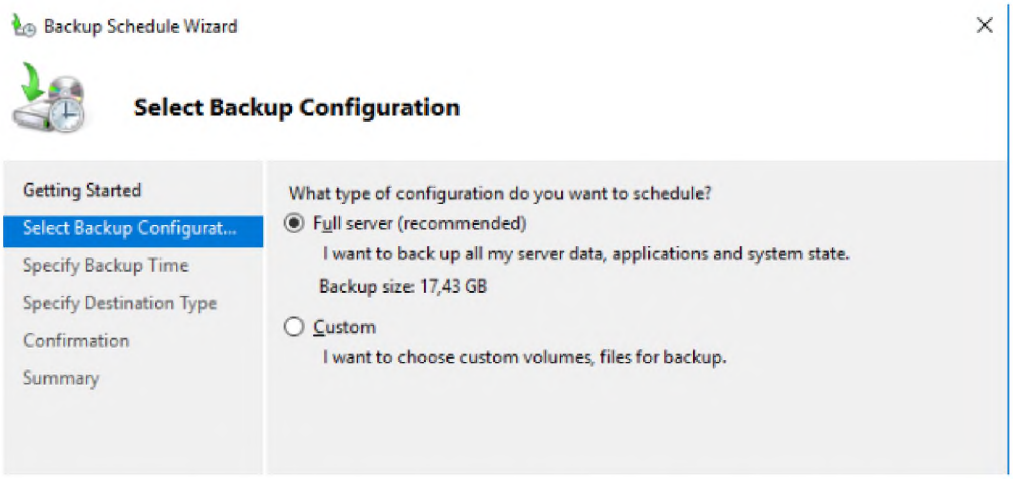

Рисунок 2.40 – Резервне копіювання всієї системи

На наступному кроці потрібно встановити частоту створення резервної копії та час. Час можна обрати з запропонованого списку. Потрібно розуміти, якщо не сервері велика кількість інформації то резервне копіювання займе велику кількість часу, також при резервному копіюванні користувачі не будуть мати змогу користуватись сервером [27]. Враховуючи ці фактори і те, що сервери в компанії ТОВ СМС працюють постійно, було прийняте рішення робити Backup кожен день в 23:00, для того щоб користувачі мали доступ до серверу в робочій час.

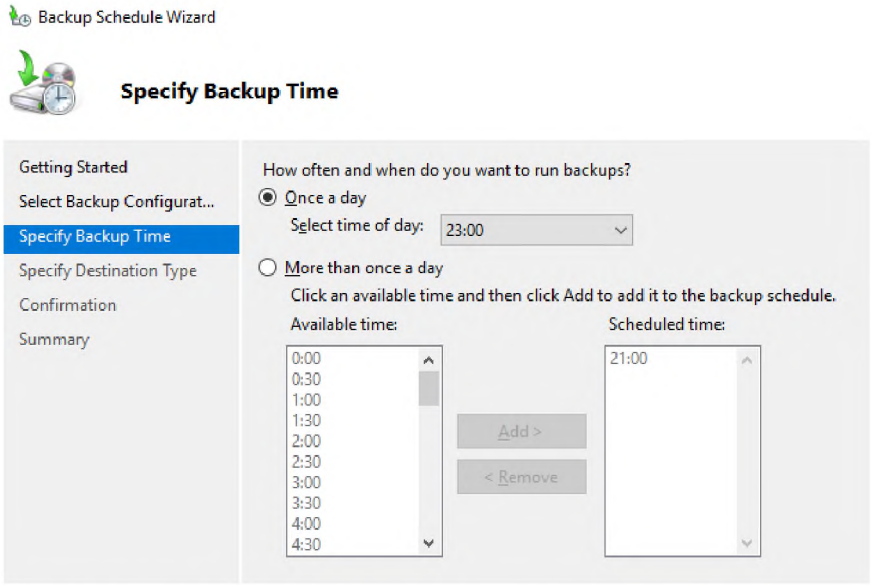

Рисунок 2.41 – Час резервного копіювання

Обравши час коли наш сервер буде робити резервне копіювання, потрібно обрати місце куди буде робитись Backup [28]. Для резервного копіювання інформації на сервері було встановлено додатковий жорсткий диск.

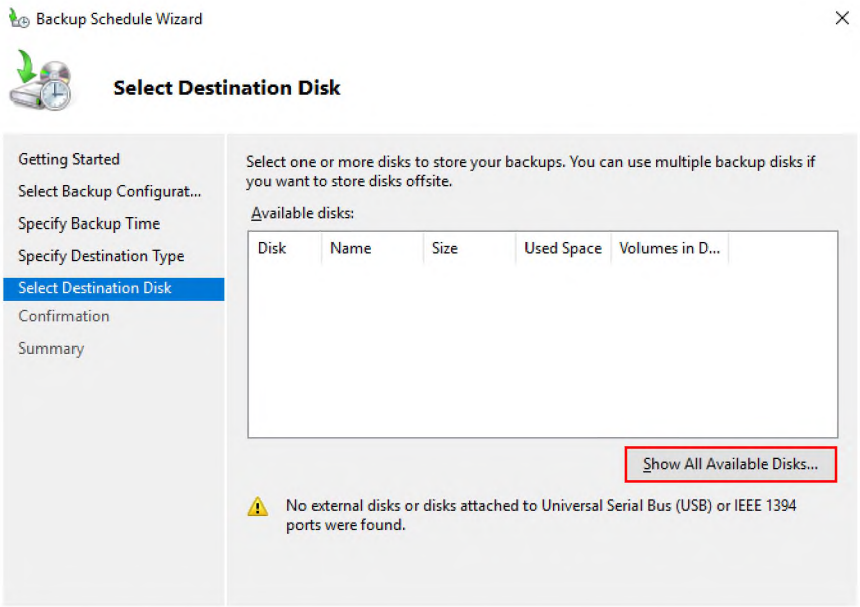

Рисунок 2.42 – Вибір диску для резервного копіювання

В наступному вікні нам потрібно обрати жорсткий диск для резервного копіювання, після чого натискаємо «ОК», після вибору жорсткого диску нам потрібно підтвердити форматування та перевірити налаштування, після чого почнеться форматування [29]. Після закінчення форматування можна перевірити налаштування які були встановлені. Після того, як у вказаний час буде запущено резервування компонентів, у головному меню можна побачити кількість копій, статус та час останнього резервування [29].

3.3 Хешування інформації

Простими словами, хешування означає введення інформації будь-якої довжини та розміру у вихідному рядку та видачу результату фіксованої довжини заданої алгоритмом функції хешування. У контексті криптовалют, таких як Біткоїн,

транзакції після хешування на виході виглядають як набір символів певної алгоритмом довжини (Біткоїн використовує SHA-256) [36].

Хешування – це перетворення вхідного масиву даних довільної довжини у вихідний бітовий рядок фіксованої довжини. Такі перетворення також називаються хеш-функціями чи функціями згортки, які результати називають хешом, хеш-кодом чи дайджестом повідомлення [40].

Хешування застосовується порівняння даних: якщо в двох масивів хеш-коди різні, масиви гарантовано різняться, якщо однакові - масиви, швидше за все, однакові. У загальному випадку однозначної відповідності між вихідними даними та хеш-кодом немає через те, що кількість значень хеш-функцій менша ніж варіантів вхідного масиву, існує безліч масивів, що дають однакові хеш-коди - так звані колізії. Імовірність виникнення колізій грає важливу роль оцінці якості хеш-функцій [42].

Існує багато алгоритмів хешування з різними характеристиками (розрядність, обчислювальна складність, криптостійкість тощо). Вибір тієї чи іншої хеш-функції визначається специфікою задачі, що розв'язується. Найпростішими прикладами хеш-функцій можуть бути контрольна сума або CRC [42].

С хешуванням працюють такі спеціалісти як :

- ІТ-фахівці, розробки яких зберігають чутливу конфіденційну інформацію. Наприклад, у веб-розробці хеш зазвичай потрібні для перевірки паролів. Замість них на сервері зберігаються хеш, а коли користувач вводить пароль, той автоматично хешується, і хеш порівнюється зі збереженим на сервері [42].

- Розробники, які мають справу зі складними структурами даних, такими як асоціативні масиви та хеш-таблиці.

- Етичні хакери та фахівці з інформаційної безпеки для забезпечення конфіденційності даних або, навпаки, для перевірки тієї чи іншої інформації. Наприклад, конкретний вірус можна розпізнати характерним хешем [45].

Основне призначення хешування – перевірка інформації. Це завдання важливе у величезній кількості випадків: від перевірки паролів на сайті до складних обчислень у блокчейни. Оскільки хеш - це унікальний код певного набору даних,

можна зрозуміти, чи відповідає інформація очікуваної [45]. Тому програма може зберігати хеш замість зразка даних для порівняння. Це може бути потрібне для захисту чутливих відомостей або економії місця.

Приклад застосування хешування :

- замість паролів на сервері зберігаються хеші паролів;
- антивірус зберігає у основі хеші вірусів, а чи не зразки самих програм;
- електронний підпис використовує хеш для верифікації;
- інформація про транзакції криптовалюти зберігається у вигляді кешів;
- комміти в Git ідентифікуються за хешем [47].

3.4 Економічне обґрунтування модернізації інформаційної системи підприємства

Економічна ефективність – це результат, який можна отримати, порівнюючи показники прибутковості виробництва по відношенню до загальних витрат та використаних ресурсів. Якщо перший показник вищий у порівнянні з другою складовою, отже, цілей досягнуто, всі потреби задоволені. Якщо ситуація навпаки, отже, економічного ефекту немає і підприємство зазнає збитків.

Суть економічної ефективності у тому, щоб із доступних підприємству ресурсів отримувати більше результатів виробництва, окупивши витрати на придбання ресурсів.

Етап 1. Оцінка затрат на інформаційні технології. На даному етапі визначається обсяг інвестицій в інформаційні технології необхідний для досягнення поставлених цілей.

Оцінка витрат на інформаційні технології здійснюється в свою чергу в два етапи:

Оцінювання витрат проекту прогнозує визначення усіх капітальних і поточних витрат, поєднаних з впровадженням а саме:

а) оцінка прямих витрат визначається за формулою:

$$В_П = В_{ТЗ} + В_{ППЗ} + В_{ОП} + В_{ВСЗ} + В_{ПСП} + В_У + В_{РПЗ} + В_І, \quad (3.1)$$

$$= 16{,}300+16{,}000+10{,}000+0+0+5{,}300+0+1000=48{,}600$$

де: $В_{ТЗ}$ – купівля оперативної пам'яті, жорстких дисків, мережевих карт та термопасти; $В_{ППЗ}$ – купівля серверної Windows Server 2016; $В_{ОП}$ – оплата за створення, налаштування та адміністрування доменного сервера (Системний адміністратор); $В_{ВСЗ}$ – соціальні заходи не потрібні для створення доменного серверу; $В_{ПСП}$ стороні підприємства відсутня; $В_У$ – підключення та проведення інтернету 500 грн. також потрібна оплата тарифного плану 400 грн/міс. Річна плата становить 5300 грн.; $В_{РПЗ}$ – все програмне забезпечення окрім операційної системи є безкоштовним; $В_І$ – Навчання персоналу (підключення до серверу Active Directory) 1000 грн.

б) оцінення непрямих витрат на проект впровадження який визначається за формулою, грн:

$$В_Н = В_{Н1} + В_{Н2}, \quad (3.2)$$

$$= 1000+100=1{,}100$$

де: $В_{Н1}$ – витрати пов'язані з простоями, тобто вихід з ладу доменного сервера 1000 грн за тестування; $В_{Н2}$ – витрати пов'язані з людським фактором, наприклад пошкодження кабелю Ethernet, 100 грн за заміну.

в) оцінення витрат на обслуговування доменного серверу за період його життєвого циклу.

$$В_{УТР} = В_{ОП} + В_{ВСЗ} + В_П + В_І, \quad (3.3)$$

$$=10{,}000+0+48{,}600+2000=60{,}600$$

де: $В_{ОП}$ – витрати на оплату зарплатні системному адміністратору; $В_{ВСЗ}$ – соціальні заходи не використовувались; $В_П$ – оцінка непрямих витрат 48,600; $В_І$ – витрати на вдосконалення серверу 2000грн.

Визначення загальних витрат на проект буде розраховуватися за формулою:

$$В_{ІТ}=В_П+В_Н+В_{УТР}, \quad (3.4)$$

$$= 48{,}600+1{,}100+60{,}600=110{,}300$$

Етап 2. Оцінення вимог використання інформаційних технологій.

Впровадження проекту на підприємстві, виконується за допомого результатів операційної діяльності які здійснюється помісячно, приклад показано в табл.3.1.

Таблиця 3.1 – Операційна діяльність по проекту

Показники	Значення на кроці, тис. грн.	
	1	2
1. Ціна, грн./ш	10.000	8.000
2. Виручка, тис. грн.	50.000	50.000
4. Постійні витрати, тис. грн.	400	400
5. Амортизація устаткування, тис. грн.	800	800
7. Результат від операційної діяльності, тис. грн.	25.296	25.296

Дохід оподаткування розраховується за формулою:

$$Пр = Виручка – Затрати = 500.000\text{-}110.300 = 389.700 \quad (3.5)$$

Податок на приріст:

$$Под = Пр \cdot Ст_{под} = \quad 389.700*0.25 = 97.425 \quad (3.6)$$

де: $Ст_{под}$ – ставка податку на приріст використовує стале значення 0,25

Чистий приріст складе:

$$Прч = Пр – Под = 389.700 – 97.425 = 292.275 \quad (3.7)$$

Підсумок операційної діяльності буде складати:

$$CF_2(t) = Пр_ч + А = 292.275 + 1.600 = 293.875 \quad (3.8)$$

Для розробки, впровадження та навчання персоналу доменного серверу потрібно затрати підприємству на даний момент 48.600 грн.

Етап 3. На цьому етапі ми розрахуємо економічну ефективність проекту по створенню доменного серверу в компанії ТОВ СМС «Системи модернізації складів». Потрібно розрахувати чисту вартість при одноразовому здійснені інвестиційних витрат на початку здійснення проекту. Розрахування буде здійснюватися за допомогою формули :

$$NPV = \sum_{t=1}^{n} \frac{CF_t}{(1+i)^t} – INV_0 \quad (3.9)$$

$$NPV = \sum_{t=1}^{n} \frac{250000_1}{(1+25)^1} – INV_0 = 450.000$$

Наступним кроком буде показник бухгалтерської рентабельності

інвестиційного проекту (ROI)

$$\text{ROI} = \frac{AP}{(INV_1 + INV_2)/2} * 100. \quad (3.10)$$

$$\text{ROI} = \frac{293{,}875}{(110{,}300_1 + 110{,}300_2)/2} * 100 = 266{,}432$$

Для розробки, впровадження та адміністрування серверу компанії доведеться витратити 110.300 грн, що впорядкувати систему облікових записів та контролю за безпекою інформації.

Висновки до розділу 3

На впровадження серверу домена можна виділяти різні суми, так як для створення серверу можна використовувати вже існуючий сервер за допомогою чого зменшити витрати на купівлю нового, якщо сервер має досить великі апаратні показники то навіть не потрібно його вдосконалювати для розгортання Active Directory, достатньо просто зробити деякі зміни в програмній частині.

Якщо підприємство не бажає виділяти кошти для купівлі спеціального серверного обладнання для реалізації проекту доменного сервера, сервер можна розгорнути на звичайному персональному комп'ютері, для цтого потрібно встановити серверне програмне забезпечення, але непотрібно забувати, що доменний сервер повинен працювати цілодобово, не завжди звичайна комп'ютерна техніка може витримати такі навантаження.

Впровадження Active Directory є економічно вигідним, так як підприємство буде мати змогу скоротити витрати на програмне забезпечення, за допомогою якого відбувався захист інформації.

ВИСНОВКИ

Забезпечення безпеки мережі потребує постійної роботи та ретельної уваги до деталей. Ця робота передбачається у передбаченні можливих дій подій, плануванні заходів захисту та постійному забезпеченні користувачів. Якщо ж вторгнення відбулося, то безпека повинна мати властивості в системі захисту.

Формуючи безпекову політику, адміністратор насамперед проводить інвентаризацію ресурсів, захист яких планується, ідентифікує користувачів, яким потрібний доступ до кожного з цих ресурсів, і з'ясовує найімовірніші джерела небезпеки для кожного з цих ресурсів. Маючи цю інформацію, можна розпочинати побудову політики забезпечення безпеки, яку користувачі будуть зобов'язані виконувати.

Політика забезпечення безпеки - це не звичайні правила, які й так усім зрозумілі. Вона має бути подана у формі серйозного друкованого документа. Щоб постійно нагадувати користувачам про важливість забезпечення безпеки, можна розіслати копії цього документа по всьому офісу, щоб ці правила завжди були перед очима співробітників. Якщо ж користувачі не дотримуються правил безпеки, то потрібно обмежити їм доступ до певних ресурсів системи, це можна зробити за допомогою доменного сервера (Active Directory).

Хороша політика безпеки включає кілька елементів, у тому числі такі:

- Оцінка ризику. Що ми захищаємо і від кого? Потрібно ідентифікувати цінності, що знаходяться в мережі, та можливі джерела проблем.
- Відповідальність. Необхідно вказати відповідальних за вжиття тих чи інших заходів щодо безпеки, починаючи від затвердження нових облікових записів і закінчуючи розслідуванням порушень.
- Правила використання мережевих ресурсів. У політиці має бути прямо сказано, що користувачі не мають права використовувати інформацію не за призначенням, використовувати мережу в особистих цілях, а також свідомо завдавати шкоди мережі або розміщеної в ній інформації.
- Процедури відновлення системи захисту. Слід зазначити, що має бути

зроблено у разі порушення системи захисту та які дії будуть вжиті проти тих, хто спричинив таке порушення.

Всі ці фактори частіше враховує системний адміністратор при побудові мережі, та встановлені безпеки на робочі станції. За допомогою серверу домена, системний адміністратор має змогу не тільки захистити компанію від проникнення з мережі, а й від внутрішнього проникнення (злому). На доменному сервері розписані ролі для групи користувачів, за допомогою яких користувач не зможе встановлювати програми та компоненти без дозволу системного адміністратору, також користувачам заборонено змінювати системні файли та конфігурацію яку перестановлено на робочій машині. Також великою перевагою доменного сервера є те, що вхід на ноутбук чи комп'ютер робиться за допомогою облікових записів які додані в домен, інший користувач не буде мати змогу дістатися до файлів іншого.

У ході виконання кваліфікаційної роботи були проаналізовані наукові роботи в яких була інформація про забезпечення безпеки мережі та облікових засобів на підприємстві, проаналізовано новітні програмні засоби які розроблені для цілісності інформації на підприємстві, були враховані можливості подальшого апгрейду серверного обладнання.

Встановивши домену структуру в компанії ТОВ СМС «Системи модернізації складів», безпека компанії стала більш новітньою. Враховуючи той фактор, що на підприємстві є більше 150 робочих місць на яких використовують комп'ютерну техніку, встановлення домену було необхідним, так як дуже важко стежити за такою кількістю робочих станцій та облікових засобів.

Подальші дослідження можна направити на ознайомлення компаніям, а саме інформаційному відділу підприємств на яких використовують велику кількість комп'ютерної техніки.