Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Навчально-науковий

інститут електроенергетики

Факультет інформаційних технологій

Кафедра інформаційних технологій та комп'ютерної інженерії

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента Каінова Дмитра Романовича

академічної групи 123м-22-1

спеціальності 123 «Комп'ютерна інженерія»

на тему: «Обґрунтування структури та параметрів комп'ютерного комплексу контролю наявності учнів в школах міста Дніпро із застосуванням системи «Безпечна Школа»»

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І			
розділів:				
теоретичний розділ	проф. Цвіркун Л.І.			
синтез системи	доц. Бешта Д.О.			
Розроблення програмного забезпечення	ас. Панферова Я.В.			

Рецензент:				

Нормоконтролер:	Доц. Шедловська Я.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій та
комп'ютерної інженерії
(повна назва)
_____ Гнатушенко В В.
(підпис) (прізвище, ініціали)
«____»_____ 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістра
(бакалавра, спеціаліста, магістра)

студенту Каінов Д.Р. **академічної групи** 123м-22-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньою-професійною програмою 123«Комп'ютернаінженерія»
(офіційна назва)

на тему «Обґрунтування структури та параметрів комп'ютерного комплексу контролю наявності учнів в школах міста Дніпро із застосуванням системи «Безпечна Школа»»,
затверджену наказом ректора НТУ «Дніпровська політехніка» від 09.10.2023 р. № 1227с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	З матеріалів отриманих під час проходження практики та інших науково-технічних джерел сформулювати наукове завдання, конкретизувати предмет та мету досліджень	15.10.2023
Теоретичний	Обґрунтувати теоретичну базу розв'язання наукового завдання, якому присвячено роботу	30.10.2023
Синтез системи	Синтез системи контролю наявності учнів «Безпечна Школа»	18.11.2023
Розроблення програмного забезпечення	Розробка програмного забезпечення для системи контролю «Безпечна Школа»	28.11.2023
Експериментальний розділ	Проведення і обробка результатів експериментів	05.12.2023

Завдання видано _____ проф. Цвіркун Л. І.
(підпис керівника) (прізвище, ініціали)
Дата видачі 06 вересня 2023 р.
Дата подання до екзаменаційної комісії 10.12.2023 р.
Прийнято до виконання _____ Каінов Д.Р.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка 85 с., 43 рис., 1 табл., 28 джерел, 1 додаток

ВІРТУАЛІЗАЦІЯ, ГІПЕРВІЗОР, ВІРТУАЛЬНА МАШИНА, ІДЕНТИФІКАЦІЯ, ВІДСТЕЖЕННЯ, ВІДЕОФІКСАЦІЯ, СИСТЕМА КОНТРОЛЮ УПРАВЛІННЯ ДОСТУПОМ

Об’єкт дослідження: комп’ютерна система контролю «Безпечна Школа»

Мета роботи: розробка комп’ютерної системи контролю наявності учнів в школах міста Дніпро із застосуванням програми «Безпечна Школа». Обґрунтування вдосконалення системи контролю за учнями на основі існуючої комп’ютерної системи.

Пояснювальна записка має аналіз існуючої системи контролю наявності учнів у школах, описує роботу та недоліки від поточної системи.

Використовуючи ці данні сформовано завдання дослідження.

У розділі «Стан питання та постановка завдання» на основі отриманої інформації під час проходження практики розглянуто основні принципи віртуалізації.

У теоретичному розділі розглянуто гіпервізор ESXI, проаналізовано існуючі типи СКУД та їх інтеграцію, обрано найбільш підходящу систему під завдання, що виконуються в школі.

У розділі синтезу системи проведена розробка модифікації комп’ютерної моделі на основі існуючої програми «Безпечна Школа».

У розділі розробки програмного забезпечення створено віртуальну інфраструктуру для системи «Безпечна Школа».

У експериментальному розділі проведено ряд досліджень для виявлення оптимальної конфігурації кожної віртуальної машини.

ABSTRACT

Explanatory note 85 p., 43 figures, 1 table, 28 sources, 1 supplement

VIRTUALIZATION, HYPERVISOR, VIRTUAL MACHINE, IDENTIFICATION, TRACKING, VIDEO RECORDING, ACCESS CONTROL SYSTEM

Object of research: computer control system "Safe School"

The purpose: to develop a computer system for monitoring the presence of students in schools in the city of Dnipro using the Safe School program. Rationale: to improve the system of control over students on the basis of the existing computer system.

The explanatory note analyses the existing system of controlling the presence of students in schools, describes the work and shortcomings of the current system.

Using these data, the research objectives were formed.

In the section "State of the issue and task statement", the basic principles of virtualisation are discussed based on the information obtained during the internship.

In the theoretical section, the ESXI hypervisor is considered, the existing types of ACS and their integration are analysed, and the most suitable system for the tasks performed at the school is selected.

In the section on system synthesis, a modification of the computer model based on the existing Safe School programme is developed.

In the software development section, a virtual infrastructure for the Safe School system was created.

In the experimental section, a number of studies were conducted to identify the optimal configuration of each virtual machine.

ЗМІСТ

Перелік умовних позначень, символів, скорочень і термінів

AD (Active Directory) – система директорій для управління ресурсами та автентифікації користувачів у мережах Windows.

AD DS (Active Directory Domain Services) – служба керування доменами у операційних системах Windows Serve.

API (Application programming interface) – дозволяє програмам взаємодіяти одна з одною.

CPU (Central Processing Unit) – основний обчислювальний елемент комп'ютера.

ESX (Elastic Sky X) – платформа для створення та управління віртуальними машинами.

ESXI (Elastic Sky X Integrated) – вбудована платформа віртуалізації, що дозволяє створювати та управляти віртуальними машинами.

GPS (Global Positioning System) – система глобального позиціонування для визначення місцезнаходження.

HDD (Hard Disk Drive) – пристрій для зберігання даних на постійний час.

HYPER-V (Hypervisor-based Virtualization) – технологія віртуалізації для створення та управління віртуальними машинами.

IP (Internet Protocol) – протокол, що визначає адресацію та маршрутизацію даних в Інтернеті.

LDAP (Lightweight Directory Access Protocol) – протокол доступу до легкодоступного каталогу для управління та пошуку інформації.

LUN (Logical Unit Number) – логічний номер блоку даних на пристрої зберігання.

PIN (Personal Identification Number) – особистий ідентифікаційний номер для автентифікації користувача.

POE (Power over Ethernet) – технологія передачі електропостачання через кабель Ethernet.

RAID (Redundant Array of Independent Disks) – система організації даних на декількох жорстких дисках для забезпечення надійності та швидкодії.

RAM (Random Access Memory) – використовується для тимчасового зберігання даних для обробки програм.

RDP (Remote Desktop Protocol) – протокол віддаленого робочого столу для віддаленого керування комп’ютером.

RFID (Radio-Frequency Identification) – ідентифікації за допомогою радіочастотних міток.

RJ-45 (Registered Jack-45) – стандартний роз’єм для мережевих кабелів Ethernet.

RS-485 (Recommended Standard 485) – стандарт для передачі даних у послідовних мережах.

VM (Virtual Machine) – емулює апаратне забезпечення для виконання операційних систем.

VMM (Virtual Machine Monitor) – програмний шар для управління та моніторингу віртуальних середовищ.

ЕОМ Електронно-обчислювальна машина

ОЗП Оперативна пам’ять

ПК Персональний комп’ютер

СКУД Система контролю і управління доступом

ЦП Центральний процесор

ВСТУП

Мета і завдання дослідження. Метою роботи є обґрунтування та дослідження методів контролю наявності учнів у школах з урахуванням вже існуючої системи контролю.

Для досягнення мети поставленої мети необхідно вирішити такі завдання:

– провести дослідження віртуального серверу на предмет інтеграції системи контролю управління доступом;

– виконати аналіз стану можливостей існуючої системи, що працює у школі та на основі цього обґрунтувати модель покращення системи;

– дослідити особливості діяльності окремих систем контролю управління доступу та на основі отриманих результатів обрати підходящу систему ідентифікації;

– обґрунтувати можливий варіант вдосконалення системи контролю наявності учнів у школі міста Дніпро.

Об’єкт дослідження – система контролю наявності учнів у школах.

Предмет дослідження – обґрунтування структури та параметрів комп’ютерного комплексу контролю наявності учнів в школах міста Дніпро із застосуванням системи «Безпечна Школа»

Методи дослідження: Для досягнення поставленої мети використовувались методи теоретичного аналізу, методи оцінки результатів експертами, метод експериментального дослідження.

Наукові положення:

1. Встановлено, що при перевантажені ресурсів оперативної пам’яті серверу, надаючи надлишкові параметри для віртуальної машини, вони автоматично розподіляються враховуючи потреби у ресурсах на виконання поставленої задачі.

2. Перевантаження ресурсів ядер центрального процесора шляхом проведення стрес-тесту віртуальної машини показує, що гіпервізор не може, на

відміну від оперативної пам’яті, розподілити чи збільшити обсяг ядер для виконання задачі.

Наукові результати:

1. Одержані нові практичні відомості з побудови віртуальної інфраструктури для системи, яка працює на основі роботи біометричної системи контролю управління доступом.

2. Обґрунтовано застосування віртуального серверу, який, на відміну від фізичного, має більше можливостей та гнучкіші інструменти для розподілу технічних ресурсів, також система стане більш надійною завдяки створенню єдиного центру управління віртуальної інфраструктури.

3. Обґрунтовано вибір біометричної систем контролю управління доступом для наявності учнів у школах та застосування нових камер із системою розпізнавання обличь, що, на відміну від наявної системи контролю, забезпечить надійний контроль та упередження проникнення сторонніх персон.

Практичне значення отриманих результатів полягає у впровадженні системи контролю, яка не тільки контролює наявність, але й управляє доступом до різних ресурсів та приміщень. Методи, які успішно впроваджено, посприяють покращенню безпеки у школах міста Дніпро.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

У сучасному світі, де вимоги до обчислювальних ресурсів необхідних для ефективного функціонування підприємств та організацій стрімко зростають, віртуалізація стає ключовою стратегією оптимізації інфраструктури. Цей технологічний підхід визначається як процес створення віртуальних машин на одному фізичному пристрої, дозволяючи оптимізувати використання апаратних ресурсів та забезпечити більш гнучку та швидку масштабованість інфраструктури.

Стан питання в галузі віртуалізації серверів на сьогоднішній день представляється як напрям, що активно розвивається та важливий для інформаційних технологій та бізнес-середовища. Існує низка технологій та підходів до віртуалізації, які варто розглянути з урахуванням конкретних потреб користувача.

Постановка завдання в даному контексті полягає в ретельному вивченні та аналізі сучасних методів віртуалізації серверів, виборі оптимальних рішень для конкретного використання та визначенні можливостей для підвищення продуктивності та безпеки системи. Особлива увага буде приділена порівняльному аналізу різних підходів та їхньому впливу на загальну архітектуру та функціонування IT-інфраструктури.

У цьому контексті, дослідження віртуалізації серверів має на меті виявлення оптимальних рішень для підвищення ефективності, надійності та забезпечення гнучкості управління обчислювальними ресурсами. Здійснюючи глибокий аналіз сучасних технологій віртуалізації та їхніх переваг, дослідження спрямоване на визначення найбільш оптимальних стратегій використання віртуалізації серверів в конкретних умовах ведення бізнесу чи функціонування організації.

Це дослідження вважається важливим в контексті швидкозмінюваного IT-середовища, де використання ресурсів та їхній оптимальний розподіл стає ключовим фактором для досягнення конкурентної переваги та стабільності бізнесу.

1.1. Аналіз існуючих типів віртуалізації

Існує багато типів віртуалізації, які варіюються в залежності від використовуваного обладнання та додатків, але виділяються основні з них, а саме:

- серверна віртуалізація;
- мережева віртуалізація;
- віртуалізація дата-центру;
- віртуалізація служб і додатків;
- віртуалізація клієнтів і робочих столів.

1.1.1 Серверна віртуалізація

Віртуалізація серверів – це процес розділення фізичного сервера на кілька унікальних та ізольованих віртуальних серверів за допомогою спеціалізованого програмного забезпечення. Кожен з цих віртуальних серверів може функціонувати самостійно з власною операційною системою, незалежно один від одного. На рисунку 1.1 можна побачити порівняння між звичайним сервером і віртуальним сервером [8]. До переваг віртуального сервера можна віднести:

- дешевші експлуатаційні витрати;
- підвищення продуктивності додатків;
- швидке налаштування нових машин.

Віртуалізацію серверу можна поділити на 3 типи, такі як:

Повна віртуалізація використовує гіпервізор, спеціальний вид програмного забезпечення, який прямо взаємодіє з фізичним сервером для обробки дискового простору та ресурсів процесора. Гіпервізор відповідає за управління ресурсами фізичного сервера і забезпечує повну ізоляцію для кожного віртуального сервера, виключаючи взаємодію між ними. При запуску програм гіпервізор розподіляє ресурси фізичного сервера між віртуальними серверами, дозволяючи їм працювати незалежно. Проте, слід зауважити, що в повній віртуалізації гіпервізор також обробляє додаткові дані, що може вплинути на продуктивність сервера та спричинити затримки у роботі програм [1].

Паравіртуалізація, на відміну від повної віртуалізації, розглядає мережу як ціле, де кожна операційна система на віртуальних серверах обізнана про інші операційні системи. У паравіртуалізації гіпервізор не потребує великої обчислювальної потужності для управління операційними системами, оскільки вони взаємодіють та спільно керують ресурсами [1; 27].

Віртуалізація на рівні операційної системи навпаки від повної та пара-віртуалізації, обходиться без гіпервізора. Замість цього, вбудована в операційну систему фізичного сервера функція віртуалізації відповідає за всі операції, які зазвичай виконує гіпервізор. Проте, варто зауважити, що в цьому методі всі віртуальні сервери мають працювати під управлінням однієї і тієї ж операційної системи [27].

Рисунок 1.1 – Порівняння архітектури фізичного та віртуального серверу

1.1.2. Мережева віртуалізація

Мережева віртуалізація перетворює мережеві ресурси, звичайно представлених у вигляді апаратного забезпечення, у програмне забезпечення. Це дозволяє віртуальним машинам об’єднати кілька фізичних мереж в одну віртуальну, програмну мережу або розділити одну фізичну мережу на окремі, незалежні віртуальні мережі. Програмне забезпечення для віртуалізації мережі дозволяє мережевим адміністраторам переміщувати віртуальні машини між різними доменами без необхідності зміни конфігурації мережі. Воно створює мережевий шар, який може запускати окремі віртуальні мережеві сегменти поверх тієї ж фізичної мережевої інфраструктури. На рисунку 1.2 наведено схему віртуальної мережі [8].

Віртуалізація мережі дозволяє відокремити мережеві сервіси від фізичного обладнання та надає можливість програмно надавати послуги для всієї мережі. Це дозволяє створювати, надавати послуги та керувати мережею за допомогою програмного забезпечення, при цьому продовжуючи використовувати основну фізичну мережу як магістраль для пересилання пакетів. Ресурси фізичної мережі, такі як комутація, маршрутизація, брандмауер, балансування навантаження та віртуальні приватні мережі об’єднуються в пул, надаються програмному забезпеченню та вимагають лише пересилання пакетів айпі з основної фізичної мережі [2; 26].

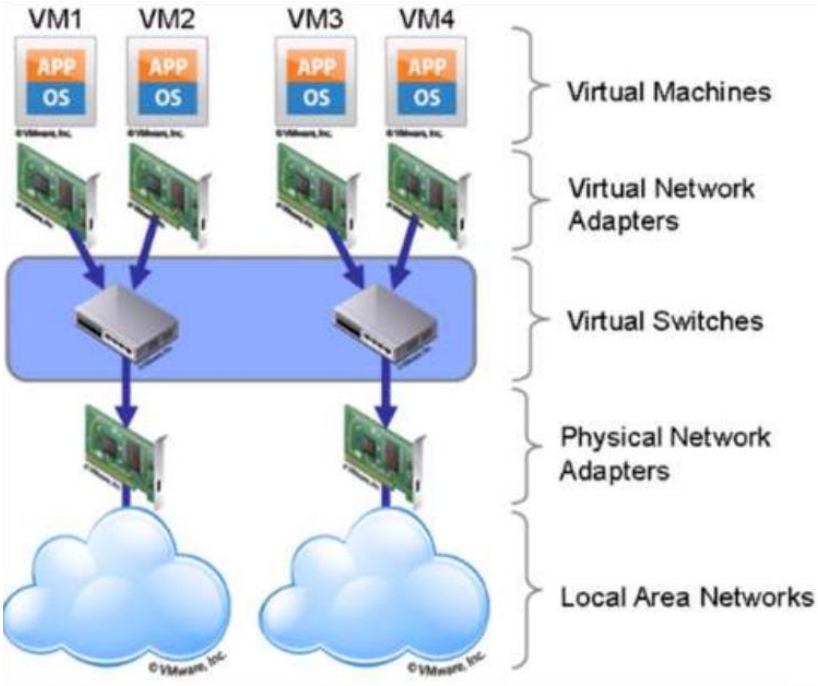

Рисунок 1.2 – Схема віртуальної мережі

Мережева віртуалізація допомагає організаціям досягти значних успіхів у швидкості, гнучкості та безпеці шляхом автоматизації та спрощення багатьох процесів, пов’язаних з роботою мережі центру обробки даних та управлінням мережею і безпекою в хмарному середовищі. Ось деякі з ключових переваг віртуалізації мережі:

– скорочення часу на підготовку мережі з тижнів до хвилин;

– досягнення більшої операційної ефективності за рахунок автоматизації ручних процесів;

– розміщення та переміщення робочих навантажень незалежно від фізичної топології;

– покращення мережевої безпеки в центрі обробки даних.

1.1.3. Віртуалізація дата центрів

Віртуалізація сховища інформації – це метод об’єднання фізичних пристроїв зберігання даних таким чином, щоб до них можна було звертатися через один «віртуальний» пристрій зберігання даних. Хоча зараз віртуалізація сховища даних часто асоціюється з хмарними моделями, вона надає значні переваги у плані ефективності та економії порівняно з фізичними сховищами даних. На рисунку 1.3 представлено схему віртуального сховища даних [8].

Віртуалізація сховища даних допомагає організаціям подолати проблеми сумісності, підвищує продуктивність і забезпечує покращену безпеку в середовищі зберігання даних. Цей підхід може бути реалізований за допомогою програмних додатків або спеціальних пристроїв. Існує три важливі причини для впровадження віртуалізації сховища:

– покращене управління сховищем в IT-середовищі;

– підвищення доступності та оцінка часу простою завдяки автоматизованому управлінню;

– краще використання ресурсів сховища.

Віртуалізація сховища може бути застосована до будь-якого рівня SAN. Методи віртуалізації також можна застосовувати до різних функцій сховища, таких як фізичне сховище, RAID-групи, номери логічних блоків LUN, підрозділи LUN, зони зберігання і логічні томи тощо [3].

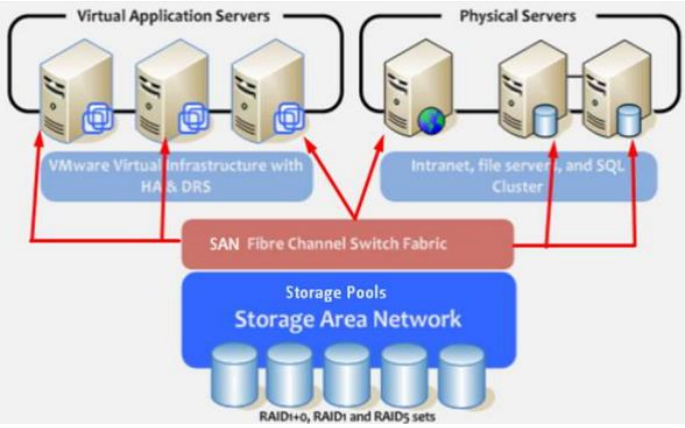

Рисунок 1.3 – Схема віртуального сховища інформації

1.1.4. Віртуалізація клієнтів і робочих столів

Віртуалізація клієнтів і робочих столів – метод, що дозволяє створювати віртуальну модель робочого місця користувача, яка стає доступною з віддалених пристроїв. Шляхом абстрагування від фізичного робочого столу користувача, організації можуть надавати можливість працювати з будь-якого місця, де є підключення до мережі, використовуючи різні пристрої, такі як ноутбуки, планшети або смартфони, для доступу до корпоративних ресурсів, незалежно від операційної системи або пристрою, який вони використовують.

Віртуалізація віддалених робочих столів є ключовою складовою цифрового робочого простору. Виконання користувацьких завдань на віртуальних робочих столах відбувається на серверах віртуалізації робочих столів, які зазвичай працюють на віртуальних машинах у локальних центрах обробки даних або в публічних хмарах.

Однією з основних переваг віртуалізації робочих столів є знижений ризик для організації у випадку втрати чи крадіжки клієнтських пристроїв. Усі дані та програми користувача зберігаються на сервері віртуалізації робочих столів, а не на самому пристрої.

Віртуалізація робочих столів приносить організації такі переваги, як підвищена безпека, ефективне використання ресурсів та можливість віддаленої роботи. Приклад та схему віртуальних робочих столів можна знайти на рисунку 1.4 [8].

Оптимізація використання ресурсів – віртуалізація настільних комп’ютерів концентрує ресурси в центрі обробки даних, що сприяє підвищенню ефективності. Організації можуть використовувати менш потужні та більш економічні клієнтські пристрої, оскільки вони лише відображають віртуалізований робочий стіл і не вимагають встановлення або оновлення операційних систем та додатків.

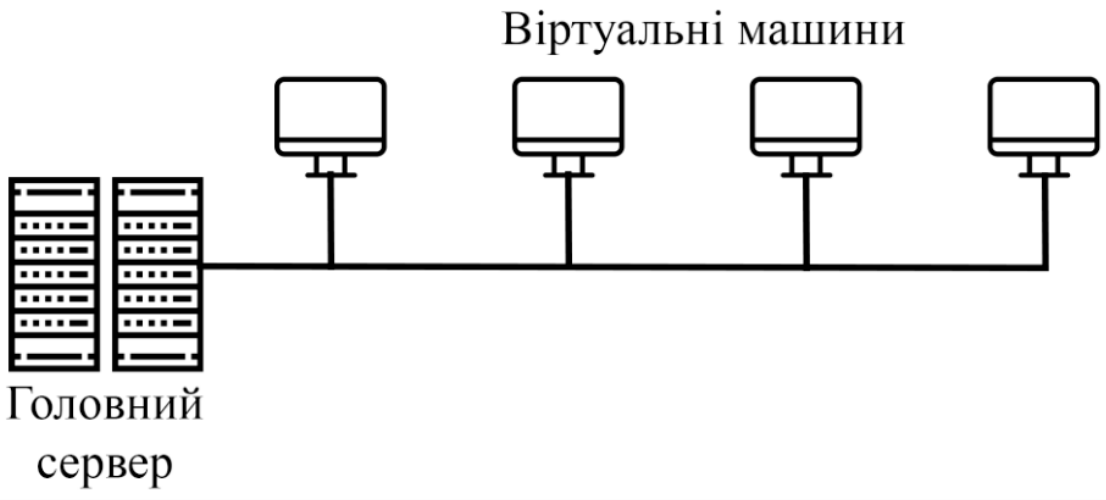

Рисунок 1.4 – Схема роботи віддалених робочих столів

Забезпечення безпеки – віртуалізація робочих столів дозволяє централізовано керувати безпекою. Безпека базується на серверах віртуалізації, з обмеженими потребами в апаратній безпеці на клієнтських пристроях. Акцент робиться на управлінні ідентифікацією та доступом, що базується на ролях, які обмежують користувачів залежно від їхнього доступу до додатків та даних.

Віддалена робота – віртуальні робочі столи знаходяться на централізованих серверах, і нові робочі столи користувачів можуть бути створені дуже швидко та стати доступними для нових користувачів. Користувачі можуть отримувати доступ до своїх додатків з будь-якого місця з підключенням до Інтернету. Цей підхід спрощує роботу на віддалених робочих столах та дозволяє легко віддалено адмініструвати робочі столи користувачів [4].

1.1.5. Віртуалізація служб та додатків

Віртуалізація служб та додатків – це процес, який дозволяє зманіпулювати стандартний додаток так, щоб він вважав, ніби взаємодіє безпосередньо з операційною системою, хоча насправді це не так. Замість розподілу процесів програми по всій операційній системі, їх спрямовують в один файл. Це дозволяє програмі легко працювати на різних пристроях, і навіть раніше несумісні програми можуть запускатися паралельно.

Сучасний цифровий робочий простір об’єднує пристрої, програми та сервіси, які необхідні користувачам. Управління цим робочим простором повинно бути безпечним та уніфікованим для забезпечення спільного доступу на всьому підприємстві. Віртуалізація додатків і настільних комп’ютерів дозволяє централізовано керувати мережею настільних комп’ютерів. Організаціям потрібно виправити лише кілька образів програм та віртуальних робочих столів, а не кожен окремий кінцевий пункт. Таким чином, розгортання оновлень може бути виконано послідовно, швидко та ефективно. Схему роботи віртуалізації служб та додатків наведено на рисунку 1.5 [8; 27].

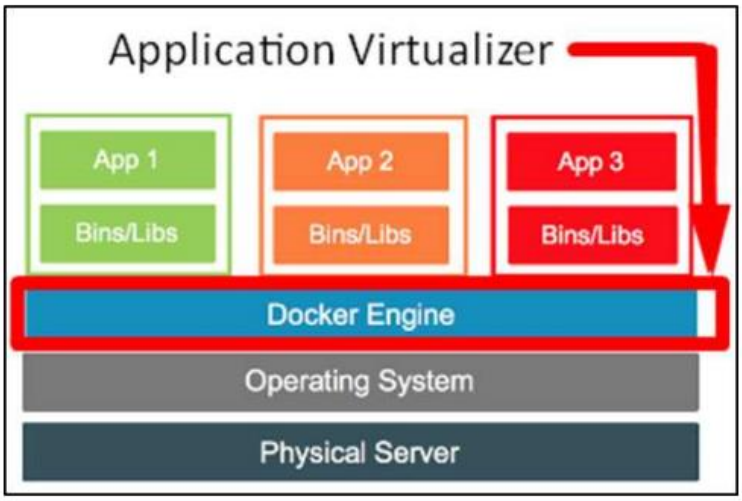

Рисунок 1.5 – Схема віртуалізації додатків

Оскільки програмне забезпечення та оновлення безпеки зберігаються на серверах центрів обробки даних, вразливість кінцевих пристроїв до загроз значно зменшується. Кінцевий пристрій – це лише термінал для відображення даних.

До інших переваг віртуалізації служб та додатків включають:

– можливість запускати застарілі програми розроблені для застарілих операційних систем, таких як Windows 7 чи XP;

– забезпечення крос-платформної роботи, запуск додатків Windows на IOS, Android, MacOS і Chrome OS);

– запобігання конфліктам з іншими віртуалізованими програмами (наприклад, конфліктуючим антивірусним програмним забезпеченням);

– користувачі можуть запускати кілька екземплярів програми – якщо програма не віртуалізована, багато програм можуть виявити запущений екземпляр і не дозволять запускати нові.

Щоб знизити витрати і підвищити продуктивність, організації повинні розвивати свій цифровий робочий простір. Це означає міграцію мережевих активів з локальної мережі в хмару [5; 27].

1.2 Аналіз існуючих інструментів віртуалізації

Продукція компанії VMware

Компанія VMware стала одним з піонерів у сфері віртуалізації, починаючи з 1998 року. З того часу вона розробила та випустила ряд високоефективних та професійних продуктів для віртуалізації на різних рівнях: від VMware Workstation для настільних ПК до VMware ESX Server, який дозволяє об’єднувати фізичні сервери підприємства в віртуальній інфраструктурі.

Важливо зауважити, що, на відміну від ЕОМ, пристрої на основі архітектури x86 не повністю підтримують віртуалізацію. Це вимагало від компанії VMware вирішити численні технічні проблеми при створенні віртуальних машин для комп’ютерів на базі x86. Основна функція більшості процесорів, як у ЕОМ, так і в ПК, полягає в виконанні послідовності збережених програм. Однак процесори на основі архітектури x86 включають 17 спеціальних інструкцій, які створюють проблеми під час віртуалізації. Ці інструкції можуть спричинити попередження, зупинити виконання програми або призвести до збою операційної системи. Таким чином, ці 17 інструкцій ускладнювали початковий процес впровадження віртуалізації для комп’ютерів на базі x86.

Для подолання цього обмеження компанія VMware розробила адаптивну технологію віртуалізації, яка перехоплює ці інструкції на етапі їх створення і перетворює їх у безпечні інструкції, які можна віртуалізувати, не впливаючи на виконання інших інструкцій. Як результат, отримується високопродуктивна віртуальна машина, яка відповідає апаратним можливостям обладнання та підтримує повну сумісність з програмами. Компанія VMware стала першою, хто розробив і впровадив цю інноваційну технологію, і сьогодні вона визнається лідером у галузі технологій віртуалізації.

VMware Workstation – це програма від компанії VMware, яка призначена для віртуалізації на рівні робочої станції. Вона дозволяє користувачам створювати та запускати віртуальні машини на власному комп’ютері.

VMware Workstation – продукт який призначений для віртуалізації на рівні робочої станції. VMware Workstation має ряд корисних функцій:

– Workstation дозволяє користувачам створювати нові віртуальні машини з різними конфігураціями, включаючи кількість процесорів, обсяг оперативної пам’яті, обсяги дискового простору та інше;

– VMware Workstation дозволяє запуск різних операційних системи на одному комп’ютері, навіть якщо основна операційна система відрізняється від гостьових ОС. Користувач може використовувати різні операційні системи, такі як Windows, Linux, macOS та інші;

– віртуальні машини запускаються в ізольованому середовищі, що допомагає зберігати безпеку основної операційної системи.

VMware vSphere – це програмне забезпечення для віртуалізації і обліку ресурсів обчислювального центру, дозволяє створювати віртуальні обчислювальні середовища, які об’єднують фізичні сервери, зберігання та мережеві ресурси в єдиній інфраструктурі. Основними компонентами vSphere є:

VMware ESX – це гіпервізор, який розбиває сервер на віртуальні машини. Є основою пакету vSphere.

VMware vCenter Server – надає централізовану точку керування для всіх віртуальних машин, що використовуються у віртуалізованому середовищі. Забезпечує регулярне резервне копіювання і відновлення віртуальних машин та даних. Створює шаблони створених раніше віртуальних машин для швидкого та зручного налаштування нових.

VMware Horizon – виконує віртуалізацію робочих столів та додатків для корпоративних клієнтів. Створює віртуальні робочі столи та додатки користувачам в будь-якому місці.

Citrix Xen

Розробка некомерційного гіпервізора Xen стартувала як дослідницький проєкт у Кембриджському університеті, головним у розробці був Іен Претта, який став засновником компанії XenSource, що займалася розробкою комерційних платформ для віртуалізації на основі розробленого гіпервізора Xen (XenServer, XenEnterprise), а також підтримкою Open Source некомерційного продукту. Xen був найрозвиненішою платформою, яка підтримувала технології паравіртуалізації. У 2007 році компанія XenSource була поглинена компанією Citryx Systems.

XenServer – використовує гіпервізор Xen для віртуалізації кожного сервера, на якому він встановлений, що дозволяє розміщувати кілька віртуальних машин одночасно з високою продуктивністю. XenServer також можна використовувати для об’єднання декількох серверів з підтримкою Xen у потужний пул ресурсів, використовуючи стандартні галузеві архітектури спільного зберігання даних і кластеризацію ресурсів. Таким чином, XenServer забезпечує безперешкодну віртуалізацію декількох серверів у вигляді пулу ресурсів. Ці ресурси динамічно контролюються для забезпечення оптимальної продуктивності, підвищеної відмовостійкості та доступності, а також максимального використання ресурсів центру обробки даних [10].

XenApp – ця служба призначена для віртуалізації додатків з метою оптимізації доставки сервісів у компаніях, цей інструмент може скоротити час транзакцій для операцій клієнт/сервер на 300 %, одночасно підтримуючи такі стратегії, як «принеси свій власний пристрій», обслуговуючи розподілену мережу з віддаленим доступом і гнучким дизайном. Забезпечуючи те, що Citrix називає «віртуальним доступом до додатків», Citrix XenApp є частиною узгодженої стратегії створення сервісів, які максимально використовують нові технології, такі як хмарні обчислення, програмне забезпечення як послуга і віртуалізація мережевого обладнання [11].

XenDesktop – це інструмент від Citrix Systems, який пропонує доставку віртуальних робочих столів. Він дозволяє користувачам зробити програми

Windows різних поколінь доступними на будь-якому пристрої і в будь-якому місці. Ресурси віртуального робочого столу приносять потужність декількох додатків і утиліт на віддалені пристрої для віддаленої роботи.

Microsoft

У 2003 році Microsoft придбала компанію Connectix, яка розробляла програмне забезпечення для віртуалізації під Windows, включаючи продукт Virtual PC. Він конкурував з VMware Workstation, але Microsoft недостатньо уваги приділяла його розвитку. Потім Microsoft випустила Virtual Server 2005, але VMware вже займала провідну позицію на ринку. У 2006 році VMware зробила свій продукт VMware GSX Server безкоштовним і сфокусувалася на VMware Server і VMware ESX Server. Microsoft також вирішила зробити свій Microsoft Virtual Server 2005 безкоштовним, об’єднавши раніше окремі видання. Пізніше в 2008 році Microsoft випустила платформу віртуалізації Microsoft Hyper-V, яка була інтегрована в Windows Server 2008.

Hyper-V – це гіпервізор, розроблений і випущений компанією Microsoft. Гіпервізор – це програмне забезпечення або апаратний засіб, який дозволяє створювати та управляти віртуальними машинами на фізичному сервері. Hyper-V дозволяє вам запускати кілька віртуальних операційних систем на одному фізичному сервері, що дозволяє оптимізувати використання ресурсів сервера та спрощує управління і підтримку інфраструктури [12].

Hyper-V підтримує як віртуальні сервери для операційних систем Windows, так і для інших операційних систем, таких як Linux. Це робить його важливим інструментом для віртуалізації і обліку у сфері інформаційних технологій та дозволяє компаніям оптимізувати використання своїх серверних ресурсів та полегшити управління і підтримку серверної інфраструктури. На рисунку 1.6 наведено архітектуру Hyper-V.

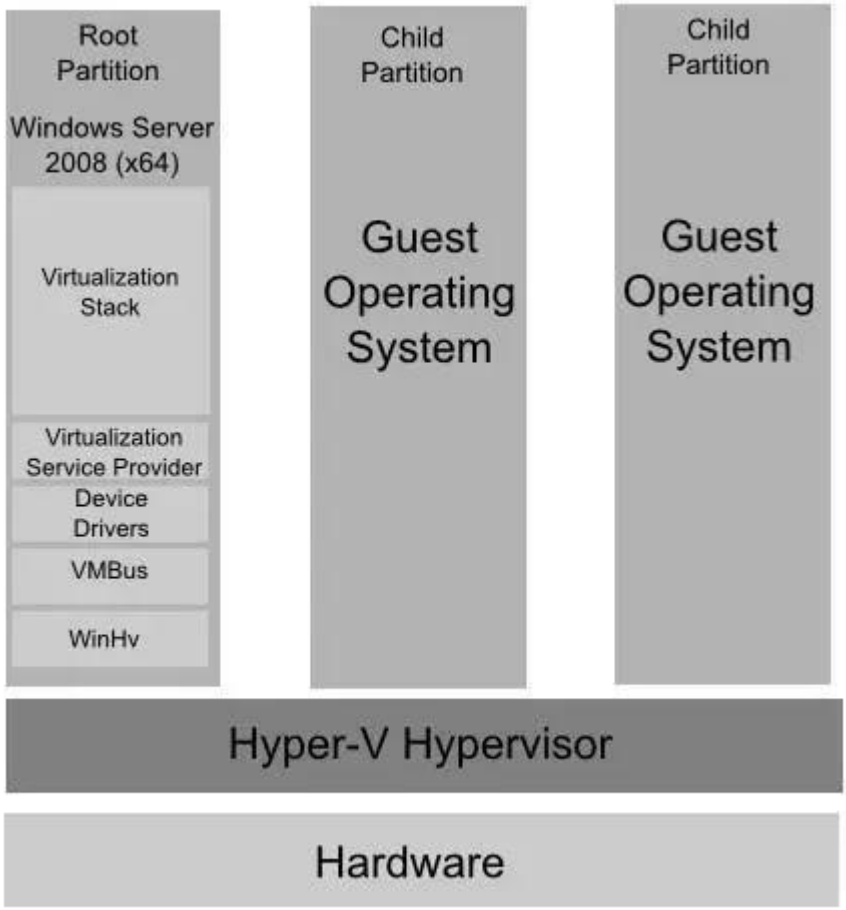

Рисунок 1.6 – Архітектура Hyper-V

Hyper-V – це гіпервізор першого типу, оскільки код гіпервізора знаходиться безпосередньо на апаратному забезпеченні. Однак номенклатура дещо відрізняється – замість гостей, віртуалізовані робочі навантаження називаються розділами. Подібно до моделі Xen, для цього потрібен спеціальний батьківський розділ, який має прямий доступ до апаратних ресурсів. Як і у випадку з Dom0, на батьківському розділі встановлена операційна система – у цьому випадку Windows Server 2008. Оскільки він використовує модель, подібну до XenServer, він схильний до тих самих вразливостей, що стосуються виправлень і суперечок.

Root Partition – складається з компонентів, яких немає у Child Partilion. Створюється системою у першу чергу, як тільки гіпервізор починає роботу. Root Partition створюється для операційних систем з Hyper-V роллю.

Root Partition використовується для створення та управління Child Partilion системи і включає WMI провайдера, котрий надає інтерфейс для віддаленого доступа.

– Root Partition керує та розподіляє ресурси, за винятком процесу фізичного розподілу пам’яті, який здійснюється безпосередньо гіпервізором;

– ресурси Root Partition виділяються для використання у Child Partilion;

– Root Partition керує «plug-n-play» операціями та веде записи про неполадки апаратного забезпечення.

Стек віртуалізації – ряд компонентів, що розташовується у Root Partition. Стек віртуалізації має прямий доступ до апаратного забезпечення хост комп’ютера. Складається з наступних компонентів:

– Virtual Machine Management Service;

– Virtual Machine Worker Process;

– Virtual Devices;

– Virtual Infrastructure Driver;

– Windows Hypervisor Interface Library.

Child Partilion – підтримує функціюванні гостьові операційні системи, підтримує три основні типи дочірніх розділів:

– Операційна система, сімейства Windows з встановленими компонентами інтеграції;

– Операційна система, відміна від сімейства Windows з встановленими компонентами інтеграції;

– Операційна система, що не підтримує інтеграцію.

Для кожного випадку набір компонентів буде різним.

Child Partilion з Windows і встановленими компонентами інтеграції містить наступні компоненти:

– Служба віртуалізації, пристрої дозволять Child Partilion отримати доступ до апаратних ресурсів;

– Покращення – зміна коду операційної системи. Child Partilion, в якому встановлені компоненти інтеграції, використовує сторонні клієнти служб віртуалізації для доступу до апаратних ресурсів, і він відрізняється від операційної системи Windows.

RDP – це мережевий протокол, який дозволяє здійснювати віддалене підключення до іншого комп’ютера. RDP надає графічний інтерфейс для отримання віддаленого доступу до іншого комп’ютера. Для використання RDP користувач, який ініціює з’єднання, повинен мати клієнтське програмне забезпечення RDP встановлене на своєму комп’ютері. Комп’ютер, до якого користувач намагається підключитися, повинен мати програмне забезпечення RDP-сервера, яке дозволяє клієнтові здійснити віддалений доступ. Після підключення користувач, який ініціював запит, отримує можливість перегляду робочого столу комп’ютера, до якого він підключився за допомогою RDP, і отримує доступ до програм і даних на цьому робочому столі [13].

1.3 Аналіз недоліків від віртуалізації

1.3.1 Переваги від віртуалізації

Багато IT-організацій розгортають сервери, які працюють лише наполовину своєї потужності, часто через те, що вони призначають свій фізичний сервер конкретному додатку. Зазвичай це є неефективним механізмом, оскільки надлишкова потужність залишається невикористаною, що призводить до збільшення витрат.

В спробах підвищити використання потужностей і знизити витрати було розроблено віртуалізацію. До переваг віртуалізації відносяться наступні аспекти:

1. Ефективне використання ресурсів: Віртуальні машини ефективно використовують апаратне забезпечення, зменшуючи кількість пов’язаного обладнання, витрати на обслуговування і споживання енергії, а також розподіляючи ресурси пам'яті, дискового простору та процесора.

2. Використання віртуалізації для підвищення доступності: Платформи віртуалізації надають розширені функції, недоступні на фізичних серверах, що підвищує час безперебійної роботи та доступність. Такі технології забезпечують безперебійну роботу віртуальних машин або можливість їх відновлення після непередбачених збоїв.

3. Аварійне відновлення: Відновлення після аварії стає простішим, коли ваші сервери віртуалізовані. Завдяки моментальним знімкам віртуальних машин, ви можете швидко відновити роботу. Організація може легко створити доступне місце для реплікації та переміщення віртуальних машин до інших серверів або до хмарного провайдера у разі аварії в центрі обробки даних.

4. Швидке розгортання серверів: Швидке клонування образу, основного шаблону або існуючої віртуальної машини дозволяє запустити сервер за лічені хвилини. За допомогою віртуальних інструментів резервного копіювання, повторне розгортання образів стає настільки швидким, що користувачі можуть не помічати виникнення проблеми [10].

1.3.2 Недоліки віртуалізації

Мінуси віртуалізації включають такі аспекти:

1. Додаткові витрати: виникає необхідність в додаткових інвестиціях у програмне забезпечення для віртуалізації, і, можливо, додатковому обладнанні, щоб забезпечити можливість віртуалізації. Це залежить від існуючої мережі. Багато компаній можуть впровадити віртуалізацію без значних витрат, але якщо ваша інфраструктура застаріла, може знадобитися початковий бюджет для її оновлення.

2. Ліцензування програмного забезпечення: це стає меншою проблемою, оскільки все більше постачальників програмного забезпечення пристосовуються до віртуалізації. Тим не менш, важливо отримати консультацію від постачальників програмного забезпечення, щоб зрозуміти їхні умови щодо використання програм у віртуалізованому середовищі.

3. Ознайомлення з новою інфраструктурою: Впровадження та управління віртуалізованим середовищем вимагає наявності досвіду у IT-персоналу в галузі віртуалізації. З точки зору користувача, типове віртуальне середовище працює так само, як і невіртуальне. Проте існують програми, які можуть мало ефективно адаптуватися до віртуального середовища [10].

.

1.5. Аналіз результатів

Досліджено основні аспекти архітектури серверної віртуалізації та різні типи віртуалізації. Серверна віртуалізація є ключовою технологією для сучасних інформаційних систем і дата-центрів. Основна відмінність між гіпервізорами першого та другого типу визначається їхньої продуктивністю та безпекою.

Кожен тип віртуалізації має свої переваги і використовується в залежності від конкретних потреб. Гіпервізори другого типу зручні для розробки та тестування, оскільки їх легше налаштовувати та використовувати на робочих станціях. Також розглянуто розподіл ресурсів комп’ютеру між віртуальними машинами, що включає в себе оперативну пам’ять, потужності процесору та мережеві ресурси.

Також розглянуто доступні інструменти віртуалізації від різних постачальників, досліджено існуючі типи гіпервізора, з’ясовано, що гіпервізори першого типу, які працюють на апаратному забезпеченні, є більш продуктивними та безпечними, оскільки гостьові операційні системи не впливають один на одного.

Кожен тип віртуалізації має свої переваги і використовується в залежності від конкретних потреб. Гіпервізори другого типу зручні для розробки та тестування, оскільки їх легше налаштовувати та використовувати на робочих станціях. Також розглянуто розподіл ресурсів комп’ютеру між віртуальними машинами, що включає в себе оперативну пам’ять, потужності процесору та мережеві ресурси.

2 ТЕОРЕТИЧНИЙ РОЗДІЛ

2.1 Загальна характеристика гіпервізору ESXI

Гіпервізор ESXi визнаний як один із важливих компонентів в сфері віртуалізації серверів, впровадження якого в інфраструктурі дозволяє підняти ефективність використання обчислювальних ресурсів та надає гнучкість в конфігурації серверів. У даному розділі ми ретельно розглянемо функціонал гіпервізора ESXi, вивчаючи його ключові особливості та можливості, що визначають його значущість у сучасних інформаційних технологіях.

Віртуалізація серверів, що базується на гіпервізорі ESXi, визначається як високоефективний метод оптимізації роботи серверних ресурсів. ESXi входить до складу фірмового виробника VMware і відзначається своєю легкістю використання та потужністю функціоналу.

У розділі проаналізовано широкий спектр функцій, доступних у гіпервізорі ESXi. Від ресурсного управління та безпеки до можливостей масштабованості та резервування ресурсів – кожен аспект функціоналу буде розглянутий з урахуванням його впливу на продуктивність та надійність інфраструктури.

Надаючи високий рівень ізоляції та оптимізації використання апаратних ресурсів, гіпервізор ESXi заслуговує на увагу в контексті облаштування великих дата-центрів, де ефективне розподіл ресурсів та забезпечення високої доступності є пріоритетними завданнями.

2.1.1 Аналіз роботи гіпервізору ESXI

VMware ESXi є гіпервізором першого типу, тобто він встановлюється не на операційну систему, а інтегрує компоненти операційної системи в себе. Така функціональність дозволяє використовувати загальну потужність вашого обладнання, ефективно розподіляючи ресурси у віртуалізованих середовищах для малого або великого розгортання. Крім того, ESXi дозволяє конфігурувати кількість процесорів, пам'яті, жорстких дисків, а також кількість пристроїв зберігання даних або мережевих адаптерів, що підключаються, відповідно до потреб середовища.

VMware ESXi забезпечує надійний рівень віртуалізації між апаратним забезпеченням та ОС. Оскільки він є автономним, перед встановленням на апаратне забезпечення не потрібно встановлювати жодної операційної системи. Після встановлення ви зможете керувати та контролювати свій хост.

VMware ESXi розділяє сервер на кілька захищених і рухомих віртуальних машин, які працюють пліч-о-пліч на одному обладнанні. Кожна ВМ є повноцінною системою, ізольованою одна від одної за допомогою віртуального рівня. Ця ізоляція запобігає впливу однієї несправної ВМ на іншу.

Архітектура «голий метал» дає VMware ESXi контроль над ресурсами сервера, виділеними для кожної віртуальної машини, і забезпечує продуктивність, близьку до нативної, та масштабованість на рівні підприємства. Крім того, VMware ESXi пропонує вбудовані функції високої доступності, управління ресурсами та безпеки, що забезпечують більш високий рівень обслуговування програмних додатків, ніж у статичних фізичних середовищах [14].

2.1.2 Переваги використання гіпервізора ESXI

Однією з ключових переваг VMware ESXi є його спрощена архітектура, що значно полегшує процес підтримки узгодженої віртуальної інфраструктури. Ця модель «голий метал» обмежена у конфігураційних опціях, але це аналогічно використанню панелі керування з обмеженою кількістю кнопок, що спрощує користування для кінцевих користувачів. Це забезпечує зручність у підтримці віртуальної інфраструктури, що є важливим перевагою для будь-якої компанії [15].

Важливим аспектом є висока безпека VMware ESXi, яка може бути ще важливішою, ніж його зручність для користувача. Функціональність управління вбудована в ядро віртуальної машини та використовує обмежений обсяг пам'яті, знижуючи його споживання і зроблюючи його менш вразливим до атак шкідливого програмного забезпечення та інших загроз. Це сприяє високій стійкості системи та збільшує її надійність в щоденному використанні.

Для адміністрування не потрібен один великий обліковий запис адміністратора; натомість можна створити окремі облікові записи з визначеними ролями та привілеями. Це означає, що компрометація одного облікового запису не становить загрози для всієї системи [15].

Завдяки поєднанню функцій безпеки та адміністрування, VMware ESXi веде докладний журнал всіх дій користувачів для забезпечення їх підзвітності та забезпечує простий та безперервний аудит.

Управління VMware ESXi використовує API, що означає, що підхід без агентів не потребує додаткового встановлення чи ліцензування опцій управління. Віддалені командні рядки, такі як інтерфейс командного рядка vSphere та PowerCLI, забезпечують більш точне, швидке та контрольоване виконання команд та створення сценаріїв для конфігурації та діагностики.

VMware ESXi також підтримує роботу віртуальних машин, створених за допомогою Microsoft Virtual Server, Microsoft Virtual PC або VMware Server, і забезпечує підтримку конвертації з фізичних машин та інших джерел [15].

2.1.3 Архітектурні особливості гіпервізора ESXI та основні компоненти

Архітектура VMware ESXi складається з базової операційної системи, яка називається VMkernel, і процесів, які виконуються поверх неї. VMkernel надає засоби для запуску всіх процесів у системі, включаючи програми керування та агенти, а також віртуальні машини. Воно контролює всі апаратні пристрої на сервері та керує ресурсами для додатків [16], на рисунку 2.1 показана схема архітектури гіпервізору ESXI [7].

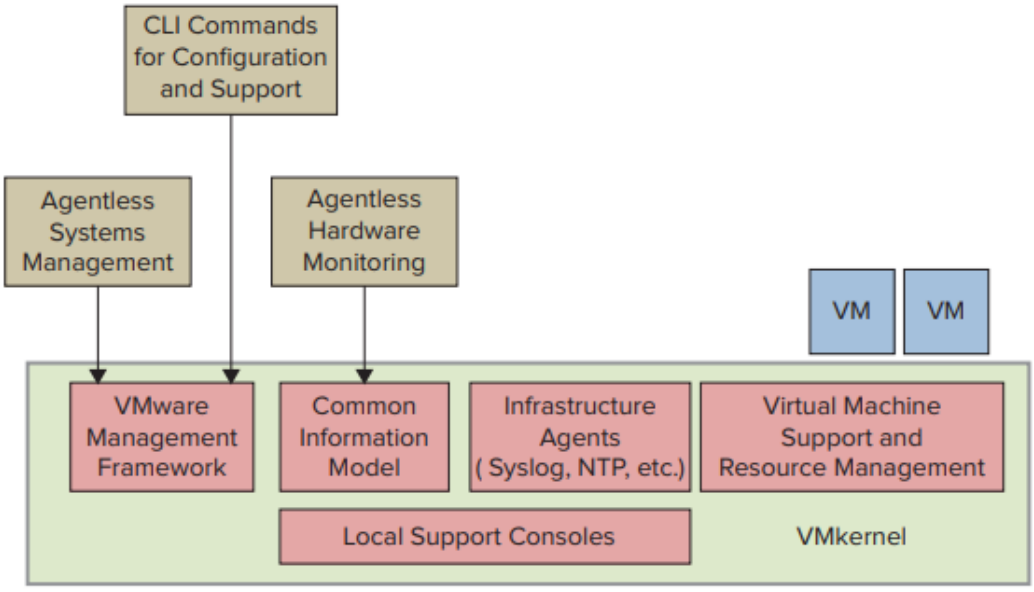

Рисунок 2.1 – Архітектура гіпервізора ESXI

VMkernel представляє собою ядро гіпервізора ESXi, що відповідає за ефективне управління фізичними ресурсами сервера, такими як процесор, пам’ять, мережа і зберігання. Воно вирішує завдання розподілу ресурсів між віртуальними машинами та гарантує їх ізоляцію одна від одної.

Гіпервізор ESXi розташовується поверх VMkernel і дозволяє створювати та запускати віртуальні машини. Він відповідає за керування їх роботою, забезпечує ізоляцію між ними та контролює доступ до фізичних ресурсів. Окрім VMkernel та гіпервізора, ESXi включає додаткові сервіси для управління та моніторингу віртуальних машин, такі як VMware Tools, а також сервіси для зберігання даних та мережевої віртуалізації [16].

ESXi має вбудований веб-інтерфейс, що дозволяє адміністраторам зручно налаштовувати та керувати віртуальними машинами. Цей інтерфейс відзначається високою інтуїтивністю та легкістю використання. Для віддаленого керування та моніторингу серверами ESXi, VMware надає інструменти, такі як VMware vCenter Server, які дозволяють адміністраторам віддалено управляти серверами ESXi, відстежувати ресурси та стан віртуальних машин.

Загалом, архітектура ESXi створена для забезпечення високої продуктивності, безпеки та ефективності віртуалізації, надаючи адміністраторам можливість легко управляти великою кількістю віртуальних машин та ефективно використовувати ресурси серверів [16].

2.2 Обґрунтування та вибір методу СКУД

Система контролю та управління доступом – це комплекс технічних пристроїв і програм, які призначені для регулювання доступу до різних місць, де необхідно контролювати, хто і коли може входити (наприклад, в офісах, лікарнях, державних установах, на підприємствах, автостоянках, приватних територіях тощо).

Створення такої системи неможливе без контролера, який можна вважати «мозком» цієї системи. Він включає в себе базу даних користувачів, які мають відповідні права для входу та виходу з конкретних приміщень. Контролер вирішує, чи можна відкривати двері, ворота або шлагбауми, надаючи або відхиляючи запити на доступ.

Посередником в системі контролю доступу виступає зчитувач, який отримує біометричні дані або інформацію з картки користувача і передає цю інформацію контролеру.

Для ідентифікації користувачів використовуються різні ідентифікатори, такі як ключ-карти, браслети з чіпами або проксі-брелки. Ці ідентифікатори містять персональний код співробітника або відвідувача. Важливою частиною системи контролю доступу є виконавчі пристрої, такі як замки, шлагбауми і турнікети. Вони відкриваються вручну або автоматично, якщо доступ був схвалений.

Ці системи широко застосовуються у різних галузях, таких як виробничі цехи, медичні та освітні установи, музеї, державні установи, паркінги, склади та інші об’єкти, де необхідна ідентифікація осіб. Для успішного впровадження ефективної СКУД, важливо чітко визначити її тип, кількість користувачів, рівень безпеки та виробника обладнання [17].

2.2.1 Аналіз роботи СКУД

СКУД базується на кількох основних принципах, які забезпечують ефективне та безпечне управління доступом користувачів. Ці принципи забезпечують роботу ефективної та надійної системи контролю та управління доступом, забезпечуючи безпеку та ефективне управління доступом до ресурсів і об'єктів. Ось основні принципи СКУД:

– Ідентифікація та аутентифікація:

СКУД починається з ідентифікації особи або об’єкта, який намагається отримати доступ. Це може бути досягнуто за допомогою біометричних даних (відбитки пальців, розпізнавання обличчя), карток доступу або інших методів.

Після ідентифікації особа або об’єкт повинні підтвердити свою ідентифікацію, представивши відповідні облікові дані, такі як пароль, PIN-код або біометричну перевірку.

– Авторизація:

Після успішної аутентифікації СКУД визначає, чи має користувач право на доступ до певного ресурсу або об’єкта. Наприклад, система може дозволити доступ співробітникові в його робоче приміщення, але заборонити доступ іншим особам.

– Моніторинг та реєстрація:

СКУД здійснює моніторинг всіх подій, пов’язаних із доступом. Це включає в себе фіксацію входу та виходу користувачів, невдалих спроб доступу, часові мітки та інші дані. Реєстрація є важливим для забезпечення безпеки та відстеження дій користувачів.

– Управління правами та ролями:

СКУД дозволяє адміністраторам визначати різні рівні доступу для користувачів і груп користувачів. Це означає, що різні користувачі можуть мати різні права доступу в залежності від їх ролі або позиції.

– Безпека і шифрування:

СКУД повинна забезпечувати високий рівень безпеки. Це включає в себе

шифрування даних, захист від несанкціонованого доступу до системи СКУД та захист від фізичних атак.

– Інтеграція та сумісність:

Система СКУД може інтегруватися з іншими системами безпеки, такими як системи відеоспостереження або системи оповіщення. Це дозволяє створити комплексну систему безпеки.

– Резервне копіювання та відновлення даних:

СКУД повинна надавати засоби для резервного копіювання даних і відновлення інформації в разі виникнення збоїв або втрати даних [18].

2.2.2 Аналіз різновидів СКУД та їх функціональних можливостей

Системи контролю та управління доступом існують у різних варіаціях з різними функціональними можливостями, що дозволяють регулювати і моніторити доступ на об’єктах. Кожна система СКУД відрізняється рівнем безпеки та надійності залежно від типу та набору обладнання. Сьогодні існує три види СКУД: Біометричні, Мережева та Автономна [18].

Біометричні системи контролю та управління доступом використовують біометричні дані для ідентифікації та автентифікації користувачів. Вони використовують унікальні фізичні або поведінкові характеристики особи для визначення її особистості та надання або відмови в доступі. На рисунку 2.2 показано типовий біометричний СКУД [24].

Рисунок 2.2 – Біометричний зчитувач

Зчитувач почне працювати лише при вдалій авторизації через картку доступу з RFID-міткою.

Біометричні СКУД підходять для об’єктів із високими вимогами до безпеки, таких як важливі установи, банки, лабораторії та інші місця, де необхідно надавати доступ лише певним особам з високою точністю та безпекою [18]. На рисунку 2.3 показано схему роботи біометричного зчитувача.

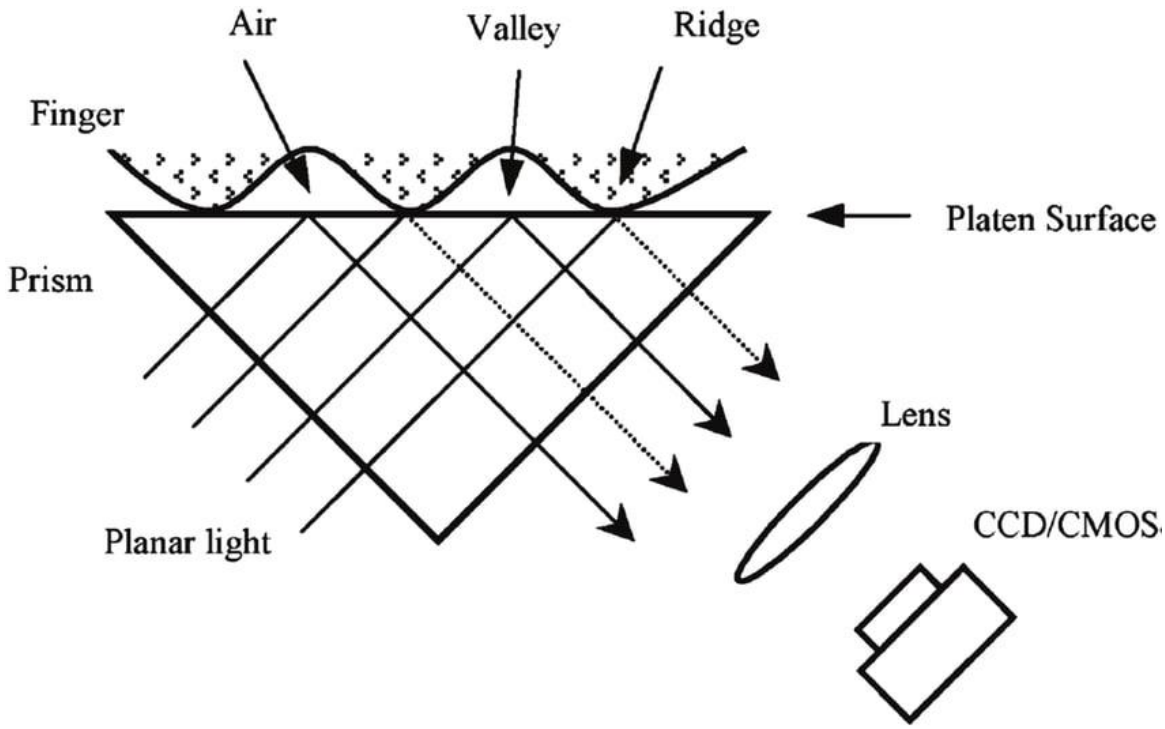

Рисунок 2.3 – Принцип роботи біометричного зчитувача

Функціональні можливості біометричних СКУД:

– Ідентифікація особи: Біометричні СКУД використовують біометричні дані, такі як відбитки пальців, розпізнавання обличчя, сканування сітківки ока або інші унікальні характеристики для ідентифікації особи. Це дозволяє точно та надійно визначити особу, що намагається отримати доступ.

– Безпека високого рівня: Біометричні дані є одними з найбільш надійних методів ідентифікації, оскільки вони є унікальними для кожної особи. Це робить біометричні СКУД дуже ефективними для об'єктів із високими вимогами до безпеки.

– Швидка ідентифікація: Біометричні СКУД зазвичай дуже швидкі у роботі. Вони можуть визначати особу в реальному часі, що дозволяє швидко та зручно входити на об’єкт.

– Інтеграція з іншими системами: Біометричні СКУД можуть інтегруватися з іншими системами безпеки, такими як системи відеоспостереження та системи оповіщення, для створення комплексної системи безпеки.

Мережеві системи контролю та управління доступом – це системи, які забезпечують контроль доступу та моніторинг за допомогою мережі, що підключає всі елементи системи. Така система має багато переваг, особливо в об’єктах з розподіленою інфраструктурою, і вона надає додаткову гнучкість та можливість віддаленого управління [18]. На рисунку 2.4 показано приклад схеми мережевого СКУД.

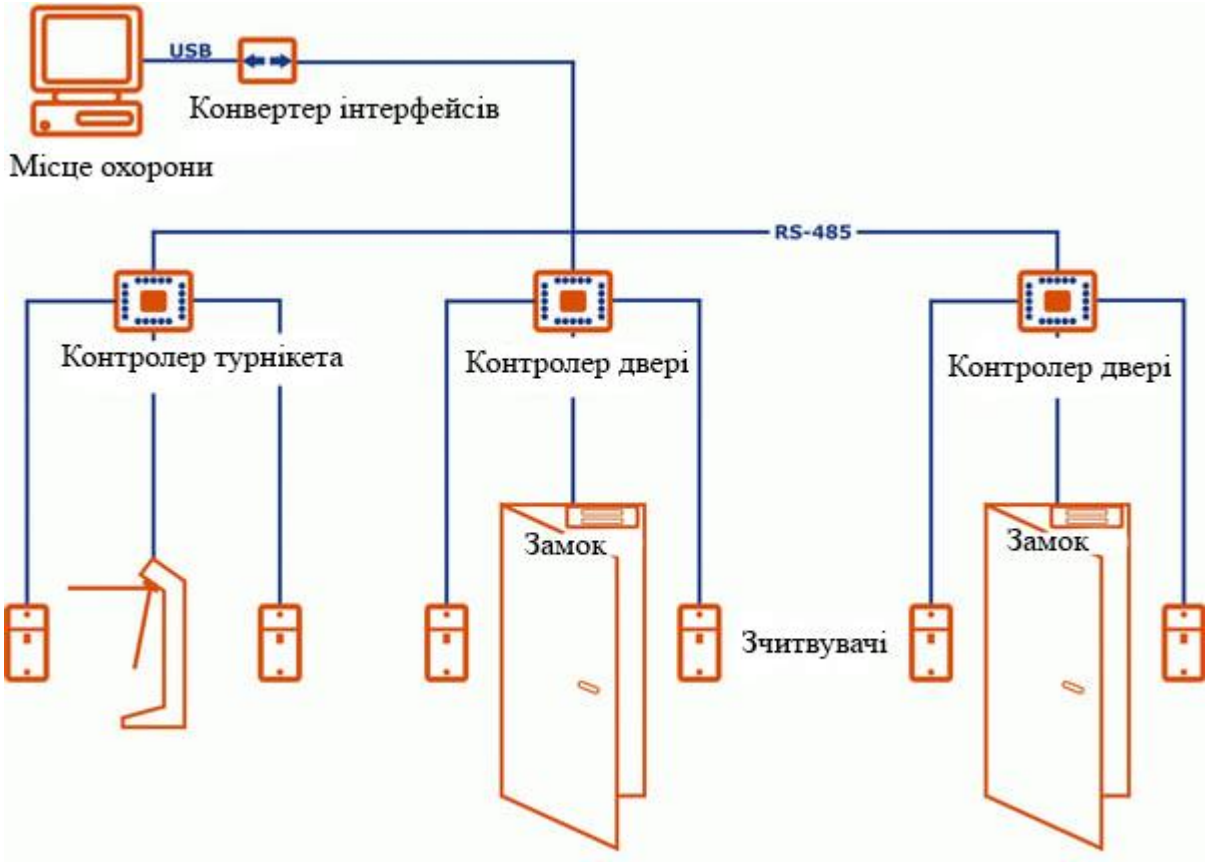

Рисунок 2.4 – Схема перепустки з використанням мережевого СКУД

Мережеві СКУД ідеально підходять для об’єктів з розподіленою структурою, таких як корпоративні офіси, мережи магазинів, великі виробничі підприємства та інші, де є централізований та віддалений контроль є важливими вимогами [18]. На рисунку 2.5 показано простий мережевий СКУДу.

Рисунок 2.5 – Приклад простого мережевої СКУД

Основні характеристики мережевих СКУД:

– Централізований контроль: Мережеві СКУД дозволяють централізовано управляти всіма аспектами контролю доступу на об’єкті. Це означає, що адміністратори можуть встановлювати правила доступу, надавати та відбирати права користувачів, а також моніторити події з центрального пункту управління.

– Мережева інтеграція: Мережеві СКУД легко інтегруються з іншими системами безпеки, такими як відеоспостереження, системи оповіщення та системи охоронної сигналізації. Це дозволяє створити комплексну систему безпеки, яка дозволяє взаємодіяти між різними компонентами.

– Гнучкість та розширюваність: Мережеві СКУД можуть легко розширюватися для включення додаткових точок доступу та користувачів. Ця гнучкість особливо важлива для об’єктів, які зростають з часом.

– Віддалений доступ: Однією з ключових переваг мережевих СКУД є можливість віддаленого управління системою через Інтернет. Це дозволяє адміністраторам віддалено керувати системою та моніторити події з будь-якого місця.

– Захист даних і безпека: Мережеві СКУД зазвичай мають рівні безпеки для захисту інформації та забезпечення конфіденційності даних. Вони використовують шифрування та інші технічні заходи для запобігання несанкціонованому доступу.

Автономні системи контролю та управління доступом – це системи, які функціонують незалежно від центрального сервера або мережі. Вони мають внутрішню логіку та рішення щодо контролю доступу, і не потребують постійного підключення до сервера для прийняття рішень. Автономні СКУД можуть бути особливо корисними для об’єктів, де немає можливості або потреби в підтримці централізованої мережі. На рисунку 2.6 показано комплект автономного СКУД.

Рисунок 2.6 – Автономний СКУД

Автономні СКУД ідеально підходять для об'єктів, де важко або дорого побудувати мережу або де вимагається незалежність від зовнішніх мережевих факторів. Вони можуть бути використані на віддалених будівництвах, складах, готелях, ресторанах та інших місцях, де необхідний контроль доступу.

Основні характеристики Автономних СКУД:

– Незалежність від мережі: Однією з ключових переваг Автономних СКУД є їхня здатність працювати навіть при відсутності мережевого підключення. Вони можуть приймати рішення про контроль доступу локально, без необхідності звертатися до центрального сервера.

– Локальне управління: Автономні СКУД зазвичай мають інтерфейс для локального управління та налаштувань. Це дозволяє адміністраторам встановлювати правила доступу та моніторити події на місці, без необхідності використання центрального сервера.

– Проста установка та розгортання: Автономні СКУД зазвичай менше вимагають інфраструктури та складнішої установки порівняно з централізованими системами. Це полегшує їх впровадження в об’єкти.

– Місцеве зберігання даних: Деякі Автономні СКУД забезпечують місцеве зберігання даних про користувачів та події, що дозволяє забезпечити доступ до інформації навіть при відсутності мережі.

– Локальні контролери доступу: В Автономних СКУД часто використовуються локальні контролери доступу, які можуть приймати рішення про відкриття чи закриття дверей, бар’єрів тощо без необхідності підключення до сервера.

– Безпека даних: Як і інші системи контролю доступу, Автономні СКУД зазвичай забезпечують високий рівень безпеки для захисту інформації та даних про користувачів [19].

2.3 Інтеграція СКУД з гіпервізором ESXI

Мета інтеграції СКУД з гіпервізором ESXi – забезпечити безпеку доступу до віртуальних машин та ресурсів, контролювати і аудитувати цей доступ і виконувати управління правами користувачів ефективно та безпечно. Реалізація інтеграції залежить від вибору систем СКУД і гіпервізора ESXi, а також від потреб у забезпеченні безпеки та контролю доступу. Інтеграція гіпервізора VMware ESXi і системи СКУД дозволяє ефективно керувати безпекою і доступом до інфраструктури.

Існує три види інтеграції системи контролю доступом та гіпервізором ESXI, а саме api-інтеграція, LDAP/Active Directory інтеграція та контролерами доступу на рівні гіпервізору.

API-інтеграція дозволяє СКУД-системі використовувати функції та можливості ESXi для керування доступом до віртуальних машин та ресурсів. Включає створення, зміну та видалення прав доступу для користувачів, моніторинг активності і багато іншого. Такий тип інтеграції надає більшу гнучкість у налаштуванні та автоматизації процесів. Системний адміністратор може програмно керувати доступом та виконувати дії через програмні запити. API-інтеграція дозволяє автоматизувати багато завдань, такі як додавання нових користувачів, зміна прав доступу та інше.

LDAP і Active Directory інтеграція є одним із способів інтегрування СКУД з гіпервізором VMware ESXi. Метод використовує централізовану директорію користувачів, таку як Active Directory, для управління доступом до віртуальних машин та інфраструктури ESXi. Вже встановлена директорія користувачів може бути використана для автентифікації та авторизації користувачів [20].

Протокол LDAP використовується для керування директоріями користувачів та ресурсів через мережу. Протокол дозволяє системі СКУД взаємодіяти з active directory. Цей метод передбачає конфігурацію системи СКУД для використання active directory або іншої LDAP директорії для автентифікації користувачів. СКУД отримує доступ до даних користувачів з active directory для перевірки ідентифікації користувача. Права доступу до віртуальних машин та

ресурсів на ESXi визначаються з урахуванням груп та політик безпеки, встановлених в active directory. Адміністратори можуть налаштовувати права доступу для користувачів через групи та об’єкти в active directory [20].

LDAP/ active directory інтеграція має ряд наступних переваг [20]:

– Централізованое управління – всі данні про користувача та груп зберігаються в одній централізованій директорії;

– Єдина точка автентифікації – існуюча інфраструктура active directory дозволяє мати єдину автентифікацію для всіх ресурсів;

– Спадкування прав доступу – права доступу успадковуються від позиції ресурсу у active directory.

Контролери доступу на рівні гіпервізора – це інтеграція системи СКУД безпосередньо в гіпервізор VMware ESXi. Інтеграція дозволяє адміністраторам керувати правами доступу до віртуальних машин і інфраструктури віртуалізації безпосередньо через графічний інтерфейс ESXi або командний рядок, якщо вони не хочуть використовувати зовнішню СКУД-систему. Адміністратори завдяки цій інтеграції можуть налаштовувати права доступу, контролювати доступ до віртуальних машин і ресурсів прямо в гіпервізорі.

При інтеграції контролера доступу на рівні гіпервізора, адміністратори можуть налаштовувати права доступу для користувачів та груп безпосередньо в ESXi. Це може бути виконано через веб-інтерфейс або командний рядок [21].

2.4 Висновки до розділу

У розглянуто гіпервізор ESXi та систем контролю доступу СКУД. Розділ містить детальний опис функціоналу гіпервізора ESXi та аналіз систем контролю доступу, включаючи їхні принципи, різновиди та інтеграцію з гіпервізором.

Гіпервізор ESXi є популярним рішенням для віртуалізації серверів. Він надає можливість створювати та управляти віртуальними машинами на фізичних серверах. Використання гіпервізора ESXi дозволяє підвищити ефективність використання обладнання, зменшити витрати на обслуговування та полегшити резервне копіювання та відновлення віртуальних машин. Гіпервізор ESXi має мінімалістичну архітектуру, що дозволяє підвищити безпеку та надійність. Основні компоненти включають гіпервізор, дисковий слой та управління.

СКУД використовується для керування доступом до приміщень та ресурсів. Основними принципами є ідентифікація, аутентифікація та авторизація користувачів. Різні системи контролю доступу мають різні функціональні можливості, включаючи використання карточок, біометричні методи, системи відеоспостереження та інші. Інтеграція СКУД з гіпервізором ESXi може покращити безпеку і зручність управління доступом до віртуальних машин та серверів. Це дозволяє обмежувати доступ до важливих ресурсів і віртуальних середовищ.

Гіпервізор ESXi є потужним і ефективним інструментом для віртуалізації серверів, інтеграція систем контролю доступу може забезпечити додатковий рівень безпеки та контролю доступу до віртуальних ресурсів. Розуміння цих технологій і їхнє правильне використання підвищить ефективність та безпеку інформаційної інфраструктури.

3 СИНТЕЗ СИСТЕМИ КОНТРОЛЮ НАЯВНОСТІ УЧНІВ

Програма «Безпечна Школа» була обрана для обґрунтування під час проходження практики у КП «Інфо-рада Дніпро». Було отримано поточну інформацію про роботу цієї системи та фото пропускного контролю школи міста Дніпро, де застосовується ця програма.

Головна мета цієї програми полягає в автоматизації таких основних шкільних процесів як впровадження електронного щоденника, бази завдань та розкладу занять тощо. Також ця програма передбачає встановлення турнікетів та камер для базової безпеки у школі. Але ця програма, на наш погляд, не є дуже ефективною. Окрім встановлення турнікетів та камер слід встановити систему розпізнавання обличчя. Встановлення такого пристрою підвищить рівень безпеки у школі. Якщо залишити перепустку лише через турнікет, то є висока ймовірність, що до школи проникне стороння людина. Ідентифікація через камеру та картку перепустки знижує цю ймовірність до нуля [22].

Програма «Безпечна школа» також підвищує ефективність взаємодії батьків дитини зі школою. Це зроблено для того, щоб у разі потреби батьки могли отримати інформацію про оцінки тощо. Також батьки зможуть брати активну участь у житті школи, проходити опитування, завдяки яким буде покращуватися надання освітніх послуг, слідкувати та вносити пропозиції до харчування дітей у школі.

3.1 Цілі впровадження системи контролю доступу

Система контролю управління доступу впроваджується з метою забезпечення високого рівня безпеки та управління доступом до об’єктів. Основні цілі впровадження СКУД включають:

- захист об’єктів та інформації;
- управління ідентифікацією та контролю наявності учнів;
- моніторинг та аудит;
- вдосконалення ефективності;
- відповідність стандартам безпеки;

3.2 Формулювання технічних вимог до системи контролю наявності учнів у школі

3.2.1 Вимоги до реалізації системи

Для реалізації системи контролю доступу враховуються різноманітні аспекти та встановлені чіткі вимоги до проектування та реалізації. Основні вимоги включають:

- фізичний доступ до різних приміщень, встановлення турнікетів та додаткових електромагнітних замків;
- моніторинг та проведення аудиту для запису подій, пов’язаних із доступом, для подальшого аналізу;
- гнучкість та масштабованість системи яка адаптується до змін обсягу користувачів;

3.2.2 Вимоги до функцій виконуваних системою

Система контролю управління доступу повинна виконувати і забезпечувати наступні функції:

- рівні доступу для користувачів залежно від їх ролі у школі;
- ідентифікація використовуючи паролі, біометричні данні, картки доступу;

– моніторинг та проведення аудиту для запису подій, пов’язаних із доступом, для подальшого аналізу;

3.2.3 Вимоги до захисту інформації

Система контролю управління доступом має відповідати наступним вимогам безпеки:

– шифрування даних під час передачі та зберігання інформації повинно використовувати сучасні алгоритми шифрування;

– регулярне резервне копіювання інформації конфіденційної інформації та можливість швидкого відновлення в разі втрати даних або кібератаки;

– захист від кібератак, включаючи використання файрволів та антивірусного програмного забезпечення.

3.2.4 Вимоги до розробки структурної схеми

Для ефективної реалізації системи контролю доступу важливим етапом є розробка чіткої функціональної структури, яка визначає ключові елементи та їх взаємодію:

– модулі ідентифікації та аутентифікації забезпечують збір та перевірку інформації використовуючи біометричні дані та надає доступ користувачам, які пройшли перевірку;

– модуль управління рівнем доступу забезпечує гнучке управління привілеями;

– модуль інтеграції з іншими системами управління доступом, такими як камери спостереження;

– модуль гнучкості та масштабованості дозволяє масштабувати систему та адаптувати до змін в обсягах користувачів.

3.3 Огляд існуючої системи

Вибір апаратних засобів є критичною частиною процесу розробки системи контролю доступу. Визначення оптимального обладнання впливає на продуктивність, надійність та загальну ефективність системи.

На даний момент система контролю наявності учнів виконана на не достатньому рівні. На рисунках 3.1 та 3.2 показано прохідну школи та структурну схему з програмою цифровізації шкіл «Безпечна Школа».

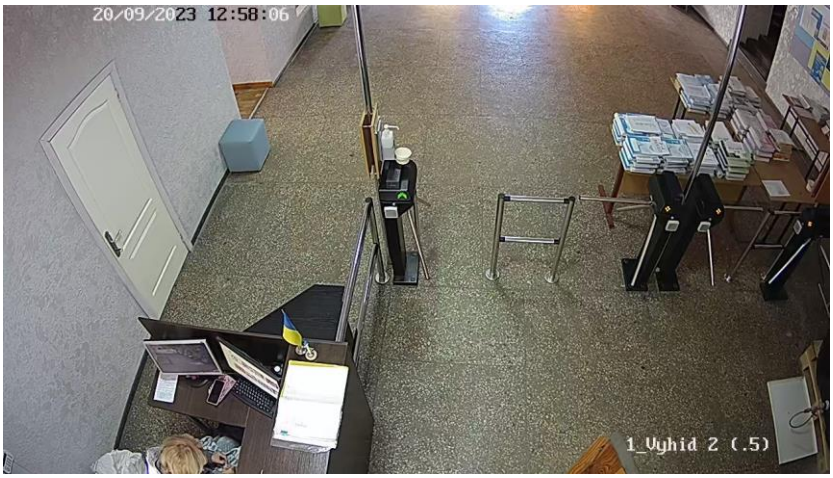

Рисунок 3.1 – Пропускний контроль з системою «Безпечна Школа»

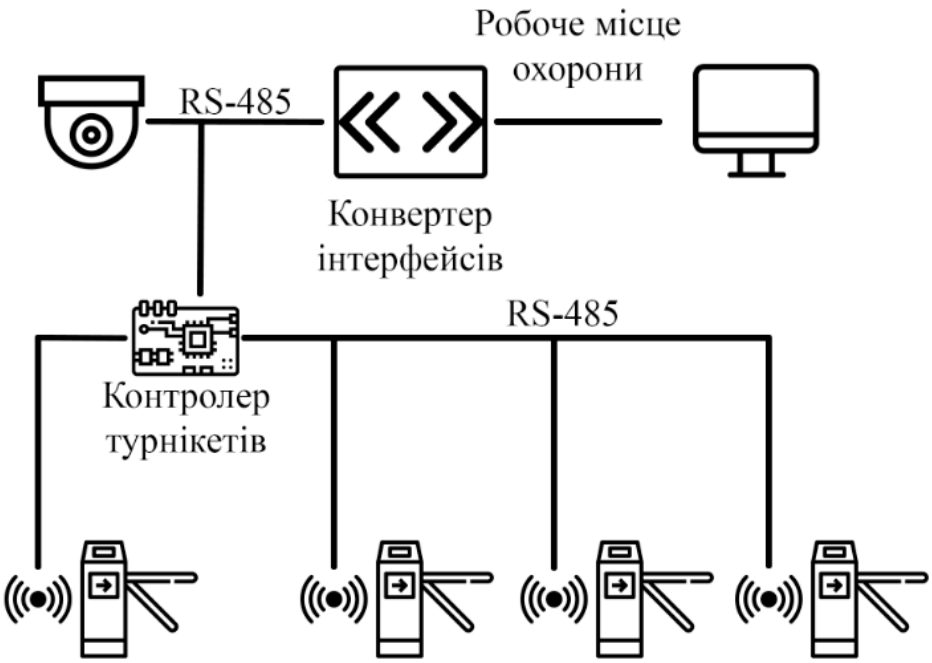

Рисунок 3.2 – Структурна схема наявною систем пропуску

На фото (рисунок 3.1) представлені стандартні турнікети зі зчитувачем RFID для фіксації проходу учнів. Така система контролю передбачена тільки для контролю входу у приміщення школи та відео спостереження за входом у приміщення.

3.3.1 Синтез структурної схеми системи за заданими показниками

Синтез структурної схеми системи враховує конкретні вимоги та показники, що були визначені на попередніх етапах. Під час детального аналізу вимог, визначення функціоналу та обрання технологій було розроблено структурну схему, спрямовану на виконання наступних ключових функцій:

– сканування через біометричні дані забезпечить безпеку в школі шляхом сканування біометричних даних учнів та персоналу. Параметрам, зазначеним у попередніх розділах, відповідає сканер моделі Hikvision DS-K1T341CM з можливістю запам’ятовувати до 3000 обличь;

– вдосконалена система відеоспостереження, яка вміє розпізнавати обличчя людини, має широкий кут спостереження та можливість його зміни. Це надасть школі засоби для вдосконалення безпеки та відслідковування подій. Обрано для розробки структурної схеми ір-камеру з ПОЕ інтерфейсом моделі Dahua DH-SD29204UE;

– забезпечення безпеки інформації, пов’язаної з біометричними даними та відеоінформацією, щоб уникнути несанкціонованого доступу та зберегти конфіденційність;

– масштабованість системи має легко адаптуватися до зростаючих потреб школи. Це включає резервні можливості та гнучкість в конфігурації. З цією задачею дуже гарно впорається комутатор TP-LINK TL-SL1218MP, забезпечить високу швидкість підключення та надійну роботу камер з ПОЕ інтерфейсами.

На рисунку 3.3 представлена вдосконалена структурна схема із застосуванням описаних раніше потреб та вимог.

На основному сервері налаштовано домен з правами доступу для шкільної мережі. Це необхідно для об’єднання в єдиний робочий простір. Також комп’ютери, які розташовані по всій школі, повинні мати обмеження на доступ до шкідливих ресурсів. Це необхідно для безпеки та запобігання витоку інформації.

Встановлення додаткового біометричного сканера разом з турнікетом, який розпізнає обличчя. Таким чином, сторонні люди не зможуть скористатися карткою учня, а в разі спроби вона буде невдалою і викличе на себе зайву увагу, а потім негайну реакцію охорони школи.

Для поліпшення системи відеоспостереження потрібне встановлення додаткових камер з можливістю отримати електроживлення від мережі інтернет через POE-інтерфейс на комутаторі та самій камері. Камери також мають можливість відстежувати та фіксувати обличчя людини, яка потрапляє в радіус огляду.

Використовується сервер, на якому зберігається та здійснюються обробка усіх робочих процесів на віртуальній основі.

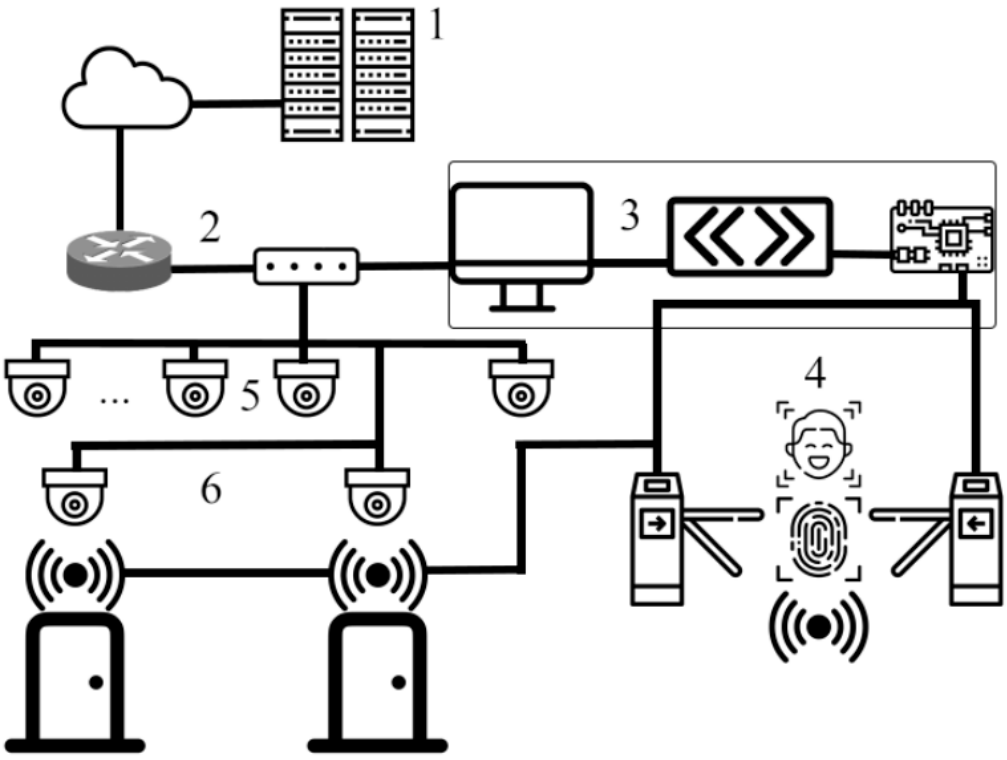

Рисунок 3.3 – Вдосконалена структурна схема, де

1 – Головний віртуальний сервер з налаштованим доменом та програмою контролю СКУД інформацією, 2 – Комутаційна шафа з маршрутизатором та комутатором, 3 – Кімната охорони з конвертером інтерфейсів з RS-485 на USB та контролер за пристроями СКУД, 4 – Вдосконалені турнікети із застосування біометричних СКУД, 5 – Вдосконалена система відеоспостереження на основі ip-камер, 6 – Важливі об’єкти школи з системою спостереження та магнітними замками.

Камери та усі мережеві пристрої підключаються через роз’єм RJ-45. Цей тип підключення забезпечить електроживлення на камерах відеоспотереження, що трохи зменьшить обсяг додаткових налаштувань з камерою.

3.3.2 Обґрунтування вимог до пристроїв контролю

У виборі пристроїв контролю ключовим є вибір технологій, які забезпечать надійність та ефективність системи контролю доступу. Для удосконалення системи комп’ютерного комплексу контролю наявності учнів вважаємо за необхідне застосувати наступні заходи безпеки:

– система розпізнавання обличчя підвищить час вирішення конфліктних ситуацій за рахунок бази обличь та забезпечить сканування та занесення нових до бази. Потрібна камера з широким кутом та можливістю змінювати його;

– біометричні сканери усунуть можливість проникнення на територію школи сторонніх людей та полегшить відстеження;

– резервне живлення забезпечить швидкий перехід на резервне у разі відключення основного джерела електроживлення;

– електромагнітні замки забезпечать надійний фізичний контроль доступу, централізоване управління замками;

– камери з можливістю отримати електроживлення через POE інтерфейс для того, щоб мінімізувати процес налаштування системи.

3.3.3 Обґрунтування вимог до мережевого обладнання

Вибір мережевого обладнання є важливим етапом при розробці системи контролю доступу, оскільки стабільність та швидкість передачі даних визначають ефективність всієї системи:

– стабільність та надійність, сумісність обладнання з актуальними стандартами зв’язку, що гарантує ефективну взаємодію з іншими пристроями;

– можливість розширення потенційно збільшує обсяг даних та кількість підключених пристроїв у майбутньому, слід звертати увагу обираючи обладнання для можливості легкого розширення;

– захист даних через використання шифрування та інших засобів безпеки мережі;

– маршрутизація та комутація даних для забезпечення швидкого та надійного обміну інформацією;

– простота управління мережевим обладнанням з інтуїтивним і простим інтерфейсом управління для забезпечення легкості конфігурації та моніторингу.

3.3.4 Обґрунтування вимог до серверного обладнання

Вибір відповідного серверного обладнання для системи контролю доступу визначає надійність, продуктивність та безпеку операцій:

– потужність обчислювальних ресурсів серверу повинно мати ефективний процесор, який має відповідати обчислювальним потребам системи;

– зберігання даних повинно виконуватись на швидких та надійних носіях, обсяг зберігання, що враховує потреби системи та можливість збільшення в майбутньому;

– резервне копіювання та відновлення системи забезпечить можливість регулярного копіювання даних для запобігання втратам у випадку непередбачуваних ситуацій;

– єдиний пункт керування системою, серверне обладнання, яке може бути легко інтегровано в систему керування всією інфраструктурою;

– віддалене управління забезпечить можливість віддаленого моніторингу та керування системою.

3.4 Вибір обладнання для системи контролю

Для серверного обладнання обрано фізичний сервер з наступними характеристиками, на якому налаштовано гіпервізор та буде створено усю віртуальну інфраструктуру:

- 2 процесори моделі Intel(R) Xeon(R) CPU E5506 2.13GHz;
- 32 гігабайти оперативної пам’яті;
- 2 терабайти жорсткий диск.

Для мережевого обладнання у школі під надані характеристики підходить наступне обладнання:

- маршрутизатор TP-LINK TL-R470T+;
- комутатор TP-LINK TL-SL1218MP із poe інтерфейсами для живлення відеокамер;
- декілька додаткових комутаторів моделі TP-LINK TL-SG1005D.

Усе мережеве обладнання підключається через кабелі типу RJ-45.

Для системи контролю за школою обрано наступні пристрої:

- контролер для СКУД моделі A1TX1;
- біометричний сканер із функцією сканування обличчя Hikvision DS-K1T341CM;
- камера відео спостереження із функцією розпізнавання обличчя Dahua DH-SD29204UE;
- додаткові магнітні замки та зчитувачі RFID міток моделі NT-180.

Ці пристрої підключаються до контролеру через кабель RS-485, який конвертує його у звичайний USB кабель та підключається до комп’ютеру охорони.

3.5 Висновки до розділу

У цьому розділі була проведена робота з синтезу структурної схеми системи відповідно до конкретних вимог та показників, визначених на ранніх етапах проєкту. Розроблена структурна схема системи включає ключові компоненти, які детально обґрунтовані та підкріплені аналізом вимог.

Спеціальна увага була приділена важливим аспектам, таким як сканування через біометричні дані, вдосконалена система відеоспостереження, забезпечення безпеки інформації та можливість масштабування системи. Кожен з цих елементів вигідно впливає на функціональність системи та її спроможність відповідати визначеним завданням.

Запропоновані покращення визначено як стратегічно важливі для забезпечення високої ефективності та безпеки у навчальному середовищі. Структурна схема, розроблена в рамках цього розділу, є основою для подальшого розвитку та втілення проєкту. Результати даного етапу створюють надійний фундамент для реалізації передових технологій у шкільному середовищі та вдосконалення системи забезпечення безпеки та контролю.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ СИСТЕМИ «БЕЗПЕЧНА ШКОЛА»

4.1 Призначення й сфера застосування програми

Сервер здійснює охоплення широкого спектру завдань, пов’язаних із забезпеченням як фізичної, так й інформаційної безпеки, а також управлінням доступом та взаємодією з іншими системами безпеки. Зокрема, вирішує завдання контролю над фізичними та електронними аспектами безпеки, забезпечуючи необхідну взаємодію з інфраструктурою безпеки та оперативні дії у випадках аварій чи потенційних загроз.

4.2 Обґрунтування технічних характеристик програми

Оскільки сервер працює під управлінням гіпервізора ESXi, обрані технічні характеристики повинні максимально підтримувати віртуалізацію. 32 ГБ реєстрової оперативної пам’яті та процесор із спеціальними серверними інструкціями забезпечать ефективну роботу кількох віртуальних машин одночасно та високу продуктивність.

Використання SSD диска вкрай необхідно для швидкого доступу до даних, що є важливим для оптимальної роботи віртуальних машин та забезпечення ефективного функціонування системи контролю в реальному часі.

Обрані технічні характеристики забезпечують потужність та резерв для масштабування системи. Це важливо для додавання нових функцій, модулів та віртуальних машин у майбутньому без значної зміни апаратної інфраструктури.

Стійкість та надійність є ключовими характеристиками для системи безпеки. 32 ГБ оперативної пам’яті дозволяють обробляти великий потік даних, а серверний процесор забезпечує високий рівень продуктивності, покращуючи ефективність системи та її відповідність вимогам безпеки.

Технічні характеристики повинні бути сумісними з іншими системами безпеки та легко інтегровуватися в існуючу інфраструктуру освітнього закладу, що є важливим для сприяння взаємодії та обміну даними.

Система серверу оптимізована з точки зору вартості відносно вимог до програми. Це дозволяє забезпечити ефективність та потужність за рахунок розумного використання ресурсів.

Очікується, що обрана конфігурація сервера забезпечить ефективну роботу з високими навантаженнями та зможе працювати із зростаючим обсягом даних і запитів.

4.3 Опис розробленої програми

Сервер діє як ключовий елемент, що забезпечує операційну базу для віртуальних машин та системи контролю доступу. Працює використовуючи гіпервізор ESXi, виступає платформою для створення та управління віртуальними образами операційних систем. Сервер створює потужне та ефективне середовище для роботи з віртуальними машинами, що дозволяє оптимально використовувати ресурси та забезпечує високий рівень функціональності.

4.3.1 Загальні відомості

Використовується гіпервізор ESXI версії 6.5 на фізичному сервері з наступними технічними характеристиками:

- два процесори моделі Intel(R) Xeon(R) CPU E5506 2.13GHz;
- 32 гігабайти реєстрової оперативної пам’яті;
- 1 терабайт пам’яті на ССД диску.

Другий фізичний сервер з наступними технічними характеристиками:

- Один процесор Intel(R) Xeon(R) CPU E5506 2.13GHz;
- 4 гігабайти оперативної пам’яти;
- 1 диск на обсяг 4 терабайти.

В цілому цих серверів буде достатньо для шкільних потреб, а саме створити домен з ролями для користувачів у школі, сховища інформації для збереження персональних даних та керування камерами та системами ідентифікації учнів.

4.3.2 Функціональне призначення

Перший фізичний сервер на платформі ESXi має наступні ключові функції:

– робота ПЗ для контролю фізичної безпеки: використання відеоспостереження та детекції руху для нагляду за територією школи;

– робота ПЗ для контролю доступу: модулі ідентифікації та аутентифікації, що обмежують доступ та забезпечують безпеку;

– робота ПЗ для інтеграції з іншими системами: можливість взаємодії з іншими системами безпеки, такими як камери відеоспостереження та системи контролю доступу;

– гнучкість та масштабованість: здатність адаптувати систему до змін вимог та обсягів користувачів.

Другий фізичний сервер має забезпечувати регулярне резервне копіювання даних системи.

4.3.3 Використані технічні засоби

На раніше означеному обладнанні проведено установка та налаштування гіпорвізору ESXI 6.5.0, на базі цього ПЗ буде розгорнуті сервера з наступними ролями:

– сервер служби ліцензування віддалених робочих столів;

– контролер домену;

– сервер додатків;

– сервер бази даних.

Гіпервізор встановлюється та налаштовується наступним чином:

1) завантаження з носія образу ESXI 6.5 (рисунок 4.1);

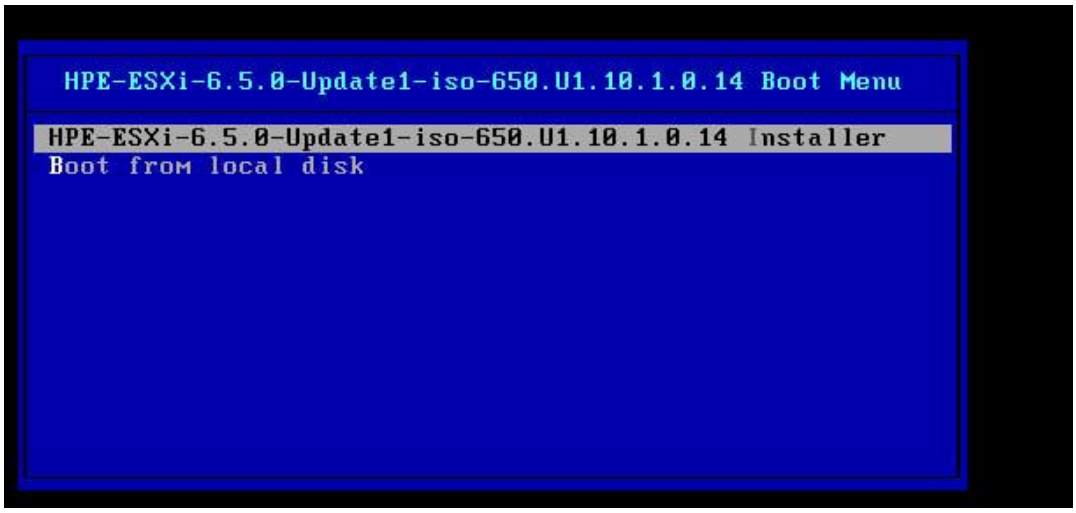

Рисунок 4.1 – Завантаження образу з носія

2) вибір диска, на який проводиться інсталяція системи (рисунок 4.2);

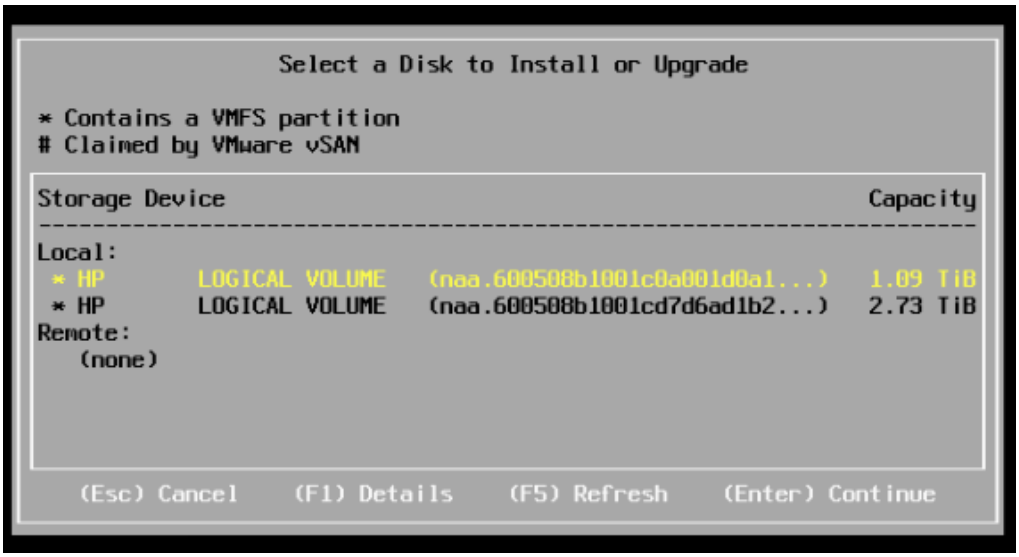

Рисунок 4.2 – Інсталяція на заданий диск

3) створення пароля для користувача-адміністратора root (рисунок 4.3).

Рисунок 4.3 – Задання паролю користувача адміністратора

Після виконаних кроків налаштування та інсталяції гіпервізора ESXI він перезавантажиться та буде готовий до початку роботи.

Робота з гіпервізором виконується через зручний веб-інтерфейс, на який ми потрапимо вписавши його айпі-адресу до браузеру. На рисунку 4.4 показано веб-інтерфейс гіпервізора та його технічні характеристики.

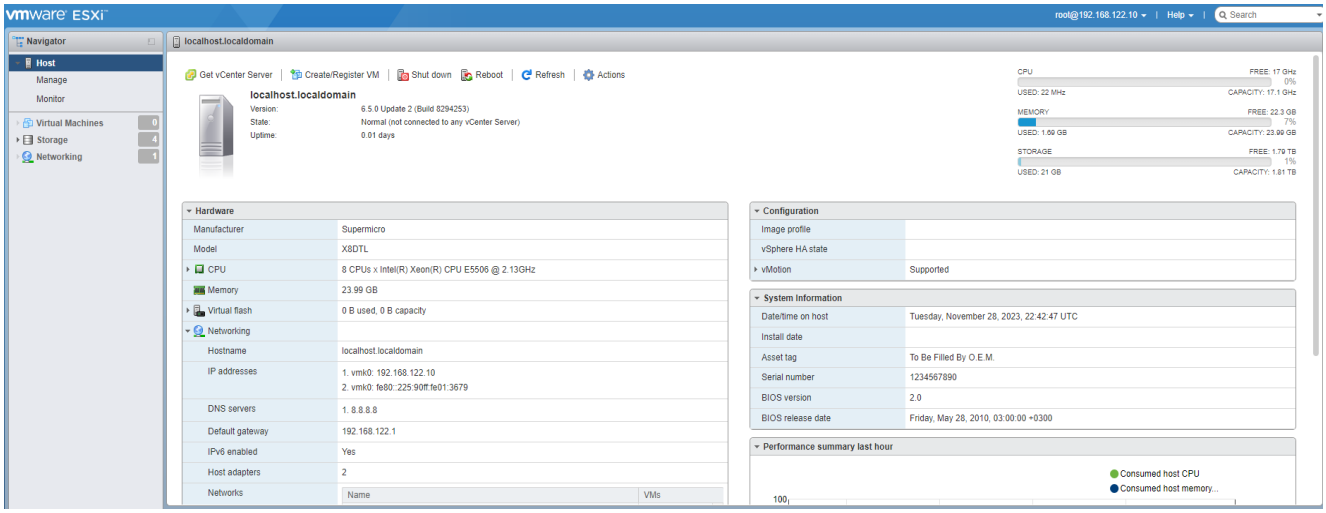

Рисунок 4.4 – Веб-інтерфейс гіпервізора ESXI

Додавання нових віртуальних машин у гіпервізор ESXi включає кілька етапів, які дозволяють налаштувати та розгорнути віртуальні середовища. У веб-інтерфейсі ESXi обирав вкладку «Virtual Machines», «Create/Register VM». Новий сервер відповідає за ліцензування віддалених робочих столів та створення домену. На рисунку 4.5 продемонстровано надання назви серверу.

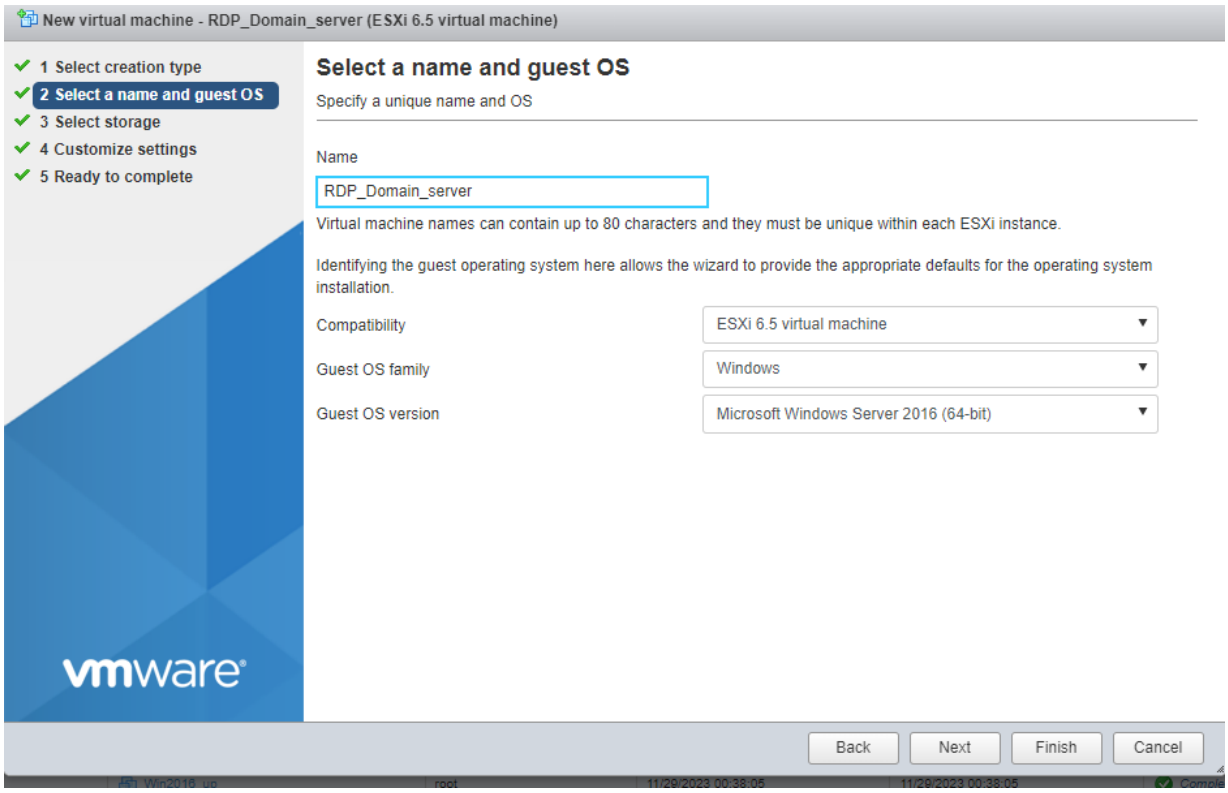

Рисунок 4.5 – Створення серверу відповідального за службу rdp та Active Directory

На рисунку 4.6 показано вибір диску, на якому буде виконуватись інсталяція образу серверу.

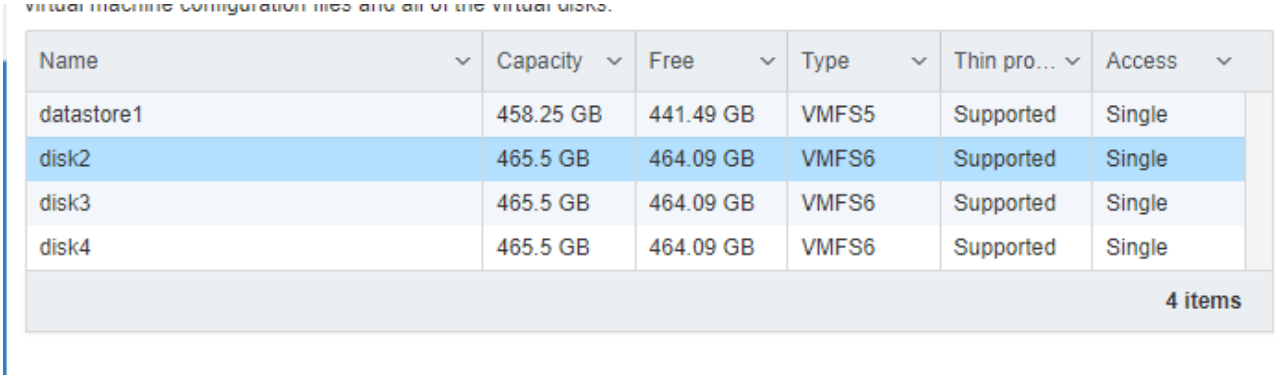

Рисунок 4.6 – Вибір диску для інсталяції

Для віртуального серверу з такими важливими службами потрібно виділити достатню кількість ресурсів, а саме кількість ядер процесора, об’єм оперативної пам’яті та місця на диску.

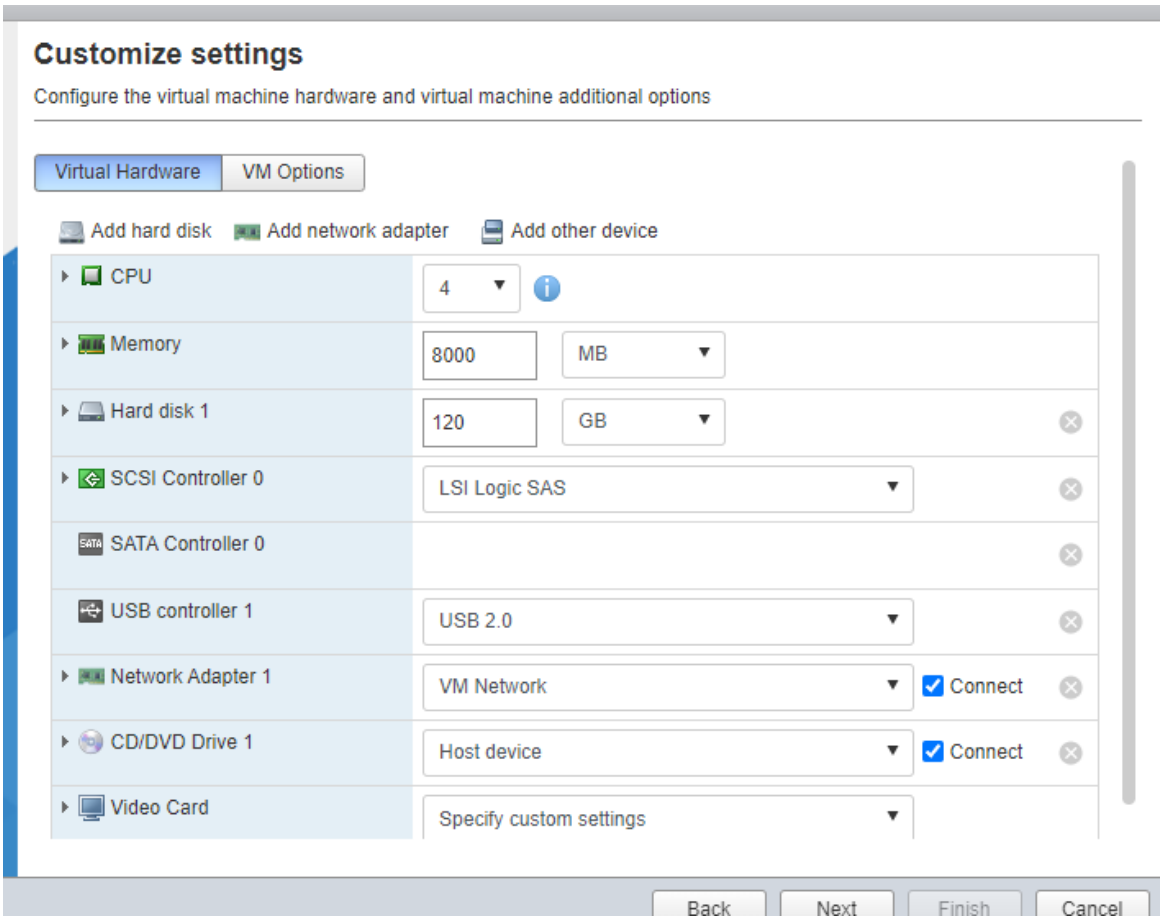

Рисунок 4.7 – Розподілення ресурсів для серверу

На створеному сервері буде налаштовано Remote Desktop Services та активовано ліцензування. Далі описано покрокову інсталяцію та активацію термінального серверу.

Налаштування ролі Remote Desktop Services.

У вікні «Server Management» обрати «Add roles and features», у новому вікні залишити все як є та перейти до списку ролей, у списку обрати «Remote Desktop Services» та «DNS». У вікні «Select role services» потрібно обрати дві ролі для RDP, а саме «Remote Desktop Licensing» та «Remote Desktop Session Host». У разі вдалої установки усіх компонентів та ролей з’явиться вікно, як на рисунку 4.8.

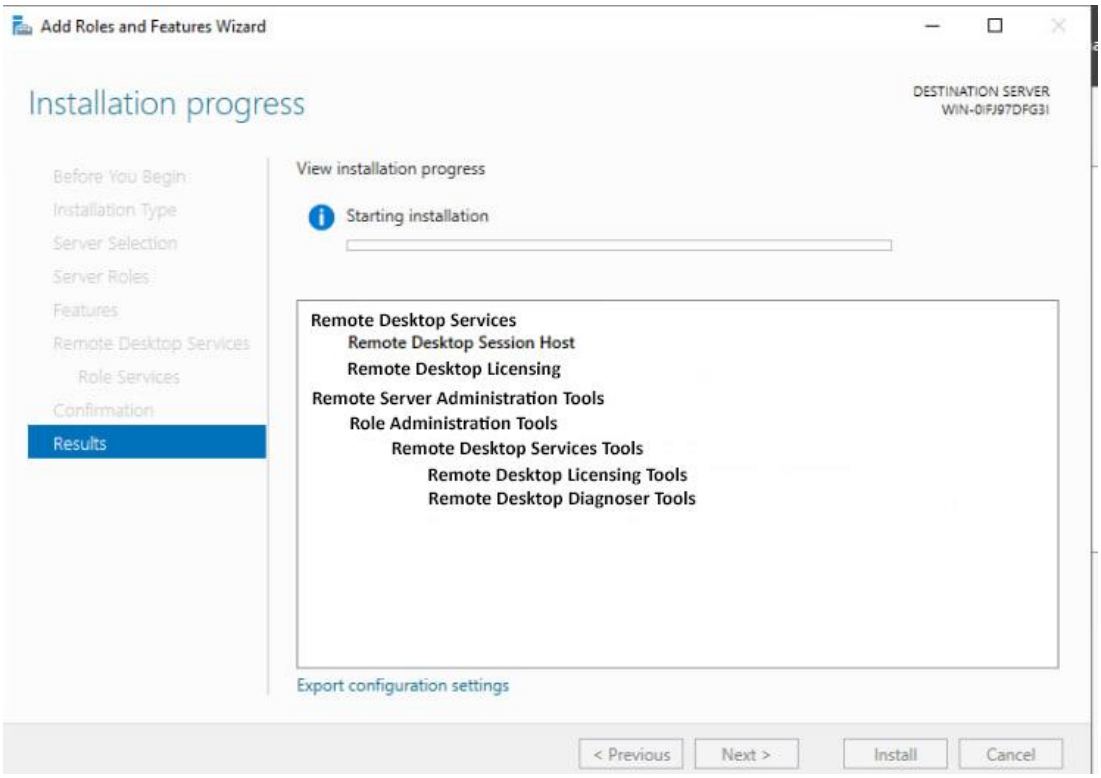

Рисунок 4.8 – Вдала установка усіх компонентів RDP-серверу

Після усіх налаштувань потрібно активувати ліцензію для серверу, для чого слід викликати вікно командної строки та вписати наступну команду – «licmgr.exe», правою кнопкою миші натиснути на сервер та обрати «Activate Server». Нове вікно пропонує варіант активації, обираємо «Web Browser» та заносимо ключ активації термінального серверу. Після цих кроків повинно з’явитися вікно, зображене на рисунку 4.9.

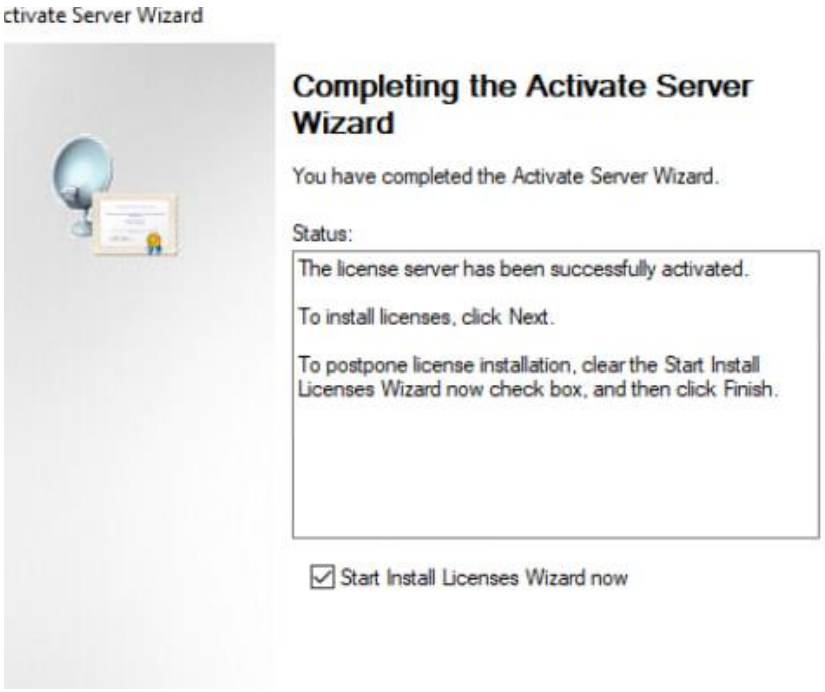

Рисунок 4.9 – Активація термінального серверу

Після активації слід перевірити наявність ліцензії у «RD Licensing Manager», знову вписавши команду «licmgr.exe». Якщо все пройшло успішно, то сервер буде активовано та показано доступну кількість ліцензій на віддалених користувачів. Ця ліцензія призначена для десяти віддалених користувачів. На рисунку 4.10 показано результат активації серверу терміналів та ліцензій користувачів.

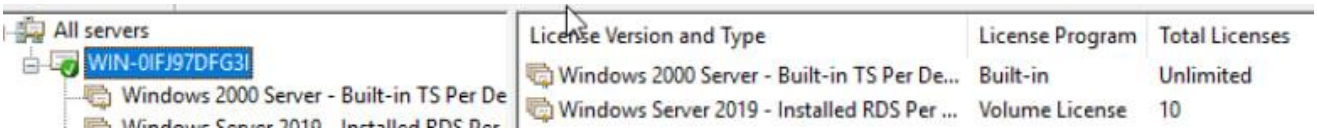

Рисунок 4.10 – Активований сервер

Останнім кроком налаштування серверу віддалених робочих станцій буде занесення правки до реєстру. Це можна зробити наступним чином: викликати командну строку через клавіши Win + r та вписати «gpedit.msc», і йти згідно цьому шляху Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\ Licensing. Далі необхідно зайти до Use the specified Remote License Servers. У цьому вікні

потрібно поставити позначку на «Enabled» і вписати айпі адресу серверу «192.168.122.233», а у вікно Set the Remote Desktop licensing поставити режим на «Per User».

Після перезавантаження серверу слід перевірити зміну політик через «адмін панель power shell», для чого потрібно написати наступну команду «gpupdate /force». З'явиться наступна інформація, яка буде свідчити про те, що політики вдало змінено (показано на рисунку 4.11).

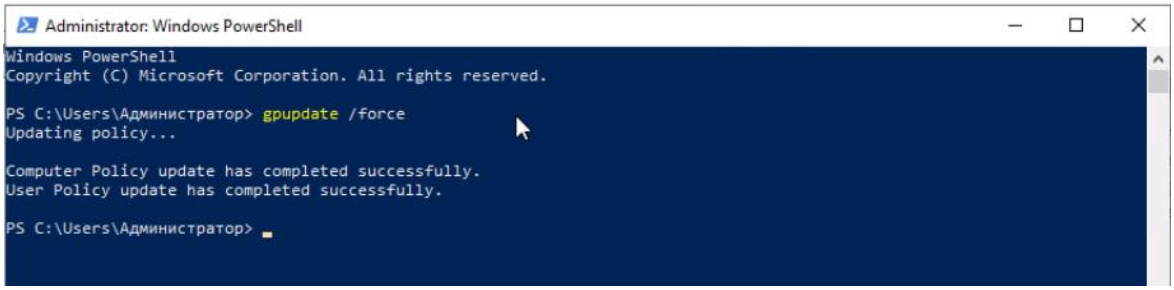

Рисунок 4.11 – Перевірка політики

При вдалому виконанні усіх налаштувань у вікні «RD Licensing Diagnoser» відображатиметься інформація про вдале налаштування та кількість ліцензованих користувачів (показано на рисунку 4.12).

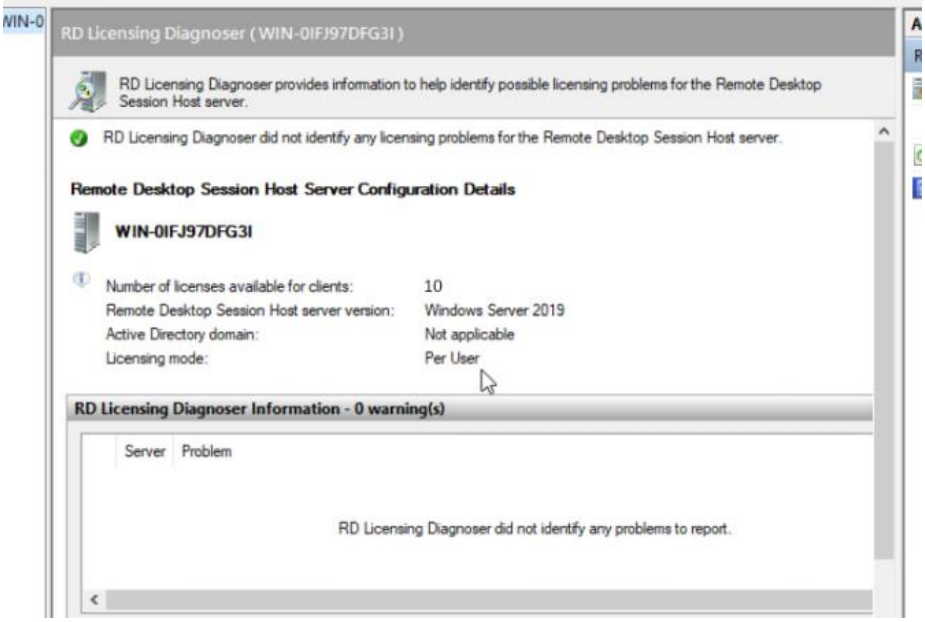

Рисунок 4.12 – Результат вдалого ліцензування серверу

Налаштування ролі Active Directory Domain Controller.

Першим кроком налаштування потрібно виконати таку послідовність дій: відкрити вкладку «Server Management», додати ролі та функції «Manage», «Add Roles and Feaers», обрати сервер, обрати роль «Active Directory Domain Services», у вікні, що з’явилося, натиснути «Next» та натиснути «Install». На рисунку 4.13 продемонстровано вдалу інсталяцію ролі Active Directory Domain Controller.

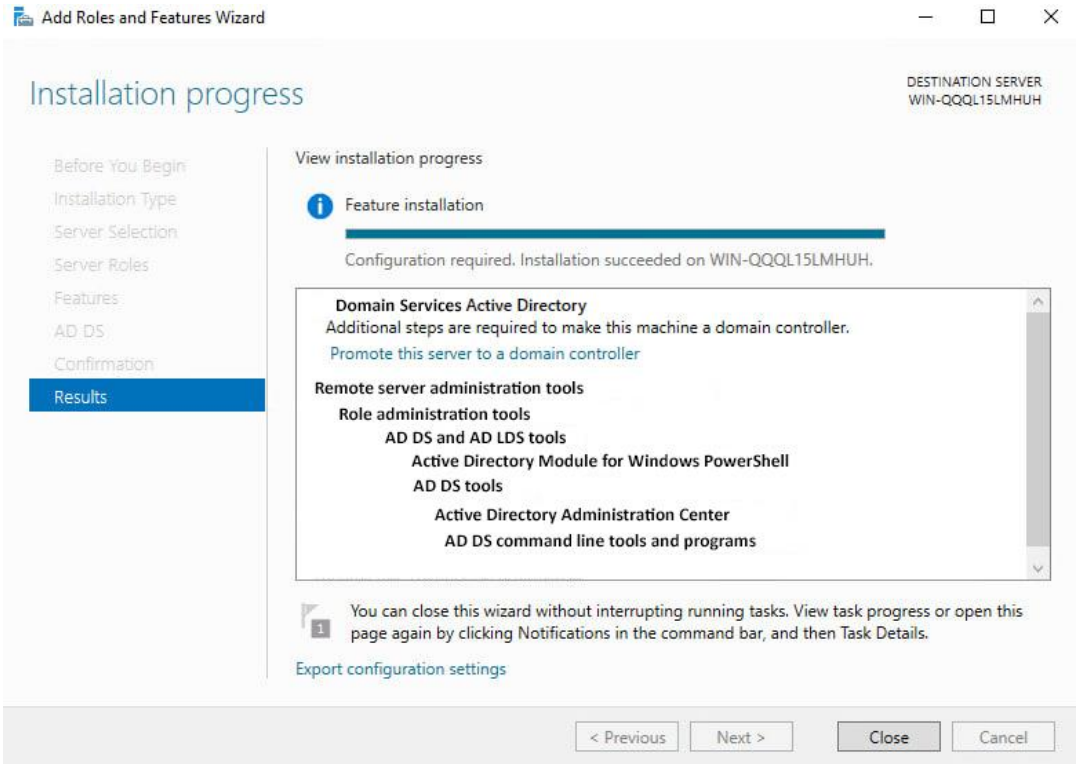

Рисунок 4.13 – Вдала установка ролі Active Directory Domain Controller

Тепер потрібно налаштувати сам домен контролер. Першим кроком потрібно налаштувати новий ліс та задати ім’я домену (показано на рисунку 4.14).

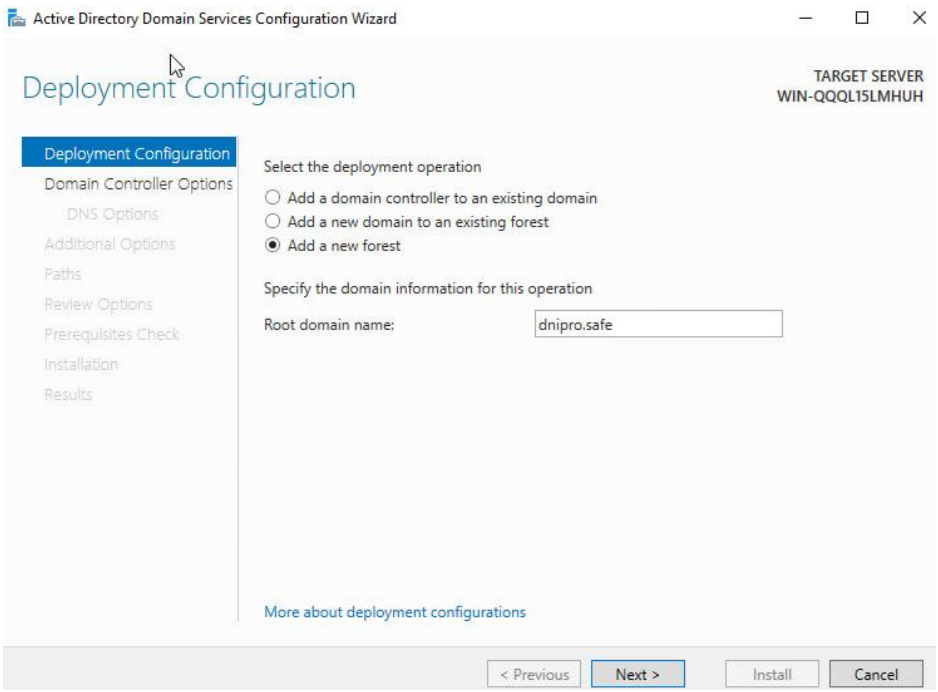

Рисунок 4.14 – Налаштування нового домену

У пункті «Domain controller options» необхідно вказати функціональний рівень домену та лісу AD. Вибираємо схему, що відповідає редакції нашого сервера. Оскільки на цьому сервері буде піднято роль DNS сервера, потрібно натиснути чекбокси «DNS-server» та «Global catalog» і вказати пароль адміністратора для входу в DSRN режим. Далі потрібно підтверджувати натискаючи «Next» та «Install». На рисунку 4.15 показано результат процедури створення.

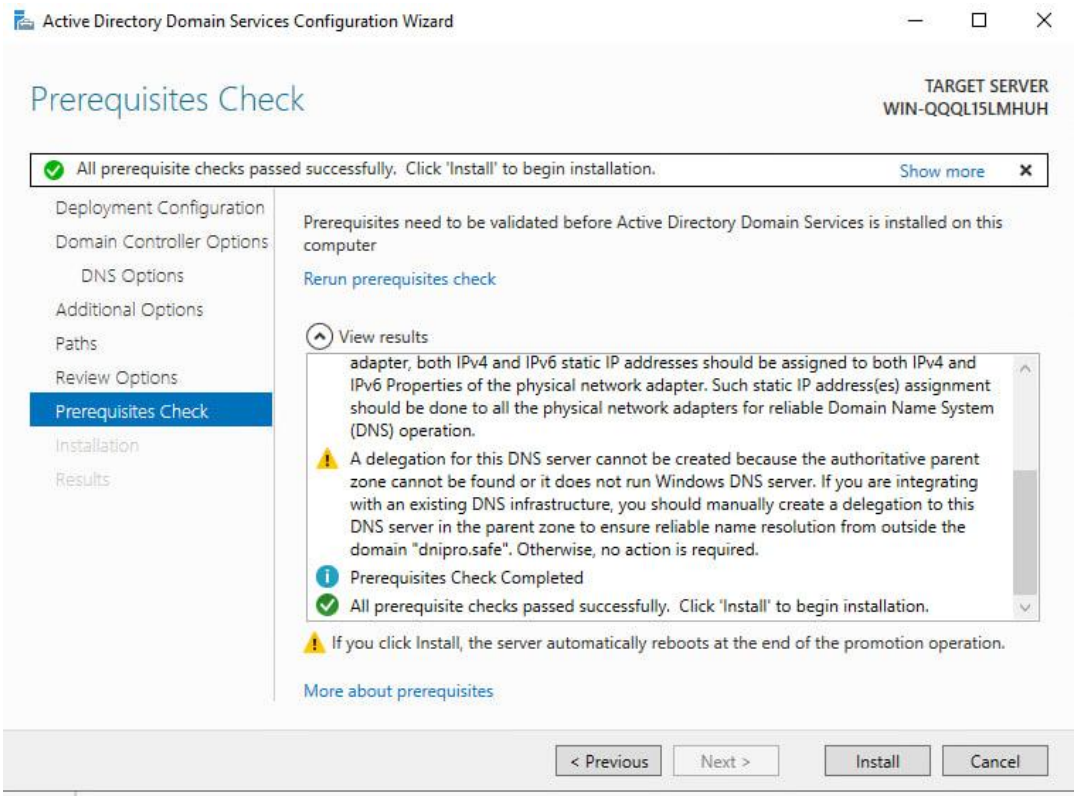

Рисунок 4.15 – Результат налаштування лісу

Після налаштування сервер перезавантажиться, тепер робота на ньому буде проводитись під обліковим записом домену. Для роботи у домені потрібно створити список комп’ютерів домену для присвоєння їх до робочих станцій, що допоможе легше керувати системою. На рисунку 4.16 створено первинні комп’ютери для робочих серверів.

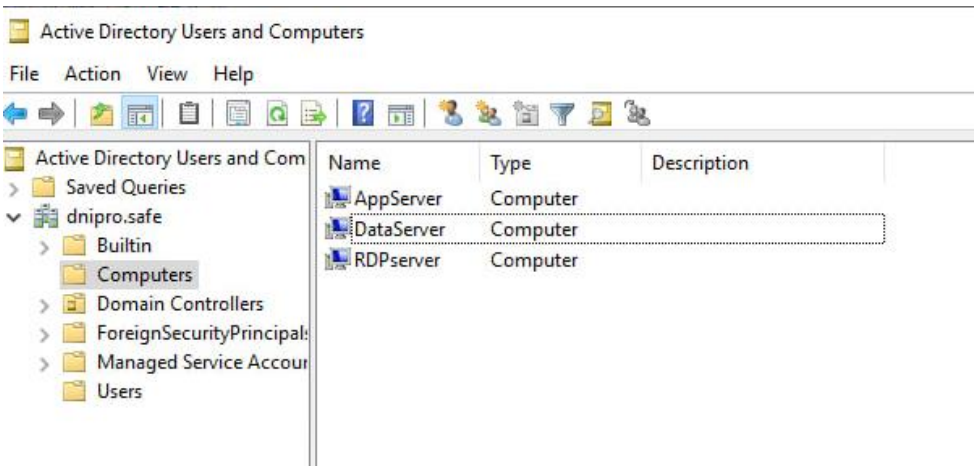

Рисунок 4.16 – Робочі станції для домену

Але сервер керування доменом виступає тепер і як DNS-сервер, тож потрібно провести налаштування параметрів адаптеру згідно з айпі-адреси встановленої на сервері. За замовчуванням буде стояти адреса 127.0.0.1, її потрібно змінити. На рисунку 4.17 показано налаштування адаптеру на AD DS сервері. Якщо цього не зробити, то не вдасться додати машину у домен. Аналогічно зроблено на інших машинах.

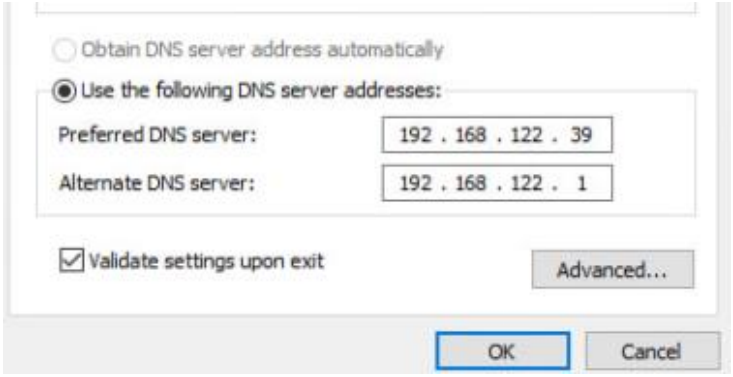

Рисунок 4.17 – Налаштування DNS на сервері

Для запису комп'ютеру у домен потрібно зайти у «Властивості комп'ютера», «Додаткові властивості системи», «Ім'я комп'ютера», «Змінити», ввести нове ім'я комп'ютера «rdpserver» та ім'я домену «dnipro.safe». На рисунку 4.18 показано процес додавання комп'ютера у домен.

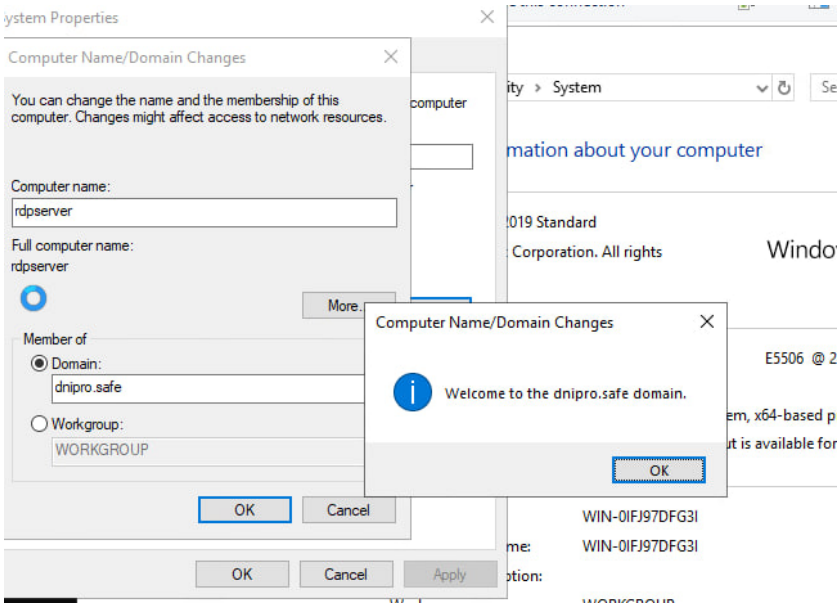

Рисунок 4.18 – Додавання RDP-серверу у домен

Також створено декілька користувачів для домену з правами адміністратора та можливістю використовувати RDP підключення (показано на рисунку 4.19). На інших віртуальних машинах проведено налаштування домену згідно попереднього прикладу.

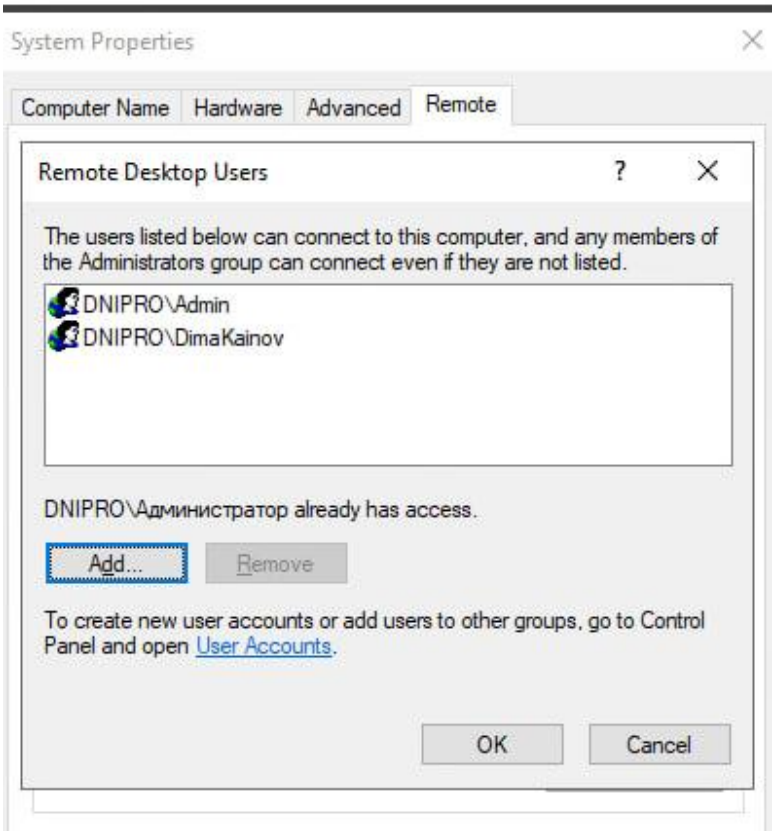

Рисунок 4.19 – Користувачі для RDP та домену

Налаштування домену також можна виконувати також через програму написану на powershell, це значно швидше та зручніше, компілятором програми виступає Windows PowerShell ISE. На рисунку 4.20 процес інсталяції з цією програмою.

```
Import-Module ServerManager
Add-WindowsFeature -Name AD-Domain-Services -IncludeAllSubFeature -IncludeManageme
Import-Module ADDSDeployment
Inaistall-ADDSForest `
-CreateDnsDelegation:$false `
-DatabasePath "C:\Windows\NTDS" `
-DomnMode "WinThreshold" `
-DomainName "safednipro.com" `
-DomainNetbiosName "SAFEDNIPRO" `
-ForestMode "WinThreshold" `
-InstallDns:$true `
-LogPath "C:\Windows\NTDS" `
-NoRebootOnCompletion:$false `
-SysvolPath "C:\Windows\SYSVOL" `
-Force:$true
```

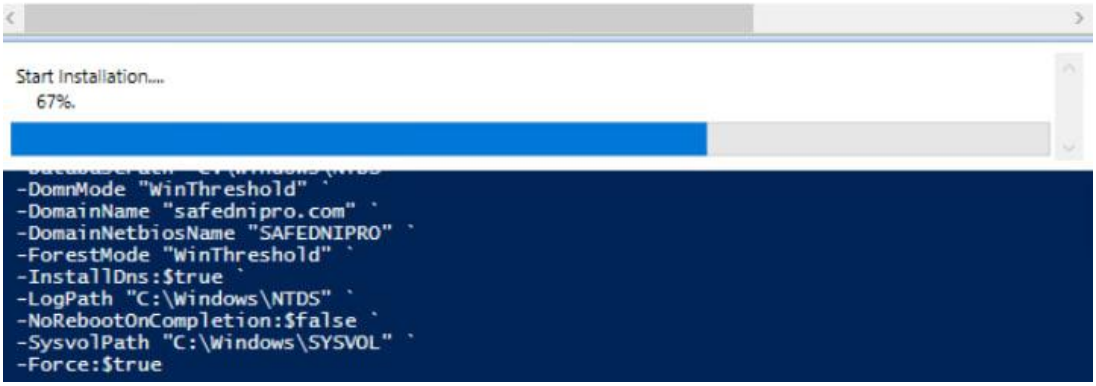

Рисунок 4.20 – Інсталяція програми

Після вдалої інсталяції потрібно увести пароль для резервного відновлення системи. На рисунку 4.21 показано вікно введення паролю для відновлення.

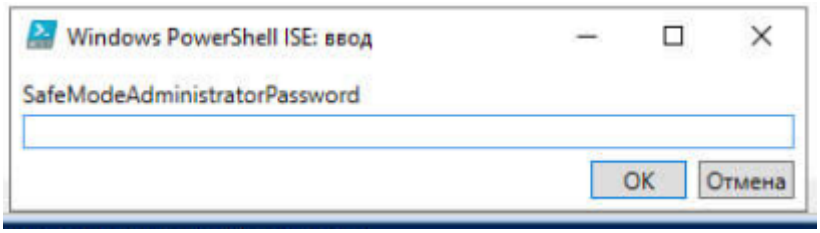

Рисунок 4.21 – Вікно для резервного паролю

Після цього запуститься процес налаштування нового лісу домену. На рисунку 4.22 показано процес інсталяції лісу.

Рисунок 4.22 – Інсталяція нового лісу

Налаштування біометричного приладу СКУД

Для роботи у школі необхідно мати пристрій СКУД з можливістю запам’ятовувати до 3000 обличь, інші налаштовані сервера будуть використовуватись як станції контролю за роботою СКУД, на яких буде налаштовано програмне забезпечення, яке йде у комплекті з самим пристроєм, але на пристрої також можна налаштувати через зручний веб-інтерфейс.

На рисунку 4.23 продемонстровано веб інтерфейс пристрою на етапі створення нового користувача. Ручне введення через веб інтерфейс набагато зручніше, оскільки є можливість додавання фото учня, а не сканування його. Таким чином, введення нового учня в базу даних займе набагато менше часу, для цього потрібно тільки фотокартка у форматі 4x3 у високій роздільній здатності.

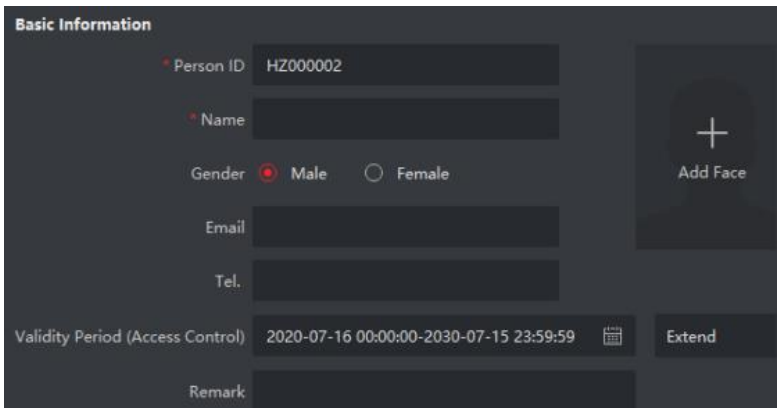

Рисунок 4.23 – Веб-інтерфейс пристрою

Датчик передбачає великий список можливих варіантів і комбінацій для авторизації, але бажано встановити комбінацію авторизації через ідентифікацію обличчя та сканування карти доступу. Але за ситуації, коли учень залишив картку вдома, охоронець має можливість відкриття вручну через програму контрою чи веб інтерфейс. На рисунку 4.24 продемонстровано вікно налаштування режиму роботи.

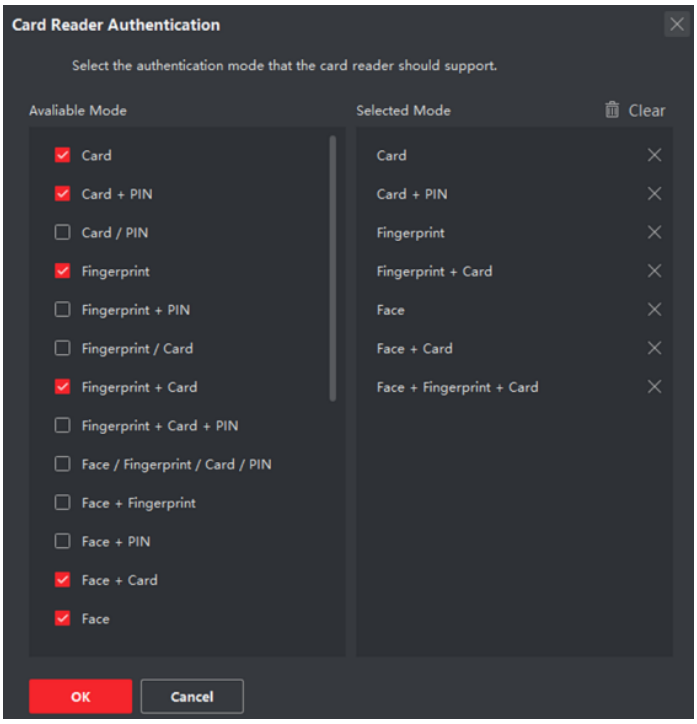

Рисунок 4.24 – Список можливих варіантів авторизації

4.4 Очікувані технічно-економічні показники

Система буде працювати більш ефективніше та значно надійніше через віртуалізацію серверів з усією конфіденційною інформацією у порівнянні із звичайною системою. Кожен сервер повинен працювати як самостійна віртуальна машина, що дозволить підняти надійність системи та більш гнучкіше розподілити ресурси кожній віртуальній машині, на відміну від фізичних серверів. Таким чином, система буде коштувати значно менше.

Біометричні технології, такі як сканування відбитків пальців чи розпізнавання обличчя, забезпечують високий рівень ідентифікації осіб, ускладнюючи можливість використання фальсифікованих або втрачених карток доступу. Використання високоякісних камер та системи розпізнавання обличчя дозволяє вчасно виявляти потенційні загрози та здійснювати ефективний контроль над об’єктом.

PoE-світч ефективно використовує енергію для живлення підключених камер відеоспостереження. Знижує необхідність великої кількості окремих

джерел живлення для кожної камери, спрощуючи систему та витрати на електроенергію.

Використання віртуального сервера для моніторингу та дистанційного керування дозволяє здійснювати ефективний нагляд та управління системою з будь-якого місця з Інтернет-з’єднанням. Це спрощує проведення регулярних оглядів стану системи, виявлення можливих проблем та вчасне реагування на інциденти.

Завдяки постійному моніторингу та дистанційному керуванню можна ефективно планувати та виконувати обслуговування. Це попереджає виникнення аварій та зберігає ефективність системи на високому рівні, при цьому знижуючи витрати на несподівані ремонтні роботи.

Загалом оптимізація витрат на обслуговування через використання віртуального сервера не лише забезпечує ефективність системи контролю доступу та безпеки, але і створює економічно вигідний підхід до управління та підтримки інфраструктури, що може значно зменшити загальні витрати на експлуатацію відповідної системи.

4.5 Висновки до розділу

У розділі детально розглянуто характеристики серверу, на якому розгорнуто віртуальну інфраструктуру для роботи із шкільним сегментом. Встановлено гіпервізор ESXI 6.5 на сервер, і на його основі розроблено віртуальні станції. Встановлення гіпервізора на сервер є важливим етапом для розгортання та ефективного управління віртуальними середовищами.

Налаштовано Термінальний сервер та активовано ліцензування віддалених робочих столів для десяти користувачів, що дозволяє віддалено керувати серверами та у разі виникнення проблеми віддалено її вирішувати. Другий сервер виконує роль контролеру домену та роль DNS. Домен потрібен для централізованого керування системою та забезпечення безпеки.

Також створено дві віртуальні машини для подальшої роботи з програмним забезпеченням біометричного датчику. Програмне забезпечення покупається окремо чи йде у комплекті з пристроєм. Біометричний СКУД також можна налаштувати через веб-інтерфейс. Цей процес було розглянуто у розділі, але він не є таким зручним у порівнянні з програмою. Програма надає операторам та адміністраторам інструмент для ефективного моніторингу та управління системою, що підсилює функціональні можливості і поліпшує загальну ефективність інфраструктури.

В результаті виконаних дій, наведених у цьому розділі, система налаштована та готова до впровадження в реальному середовищі. Зазначено, що кожен крок інсталяції та налаштування має на меті забезпечити найвищий рівень безпеки та продуктивності враховуючи всі технічні та економічні аспекти.

5 ЕКСПЕРИМЕНТАЛЬНИЙ РОЗДІЛ

5.1 Мета і завдання експерименту

Мета експерименту полягає в оцінці працездатності та реагування віртуальної системи під час великого обсягу навантаження.

Завдання експерименту включає створення імітованого навантаження системи, що відобразить реальні умови експлуатації. Моніторинг реакції системи на збільшення обчислювального та мережевого навантаження.

5.2 Методика експерименту

Використовуються дві методики проведення експерименту:

– створення навантаження через працю багатьох віртуальних машин та розподіл ресурсів для ВМ;

– моніторинг та вимірювання таких ключових метрик, як використання ЦП, ОЗП, використання мережевих ресурсів.

5.3 Вимоги до експерименту

Експеримент вважатиметься успішним, якщо система здатна забезпечувати стабільну роботу та підтримувати продуктивність за встановленими вимогами.

Оцінити використання ресурсів серверу, середній час відповіді системи, пропускна здатність мережі, визначити максимальний обсяг навантаження, при якому система залишиться стабільною та забезпечуватиме прийнятні показники.

Експеримент проведено на віртуальному сервері з відповідною до раніше описаних характеристик. Тестування включає сценарій, що моделює інтенсивне використання ресурсів.

5.4 Аналіз результатів експерименту

5.4.1 Практичне застосування

Сутність експерименту полягає у тестуванні працездатності системи під навантаженням і різними характеристиками.

Перед проведенням експерименту налаштували VPN зв’язок для віддаленого підключення до мережі школи. Емуляцію цього процесу виконано використовуючи два різних провайдера з білим айпі.

На початку слід зайшли до веб-інтерфейсу роутера та налаштували VPN сервер на основі OpenVPN. Створили нового користувача «schooladmin» та завантажили конфігурацію для віддаленого підключення. Після підключення на веб-інтерфейсі зазначено, який користувач підключився. Результат налаштування показано на рисунку 5.1.

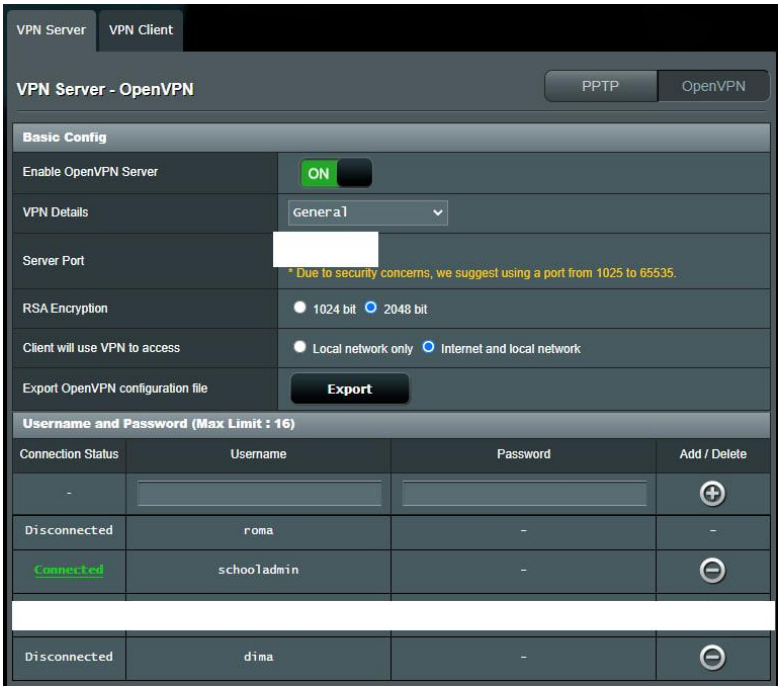

Рисунок 5.1 – Налаштований користувач для віддаленого підключення

Тестовий стенд для експерименту має наступні характеристики:

– 2 процесори Intel(R) Xeon(R) CPU E5506 2.13GHz;
– 32 гігабайти ОЗП;
– 2 терабайти жорсткий диск.

5.4.2 Результат експерименту в цифрах і фактах

Перший експеримент показує як необхідно розподілити ресурси процесору, щоб він мав змогу виконувати задачі на оптимальній конфігурації, яка підходить

для задачі, на яку він створюється. Навантаження процесору із різними конфігураціями показано на рисунку 5.2.

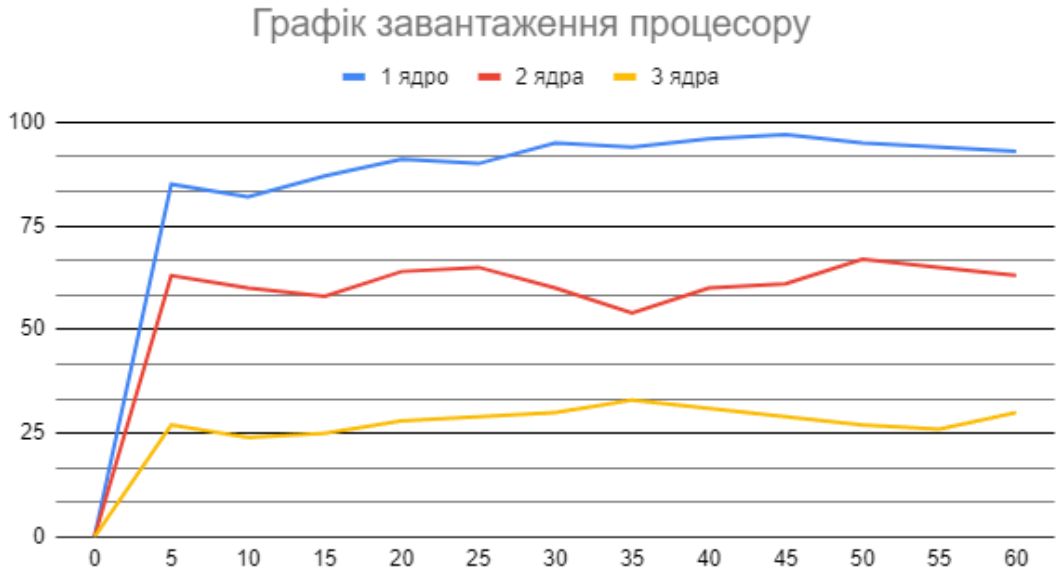

Рисунок 5.2 – Навантаження на систему із різною конфігурацією процесору

У ході проведення експерименту протягом хвилини було виявлено, що для оптимальної роботи системи серверу потрібно виділити 2 ядра процесору.

На відміну від 1-го ядра, яке працює на максимум та не зможе виконувати додаткові функції, 2 ядра показали найкращий результат, але 3 ядра є занадто надлишкові для системи і можуть призвести до простою необхідних потужностей.

Наступним експериментом є навантаження серверу для дослідження розподілення ресурсів оперативної пам’яті. На рисунку 5.3 показано роботу двох серверів з 24-ма гігабайтами ОЗП.

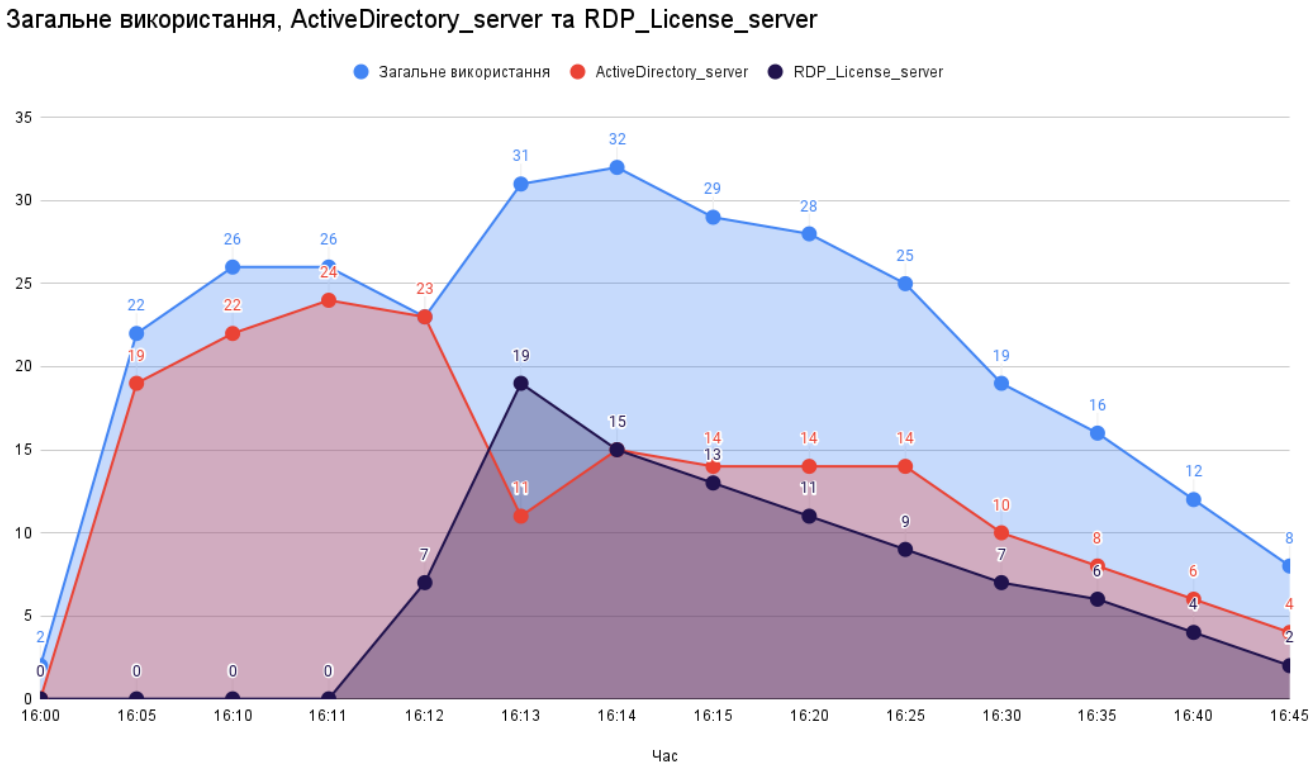

Рисунок 5.3 – Використання двох серверів із одночасно налаштованими 24-ма гігабайтами ОЗП

Сам гіпервізор виділяє на себе 2 гігабайти ОЗП, що можна побачити з початку графіку. Віртуальна машина з виділеними 24-ма гігабайтами ОЗП стартує і працює у звичному режимі. Якщо увімкнути другий сервер теж з виділеними 24-ма гігабайтами, то сервер не вимкнеться чи відмовиться запускати її, а розподілить використання під потреби системи.

Запустимо 3 сервери з конфігурацією по 16 гігабайт ОЗП. Результат експерименту показано на рисунку 5.4.

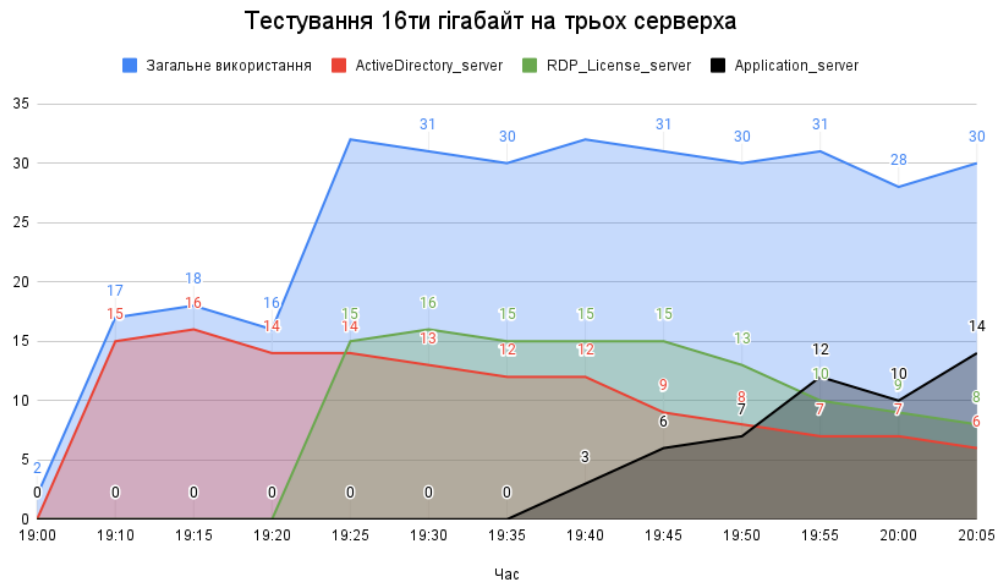

Рисунок 5.4 – Використання трьох серверів із 16ти гігабайтами ОЗП

Як зазначалось раніше, система сама розподілить ресурси на необхідні задачі. Сервер додатків виконує роль моніторингу за пристроєм СКУД і на графіку симулює активне використання під час проходу учнів.

5.4.3 Аналіз відповідності теоретичних та експериментальних досліджень

У ході виконання експерименту сформовано наступні технічні вимоги, представленні у таблиці 5.1. З цими характеристиками віртуальна інфраструктура буде виконувати усі поставлені задачі та забезпечувати достатню продуктивність.

Таблиця 5.1

Рекомендовані технічні характеристики

Назва серверу	Кількість ядер	Кількість ОЗП	Кількість місця на жорсткому диску
Data_server	2	8 Гб	240 Гб
Application_server	3	12 Гб	240 Гб
ActiveDirectory_server	1	4 Гб	120 Гб
RDP_License_server	2	4 Гб	120 Гб

5.4.4 Новизна результатів експерименту

У рамках досліджень була проведена серія експериментів, що спрямована на оцінку впливу конфігурації оперативної пам’яті та процесора на ефективність системи в різних умовах віртуального середовища.

Перший експеримент фокусувався на порівнянні різної конфігурації ядер процесора та їхнього впливу на загальну ефективність системи в умовах віртуального середовища. Виявлено, що оптимальна кількість ядер для роботи є 2 ядра.

Другий експеримент включав тестування роботи системи з різною конфігурацією ОЗП в умовах віртуального середовища. Результати показали, що ефективне розподілення обсягу пам’яті між віртуальними серверами впливає на їхню продуктивність, особливо при обмежених фізичних ресурсах.

Ці експерименти виокремлюються як новизна у визначенні оптимальних конфігурацій системи віртуального середовища. Отримані результати надають можливість подальшого практичного використання серверних ресурсів та можуть слугувати основою для подальших досліджень та вдосконалень у сфері оптимізації віртуальних інфраструктур.

5.5 Висновки до розділу

У розділі детально досліджено та проведено серію експериментів на тестування процесора серверу та оперативної пам’яті в різних сценаріях та конфігураціях. Результати демонструють стабільну працездатність обох компонентів під високим навантаженням та в різноманітних умовах експлуатації.

Основні висновки полягають у встановленні оптимальних умов для ефективної роботи процесора та операційної пам’яті. Здобуті відомості служитимуть базою для подальших оптимізацій та налаштувань серверної інфраструктури з метою забезпечення найвищого рівня продуктивності та стабільності у різних умовах експлуатації.

Цей розділ є ключовим у висвітленні результатів експериментів та надає важливий внесок у розумінні функціональності та можливостей серверної системи. Отримані висновки визначають перспективи подальших досліджень та покращень для оптимізації ресурсів та забезпечення найкращої продуктивності.

ВИСНОВКИ

Магістерська робота представляє собою завершену наукову працю, спрямовану на вирішення науково-практичної задачі контролю наявності учнів у школах міста Дніпро з використанням існуючої системи «Безпечна Школа». Застосування розроблених методів та моделей покликане підтримати обґрунтування та дослідження ефективності методів контролю:

1. Досліджено середу віртуального серверу для визначення можливостей інтеграції системи контролю управління доступом. Це дозволило виявити технологічні можливості вдосконалення системи через використання віртуалізації.

2. Дослідження особливостей різних систем контролю управління доступом дозволило вибрати оптимальний варіант ідентифікації, що враховує специфіку шкільного середовища та забезпечує ефективний контроль наявності учнів.

3. Проведений синтез на основі існуючої системи контролю у школі для обґрунтування можливого вдосконалення системи. Отримані результати під час синтезу визначають нові потреби, які сприятимуть підвищенню безпеки та ефективності відстеження наявності учнів у шкільних закладах.

4. Розроблено віртуальну інфраструктуру з декількох серверів, які покривають усі технічні запроси у школі та допоможуть ефективніше працювати із пристроями системи контролю управління доступом.

5. Проведені експерименти показали, що конфігурація, на якій проводилася розробка, відповідають нормам заданими у розділі синтезу системи. У результаті визначено технічні характеристики для кожної віртуальної машини.

6. Отримані результати мають практичне значення для шкільних установ міста Дніпро, оскільки впровадження запропонованих вдосконалень сприятиме покращенню безпеки та забезпечить ефективний контроль за доступом до різних ресурсів та приміщень. Таким чином, робота зробить свій внесок у розвиток сучасних систем контролю та безпеки в освітній сфері.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Віртуалізація сервера. *Глосарій VMware*. URL: https://www.vmware.com/topics/glossary/content/server-virtualization.html (дата звернення 10.10.2023)

2. Віртуалізація мережі. *Глосарій VMware*. URL: https://www.vmware.com/topics/glossary/content/network-virtualization (дата звернення 10.10.2023)

3. Santana G.A. Data Center Virtualization Fundamentals. 1st Edition. 2013. 929 p. URL: https://ptgmedia.pearsoncmg.com/images/9781587143243/samplepages/1587143240.pdf (дата звернення 11.10.2023)

4. Віртуалізація робочого столу. *Глосарій VMware.* URL: https://www.vmware.com/topics/glossary/content/desktop-virtualization (дата звернення 11.10.2023)

5. Віртуалізація додатків. *Глосарій VMware*. URL: https://www.vmware.com/topics/glossary/content/application-virtualization.html (дата звернення 11.10.2023)

6. Portnoy Matthew. Virtualization Essentials. 2nd Edition. 2016. 277 p. URL: https://docplayer.net/58601761-Virtualization-essentials.html (дата звернення 11.10.2023)

7. Віртуалізація 2.0 – короткий посібник. URL: https://www.tutorialspoint.com/virtualization2.0/virtualization2.0_quick_guide.htm (дата звернення 14.10.2023)

8. Різні типи віртуалізації. Дата публікації 16.12.2019. URL: https://server-shop.ua/ua/various-types-of-virtualization.html (дата звернення 14.10.2023)

9. Віртуальний сервер: переваги та недоліки. Дата публікації 05.11.2020. URL: https://tribun.com.ua/74440 (дата звернення 15.10.2023)

10. Що таке Citrix XenServer? Останнє оновлення 08.04.2023. URL: https://cloud.ibm.com/docs/virtualization?topic=virtualization-what-is-citrix-xenserver (дата звернення 16.10.2023)

11. Роуз Маргарет. Citrix XenApp. Дата публікації 22.01.2015. URL: https://www.techopedia.com/definition/31122/citrix-xenapp (дата звернення 16.10.2023)

12. Що таке Microsoft Hyper-V? URL: https://www.altaro.com/hyper-v/what-is-hyper-v/ (дата звернення 20.10.2023)

13. Що таке RDP? URL: https://www.ericom.com/glossary/what-is-rdp/ (дата звернення 21.10.2023)

14. Архітектура Серверу VMWARE ESX. Дата публікації 16.03.2019. URL: https://www.logicfinder.net/vmware-esx-server-architecture/ (дата звернення 23.10.2023)

15. VMware ESXi – що таке ESXi і які його функції? Дата публікації 22.06.2017. URL: https://www.theaccessgroup.com/en-gb/blog/chs-vmware-esxi-what-is-esxi-and-what-are-its-features/ (дата звернення 23.10.2023)

16. Архітектура VMware ESXi. URL: https://www.academia.edu/29429625/The_Architecture_of_VMware_ESXi (дата звернення 23.10.2023)

17. Що таке СКУД і як це працює? Дата публікації 23.03.2023. URL: https://idcard.com.ua/ua/blog/chto-takoe-skud-i-kak-eto-rabotaet/ (дата звернення 30.10.2023)

18. Що таке СКУД? Дата публікації 12.01.2022. URL: https://ohrana.ua/uk/stati-i-obzory/chto-takoe-skud.html (дата звернення 01.11.2023)

19. Вибір обладнання для системи контролю доступу. Дата публікації 19.06.2020. URL: https://habr.com/articles/507268/ (дата звернення 05.11.2023)

20. Що таке LDAP і як він працює? Дата останнього оновлення 15.09.2023. URL: https://www.okta.com/identity-101/what-is-ldap/ (дата звернення 05.11.2023)

21. Lee Brandon. Hypervisor Security Best Practices. Дата публікації 20.11.2019. URL: https://www.virtualizationhowto.com/2019/11/__trashed/ (дата звернення 05.11.2023)

22. Система «Безпечна школа» – переваги електронного сервісу для дітей, батьків та вчителів. Сайт Дніпровської міської ради. Дата публікації 17.08.2020.

URL: https://dniprorada.gov.ua/uk/articles/item/39837/sistema-bezpechna-shkola-perevagi-elektronnogo-servisu-dlya-ditej-batkiv-ta-vchiteliv (дата звернення 10.11.2023)

23. Модуль розпізнавання обличчя для турнікета. URL: https://viatec.ua/product/DS-K5671-ZU (дата звернення 10.11.2023)

24. Біометричний зчитувач ZKTeco F11. URL: https://securitylab.com.ua/zkteco-f11/ (дата звернення 11.11.2023)

25. Що таке система RFID, в чому її особливості використання. Дата публікації 07.10.2019. URL: https://idcard.com.ua/ua/blog/chto-takoe-sistema-rfid-v-chem-ee-osobennosti-ispolzovaniya/ (дата звернення 12.11.2023)

26. Gray K., Nadeau T. Network Function Virtualization. 1st Edition. Morgan Kaufmann. 2016. 270 p.

27. Ameen Radhwan Y., Hamo Asmaa Y. Survey of Server Virtualization. (*IJCSIS) International Journal of Computer Science and Information Security*. 2013. Vol.11. No. 3. URL: https://arxiv.org/ftp/arxiv/papers/1304/1304.3557.pdf (дата звернення 25.11.2023)

28. Цвіркун Л. І. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи магістра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, В.В. Гнатушенко, С.М. Ткаченко ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». Дніпро : НТУ «ДП», 2023. 43 с.

Додаток А

Текст програми інсталяції домену

804.02070743.23008-01 12 01

```
Import-Module ServerManager

# Установка ролі ActiveDirectory з усіма залежними компонентами

Add-WindowsFeature –Name AD-Domain-Services –IncludeAllSubFeature –
IncludeManagementTools

Import-Module ADDSDeployment

# Установка нового лісу

Install-ADDSForest `

-CreateDnsDelegation:$false `

# Шлях до бази даних NTDS

-DatabasePath "C:\Windows\NTDS" `

# Режим роботи домену

-DomainMode "WinThreshold" `

# Задавання імені домену

-DomainName "safednipro.com" `

# Налаштування NetBIOS імені

-DomainNetbiosName "SAFEDNIPRO" `

# Налаштування режиму роботи лісу

-ForestMode "WinThreshold" `

# Інсталяція DNS-серверу

-InstallDns:$true `

-LogPath "C:\Windows\NTDS" `

-NoRebootOnCompletion:$false `

-SysvolPath "C:\Windows\SYSVOL" `

-Force:$true
```