

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

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему:

«Проект комплексної системи мережевого доступу
та безпеки міської лікарні»

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

 Владислав КРАСОВСЬКИЙ

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

 Олексій ШЕЛУХА

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

 Олександр ПІРОГ

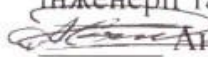
Житомир – 2025

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

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій ЄФІМЕНКО

3 березня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу бакалавра

Студент: Красовський Владислав Ігорович

Тема роботи: «Проект комплексної системи мережевого доступу та безпеки міської лікарні»

затверджена Наказом університету від 3 березня 2025 р. №79/с

Термін здачі студентом закінченої роботи 21 червня 2025 р.

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

- процес функціонування системи комплексного мережевого доступу лікарні та підсистеми відеоспостереження;
- методи та засоби проєктування та адміністрування комп'ютерних систем та мереж і систем відеоспостереження

Обладнання та програмне забезпечення:

1. Комутатор Cisco Catalyst 2960
2. Відеокамера Hikvision DS-2CD2323G2-IU
3. Мережевий емулятор GNS3, VirtualBox
4. Операційна система Windows Server 2019 з контролером домену
5. Операційна система Windows 10
6. Програмне забезпечення iVMS-4200

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

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Мельник І.І.	03.03.25	03.03.25
2	Мельник І.І.	05.03.25	05.03.25
3	Мельник І.І.	12.04.25	12.04.25

Студент В.Красовський Владислав КРАСОВСЬКИЙ

Керівник О.Шелуха Олексій ШЕЛУХА

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	03.03.2025	Виконано
2	Пошук, огляд та аналіз аналогічних розробок	08.04.2025	Виконано
3	Формулювання технічного завдання	12.04.2025	Виконано
4	Опрацювання літературних джерел	15.04.2025	Виконано
5	Проектування	12.05.2025	Виконано
6	Розгортання обладнання та налаштування системи захисту	28.05.2025	Виконано
7	Перевірка працездатності	08.06.2025	Виконано
8	Оформлення пояснювальної записки	13.06.2025	Виконано
9	Захист		

Студент В.Красовський Владислав КРАСОВСЬКИЙ

Керівник О.Шелуха Олексій ШЕЛУХА

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проект комплексної системи мережевого доступу та безпеки міської лікарні» присвячена розробці системи, що забезпечує надійне та безпечне функціонування мережевої інфраструктури та систем відеоспостереження в умовах медичного закладу. Пояснювальна записка складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

Текстова частина викладена на 60 сторінках друкованого тексту. Пояснювальна записка містить 1 додаток на 2 сторінках. Список використаних джерел містить 22 найменувань і займає 2 сторінки. В роботі наведено 83 рисунків, 10 таблиць. Загальний обсяг роботи - 75.

Метою є проектування безпечної системи, яка дозволяє централізовано керувати доступом, захищати чутливі дані та забезпечує безперебійну роботу. Для досягнення поставленої мети було визначено наступні завдання:

1. Провести аналіз сучасних технологій та рішень, для побудови комплексної системи мережевого доступу та безпеки;
2. Розробити проект мережевої інфраструктури та системи відеоспостереження;
3. Провести моделювання комплексної системи мережевого доступу та безпеки в умовах наближених до реальних;
4. Провести аналіз отриманих результатів та запропонувати напрямки подальшого розвитку.

В ході роботи було проведено налаштування мережевих пристроїв для забезпечення зв'язку та сегментації мережі; виконано розгортання Microsoft Active Directory, проведено налаштування контролерів домену, служб DHCP, DNS, RDS та створення користувачів і груп; виконано налаштування групових політик, впроваджено правила безпеки для користувачів та комп'ютерів; налагоджено системи відеоспостереження, виконано конфігурацію програмного забезпечення

					ККІКБ.КР.Б – 123 – 8 – ПЗ				
Зм.	Арк.	№ докум.	Підпис	Дата	Проект комплексної системи мережевого доступу та безпеки міської лікарні	Літ.	Арк.	Аркушів	
Розроб.		Красовський В.І.	<i>[підпис]</i>	12.06					
Керівник		Шелуха О.О.	<i>[підпис]</i>	12.06			4	75	
Реценз.		Пірог О.В.	<i>[підпис]</i>	12.06					
Н. контр.		Шелуха О.О.	<i>[підпис]</i>	12.06					
Затверд.		Сфіменко А.А.	<i>[підпис]</i>	12.06					
						ФІКТ, Гр. КІ-21-1			

та інтелектуальних функцій IP-камер, включаючи частину, реалізовану на реальному обладнанні, а також проведено тестування системи, перевірено працездатність всіх компонентів, коректність адресації та ефективність механізмів безпеки.

Проект також включає аналіз сучасних тенденцій у розвитку мережевих технологій та порівняння різних підходів до побудови захищених корпоративних мереж. Результати роботи показують, що запропонована система є високоефективною, надійною, відповідає поточним стандартам безпеки та має значний потенціал для подальшого розвитку та успішного впровадження у сучасних медичних закладах.

КЛЮЧОВІ СЛОВА: КОНТРОЛЕР ДОМЕНУ, МЕРЕЖЕВА ІНФРАСТРУКТУРА, МЕРЕЖЕВА БЕЗПЕКА, ВІДЕОСПОСТЕРЕЖЕННЯ, ВІДДАЛЕНИЙ ДОСТУП.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ANNOTATION

The qualification work on the topic "Project of a comprehensive network access and security system for a city hospital" is dedicated to the development of a system that ensures reliable and safe functioning of the network infrastructure and video surveillance systems in a medical institution. The explanatory note consists of an introduction, three sections, conclusions, a list of sources used and appendices.

The text part is set out on 60 pages of printed text. The explanatory note contains 1 appendix on 2 pages. The list of sources used contains 22 items and occupies 2 pages. The work contains 83 figures, 10 tables. The total volume of work is 75.

The goal is to design a secure system that allows centralized access management, protects sensitive data and ensures uninterrupted operation. To achieve the goal, the following tasks were defined:

1. To conduct an analysis of modern technologies and solutions for building a comprehensive network access and security system;
2. Develop a network infrastructure and video surveillance system project;
3. Conduct simulation of a comprehensive network access and security system in conditions close to real ones;
4. Analyze the results obtained and propose directions for further development.

During the work, network devices were configured to ensure communication and network segmentation; Microsoft Active Directory was deployed, domain controllers, DHCP, DNS, RDS services were configured, and users and groups were created; group policies were configured, security rules for users and computers were implemented; video surveillance systems were set up, software and intelligent functions of IP cameras were configured, including the part implemented on real equipment, and the system was tested, the operability of all components, correct addressing, and the effectiveness of security mechanisms were checked.

The project also includes an analysis of current trends in the development of network technologies and a comparison of different approaches to building secure corporate

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		6

networks. The results of the work show that the proposed system is highly efficient, reliable, meets current security standards and has significant potential for further development and successful implementation in modern medical institutions.

KEYWORDS: DOMAIN CONTROLLER, NETWORK INFRASTRUCTURE, NETWORK SECURITY, VIDEO SURVEILLANCE, REMOTE ACCESS.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	9
ВСТУП	10
РОЗДІЛ 1. ОГЛЯД ТЕХНОЛОГІЙ ТА ПРОТОКОЛИ ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖІ	12
1.1 Аналіз сучасних методів організації комп'ютерних мереж в медичних установах	12
1.2 Аналіз можливостей контролера домену Active Directory	15
1.3 Аналіз застосування систем відеоспостереження у медичних установах	17
1.4 Аналіз програмного забезпечення для управління відеоспостереженням ...	18
1.5 Постановка технічного завдання.....	20
Висновок до першого розділу	20
РОЗДІЛ 2. ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ.....	22
2.1 Обґрунтування вибору обладнання	22
2.2 Проектування топології комп'ютерної мережі міської лікарні.....	27
2.3 Розробка схеми адресації мережі	28
2.4 Розмежування доступу користувачів.....	33
Висновки до другого розділу.....	37
РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ	38
3.1 Налагодження мережевих пристроїв	38
3.2 Розгортання Microsoft Active Directory	42
3.3 Налагодження системи відеоспостереження	54
3.4 Тестування системи	61
3.5 Перспективи розвитку	66
Висновок до третього розділу	68
ВИСНОВКИ.....	69
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	71
ДОДАТКИ.....	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD - Active Directory

AD DS - Active Directory Domain Services

DHCP - Dynamic Host Configuration Protocol

DVR - Digital Video Recorder

GPO - Group Policy Object

NVR - Network Video Recorder

VMS - Video Management System

ПЗ – Програмне забезпечення

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Проектування та розробка сучасної, надійної та безпечної мережевої інфраструктури для медичних установ є надзвичайно актуальним завданням у контексті сучасних технологічних, соціальних та регуляторних вимог. Зростаюча цифровізація медичної галузі, що включає електронні медичні записи, інтегровані діагностичні системи та системи безпеки, вимагає створення мережевих рішень, здатних забезпечити швидкий, безперебійний та захищений доступ до критично важливих даних та сервісів.

Централізовані системи управління, такі як Microsoft Active Directory, спрощують адміністрування та забезпечують високий рівень безпеки завдяки автентифікації, груповим політикам. Інтеграція систем відеоспостереження з Active Directory є невід'ємною частиною фізичної безпеки та централізованого управління доступом.

Людство має значний досвід у проектуванні мереж, але сучасні реалії вимагають постійного вдосконалення для забезпечення стабільності та захищеності. Тому ця кваліфікаційна робота присвячена актуальній темі проектування комплексної мережевої інфраструктури для міської лікарні, що забезпечить якісну взаємодію з дотриманням вимог безпеки.

Метою кваліфікаційної роботи є розробка комплексної та безпечної системи мережевого доступу та відеоспостереження для міської лікарні. Ця система повинна забезпечити централізоване управління ресурсами, захист чутливих даних та високу доступність сервісів, враховуючи специфіку медичного середовища.

Об'єктом дослідження є процес проектування та впровадження інтегрованої системи мережевого доступу та безпеки в умовах медичної установи.

Предметом дослідження є сучасні технології, методи та засоби проектування, розробки та налагодження мережевої інфраструктури, Active Directory та систем відеоспостереження в медичних закладах.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				10
Змн.	Арк.	№ докум.	Підпис	Дата		

У роботі проаналізовано технології, розроблено архітектуру мережі, проведено моделювання та тестування системи в GNS3, підтвердивши її функціональність та ефективність для медичного закладу.

У процесі виконання кваліфікаційної роботи було розроблено проєкт комплексної системи мережевого доступу та безпеки міської лікарні. У межах цього проєкту особлива увага була приділена аналізу технологій, розробці архітектури мережі з підбором необхідного обладнання та схемою адресації. Частина, що стосується відеоспостереження, була реалізована та протестована на реальному обладнанні. Загалом, здійснено моделювання та тестування системи в середовищі GNS3. Розроблена система демонструє здатність задовольняти вимоги сучасного медичного закладу щодо мережевої інфраструктури та безпеки.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				11
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1. ОГЛЯД ТЕХНОЛОГІЙ ТА ПРОТОКОЛИ ДЛЯ ПРОЕКТУВАННЯ МЕРЕЖІ

1.1 Аналіз сучасних методів організації комп'ютерних мереж в медичних установах

У сучасному світі лікарні та інші медичні установи мають зростаючу потребу в надійних та безпечних інформаційних системах для обміну даними, керування доступом до медичних ресурсів та захисту чутливих персональних даних. Одним з основних аспектів для досягнення цього є ефективна організація мережі, яка забезпечить безпеку, надійність та швидкість доступу до ресурсів. Системи, що застосовуються в медичних установах для організації мережевого доступу, повинні відповідати кільком основним вимогам: захист від несанкціонованого доступу, надійність і висока доступність для користувачів, а також зручність управління для адміністраторів мережі [1],[2].

Для вирішення задачі централізованого керування та захисту локальної мережі лікарні існує безліч сучасних рішень. Вибір найбільш підходящої технології залежить від розміру медичної установи, специфіки її роботи, а також бюджету, виділеного на створення чи покращення мережі [3].

У лікарнях, як і в інших організаціях, можуть бути застосовані різні моделі організації мережі. Зазвичай мережі медичних установ поділяються на дві основні категорії:

Однорангові мережі (Peer-to-Peer) - у таких мережах кожен комп'ютер має рівний доступ до ресурсів, без централізованого контролю або серверного управління. Це означає, що всі пристрої в мережі мають однакові права та обов'язки. Однак однорангові мережі не є оптимальними для медичних установ, оскільки вони не можуть забезпечити належний рівень безпеки для чутливих даних, таких як медичні записи, і мають обмеження в масштабуванні при збільшенні кількості користувачів або пристроїв [4].

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				12
Змн.	Арк.	№ докум.	Підпис	Дата		

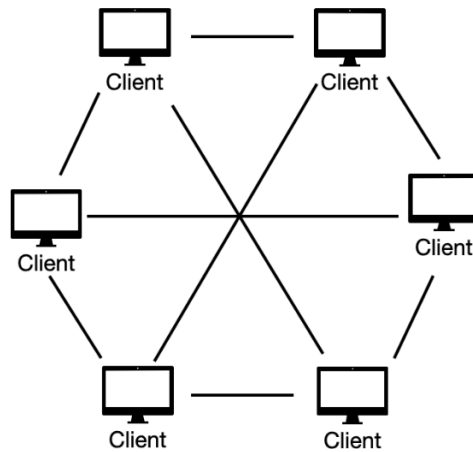


Рисунок 1.1 - Приклад однорангової мережі

Та мережі з виділеним сервером (Client-Server) - у таких мережах наявний один або кілька серверів, які надають свої ресурси для використання іншими пристроями мережі. Сервери здійснюють централізоване управління всіма ресурсами та інформацією, а також забезпечують безпеку і контроль доступу до медичних даних. Ця модель є набагато більш ефективною для медичних установ, оскільки дозволяє централізовано адмініструвати мережу, забезпечувати доступ до критично важливої інформації та впроваджувати політики безпеки [5],[1].

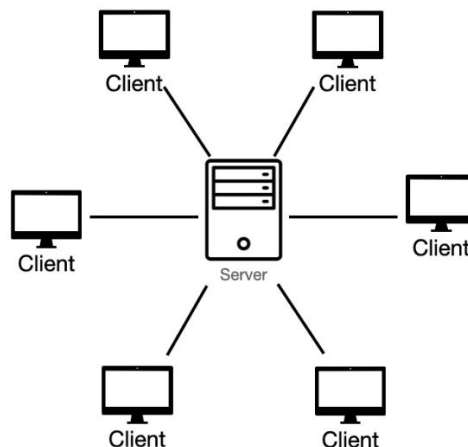


Рисунок 1.2 - Приклад мережі з виділеним сервером

Ці мережі мають свої бази даних пацієнтів, медичні зображення, лабораторні результати та інші чутливі документи, зберігаються на спеціально налаштованих серверах. Комп'ютери лікарів, медсестр, адміністративного персоналу підключаються до цих серверів для доступу до даних та спільного використання ресурсів.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

Сервери можуть бути налаштовані таким чином, щоб обмежувати доступ до різних типів інформації залежно від ролі користувача. Наприклад, лікарі мають доступ до повних медичних карт пацієнтів, а медсестри або адміністративний персонал - лише до обмежених даних. Це дозволяє забезпечити високий рівень безпеки та конфіденційності даних.

Перевагами мережі з виділеним сервером для медичних установ є централізація управління доступом. Один із головних аргументів на користь використання мереж з виділеним сервером - це можливість централізованого управління. Адміністратор може налаштовувати права доступу до ресурсів і даних лікарні для різних категорій користувачів, а також забезпечувати захист від несанкціонованого доступу.

Використання політик безпеки в умовах сучасної лікарні забезпечує максимальний захист медичних даних. В мережах з виділеним сервером можливе впровадження багатьох механізмів захисту, такий як:

- Шифрування переданих даних для захисту чутливих даних від перехоплення при передачі через мережу.

- Механізми автентифікації користувачів, що дозволяють додатково забезпечити безпеку доступу до чутливої інформації.

- Контроль за доступом до різних програмних продуктів чи баз даних, таких як електронні медичні карти, лабораторні системи, що дозволяє відслідковувати і обмежувати права доступу.

- Масштабованість, мережа може бути налаштована для підтримки великої кількості користувачів, що є важливим для лікарень з великою кількістю персоналу та пацієнтів. Такі мережі можуть масштабуватись в залежності від потреб установи додаючи нові сервери або робочі станції без значних змін в топології мережі.

- Надійність та безперебійна робота є основою таких систем, вони повинні бути налаштовані на автоматичне резервне копіювання даних, а також на захист від можливих збоїв у роботі системи. Це забезпечує безперебійний доступ до медичних даних навіть у разі технічних несправностей.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

- Управління та адміністрування у мережах з виділеним сервером може централізовано керуватися всіма аспектами мережі, від налаштування прав доступу до моніторингу безпеки. Це спрощує адміністративні завдання та дозволяє швидко реагувати на проблеми безпеки.

1.2 Аналіз можливостей контролера домену Active Directory

Найпопулярнішим рішенням для адміністрування різних систем є Active Directory [6]. Це служба каталогів, розроблена корпорацією Microsoft для організації централізованого управління доступом і ресурсами в комп'ютерних мережах, зокрема для підприємств та організацій. Вона є основною складовою Windows Server та дозволяє організовувати облік користувачів, пристроїв і інших ресурсів в межах однієї або кількох взаємопов'язаних мереж. А сам AD працює як централізована база даних, в якій зберігається інформація про користувачів, комп'ютери, принтери, сервери та інші об'єкти в мережі. Всі ці об'єкти організовуються в ієрархічну структуру, що дозволяє ефективно керувати доступом до ресурсів і підтримувати політики безпеки.

Мета використання Active Directory - це забезпечення централізованого управління в мережі для спрощення адміністрування, підвищення безпеки і зручності доступу до інформаційних ресурсів. За допомогою AD адміністратор може створювати облікові записи користувачів, групи користувачів, політики безпеки, налаштовувати доступ до файлів і інших мережевих ресурсів, а також організовувати зручну аутентифікацію та авторизацію для користувачів [7].

Основні компоненти та можливості Active Directory:

- Active Directory Domain Services
- Group Policy Management
- Реплікація
- Active Directory Users and Computer

Active Directory Domain Services - це основний компонент, який відповідає за зберігання і управління інформацією про об'єкти в мережі. Всі об'єкти, такі як користувачі, комп'ютери, принтери, групи тощо, зберігаються в базі даних AD DS.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

Контролери домену - це сервери, які містять і обробляють інформацію з AD, що дозволяє адмініструвати доступ до ресурсів мережі [8].

Group Policy Management - це інструмент, який дозволяє адміністратору визначати і застосовувати правила для користувачів і комп'ютерів у мережі, наприклад, обмеження доступу до певних програм, налаштування паролів і багато іншого [9].

Реплікація – це механізм, який дозволяє синхронізувати дані між контролерами доменів для забезпечення їх актуальності і надійності в мережі. Це дозволяє забезпечити високий рівень доступності інформації та безперервність роботи навіть у разі відмови одного з серверів [10].

Групи та ролі користувачів в AD можуть бути об'єднані в групи з різними рівнями доступу до ресурсів. Це дозволяє адміністратору централізовано керувати правами користувачів на доступ до файлів, принтерів, програм тощо.

Ієрархічна структура – це об'єкти в AD організовані у вигляді деревної структури, що складається з доменів, піддоменів і організаційних одиниць, що полегшує управління об'єктами та розподіл обов'язків між адміністраторами [11].

Переваги Active Directory:

- Централізоване управління
- Покращена безпека
- Масштабованість
- Інтеграція з іншими сервісами
- Гнучкість

В різних організаціях, AD дозволяє централізовано керувати численними обліковими записами персоналу, забезпечувати доступ до різних медичних і адміністративних систем, а також гарантувати безпеку даних.

Для забезпечення високої безпеки важливо налаштувати Group Policy для всіх комп'ютерів і користувачів, що дозволяє застосовувати стандартизовані політики щодо захисту паролів, управління обліковими записами та контролю доступу. Це дозволяє медичним установам відповідати вимогам конфіденційності та захисту персональних даних пацієнтів.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				16
Змн.	Арк.	№ докум.	Підпис	Дата		

1.3 Аналіз застосування систем відеоспостереження у медичних установах

У сучасних медичних установах зростає потреба не лише в забезпеченні надійної інфраструктурної мережі, але й з необхідністю забезпечення фізичної безпеки, які забезпечують контроль за пацієнтами, персоналом, відвідувачами, обладнанням та критично важливими зонами. У зв'язку з цим зростає роль систем відеоспостереження, як одного з ключових елементів комплексної системи безпеки медичних закладів.

Системи відеоспостереження дозволяють здійснювати моніторинг усіх ключових зон закладу в режимі реального часу, фіксувати події, зберігати їх у відеоархів та використовувати їх, як доказову базу у випадку правопорушень, інцидентів або внутрішніх розслідувань. У лікарнях вони є особливо важливими через наявність цінного обладнання, контролю доступу до закритих зон, а також необхідності контролю поведінки персоналу та пацієнтів.

Основними завданнями відеоспостереження в лікарні виступає:

- Контроль за периметром
- Контроль за відвідувачами та персоналом
- Запобігання крадіжкам та вандалізму.

Камери є основним компонентом будь-якої системи. Вони можуть бути аналоговими або цифровими. У сучасних системах перевага надається цифровим IP-камерам через високу якість зображення, легкість інтеграції в мережеву інфраструктуру та підтримку корисних функцій, таких як виявлення руху, розпізнавання облич, підрахунок людей тощо [12].

Наступною складовою є відеореєстратор, він є центральним елементом системи, який відповідає за прийом, запис, зберігання та управління відеоматеріалом з камер. Відеореєстратори є двох видів: Network Video Recorder та Digital Video Recorder, NVR використовується з сучасними IP-камерами, а DVR з аналоговими. Переважна кількість сучасних систем базуються саме на системах з використанням NVR, оскільки вони краще інтегруються до вже існуючої інфраструктури мережі [12].

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				17
Змн.	Арк.	№ докум.	Підпис	Дата		

Функції NVR:

- Прийом та обробка відео
- Зберігання відеоматеріалу
- Автономна робота
- Віддалений доступ та управління
- Резервування та перезапис
- Інтеграція з програмним забезпеченням

Коротко розглянемо їх, NVR здійснює прийом стисненого відеопотоку з камер та здійснює його декомпресію та запис на внутрішній або зовнішній носій. Також є підтримка до зовнішніх систем зберігання NAS. Відеореєстратори по суті є спеціалізованими комп'ютерами з власною операційною системою, що дозволяє їм працювати автономно, забезпечуючи запис, перегляд у реальному часі, пошук по архіву та віддалений доступ без необхідності постійного підключення до комп'ютеру. Реєстратори можуть працювати як автономно, так і бути інтегровані в масштабні VMS, що дозволяє централізовано керувати великою кількістю камер та реєстраторів[13].

Додатковим елементом може виступати комутатор, при умові якщо NVR не має роз'ємів для підключення камер, бажано, щоб комутатор мав підтримку технології Power over Ethernet, для забезпечення живлення камер по витій парі, що буде нівелювати місце встановлення камер.

1.4 Аналіз програмного забезпечення для управління відеоспостереженням

Video Management System – це програмна платформа, яка є "мозком" комплексної системи відеоспостереження. Вона дозволяє централізовано управляти всіма її компонентами, незалежно від їхньої кількості. VMS може бути встановлена на спеціалізованому сервері або потужному комп'ютері, забезпечуючи високу гнучкість та масштабованість[14].

Основні функції VMS включають централізоване управління камерами, що дозволяє додавати, налаштовувати та контролювати велику кількість IP-камер та

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				18
Змн.	Арк.	№ докум.	Підпис	Дата		

NVR, навіть якщо вони від різних виробників, завдяки підтримці стандарту ONVIF [14]. Система забезпечує перегляд відео в реальному часі та з архіву, надаючи можливість одночасного моніторингу з кількох камер на одному екрані, а також зручний пошук та перегляд записів за датою, часом, подією або зоною.

Управління записами в VMS дозволяє налаштовувати графіки запису, керувати якістю запису, компресією та ефективним збереженням даних на дискових масивах. Багато сучасних VMS інтегрують модулі відеоаналітики, які автоматично виявляють важливі події, такі як перетин ліній, вторгнення в зону чи поява залишених предметів, та генерують сповіщення для оператора [15]. Це суттєво підвищує ефективність моніторингу, дозволяючи автоматизувати рутинні завдання та оперативно реагувати на потенційні загрози.

Особливо важливою для лікарні є функція управління користувачами та правами доступу. VMS дозволяє створювати облікові записи для операторів, адміністраторів та інших користувачів, розмежовуючи їхні права доступу до камер, функцій та архіву, що є критично важливим для безпеки даних і конфіденційності пацієнтів. Однією з ключових переваг сучасних VMS є можливість інтеграції з AD. Це забезпечує централізовану автентифікацію, дозволяючи користувачам системи відеоспостереження використовувати свої існуючі облікові записи AD для входу у VMS. Це спрощує управління обліковими записами, усуваючи необхідність створення окремих логінів та паролів. Крім того, управління правами на основі груп дозволяє призначати доступ до певних камер, функцій чи архівів не окремим користувачам, а групам AD. Це значно спрощує адміністрування: достатньо додати нового співробітника до відповідної групи в AD, і він автоматично отримає потрібні права у VMS. Інтеграція з AD також дозволяє застосовувати єдину політику безпеки, наприклад вимоги до складності паролів, терміну дії облікових записів до всіх систем, включаючи відеоспостереження [16].

Також VMS часто інтегруються з іншими системами безпеки, такими як система контролю і управління доступом, пожежна сигналізація та охоронна сигналізація. Це дозволяє автоматично запускати запис з камер при спрацюванні датчиків або відкритті дверей, надаючи повну картину події та сприяючи швидкому

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

реагуванню. Також модулі звітів та журналювання у VMS ведуть докладні записи всіх подій, хто і коли переглядав відео, які налаштування змінювалися, спрацювання аналітики, що є надзвичайно важливим для аудиту, проведення розслідувань та забезпечення відповідності регуляторним вимогам.

1.5 Постановка технічного завдання

Для успішної реалізації проєкту комплексної системи мережевого доступу та безпеки міської лікарні необхідно визначити основні технічні вимоги та характеристики, які забезпечать функціональність та ефективність системи. Це включає проєктування мережевої та програмної частин, забезпечення зручності користування, безпеки та надійності роботи системи.

Основною метою проєкту є створення інтегрованої, надійної та безпечної комплексної системи мережевого доступу та відеоспостереження для міської лікарні.

Для досягнення поставленої мети було визначено наступні завдання:

1. Провести аналіз сучасних технологій та рішень, для побудови комплексної системи мережевого доступу та безпеки;
2. Розробити проєкт мережевої інфраструктури та системи відеоспостереження;
3. Провести моделювання комплексної системи мережевого доступу та безпеки в умовах наближених до реальних;
4. Провести аналіз отриманих результатів та запропонувати напрямки подальшого розвитку.

Задане технічне завдання забезпечить створення ефективної, надійної та безпечної комплексної системи мережевого доступу та відеоспостереження для міської лікарні, яка відповідає сучасним вимогам медичних установ.

Висновок до першого розділу

У цьому розділі ми дослідили ключові аспекти комплексної системи мережевого доступу та безпеки міської лікарні. Було обґрунтовано вибір клієнт-

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

серверної мережі. Особливу увагу приділено AD як центральному рішенню для управління користувачами та мережевими об'єктами. Також ми розглянули системи відеоспостереження, їхні основні компоненти та можливості VMS. Наголошено на важливості інтеграції VMS з AD для централізованого управління доступом до відеоархівів.

В ході роботи також було визначено технічне завдання проєкту. Було виявлено, що комплексна система повинна забезпечувати інтегроване, надійне та безпечне управління мережовим доступом та відеоспостереженням, захист чутливих даних, високу доступність сервісів та можливість масштабування.

Цей розділ став основою для подальшого проєктування та реалізації комплексної системи мережевого доступу та безпеки міської лікарні, яка відповідає визначеним вимогам та стандартам, враховуючи специфіку медичного середовища.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				21
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2. ПРОЕКТУВАННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА РОЗРОБКА СИСТЕМИ АДРЕСАЦІЇ

2.1 Обґрунтування вибору обладнання

Для побудови надійної та сучасної мережевої інфраструктури міської лікарні було ретельно підібрано мережеве обладнання, що відповідає високим вимогам до продуктивності, безпеки, масштабованості та зручності адміністрування.

Всі підприємства здійснюють свою діяльність, засновану на використанні мережевих функцій. Не секрет, що Інтернет та мережеві технології відіграють дуже важливу роль у розвитку індустрії. Всі працівники отримують або надсилають завдання через доступ до мережі. Однак метою проєкту є не тільки доступ до глобальної мережі, а й побудова корпоративної мережі вздовж магістралі, по якій передається потік інформації.

В якості маршрутизаторів для ключових вузлів мережі обираються сучасні, високопродуктивні платформи, здатні забезпечити високу пропускну здатність, розширені функції безпеки, підтримку програмно-визначених глобальних мереж та можливості віртуалізації, що є критично важливим для сучасних медичних установ [17]. Флагманською лінійкою для таких завдань є Cisco Catalyst 8000 Edge Platform (Рисунок 2.1). Ці маршрутизатори працюють під управлінням сучасної операційної системи Cisco IOS XE, яка надає розширені можливості для автоматизації, аналітики, інтеграції з хмарними сервісами та передові механізми безпеки, що дозволяють ефективно керувати великими обсягами медичного трафіку та захищати чутливі дані [17]. Їх модульна архітектура дозволяє гнучко адаптуватися до зростаючих потреб та забезпечувати високу доступність.



Рисунок 2.1 - Маршрутизатори Cisco Catalyst 8000 Edge Platform

Програмне забезпечення Cisco IOS XE - це сучасна модульна операційна

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

система, яка надає розширені мережеві послуги та підтримує широкий спектр мережевих застосунків [17]. Маршрутизатори Cisco Catalyst 8000 Edge Platform Family та інші сучасні мережеві пристрої Cisco працюють під управлінням цієї передової операційної системи. Cisco IOS XE забезпечує плавне та високоефективне з'єднання розрізнених носіїв і пристроїв за допомогою різноманітних протоколів, включаючи розширені можливості для SD-WAN та хмарних інтеграцій. Спеціалізовані програмні служби управління Cisco IOS XE надають потужні інструменти, необхідні для автоматизації, масштабування, забезпечення високої безпеки та підтримки складних сучасних мереж [17].

Для цілей нашого проєкту та моделювання, з огляду на їхню перевірену функціональність та репрезентативність традиційних маршрутизаторів у віртуальних середовищах, в якості маршрутизаторів ми будемо використовувати моделі Cisco 7200 Series, що використовують програмне забезпечення Cisco IOS v12.4 (Рисунок 2.2). Хоча це і є застаріле сімейство, воно дозволяє ефективно демонструвати принципи роботи маршрутизації, сегментації та ключових мережевих протоколів, які є універсальними.



Рисунок 2.2 - Маршрутизатор Cisco 7200 Series

Програмне забезпечення Cisco IOS - це платформа, що надає мережеві послуги та підтримує мережеві програми. Маршрутизатори та сервери доступу Cisco працюють під управлінням основного програмного забезпечення Cisco IOS. Програмне забезпечення Cisco IOS забезпечує плавне з'єднання розрізнених носіїв і пристроїв за допомогою різних протоколів. Спеціалізовані програмні служби управління Cisco IOS надають інструменти, необхідні для масштабування та підтримки вашої мережі [18].

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

Для комутаторів рівня доступу, що забезпечують підключення кінцевих пристроїв у мережі, обираються моделі, які пропонують оптимальне поєднання продуктивності, безпеки та економічності. Сучасним та надійним рішенням для цих завдань є Cisco Catalyst 1000 Series (Рисунок 2.3). Ці комутатори є ідеальним вибором для малих та середніх мереж, філій та розгортань, де важлива простота адміністрування та надійність. Вони забезпечують надійний доступ до мережі з можливостями другого рівня та підтримують базові функції безпеки, такі як 802.1X та Port Security, а також Power over Ethernet, що є важливим для живлення IP-телефонів та IP-камер [19].

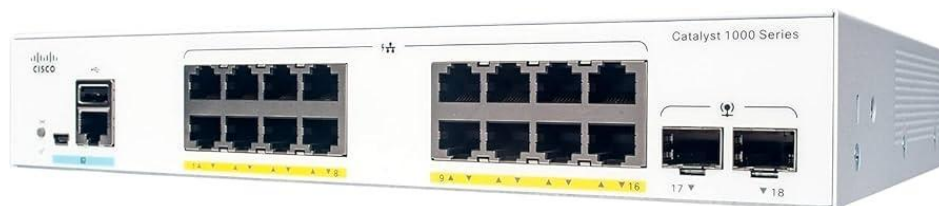


Рисунок 2.3 - Комутатор Cisco Catalyst 1000 Series

У нашому проєкті, для моделювання та практичної реалізації, в якості комутаторів рівня доступу ми будемо використовувати Cisco 2960 Series (Рисунок 2.4). Це комутатори, що зарекомендували себе як ефективне рішення для базових потреб мереж.



Рисунок 2.4 - Комутатор Cisco 2960 Series

Cisco 2960 Series - це комутатори рівня доступу, що забезпечують підключення кінцевих пристроїв у мережі. Він є бюджетним рішенням, яке ідеально підходить для малих та середніх мереж, де важливі безпека, продуктивність та зручність адміністрування. Він забезпечує надійний доступ до мережі з базовими можливостями другого рівня та підтримує функції, необхідні для сучасних корпоративних мереж.

У програмному середовищі GNS3 для моделювання маршрутизатора будемо використовувати образ c7200-adventerprisek9-mz.124-24.T2, а для комутатора образ

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

i86bi-linux-l2-adventerprisek9-15.2c. Для практичної частини під систему відеоспостереження будемо використовувати комутатор Cisco 2960 Series SI на 24 порти.

Для реалізації ефективної системи відеоспостереження у міській лікарні, яка має відповідати високим вимогам до безпеки, якості зображення та інтеграційних можливостей, було обрано IP-камеру Hikvision DS-2CD2323G2-IU (Рисунок 2.5).



Рисунок 2.5 - Камера Hikvision DS-2CD2323G2-IU

Цей вибір повністю обґрунтований низкою ключових переваг, що роблять її оптимальним рішенням для такого критично важливого об'єкта.

По-перше, камера Hikvision DS-2CD2323G2-IU забезпечує високу якість зображення з роздільною здатністю 2 мегапікселі з роздільною якістю 1920x1080. Це гарантує отримання чіткого та деталізованого відео, що є вкрай важливим для ідентифікації облич, номерних знаків, моніторингу рухів та фіксації найдрібніших деталей під час будь-яких інцидентів. Для медичної установи, де кожна деталь може мати вирішальне значення, така якість відео дозволяє ефективно розслідувати події та забезпечувати максимальну безпеку для персоналу та пацієнтів [20].

По-друге, однією з головних переваг цієї моделі є інтеграція технології Hikvision AcuSense. Ця технологія базується на алгоритмах глибокого навчання, що дозволяє камері надзвичайно точно розрізняти людей та транспортні засоби від інших об'єктів, таких як тварини, листя, опади чи світлові коливання. Це значно зменшує кількість хибних тривог, які є поширеною проблемою для багатьох систем відеоспостереження. У динамічному лікарняному середовищі,

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

де постійно присутні рухи та активність, AcuSense гарантує, що оператори отримуватимуть сповіщення лише про дійсно важливі події, що значно підвищує ефективність моніторингу та зменшує навантаження на службу безпеки. Камера підтримує такі важливі функції аналітики, як виявлення вторгнення, перетин лінії та виявлення облич, що може бути використано для певних цілей моніторингу, звісно, з дотриманням принципів приватності [21].

По-третє, камера оснащена вдосконаленою технологією EXIR 2.0 та потужним ІЧ-підсвічуванням з дальністю до 30 метрів. Це забезпечує виняткову якість зображення в умовах низької освітленості або навіть повної темряви, що є надзвичайно важливим для цілодобового спостереження за всією територією лікарні, її паркінгами, входами/виходами та внутрішніми коридорами, особливо в неробочий час. Технологія EXIR 2.0 гарантує рівномірне ІЧ-освітлення без так званих "гарячих точок", що значно покращує загальну якість нічного відео [20].

По-четверте, наявність підтримки Power over Ethernet значно спрощує та суттєво здешевлює процес монтажу та інсталяції камери. Дані та живлення передаються по одному мережевому кабелю, що усуває необхідність прокладання окремих кабелів живлення та пошуку розеток поблизу місця встановлення камери. Для такої великої будівлі, як лікарня, це дозволяє значно скоротити час та витрати на розгортання та обслуговування системи [22].

По-п'яте, камера вирізняється високою стійкістю до зовнішніх впливів та вандалізму. Вона має високий ступінь захисту від пилу та вологи за стандартом IP67, що дозволяє її надійне використання як у приміщеннях, так і на вулиці. На додаток, антивандальний корпус за стандартом IK10 забезпечує надійний захист від механічних пошкоджень, що є особливо важливим у громадських місцях, де існує ризик навмисного пошкодження обладнання [22].

І, нарешті, камера Hikvision DS-2CD2323G2-IU підтримує відкритий стандарт ONVIF. Це гарантує її сумісність з широким спектром сторонніх систем VMS, включаючи ті, що інтегровані з AD. Така сумісність забезпечує неабияку гнучкість у виборі програмного забезпечення та дозволяє легко інтегрувати її в існуючу або майбутню комплексну систему безпеки медичного закладу.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Враховуючи всі вищезазначені аргументи, вибір IP-камери Hikvision DS-2CD2323G2-IU є повністю обґрунтованим і відповідає високим вимогам, що пред'являються до сучасної системи відеоспостереження у медичній установі. Ця камера забезпечить надійний моніторинг, ефективну аналітику та простоту інтеграції, що є ключовим для функціонування комплексної системи безпеки лікарні.

2.2 Проектування топології комп'ютерної мережі міської лікарні

Тепер, коли ми визначили обладнання, з яким будемо працювати, ми можемо розробити топологію нашої мережі. Важливо врахувати, що міська лікарня, для якої проектується система, складається з трьох окремих будівель, і мережева інфраструктура розгортається з урахуванням цього розподілу, забезпечуючи зв'язок та функціональність по всьому комплексу.

Почнемо з першої будівлі. В ній ми маємо два сервери, робочу станцію для адміністратора, комутатор, до якого все приєднано, маршрутизатор та комутатор під систему відеонагляду. Далі ми маємо Mikrotik, який слугує бар'єром між нашою корпоративною мережею та доступом до глобальної мережі. Ключовим елементом є маршрутизатор R-Main-Building, який сполучає маршрутизатори в цій будівлі і слугує транспортним вузлом для нашої мережі, що сполучає інші будівлі між собою.

Далі, розглянемо другу будівлю. В ній ми маємо 2 маршрутизатори, так як будівля величезна, вони розміщені в протилежних частинах для легшого доступу та адміністрування мережі. До них приєднано по два комутатори, які виконують роль масштабування мережі. У свою чергу, до них під'єднані робочі станції персоналу.

Остання, третя будівля, має свій маршрутизатор та комутатор, до якого приєднані робочі станції. Ця структура забезпечує необхідний рівень мережевого доступу та безпеки для кожної з трьох будівель лікарні, а також ефективну взаємодію між ними.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		27

На Рисунку 2.6 наведено зображення топології спроектованої мережі міської лікарні. Жовтим кольором на ній виділено будівлі закладу, тоді як синім кольором позначено серверну кімнату. Слід зазначити, що компоненти Switch-CCTV та CCTV-1 представляють собою реальне обладнання, використане для практичної частини проєкту.

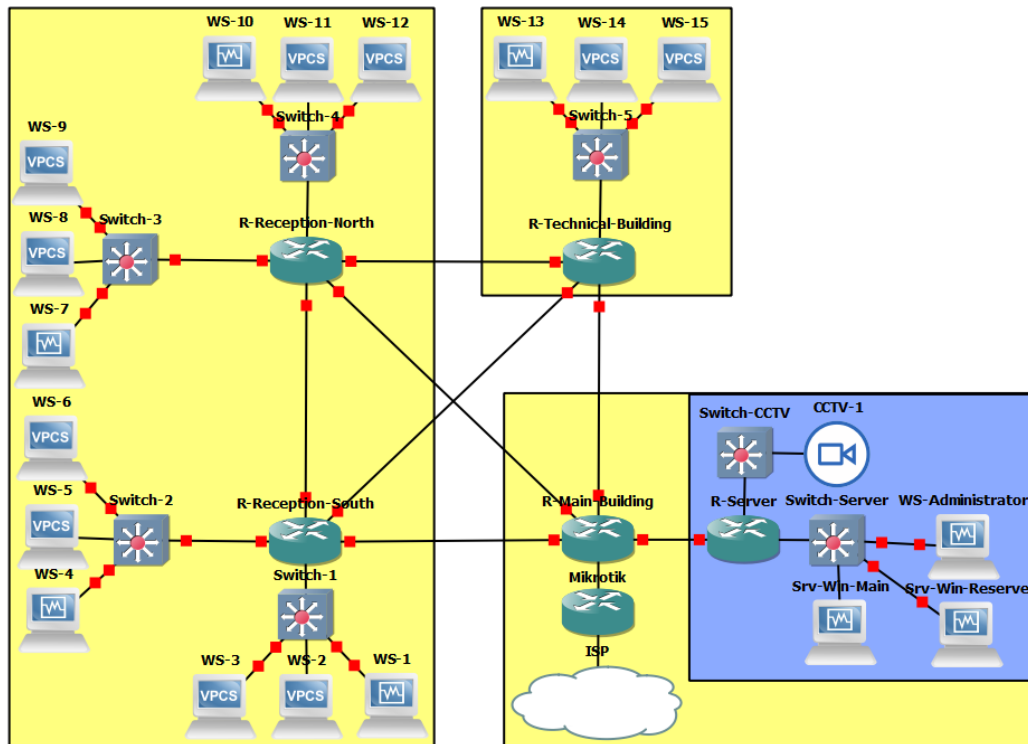


Рисунок 2.6 Топологія мережі

2.3 Розробка схеми адресації мережі

Почнемо з кінцевих пристроїв, тобто з робочих станцій, вони будуть отримувати динамічні IP-адреси за допомогою протоколу DHCP з пулу адрес, які ми створимо на контролері домену. Далі основний та резервний контролери домену будуть мати статичну IP-адресу, як і всі маршрутизатори та комутатори.

Dynamic Host Configuration Protocol - це мережевий протокол, що автоматично надає IP-адреси та іншу необхідну конфігураційну інформацію, таку як маска підмережі, шлюз за замовчуванням та адреси DNS-серверів, пристроям у комп'ютерній мережі. Він працює за моделлю "клієнт-сервер", де DHCP-сервер керує пулом доступних IP-адрес і видає їх клієнтам на певний термін оренди. Це значно спрощує адміністрування мережі, усуваючи потребу в ручному

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				28
Змн.	Арк.	№ докум.	Підпис	Дата		

налаштуванні кожного окремого пристрою та запобігаючи конфліктам IP-адрес.

До складу Windows Server входить DHCP-сервер, це додаткова роль мережевого сервера, що дозволяє автоматично призначати IP-адреси та іншу конфігураційну інформацію DHCP-клієнтам у мережі. Ця функція є невід'ємною частиною Windows Server, а клієнт DHCP входить до складу всіх операційних систем Windows та увімкнений за замовчуванням. Розгортання DHCP-сервера на Windows Server забезпечує централізоване, надійне та кероване рішення для динамічної конфігурації IP-адрес у нашій мережі.

Для легшого розуміння адресації між пристроями поділимо нашу схему на мережі, наприклад A,B,C,D,E та E та дамо їх для наших пулів. Розпочнемо з маршрутизаторів, вони мають статичні IP-адреси (Таблиця 2.1).

Таблиця 2.1

Параметри IP-адресації маршрутизаторів

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Маршрутизатор R-Main-Building	G0/0	5.0.0.2	255.255.255.252	/30
	G1/0	40.0.0.2	255.255.255.252	/30
	G2/0	35.0.0.2	255.255.255.252	/30
	G3/0	25.0.0.1	255.255.255.252	/30
	G4/0	10.0.0.2	255.255.255.252	/30
Маршрутизатор R-Reception-South	G0/0	194.21.8.1	255.255.255.224	/27
	G1/0	195.21.8.1	255.255.255.224	/27
	G2/0	30.0.0.1	255.255.255.252	/30
	G3/0	15.0.0.1	255.255.255.252	/30
	G4/0	10.0.0.1	255.255.255.252	/30
Маршрутизатор R-Reception-North	G0/0	197.21.8.1	255.255.255.224	/27
	G1/0	196.21.8.1	255.255.255.224	/27
	G2/0	35.0.0.1	255.255.255.252	/30
	G3/0	15.0.0.2	255.255.255.252	/30
	G4/0	20.0.0.1	255.255.255.252	/30

Продовження таблиці 2.1

Маршрутизатор R-Technical-Building	G0/0	198.21.8.1	255.255.255.224	/27
	G2/0	30.0.0.2	255.255.255.252	/30
	G3/0	25.0.0.2	255.255.255.252	/30
	G4/0	20.0.0.2	255.255.255.252	/30
Маршрутизатор R-Server	G0/0	192.168.0.58	255.255.255.0	/24
	G1/0	40.0.0.1	255.255.255.252	/30
	G2/0	193.21.8.1	255.255.255.224	/27
Маршрутизатор Mikrotik	G0/0	5.0.0.1	255.255.255.252	/30
	G1/0	DHCP		

Після налаштування статичних IP-адрес на маршрутизаторах, переходимо до розгляду підмереж, які обслуговують окремі сегменти мережі. Кожна мережа має свій окремий діапазон IP-адрес і підключення до відповідного комутатора та кінцевих пристроїв.

Мережа А - одна з найважливіших частин, оскільки тут знаходяться контролери доменів, робоча станція адміністратора та камери (Таблиця 2.2).

Таблиця 2.2

Параметри IP-адресації мережі А

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Мережа А		193.21.8.0	255.255.255.224	/27
Комутатор Switch-Server	Інтерфейс Vlan1	193.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1	-	-
Комутатор Switch-CCTV	Інтерфейс Vlan1	192.168.0.57	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1		
Сервер Srv-Win-Main	Мережний адаптер	193.21.8.3	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1	-	-
Сервер Srv-Win-Reserve	Мережний адаптер	193.21.8.4	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1	-	-
WS-Administrator	Мережний адаптер	DHCP		
CCTV-1	Мережний адаптер	192.168.0.56	255.255.255.0	/24

Наступною розглянемо мережу В, яка охоплює робочі станції в одній із адміністративних зон (Таблиця 2.3).

Таблиця 2.3

Параметри IP-адресації мережі В

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Мережа В		194.21.8.0	255.255.255.224	/27
Комутатор Switch-1	Інтерфейс Vlan1	194.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	194.21.8.1	-	-
WS-1	Мережний адаптер	DHCP		
WS-2	Мережний адаптер	DHCP		
WS-3	Мережний адаптер	DHCP		

Мережа С подібно до мережі В, містить ще одну групу користувачів, але вже в іншому крилі приміщення (Таблиця 2.4).

Таблиця 2.4

Параметри IP-адресації мережі С

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Мережа С		195.21.8.0	255.255.255.224	/27
Комутатор Switch-2	Інтерфейс Vlan1	195.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	195.21.8.1	-	-
WS-4	Мережний адаптер	DHCP		
WS-5	Мережний адаптер	DHCP		
WS-6	Мережний адаптер	DHCP		

Мережа D - сегментована під ще одну групу працівників, які мають свої окремі ресурси (Таблиця 2.5).

Таблиця 2.5

Параметри IP-адресації мережі D

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Мережа D		196.21.8.0	255.255.255.224	/27
Комутатор Switch-3	Інтерфейс Vlan1	196.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	196.21.8.1	-	-
WS-7	Мережний адаптер	DHCP		
WS-8	Мережний адаптер	DHCP		
WS-9	Мережний адаптер	DHCP		

Мережа E - виділена для інших підрозділів медичного закладу, з дотриманням тієї ж схеми адресації (Таблиця 2.6).

Таблиця 2.6

Параметри IP-адресації мережі E

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Мережа E		197.21.8.0	255.255.255.224	/27
Комутатор Switch-4	Інтерфейс Vlan1	197.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	197.21.8.1	-	-
WS-10	Мережний адаптер	DHCP		
WS-11	Мережний адаптер	DHCP		
WS-12	Мережний адаптер	DHCP		

Мережа F - завершує логічний розподіл мережі і містить останню групу робочих станцій (Таблиця 2.7).

Таблиця 2.7

Параметри IP-адресації мережі F

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Мережа F		198.21.8.0	255.255.255.224	/27

Комутатор Switch-5	Інтерфейс Vlan1	198.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	198.21.8.1	-	-
WS-13	Мережний адаптер	DHCP		
WS-14	Мережний адаптер	DHCP		
WS-15	Мережний адаптер	DHCP		

Таким чином, було здійснено повну IP-адресацію всіх сегментів мережі, включаючи маршрутизатори, комутатори, сервери, робочі станції та інші мережеві пристрої. Для кожної мережі визначено окремий пул адрес із відповідними шлюзами та параметрами маски підмережі. Усі IP-адреси були розподілені згідно з логічною схемою, що забезпечує простоту масштабування, адміністрування та подальшої підтримки мережевої інфраструктури.

Зведену таблицю з усіма параметрами IP-адресації наведено в Додатку А.

2.4 Розмежування доступу користувачів

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

Group Policy Object - це віртуальна колекція параметрів політики. Вона має унікальне ім'я, наприклад GUID [99].

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

У Таблиці 2.8 наведено список користувачів, їх приналежність до відділу та роль яку вони виконують на підприємстві. Це означає, що під час реалізації структури домену, потрібно буде враховувати значимість кожного з користувачів,

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				33
Змн.	Арк.	№ докум.	Підпис	Дата		

якщо конкретніше то користувачів відділу IT Staff, котрі виконують найголовнішу роль у середовищі домену.

Таблиця 2.8

Користувачі та відділи домену

Користувач	Відділ
Anton Nesterenko	Doctors
Artem Martynuk	Doctors
Artem Marchenko	Doctors
Bogdan Kolosovsky	Doctors
Lidia Dovzhenko	Doctors
Oleg Kolesnikov	Doctors
Tatiana Eysmond	Doctors
Viktor Tatura	Doctors
Viktoria Morets	Doctors
Vitaliy Primasyk	Doctors
Valentyn Byrilko	IT Staff
Vlad Krasovsky	IT Staff
Maksim Gustov	Nurses
Evgen Vygovskyi	Nurses
Nikita Juzmar	Nurses
Volodar Osinskyi	Nurses

Розмежування доступу змодельовано таким чином, аби користувачі мали змогу виконувати локальний вхід лише на робочих станціях свого відділу. Виключенням є системні адміністратори, які управляють контролерами домену, робочими станціями та мережевим обладнанням. Відповідно до розмежування мають бути створені OU для розміщення кожного з відділів підприємства з

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				34
Змн.	Арк.	№ докум.	Підпис	Дата		

розподілом користувачів у них.

У Таблиці 2.9 детальніше продемонстровано як буде розмежовано доступ між користувачами домену.

Таблиця 2.9

Доступ користувачів всередині домену

	Системний адміністратор	Користувач департаменту
Власний департамент	+	+
Інший департамент	+	-
Мережеві пристрої	+	-

З цього випливає, що звичайним користувачам домену необхідно обмежити доступ до певних функцій на робочих станціях, задля захисту від неправомірних дій.

Таблиця 2.10

Заборони користувачам

	Системний адміністратор	Користувач департаменту
Використання USB-накопичувачів	+	-
Доступ до панелі управління	+	-
Доступ до налаштувань	+	-
Доступ до Powershell/cmd	+	-
Встановлення ПЗ	+	-
Обмеження до певного ПЗ	-	+

Обґрунтуємо важливість розмежування доступу користувачів для медичної установи:

Використання USB-накопичувачів. Заборона використання USB-накопичувачів для звичайних користувачів є критично важливим заходом безпеки. Флешки

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				35
Змн.	Арк.	№ докум.	Підпис	Дата		

можуть бути джерелом шкідливого програмного забезпечення, а також засобом не-санкціонованого витоку конфіденційних медичних даних. Системні адміністратори можуть мати доступ до них для виконання службових завдань, але з суворим дотриманням політик безпеки.

Доступ до Панелі управління та налаштувань системи. Обмеження доступу до Панелі управління та системних налаштувань для рядових користувачів запобігає ненавмисним або навмисним змінам, які можуть призвести до порушення стабільності роботи системи, конфліктів у програмному забезпеченні або зниження рівня безпеки. Лише адміністратори, які розуміють наслідки таких змін, повинні мати повний контроль до них.

Доступ до Powershell/cmd Командний рядок надає потужні можливості для управління системою, включаючи запуск скриптів, зміну конфігурацій та доступ до системних файлів. Заборона доступу до цих інструментів для користувачів департаментів мінімізує ризик виконання шкідливих команд, несанкціонованих дій або спроб обійти встановлені політики безпеки.

Встановлення ПЗ. Дозвіл на встановлення ПЗ лише системним адміністраторам гарантує, що на корпоративних комп'ютерах використовується лише ліцензійне та перевірене програмне забезпечення. Це запобігає встановленню шкідливих програм, несанкціонованого ПЗ, яке може створювати вразливості, або програм, що не відповідають внутрішнім стандартам лікарні.

Обмеження до певного ПЗ. Це означає, що користувачі департаменту можуть мати обмежений доступ до певних програм, або ж їм дозволено використовувати лише визначений набір ПЗ, необхідного для виконання їхніх службових обов'язків. Таке обмеження зменшує площу для атаки, мінімізує ризик використання несанкціонованих програм та підвищує продуктивність, оскільки користувачі зосереджені на виконанні своїх прямих завдань.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Висновки до другого розділу

У цьому розділі ми детально розглянули ключові аспекти проєктування комплексної мережевої інфраструктури для міської лікарні. Було обґрунтовано вибір надійного мережевого обладнання: визначено сучасні флагманські маршрутизатори Cisco Catalyst 8000 Edge Platform Family та комутатори Cisco Catalyst 1000 Series, як актуальні рішення для даної інфраструктури. При цьому, для цілей моделювання та демонстрації принципів роботи мережі, було обґрунтовано використання маршрутизаторів Cisco 7200 Series та комутаторів Cisco 2960 Series SI. Також було обґрунтовано вибір спеціалізованої IP-камери Hikvision DS-2CD2323G2-IU, що відповідає високим вимогам до відеоспостереження у медичному закладі.

Ми розробили логічну топологію мережі, враховуючи її розподіл по трьох окремих будівлях лікарні, та детально спланували схему IP-адресації, де DHCP-сервер на базі Windows Server забезпечує автоматизоване управління адресами, а сервери та ключові пристрої мають статичні IP. Особливу увагу приділили розмежуванню доступу користувачів за допомогою групових політик AD, що є критично важливим для захисту конфіденційних медичних даних та забезпечення стабільності системи.

Цей розділ заклав основу для подальшої реалізації сучасної, безпечної та ефективної мережевої інфраструктури, повністю адаптованої до потреб медичного закладу.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				37
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3. НАЛАГОДЖЕННЯ ТА АНАЛІЗ РЕЗУЛЬТАТІВ

3.1 Налаштування мережевих пристроїв

Почнемо налаштування нашої мережі з маршрутизаторів. На маршрутизаторах ми налаштуємо адреси, динамічну маршрутизацію, віддалений доступ, створимо користувачів та налаштуємо паролі на самому маршрутизаторі.

На всіх маршрутизаторах буде майже однакові конфігурації, тому зробимо приклад базових налаштувань маршрутизатора, тільки одне буде відрізняти їх це router-id, який буде унікальний (Рисунок 3.1).

```
R-Server(config)#enable secret *****
R-Server(config)#line console 0
R-Server(config-line)#password *****
R-Server(config-line)#login
R-Server(config-line)#exit
R-Server(config)#router ospf 1
R-Server(config-router)#router-id 1.1.1.1
R-Server(config-router)#network 5.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 10.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 15.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 20.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 25.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 30.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 35.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 40.0.0.0 0.0.0.3 area 0
R-Server(config-router)#network 192.168.0.0 0.0.0.255 area 0
R-Server(config-router)#network 193.21.8.0 0.0.0.31 area 0
R-Server(config-router)#network 194.21.8.0 0.0.0.31 area 0
R-Server(config-router)#network 195.21.8.0 0.0.0.31 area 0
R-Server(config-router)#network 196.21.8.0 0.0.0.31 area 0
R-Server(config-router)#network 197.21.8.0 0.0.0.31 area 0
R-Server(config-router)#network 198.21.8.0 0.0.0.31 area 0
R-Server(config-router)#exit
R-Server(config)#ip domain-name hospital.net
R-Server(config)#crypto key generate rsa modulus 2048
R-Server(config)#ip ssh version 2
R-Server(config)#username admin privilege 15 secret adminssh
R-Server(config)#username tech privilege 7 secret techssh
R-Server(config)#ip ssh time-out 60
R-Server(config)#ip ssh authentication-retries 3
R-Server(config)#line vty 0 15
R-Server(config-line)#login local
R-Server(config-line)#transport input ssh
R-Server(config-line)#exit
R-Server(config)#service password-encryption
```

Рисунок 3.1 - Приклад базових налаштувань маршрутизатора

Після того, як ми вписали базові налаштування переходимо до індивідуальних (Рисунок 3.2-7).

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

```

Mikrotik(config)#int g0/0
Mikrotik(config-if)#ip address 5.0.0.1 255.255.255.252
Mikrotik(config-if)#ip nat inside
Mikrotik(config-if)#int g1/0
Mikrotik(config-if)#ip address dhcp
Mikrotik(config-if)#ip nat outside
Mikrotik(config-if)#exit
Mikrotik(config)#router ospf 1
Mikrotik(config-router)#router-id 1.1.1.1
Mikrotik(config-router)#access-list 1 permit 0.0.0.0 255.255.255.255
Mikrotik(config)#ip nat inside source list 1 interface g1/0 overload

```

Рисунок 3.2 - Налаштування Mikrotik

```

R-Server(config)#int g0/0
R-Server(config-if)#ip address dhcp
R-Server(config-if)#ip nat outside
R-Server(config-if)#int g1/0
R-Server(config-if)#ip address 40.0.0.1 255.255.255.252
R-Server(config-if)#int g2/0
R-Server(config-if)#ip address 193.21.8.1 255.255.255.224
R-Server(config-if)#ip nat inside
R-Server(config-if)#exit
R-Server(config)#router ospf 1
R-Server(config-router)#router-id 2.2.2.2
R-Server(config-router)#access-list 1 permit 0.0.0.0 255.255.255.255
R-Server(config)#ip nat inside source list 1 interface g0/0 overload

```

Рисунок 3.3 - Налаштування R-Server

```

R-Main-Building(config)#int g0/0
R-Main-Building(config-if)#ip address 5.0.0.2 255.255.255.252
R-Main-Building(config-if)#int g1/0
R-Main-Building(config-if)#ip address 40.0.0.2 255.255.255.252
R-Main-Building(config-if)#int g2/0
R-Main-Building(config-if)#ip address 35.0.0.2 255.255.255.252
R-Main-Building(config-if)#int g3/0
R-Main-Building(config-if)#ip address 25.0.0.1 255.255.255.252
R-Main-Building(config-if)#int g4/0
R-Main-Building(config-if)#ip address 10.0.0.2 255.255.255.252
R-Main-Building(config-if)#exit
R-Main-Building(config)#router ospf 1
R-Main-Building(config-router)#router-id 3.3.3.3

```

Рисунок 3.4 - Налаштування R-Main-Building

```

R-Reception-South(config)#int g0/0
R-Reception-South(config-if)#ip address 194.21.8.1 255.255.255.224
R-Reception-South(config-if)#ip helper-address 193.21.8.3
R-Reception-South(config-if)#int g1/0
R-Reception-South(config-if)#ip address 195.21.8.1 255.255.255.224
R-Reception-South(config-if)#ip helper-address 193.21.8.3
R-Reception-South(config-if)#int g2/0
R-Reception-South(config-if)#ip address 30.0.0.1 255.255.255.252
R-Reception-South(config-if)#int g3/0
R-Reception-South(config-if)#ip address 15.0.0.1 255.255.255.252
R-Reception-South(config-if)#int g4/0
R-Reception-South(config-if)#ip address 10.0.0.1 255.255.255.252
R-Reception-South(config-if)#exit
R-Reception-South(config)#router ospf 1
R-Reception-South(config-router)#router-id 4.4.4.4

```

Рисунок 3.5 - Налаштування R-Reception-South

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

```

R-Reception-North(config)#int g0/0
R-Reception-North(config-if)#ip address 197.21.8.1 255.255.255.224
R-Reception-North(config-if)#ip helper-address 193.21.8.3
R-Reception-North(config-if)#int g1/0
R-Reception-North(config-if)#ip address 196.21.8.1 255.255.255.224
R-Reception-North(config-if)#ip helper-address 193.21.8.3
R-Reception-North(config-if)#int g2/0
R-Reception-North(config-if)#ip address 35.0.0.1 255.255.255.252
R-Reception-North(config-if)#int g3/0
R-Reception-North(config-if)#ip address 15.0.0.2 255.255.255.252
R-Reception-North(config-if)#int g4/0
R-Reception-North(config-if)#ip address 20.0.0.1 255.255.255.252
R-Reception-North(config-if)#exit
R-Reception-North(config)#router ospf 1
R-Reception-North(config-router)#router-id 5.5.5.5

```

Рисунок 3.6 - Налаштування R-Reception-North

```

R-Technical-Building(config)#int g0/0
R-Technical-Building(config-if)#ip address 198.21.8.1 255.255.255.224
R-Technical-Building(config-if)#ip helper-address 193.21.8.3
R-Technical-Building(config-if)#int g2/0
R-Technical-Building(config-if)#ip address 30.0.0.2 255.255.255.252
R-Technical-Building(config-if)#int g3/0
R-Technical-Building(config-if)#ip address 25.0.0.2 255.255.255.252
R-Technical-Building(config-if)#int g4/0
R-Technical-Building(config-if)#ip address 20.0.0.2 255.255.255.252
R-Technical-Building(config-if)#exit
R-Technical-Building(config)#router ospf 1
R-Technical-Building(config-router)#router-id 6.6.6.6

```

Рисунок 3.7 - Налаштування R-Technical-Building

Коли маршрутизатори налаштовані ми переходимо до комутаторів. На них ми налаштовуємо Vlan, захист портів, віддалений доступ, користувачів та паролі (Рисунок 3.8-15).

```

Switch-1(config)#enable secret *****
Switch-1(config)#line console 0
Switch-1(config-line)#password *****
Switch-1(config-line)#login
Switch-1(config-line)#exit
Switch-1(config)#$net0/0-3, Ethernet1/0-3, Ethernet2/0-3, Ethernet3/0-3
Switch-1(config-if-range)#spanning-tree portfast
Switch-1(config-if-range)#spanning-tree bpduguard enable
Switch-1(config-if-range)#switchport mode access
Switch-1(config-if-range)#switchport access vlan 1
Switch-1(config-if-range)#switchport port-security
Switch-1(config-if-range)#switchport port-security maximum 1
Switch-1(config-if-range)#switchport port-security violation restrict
Switch-1(config-if-range)#switchport port-security mac-address sticky
Switch-1(config-if-range)#ip verify source
Switch-1(config-if-range)#no sh
Switch-1(config-if-range)#exit
Switch-1(config)#interface range Ethernet1/0-3, Ethernet2/0-3, Ethernet3/0-3
Switch-1(config-if-range)#sh
Switch-1(config-if-range)#exit
Switch-1(config)#spanning-tree portfast bpduguard default
Switch-1(config)#ip domain-name hospital.net
Switch-1(config)#crypto key generate rsa modulus 2048
Switch-1(config)#ip ssh version 2
Switch-1(config)#username admin privilege 15 secret adminssh
Switch-1(config)#username tech privilege 7 secret techssh
Switch-1(config)#ip ssh time-out 60
Switch-1(config)#ip ssh authentication-retries 3
Switch-1(config)#line vty 0 4
Switch-1(config-line)#exec-timeout 5 0
Switch-1(config-line)#login local
Switch-1(config-line)#transport input ssh

```

Рисунок 3.8 - Приклад базових налаштувань комутатора

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

```
Switch-1(config)#int vlan1
Switch-1(config-if)#ip address 194.21.8.2 255.255.255.224
Switch-1(config-if)#exit
Switch-1(config)#ip default-gateway 194.21.8.1
Switch-1(config)#logging 194.21.8.1
Switch-1(config)#logging trap warnings
```

Рисунок 3.9 - Налаштування Switch-1

```
Switch-2(config)#int vlan1
Switch-2(config-if)#ip address 195.21.8.2 255.255.255.224
Switch-2(config-if)#exit
Switch-2(config)#ip default-gateway 195.21.8.1
Switch-2(config)#logging 195.21.8.1
Switch-2(config)#logging trap warnings
```

Рисунок 3.10 - Налаштування Switch-2

```
Switch-3(config)#int vlan1
Switch-3(config-if)#ip address 196.21.8.2 255.255.255.224
Switch-3(config-if)#exit
Switch-3(config)#ip default-gateway 196.21.8.1
Switch-3(config)#logging 196.21.8.1
Switch-3(config)#logging trap warnings
```

Рисунок 3.11 - Налаштування Switch-3

```
Switch-4(config)#int vlan1
Switch-4(config-if)#ip address 197.21.8.2 255.255.255.224
Switch-4(config-if)#exit
Switch-4(config)#ip default-gateway 197.21.8.1
Switch-4(config)#logging 197.21.8.1
Switch-4(config)#logging trap warnings
```

Рисунок 3.12 - Налаштування Switch-4

```
Switch-5(config)#int vlan1
Switch-5(config-if)#ip address 198.21.8.2 255.255.255.224
Switch-5(config-if)#exit
Switch-5(config)#ip default-gateway 198.21.8.1
Switch-5(config)#logging 198.21.8.1
Switch-5(config)#logging trap warnings
```

Рисунок 3.13 - Налаштування Switch-5

```
Switch-Server(config)#int vlan1
Switch-Server(config-if)#ip address 193.21.8.2 255.255.255.224
Switch-Server(config-if)#exit
Switch-Server(config)#ip default-gateway 193.21.8.1
Switch-Server(config)#logging 193.21.8.1
Switch-Server(config)#logging trap warnings
```

Рисунок 3.14 - Налаштування Switch-Server

```
Switch-CCTV(config)#int vlan1
Switch-CCTV(config-if)#ip address dhcp
Switch-CCTV(config-if)#no sh
Switch-CCTV(config-if)#exit
Switch-CCTV(config)#ip default-gateway 192.168.0.1
Switch-CCTV(config)#interface range fa0/1-24, g0/1-2
Switch-CCTV(config-if-range)#switchport mode access
Switch-CCTV(config-if-range)#switchport access vlan 1
Switch-CCTV(config-if-range)#no sh
```

Рисунок 3.15 - Налаштування Switch-CCTV

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				41
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Розгортання Microsoft Active Directory

Починаємо наше розгортання з встановлення Windows Server, інсталяції подібна до звичайної Windows 10, тому перейдемо до налаштувань IP-адреси. Ми вже створили схему адресації візьмемо з неї адресу (Таблиця 2.2). Налаштуємо наш основний та резервний сервери (Рисунок 3.16).

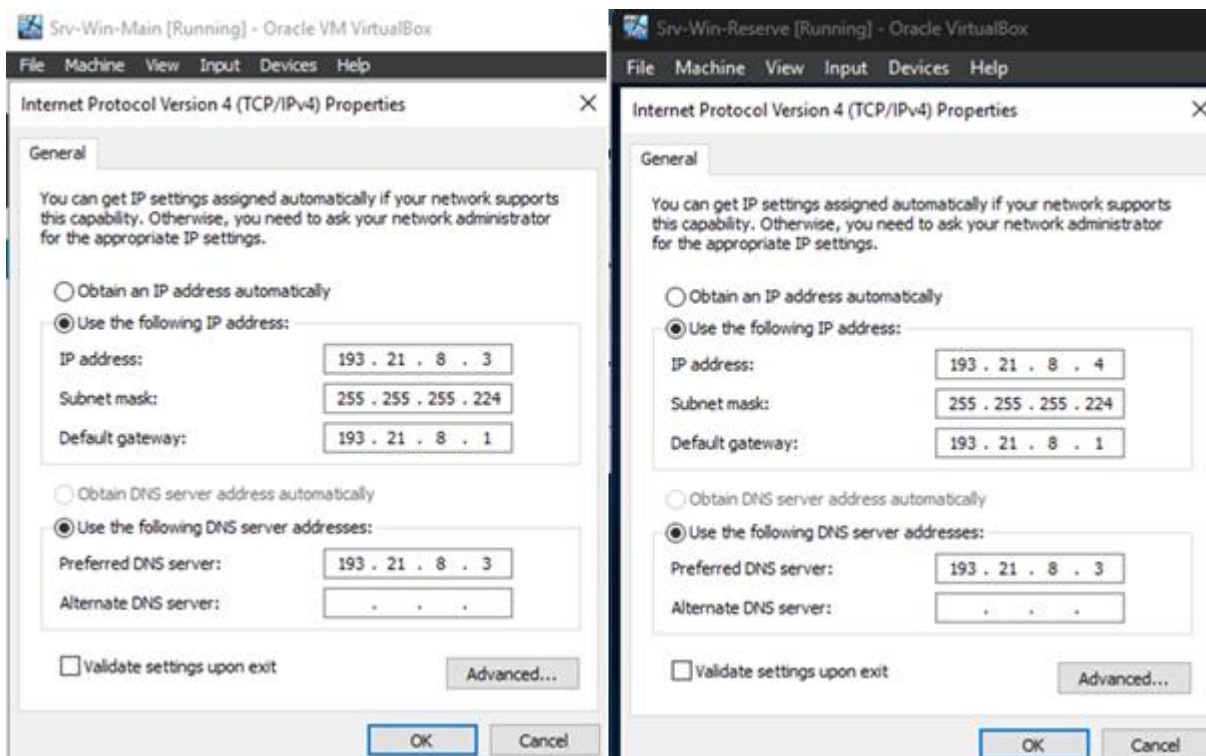


Рисунок 3.16 - Налаштування IP-адреси серверів

З метою розширення функціональності сервера та забезпечення його комплексного використання у мережевій інфраструктурі, за допомогою майстра "Add Roles and Features Wizard" було інстальовано низку ключових ролей та компонентів. Зокрема, встановлено: ADDS, DHCP Server, DNS Server, File and Storage Services, Web Services (IIS), Network Policy and Access Services, Print Services та Remote Desktop Services (Рисунок 3.17). Цей комплекс ролей створює надійну та багатофункціональну платформу, здатну задовольнити широкий спектр потреб сучасної медичної установи.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		42

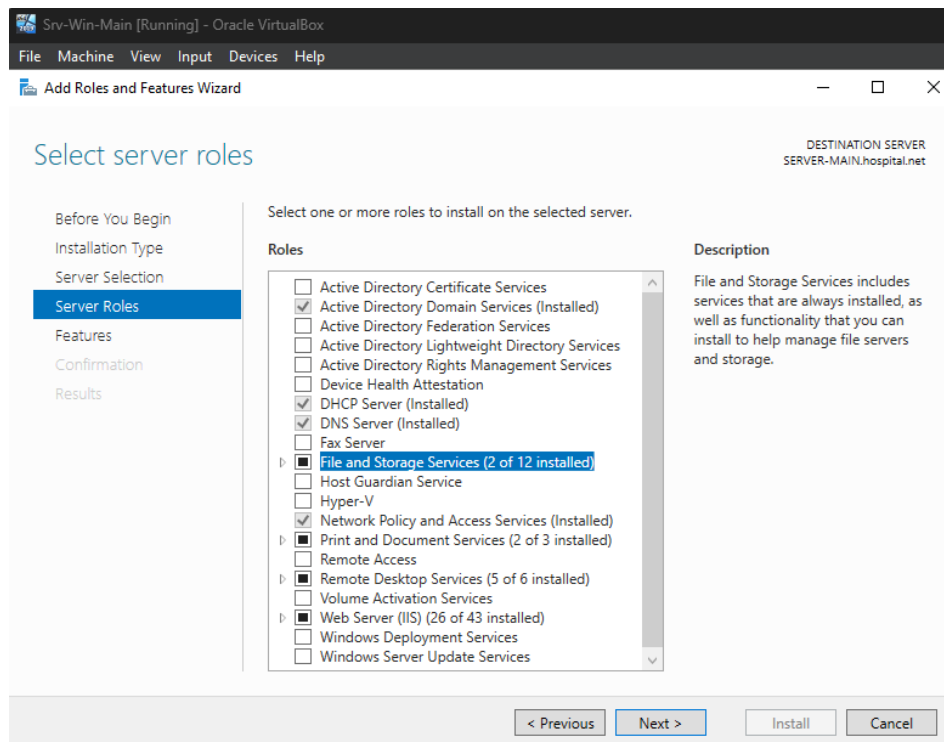


Рисунок 3.17 – Майстер додавання ролей та компонентів

Створення користувачів та груп для нашого домену здійснюється за допомогою засобу Active Directory Users and Computers (Рисунок 3.18-23). Цей процес є критично важливим для організації доступу та впровадження політик безпеки у мережі лікарні. За допомогою цього інструменту ми створюємо організаційні підрозділи, користувачів та групи відповідно до структури відділів та ролей персоналу, як це було визначено в розділі 2.

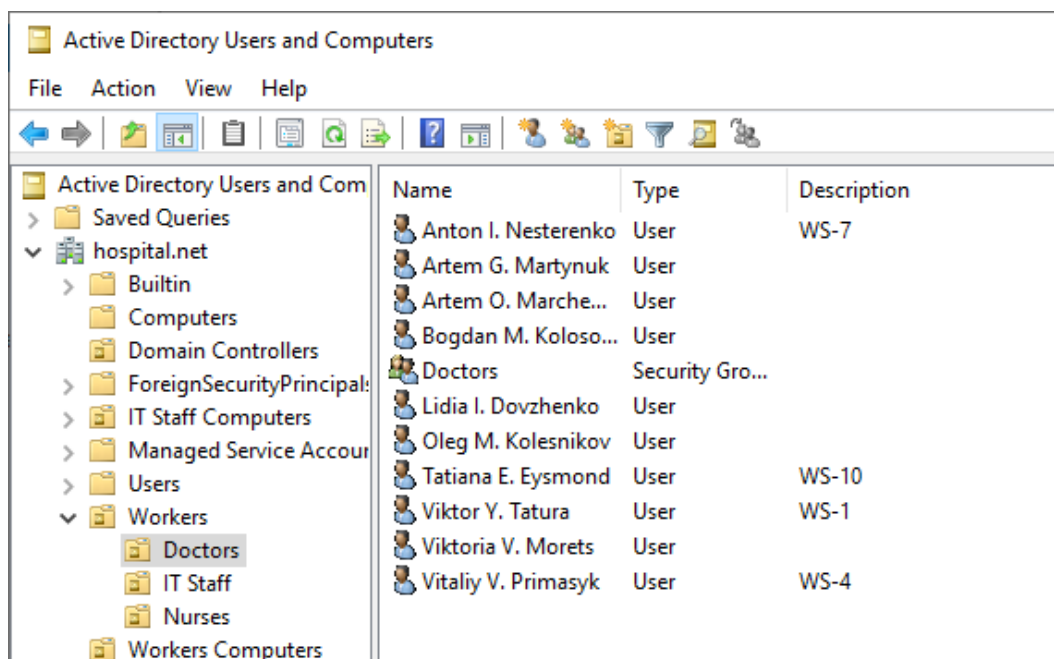


Рисунок 3.18 – Налаштування в Active Directory Users and Computers

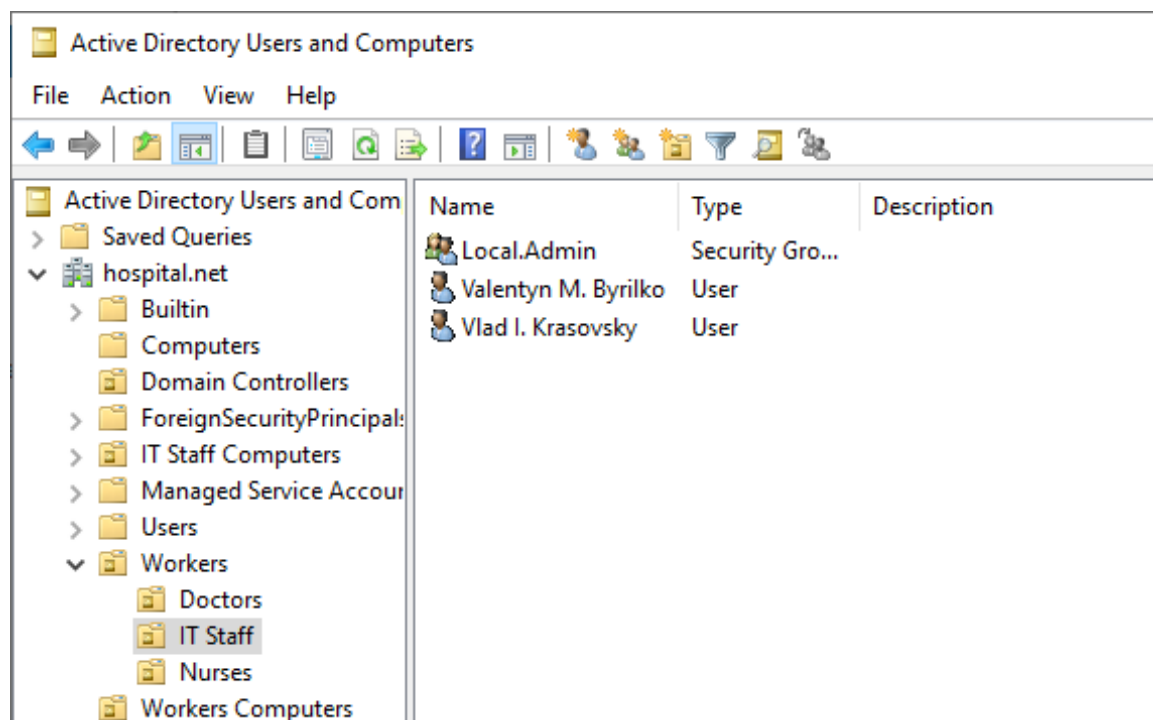


Рисунок 3.19 – Налаштування в Active Directory Users and Computers

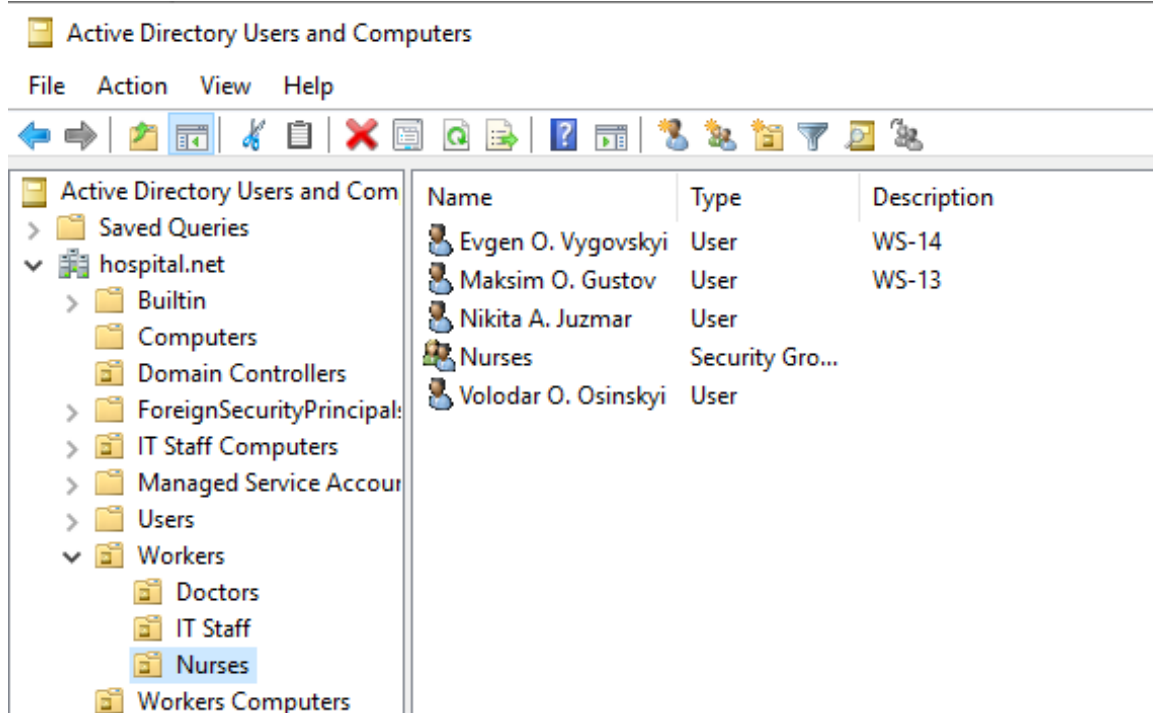


Рисунок 3.20 – Налаштування в Active Directory Users and Computers

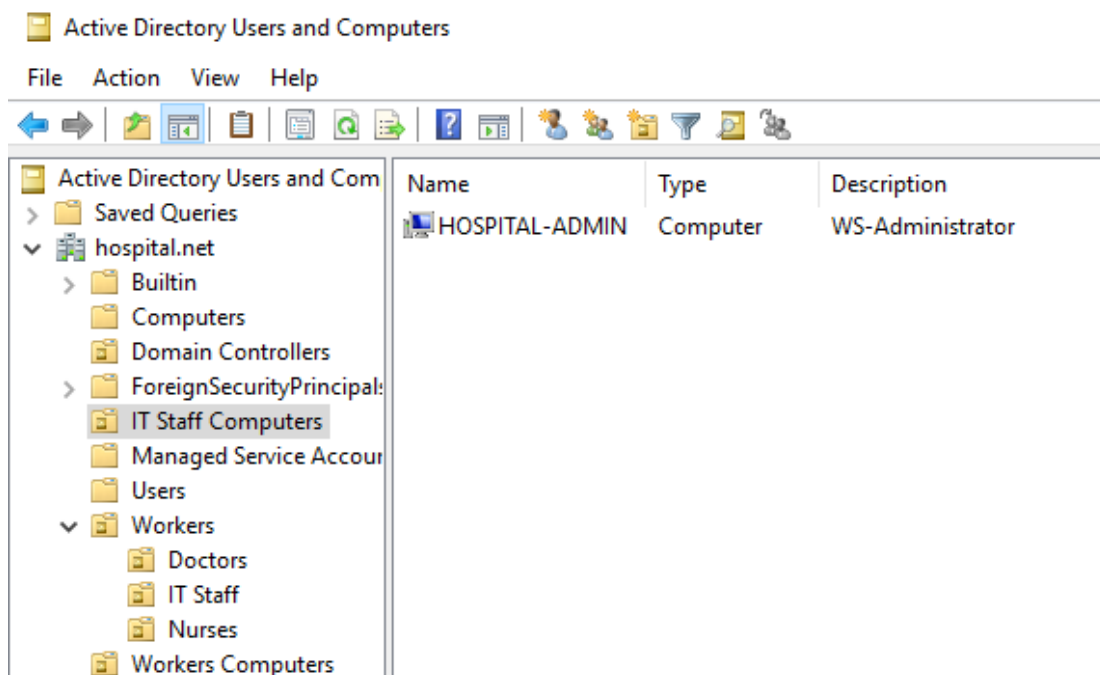


Рисунок 3.21 – Налаштування в Active Directory Users and Computers

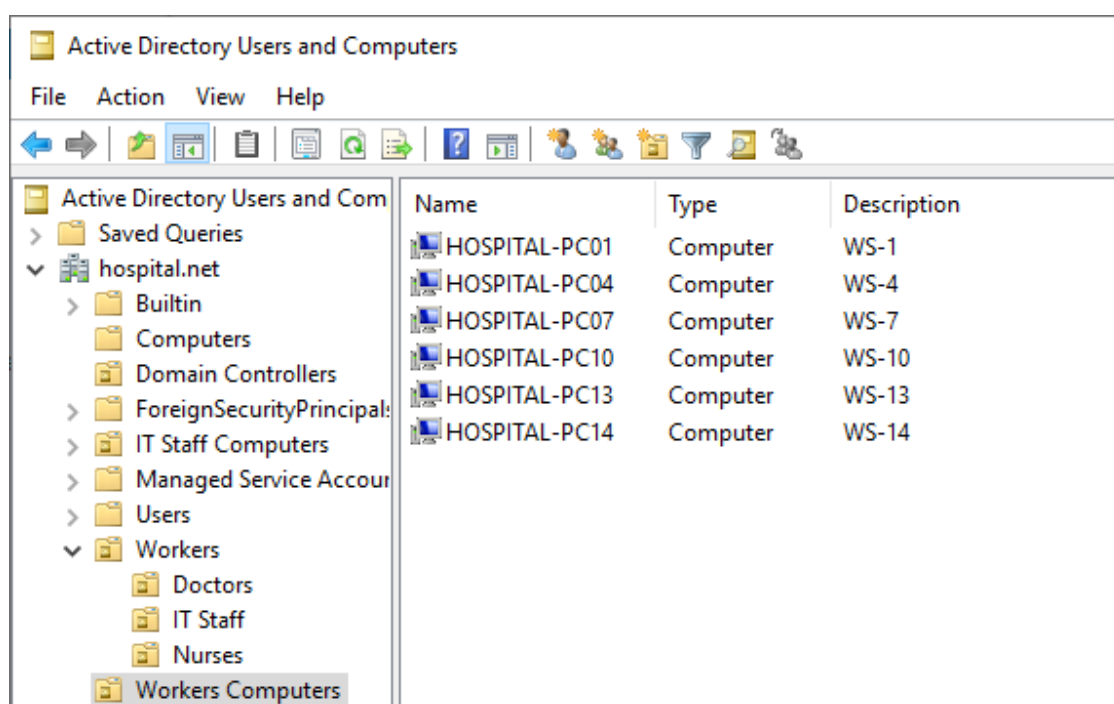


Рисунок 3.22 – Налаштування в Active Directory Users and Computers

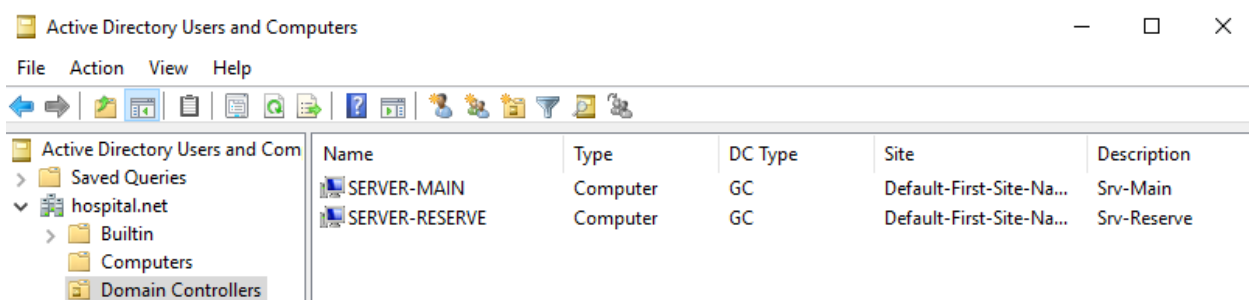


Рисунок 3.23 – Налаштування в Active Directory Users and Computers

Далі перейдемо до налаштування DHCP-сервера, де необхідно створити та налаштувати Scope для кожної з наших підмереж (Рисунок 3.24). У Scope 193.21.8.0 слід виключити перші 4 IP-адреси, тоді як в інших - лише перші 2 адреси, призначені для маршрутизатора та комутатора (Рисунок 3.25-26).

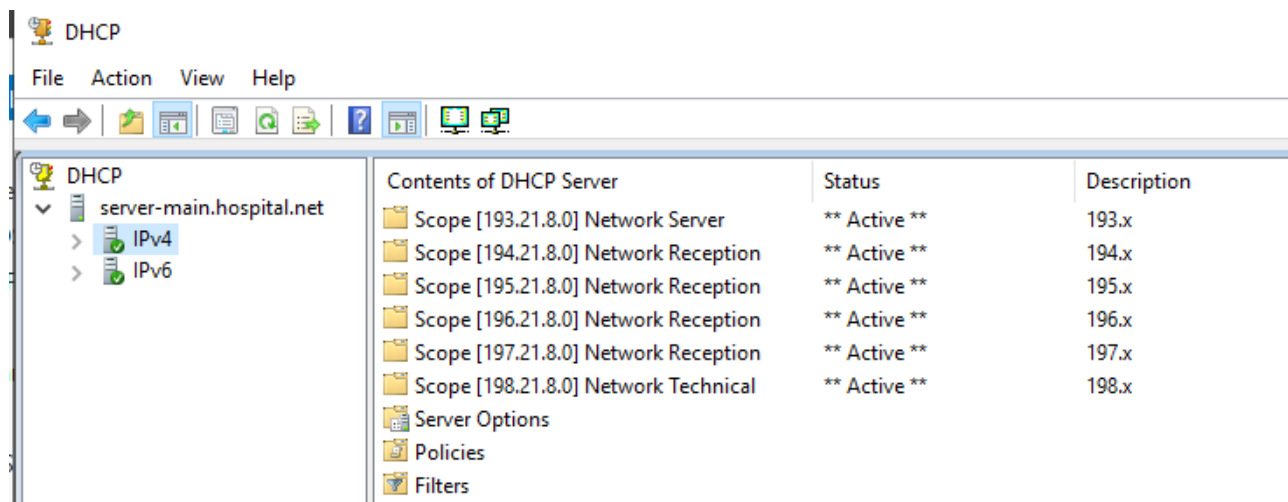


Рисунок 3.24 – Налаштування DHCP-сервера

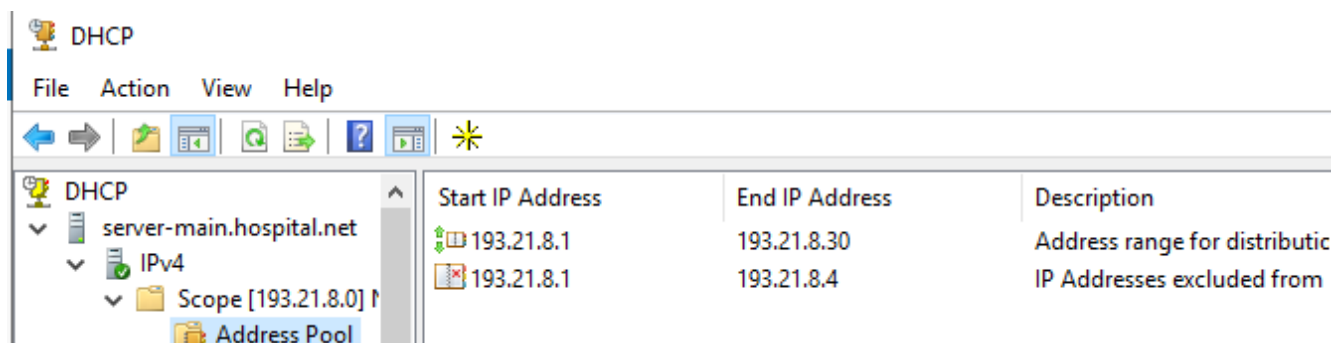


Рисунок 3.25– Налаштування DHCP-сервера

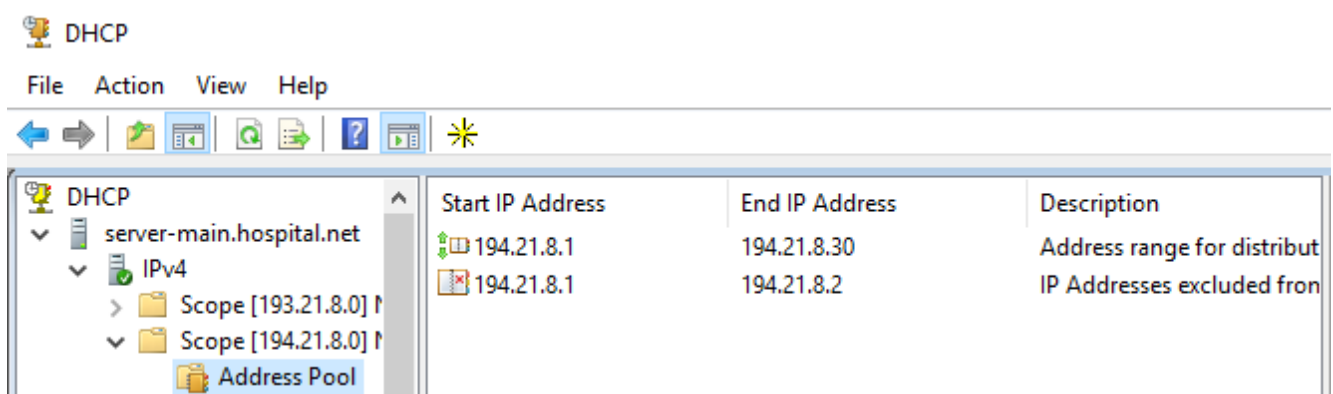


Рисунок 3.26 – Налаштування DHCP-сервера

Створюємо новий запис Host (A) у DNS для забезпечення майбутнього віддаленого доступу до сервера. Цей запис зіставлятиме доменне ім'я сервера з його

IP-адресою, що дозволить адміністраторам легко підключатися до сервера за іменем, а не за числовим IP-адресом (Рисунок 3.27).

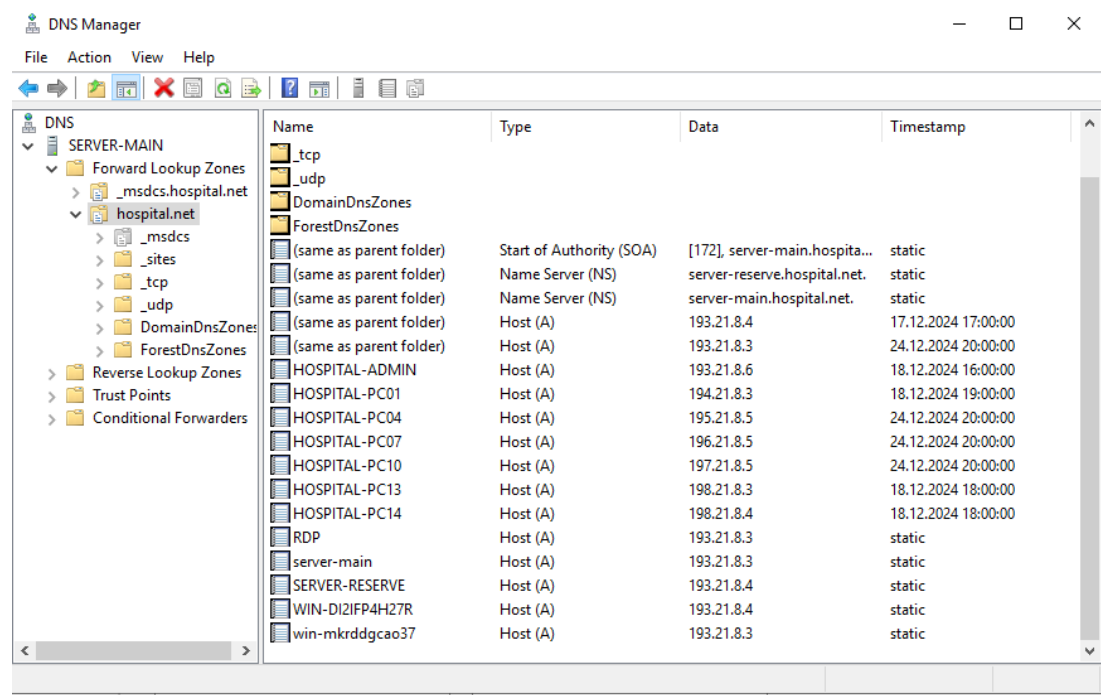


Рисунок 3.27 – Налаштування DNS

Створюємо сертифікат для забезпечення безпечного віддаленого підключення до сервера, а потім прикріплюємо його до відповідних служб для шифрування трафіку та аутентифікації (Рисунок 3.28).

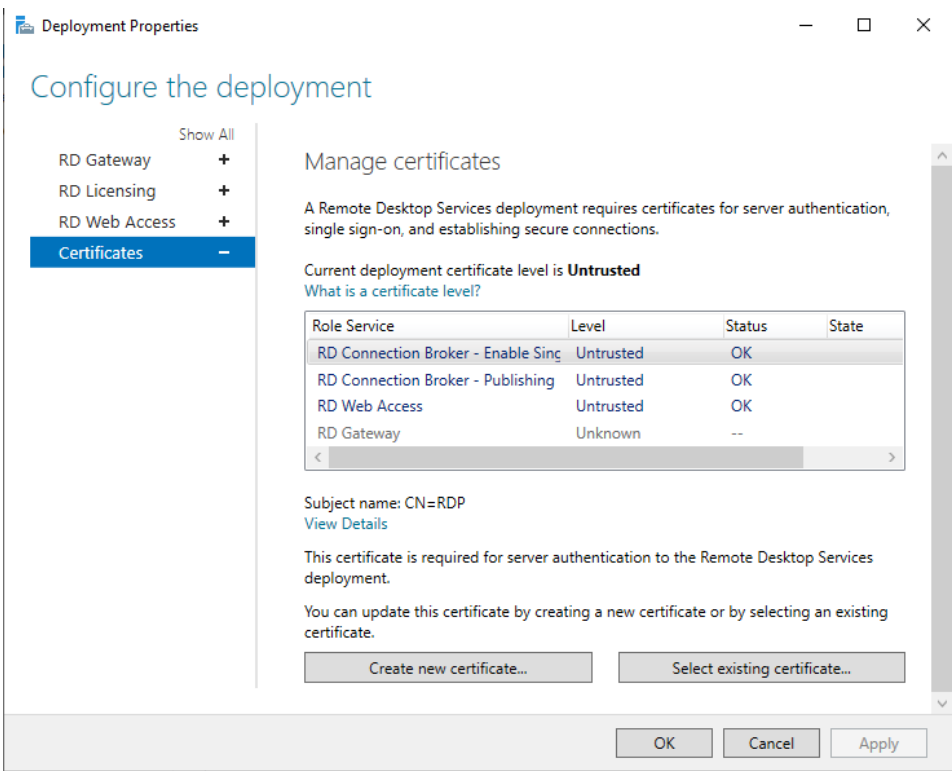


Рисунок 3.28 – Налаштування RDS

Далі переходимо до налаштування мережеских принтерів, щоб забезпечити доступ до них для всіх користувачів мережі. Це включає встановлення драйверів та надання відповідних дозволів користувачам та групам для ефективної роботи з принтерами (Рисунок 3.29).

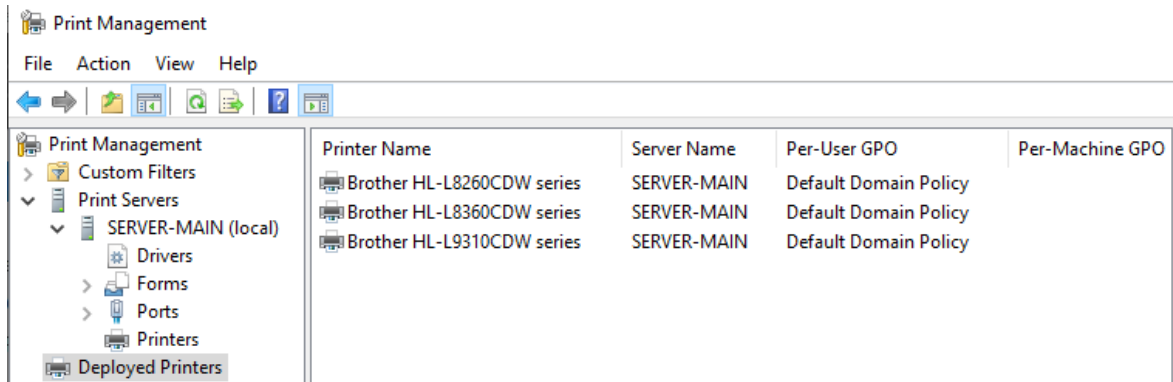


Рисунок 3.29 – Налаштування у Print Management

Створюємо мережеве сховище для користувачів домену. Це дозволить централізовано зберігати дані користувачів, забезпечувати резервне копіювання та надавати спільний доступ до необхідних ресурсів. Налаштування мережевого сховища здійснюється через відповідні служби File and Storage Services, що були встановлені раніше (Рисунок 3.30).

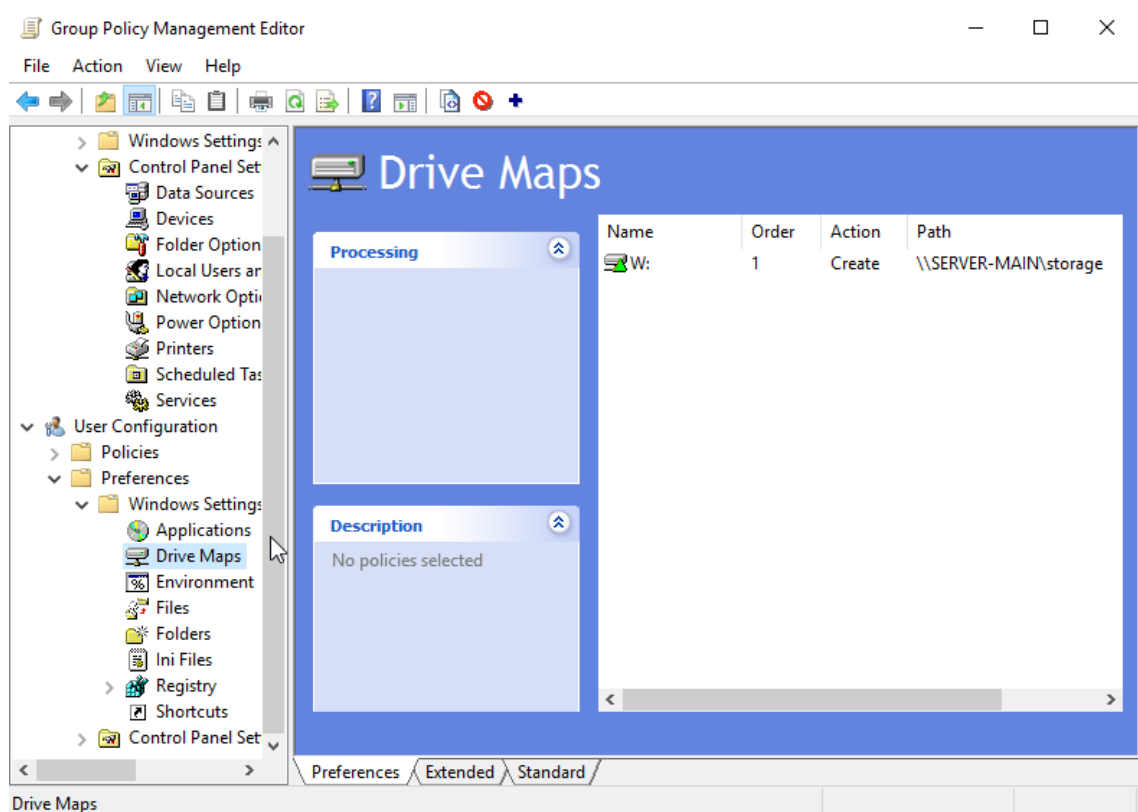


Рисунок 3.30 – Налаштування у Group Policy Management Editor

Після завершення налаштувань функціоналу нашого сервера, ми переходимо до конфігурації робочих станцій. Їх ми підключаємо до домену, після цього робочі станції автоматично отримують IP-адреси від DHCP-сервера (Рисунок 3.31-46).

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : hospital.net
    Link-local IPv6 Address . . . . . : fe80::35bd:d99d:ec4b:74f2%13
    IPv4 Address. . . . . : 193.21.8.6
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 193.21.8.1
PS C:\Users\Administrator>
```

Настройки имени компьютера, домену та рабочей группы

Имя компьютера: HOSPITAL-ADMIN

Полное имя компьютера: HOSPITAL-ADMIN.hospital.net

Описание компьютера:

Домен: hospital.net

Рисунок 3.31 – Налаштування WS-Admin

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : hospital.net
    Link-local IPv6 Address . . . . . : fe80::d091:f14e:dec7:190f%10
    IPv4 Address. . . . . : 194.21.8.3
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 194.21.8.1
PS C:\Users\Administrator>
```

Настройки имени компьютера, домену та рабочей группы

Имя компьютера: HOSPITAL-PC01

Полное имя компьютера: HOSPITAL-PC01.hospital.net

Описание компьютера:

Домен: hospital.net

Рисунок 3.32 – Налаштування WS-1

```
WS-2> show ip

NAME       : WS-2[1]
IP/MASK    : 194.21.8.4/27
GATEWAY    : 194.21.8.1
DNS        : 193.21.8.3
DHCP SERVER : 193.21.8.3
DHCP LEASE  : 31535858, 31536000/15768000/27594000
DOMAIN NAME : hospital.net
```

Рисунок 3.33 – Налаштування WS-2

```
WS-3> show ip

NAME       : WS-3[1]
IP/MASK    : 194.21.8.5/27
GATEWAY    : 194.21.8.1
DNS        : 193.21.8.3
DHCP SERVER : 193.21.8.3
DHCP LEASE  : 31535823, 31536000/15768000/27594000
DOMAIN NAME : hospital.net
```

Рисунок 3.34 – Налаштування WS-3

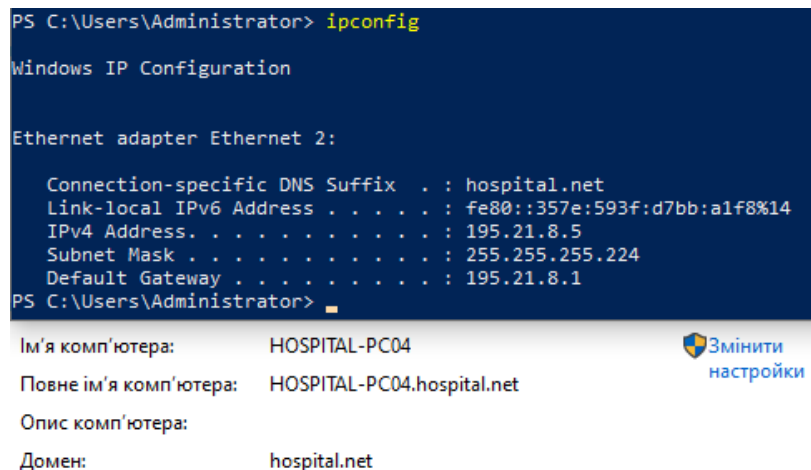


Рисунок 3.35 – Налаштування WS-4

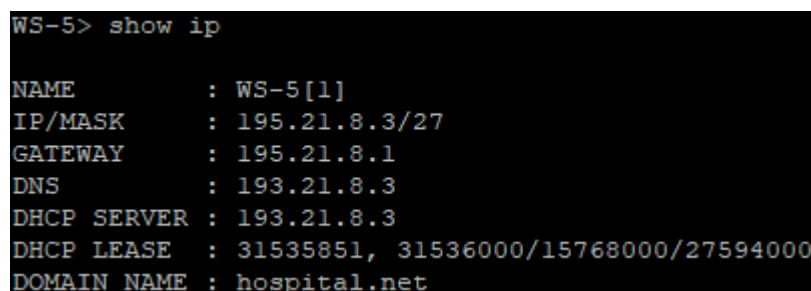


Рисунок 3.36 – Налаштування WS-5

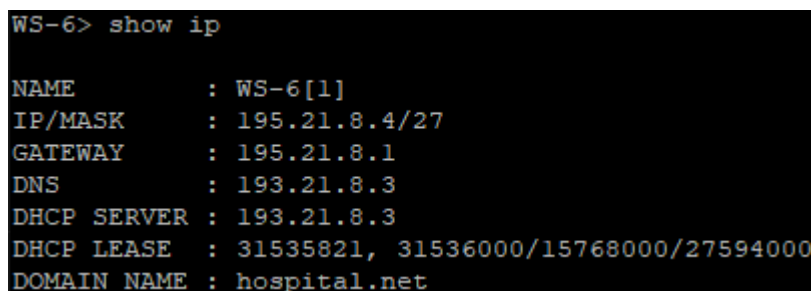


Рисунок 3.37 – Налаштування WS-6

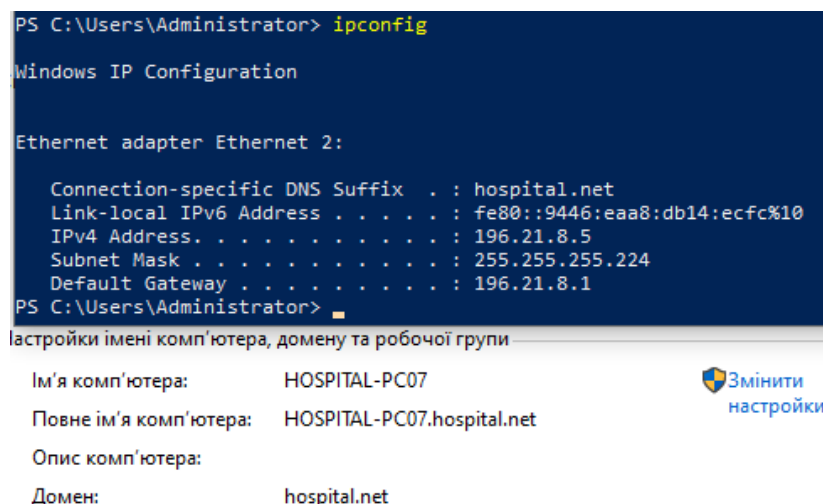


Рисунок 3.38 – Налаштування WS-7

```
WS-8> show ip
NAME       : WS-8[1]
IP/MASK    : 196.21.8.4/27
GATEWAY    : 196.21.8.1
DNS        : 193.21.8.3
DHCP SERVER : 193.21.8.3
DHCP LEASE  : 31535813, 31536000/15768000/27594000
DOMAIN NAME : hospital.net
```

Рисунок 3.39 - Налаштування WS-8

```
WS-9> show ip
NAME       : WS-9[1]
IP/MASK    : 196.21.8.3/27
GATEWAY    : 196.21.8.1
DNS        : 193.21.8.3
DHCP SERVER : 193.21.8.3
DHCP LEASE  : 31535797, 31536000/15768000/27594000
DOMAIN NAME : hospital.net
```

Рисунок 3.40 - Налаштування WS-9

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : hospital.net
    Link-local IPv6 Address . . . . . : fe80::c8c9:6559:7713:4db7%7
    IPv4 Address. . . . . : 197.21.8.5
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 197.21.8.1
PS C:\Users\Administrator>

Ім'я комп'ютера:      HOSPITAL-PC10
Повне ім'я комп'ютера:  HOSPITAL-PC10.hospital.net
Опис комп'ютера:
Домен:                hospital.net
```

Рисунок 3.41 - Налаштування WS-10

```
WS-11> show ip
NAME       : WS-11[1]
IP/MASK    : 197.21.8.3/27
GATEWAY    : 197.21.8.1
DNS        : 193.21.8.3
DHCP SERVER : 193.21.8.3
DHCP LEASE  : 31535752, 31536000/15768000/27594000
DOMAIN NAME : hospital.net
```

Рисунок 3.42 - Налаштування WS-11

```
WS-12> show ip
NAME          : WS-12[1]
IP/MASK       : 197.21.8.4/27
GATEWAY      : 197.21.8.1
DNS          : 193.21.8.3
DHCP SERVER  : 193.21.8.3
DHCP LEASE   : 31535781, 31536000/15768000/27594000
DOMAIN NAME  : hospital.net
```

Рисунок 3.43 - Налаштування WS-12

```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : hospital.net
    Link-local IPv6 Address . . . . . : fe80::1884:9943:f40b:8d6d%11
    IPv4 Address. . . . . : 198.21.8.3
    Subnet Mask . . . . . : 255.255.255.224
    Default Gateway . . . . . : 198.21.8.1
PS C:\Users\Administrator>
```

Стройки імені комп'ютера, домену та робочої групи

Ім'я комп'ютера: HOSPITAL-PC13

Повне ім'я комп'ютера: HOSPITAL-PC13.hospital.net

Опис комп'ютера:

Домен: hospital.net

Рисунок 3.44 - Налаштування WS-13

```
WS-14> show ip
NAME          : WS-14[1]
IP/MASK       : 198.21.8.3/27
GATEWAY      : 198.21.8.1
DNS          : 193.21.8.3
DHCP SERVER  : 193.21.8.3
DHCP LEASE   : 31535988, 31536000/15768000/27594000
DOMAIN NAME  : hospital.net
```

Рисунок 3.45 - Налаштування WS-14

```
WS-15> show ip
NAME          : WS-15[1]
IP/MASK       : 198.21.8.4/27
GATEWAY      : 198.21.8.1
DNS          : 193.21.8.3
DHCP SERVER  : 193.21.8.3
DHCP LEASE   : 31535995, 31536000/15768000/27594000
DOMAIN NAME  : hospital.net
```

Рисунок 3.46 - Налаштування WS-15

Тепер, коли в нас все налаштовано, переходимо до конфігурації прав користувачів та комп'ютерів за допомогою групових політик. Ми налаштовуємо наступні параметри для забезпечення високого рівня безпеки та керованості в домені:

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				52
Змн.	Арк.	№ докум.	Підпис	Дата		

- Вимагати складні паролі:
 - Enforce password history: 10 попередніх паролів
 - Minimum password length: 8 символів.
 - Password must meet complexity requirements: Enabled.
- Блокування облікового запису після невдалих спроб входу:
 - Account lockout threshold: 5 спроб
 - Account lockout duration: 15 хвилин
- Заборона використання USB-накопичувачів:
 - All Removable Storage Classes: Deny all access: Enabled
- Обмеження доступу до панелі управління:
 - Prohibit access to Control Panel and PC settings: Enabled
- Обмеження запуску певних програм:
 - Don't run specified Windows applications: Перелік програм (cmd.exe, powershell.exe, regedit.exe, taskmgr.exe)
- Користувачський екран входу в систему:
 - Always use custom logon background: Enabled
- Перенаправлення папок Documents, Desktop:
 - User Configuration → Policies → Windows Settings → Folder Redirection
- Автоматичне завершення роботи сеансу через бездіяльність:
 - Set time limit for active but idle Remote Desktop Services sessions: 4 години
- Заборона збереження паролів у браузері:
 - Enable saving passwords to the password manager: Disabled
- Автоматичне встановлення оновлень Windows:
 - Configure Automatic Updates: Enabled
 - Auto download and notify for install: Enabled
- Увімкнення брандмауера:
 - Увімкнення брандмауер для всіх профілів
- Антивірус Windows Defender:
 - Turn on real-time protection: Enabled

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				53
Змн.	Арк.	№ докум.	Підпис	Дата		

- Scan removable drives: Enabled
- Вимкнення SMBv1:
 - Enable insecure guest logons: Disabled
- Автоматичне вимикання після тривалого простою:
 - Specify the system sleep timeout: 30 хвилин
- Встановлення загальних мережевих ресурсів:
 - Це ми вже додали на рисунку 3.34
- Ввімкнення журналювання подій:
 - Maximum log size: 1 GB
- Увімкнення Remote Desktop:
 - Allow users to connect remotely using Remote Desktop Services: Enabled.
- Моніторинг аудиту доступу до файлів:
 - Audit File System: Success, Failure.

Тепер, коли правила безпеки налаштовані, їх ми перевіримо згодом. А поки перейдемо до системи відеоспостереження.

3.3 Налагодження системи відеоспостереження

Почнемо наше налагодження з встановлення програмного забезпечення iVMS-4200. Його ми завантажуюємо з офіційного сайту виробника камер HikVision (Рисунок 3.47).

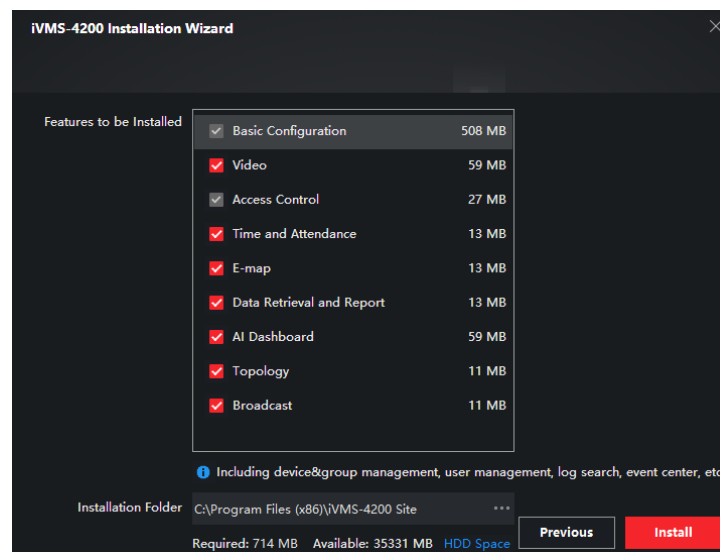


Рисунок 3.47 – Встановлення iVMS-4200

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

Після успішного встановлення ПЗ, наступним кроком є створення суперкористувача. Це критично важливо для забезпечення адміністративного доступу та повного контролю над системою (Рисунок 3.48).

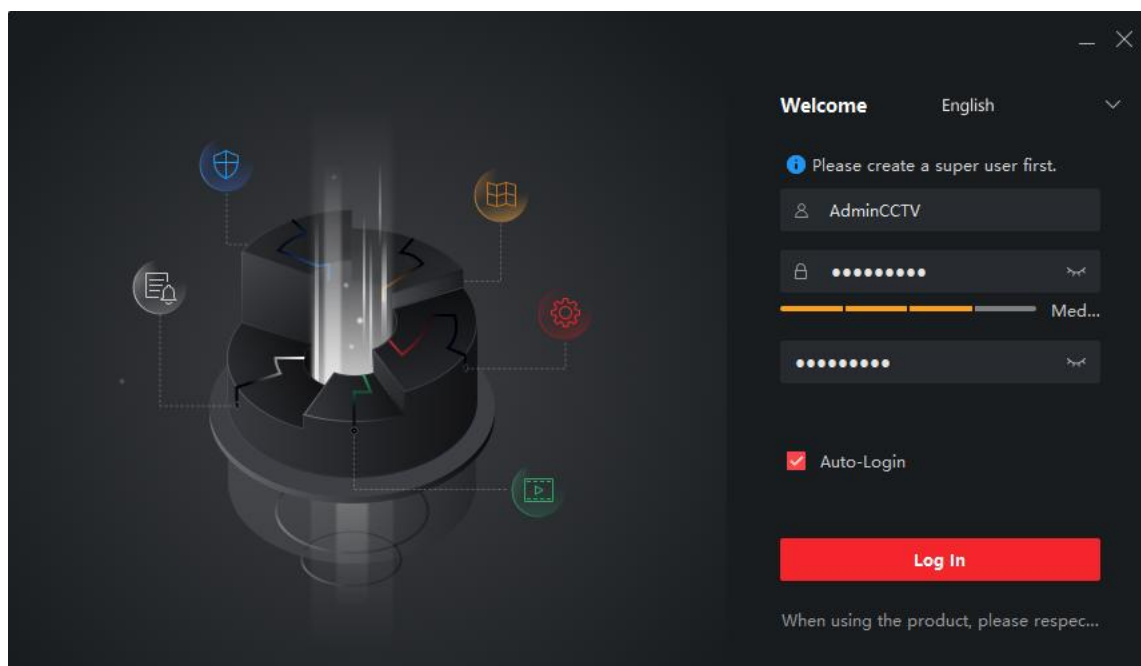


Рисунок 3.48 – Створення супер користувача

Після успішного створення користувача нас вітає головне меню ПЗ (Рисунок 3.49).

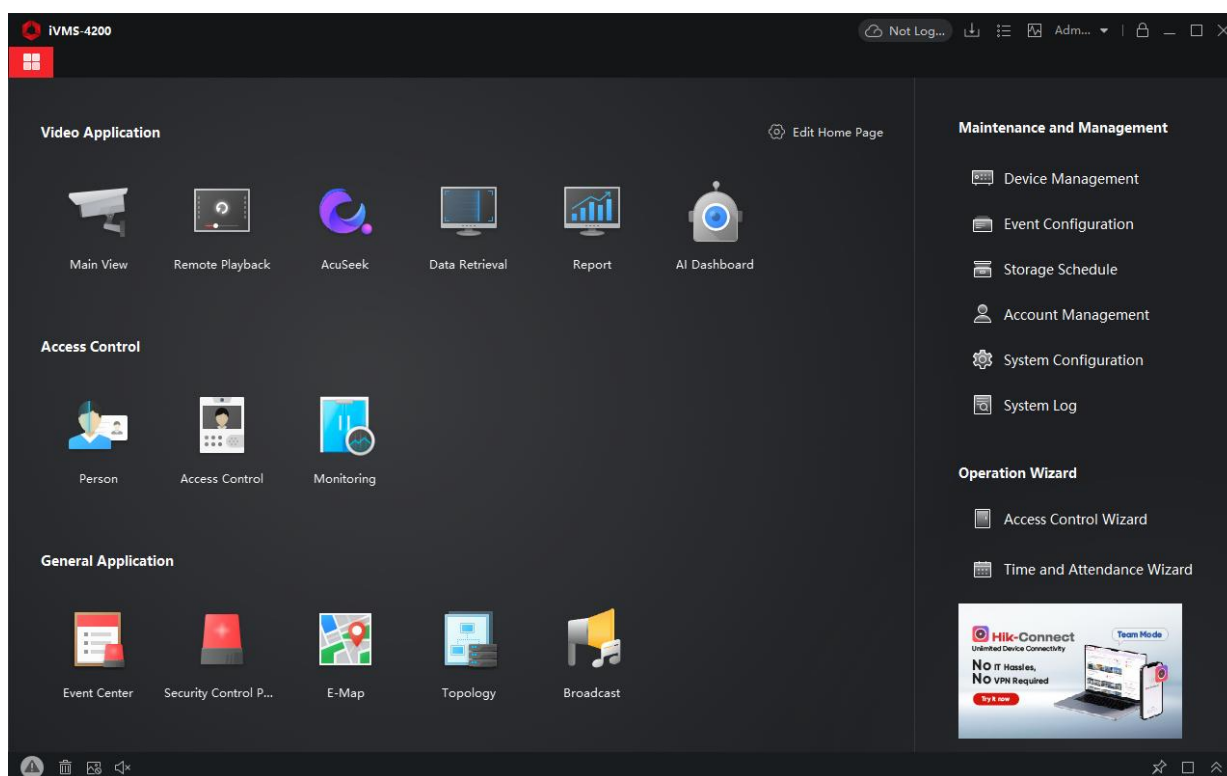


Рисунок 3.49 – Головне меню

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				55
Змн.	Арк.	№ докум.	Підпис	Дата		

Переходимо у вкладку "Maintenance and Management" для підключення камери до застосунку. Існує декілька способів для цього: якщо відомі IP-адреса камери, логін та пароль, або якщо камера ще не налаштована, її можна знайти у списку "Online", або підключити за допомогою QR-коду. Оскільки камера вже була попередньо налаштована, підключення здійснюватиметься за IP-адресою (Рисунок 3.50).

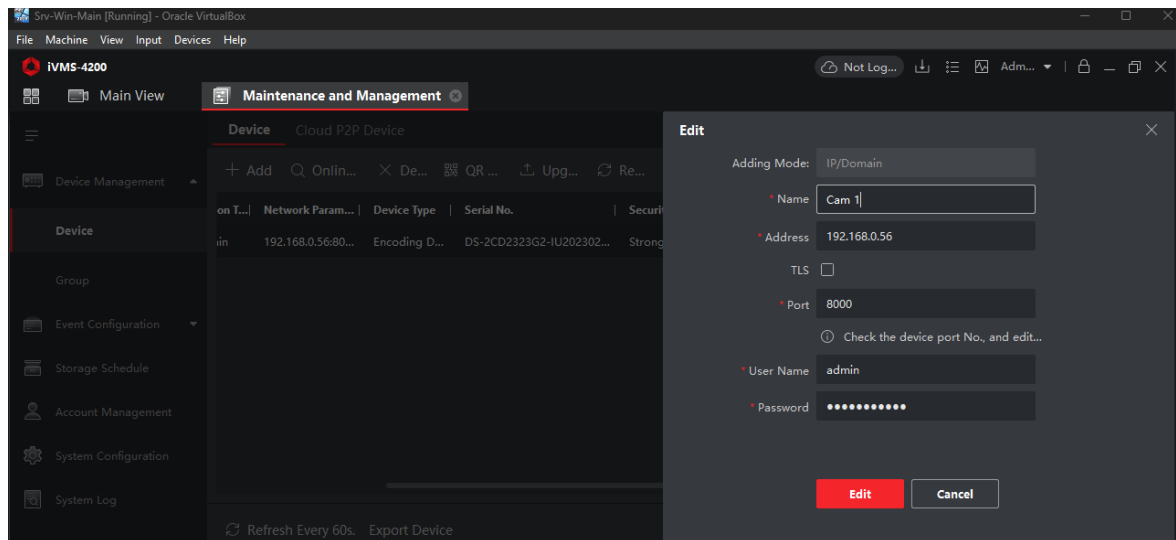


Рисунок 3.50 – Підключення камери до застосунку

Тепер, коли ми її додали, переходимо до вкладки "Main View" та переглядаємо трансляцію в реальному часі (Рисунок 3.51).

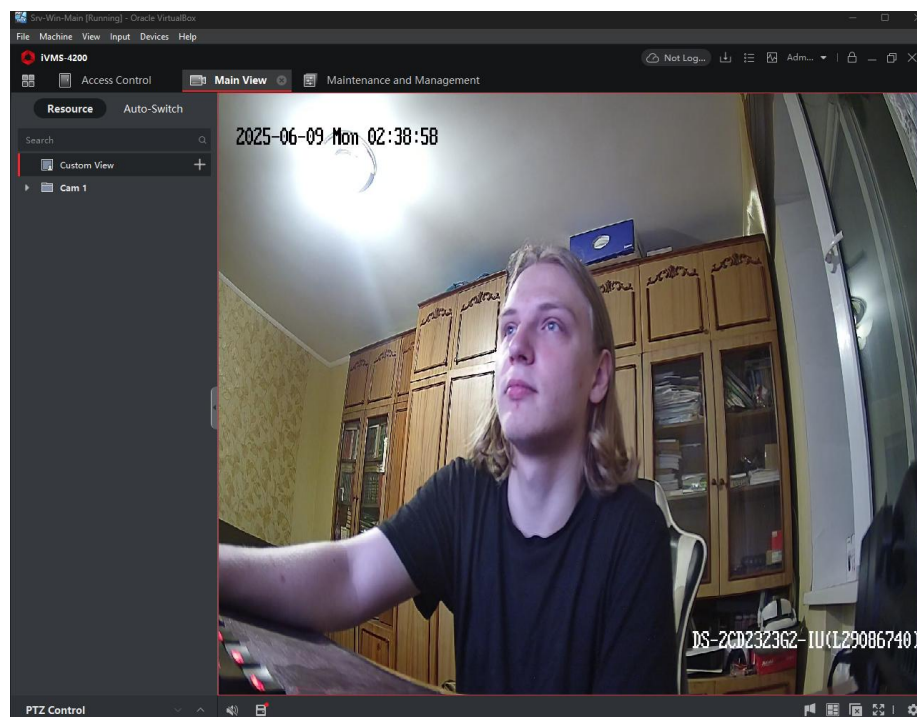


Рисунок 3.51 – Трансляція з камери

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				56
Змн.	Арк.	№ докум.	Підпис	Дата		

Бачимо, що якість картинки прекрасна. Тепер перевіримо, як камера буде працювати без джерел світла (Рисунок 3.52).

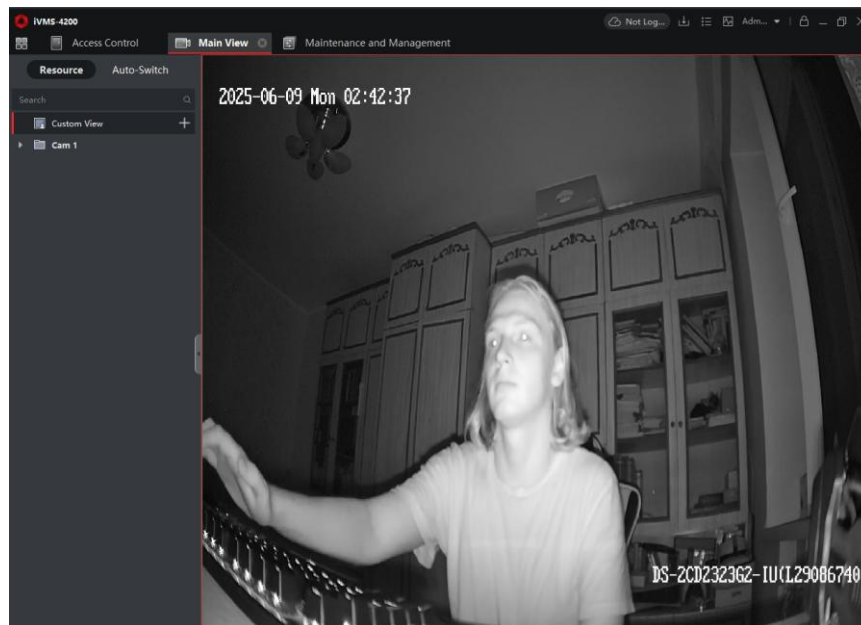


Рисунок 3.52 – Трансляція з камери

Камера повністю функціонує. Переходимо до основних налаштувань подій. Для цього заходимо в налаштування камери, переходимо до вкладки "Events" і можемо їх налаштувати. Налаштуємо подію на рух у визначеній області: для цього натискаємо "Draw Area", визначаємо потрібну зону та зберігаємо налаштування (Рисунок 3.53).

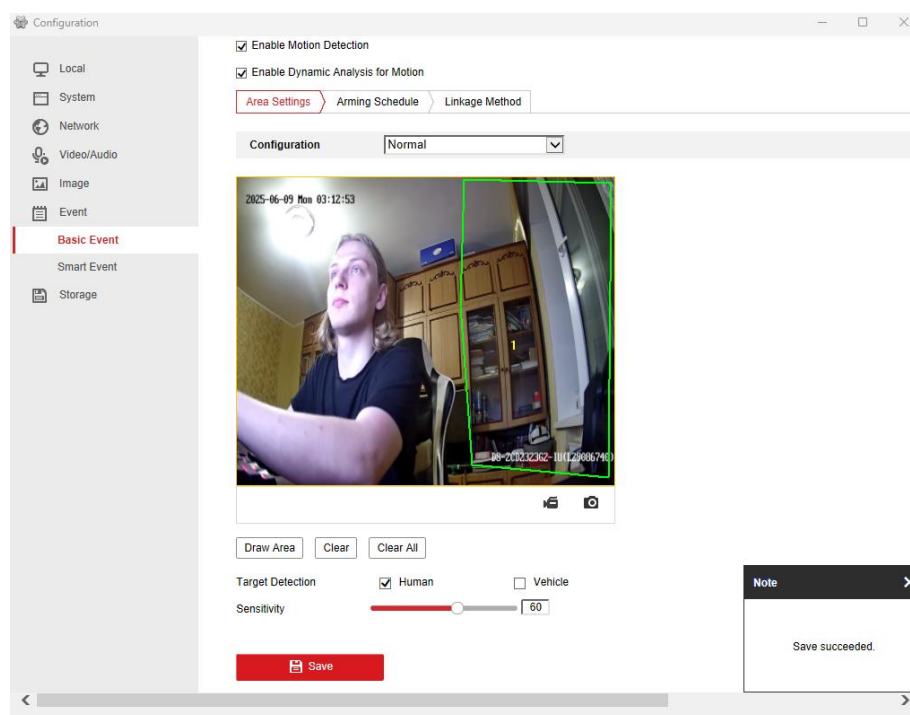


Рисунок 3.53 – Налаштування події

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				57
Змн.	Арк.	№ докум.	Підпис	Дата		

Також додамо розумні події, такі як виявлення облич та динамічний аналіз для виявлення облич (Рисунок 3.54)

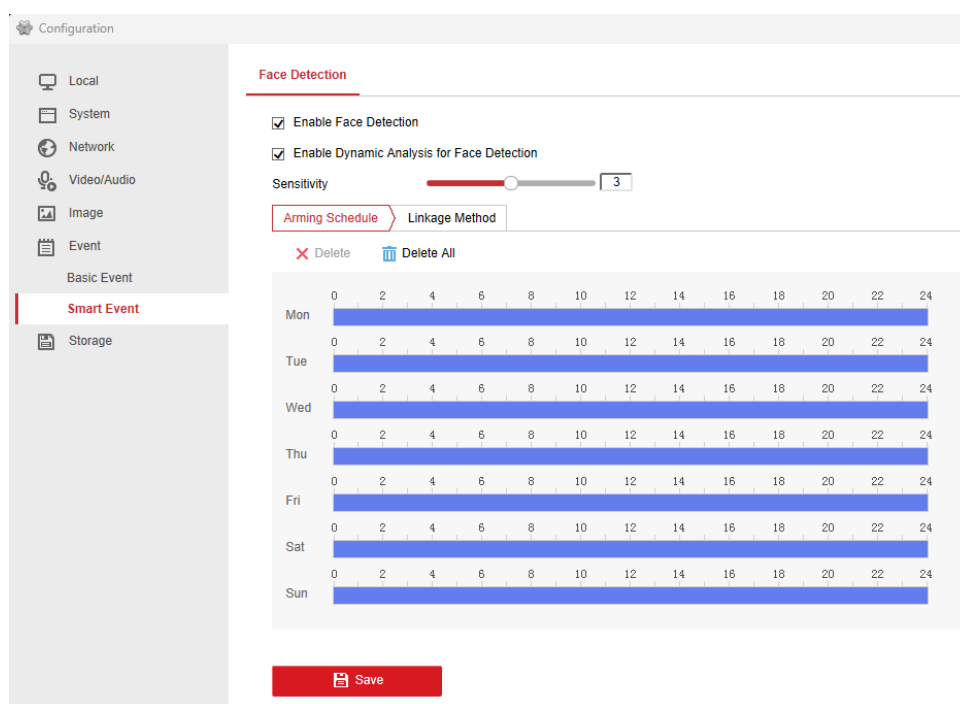


Рисунок 3.54 – Налаштування розумних подій

Через відсутність мережевого відеореєстратора, для зберігання відеоархівів будемо використовувати Hikvision Storage Server. Процес його встановлення відображено на Рисунку 3.55.

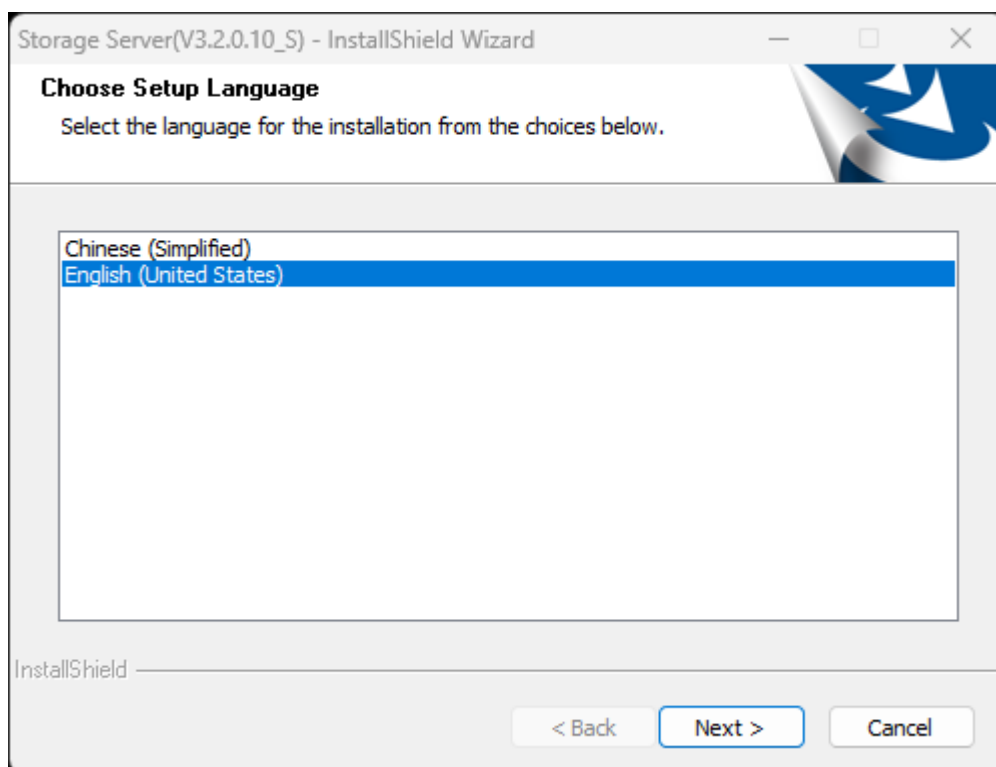


Рисунок 3.55 – Встановлення Hikvision Storage Server

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		58

Після завершення встановлення Hikvision Storage Server, наступним кроком є створення паролю для доступу до системи (Рисунок 3.56).

Рисунок 3.56 – Створення паролю

Коли всі попередні налаштування виконано, додаємо сервер до iVMS-4200. Це забезпечить інтеграцію системи зберігання відео з iVMS (Рисунок 3.57).

Рисунок 3.57 – Додаємо сервер до iVMS

Тепер необхідно перевірити, чи Storage Server з'явився у в списку пристроїв у iVMS-4200 та перевірки його статусу з'єднання (Рисунок 3.58).

Connection T...	Network Param...	Device Type	Serial No.	Security Level	Resource Us...	Firmware Upgrade	Operation
IP/Domain	192.168.0.56:80...	Encoding Device	DS-2CD2323G2-IU202302...	Strong	Online	No available version	[Icons]
IP/Domain	192.168.8.1:8000	Storage Server	DS-NVR-V120B20180309-...	Strong	Online	No available version	[Icons]

Рисунок 3.58 – Перевірка статусу з'єднання

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		59

Тепер додаємо камеру до сховища. Це дозволить збереженню відеопотоку з камери на сервері (Рисунок 3.59).

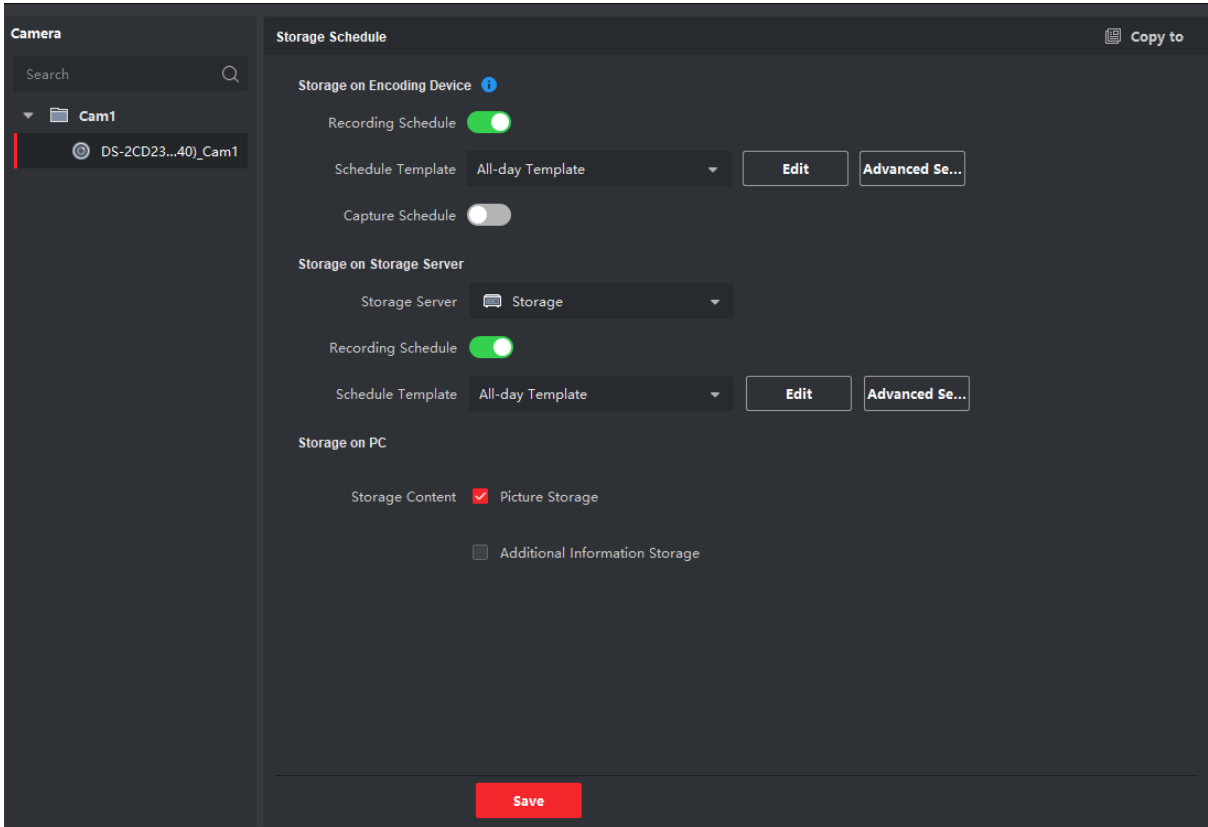


Рисунок 3.58 – Налаштування камери

Тепер, коли ми все налаштували, перевіряємо, чи збереглися якісь дані у сховищі (Рисунок 3.59)

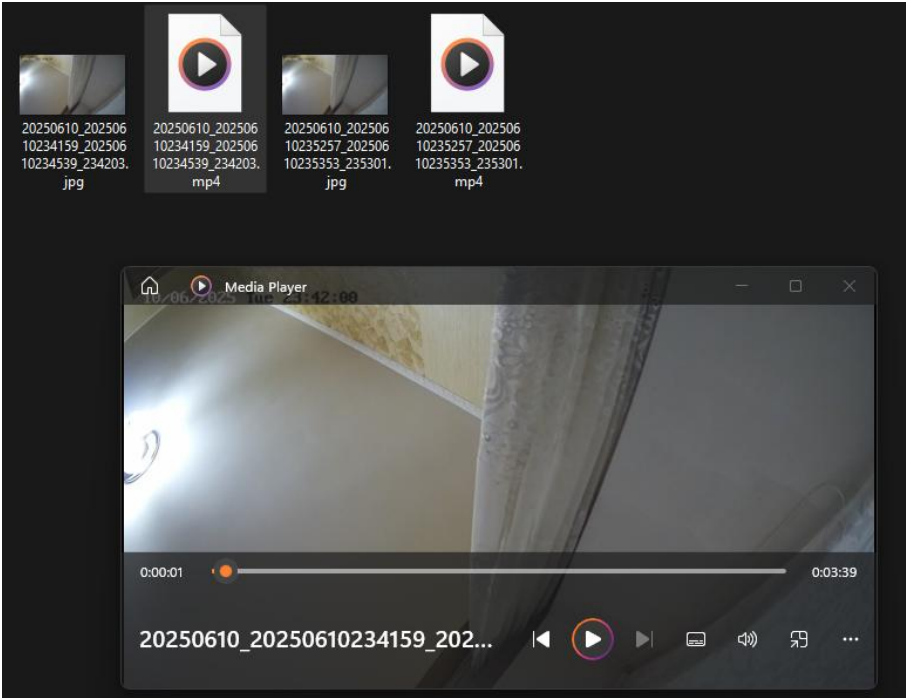


Рисунок 3.59 – Вміст сховища

3.4 Тестування системи

Всі налаштування зроблені, перейдемо до перевірки працездатності всіх систем. Розпочнемо з DHCP чи всім робочим станціям видались адреси їх підмереж (Рисунок 3.60-65).

 DHCP

File

Action

View

Help



 DHCP server-main.hospital.net IPv4 Scope [193.21.8.0] N Address Pool	<table><tr><th>Client IP Address</th><th>Name</th><th>Lease Expiration</th></tr><tr><td> 193.21.8.7</td><td>HOSPITAL-ADMIN....</td><td>09.06.2026 3:37:20</td></tr></table>	Client IP Address	Name	Lease Expiration	 193.21.8.7	HOSPITAL-ADMIN....	09.06.2026 3:37:20
Client IP Address	Name	Lease Expiration					
 193.21.8.7	HOSPITAL-ADMIN....	09.06.2026 3:37:20					

Рисунок 3.60 - Перевірка виданих адрес

DHCP

File

Action

View

Help

DHCP

server-main.hospital.net

IPv4

Scope [193.21.8.0] Net

Scope [194.21.8.0] Net

Client IP Address

Name

Lease Expiration

Type

Unique ID

194.21.8.3

WS-21.hospital.net

24.05.2026 22:26:13

DHCP

005079666...

194.21.8.4

WS-31.hospital.net

18.05.2026 19:40:42

DHCP

005079666...

194.21.8.6

HOSPITAL-PC01.ho...

06.06.2026 21:35:35

DHCP

080027b9f...

Рисунок 3.61 - Перевірка виданих адрес

DHCP

File

Action

View

Help

DHCP

server-main.hospital.net

IPv4

Scope [193.21.8.0] Net

Client IP Address

Name

Lease Expiration

Type

Unique ID

195.21.8.3

WS-51.hospital.net

18.05.2026 19:46:31

DHCP

005079666...

195.21.8.4

WS-61.hospital.net

18.05.2026 19:46:49

DHCP

005079666...

195.21.8.5

HOSPITAL-PC04.ho...

18.05.2026 19:50:58

DHCP

0800279eb...

Рисунок 3.62 - Перевірка виданих адрес

DHCP

File

Action

View

Help

DHCP

server-main.hospital.net

IPv4

Scope [193.21.8.0] Net

Client IP Address

Name

Lease Expiration

Type

Unique ID

196.21.8.3

WS-81.hospital.net

18.05.2026 19:59:42

DHCP

005079666...

196.21.8.4

WS-91.hospital.net

18.05.2026 19:59:57

DHCP

005079666...

196.21.8.5

HOSPITAL-PC07.ho...

18.05.2026 20:02:58

DHCP

08002791d...

Рисунок 3.63 - Перевірка виданих адрес

DHCP

File

Action

View

Help

DHCP

server-main.hospital.net

IPv4

Scope [193.21.8.0] Net...

Scope [194.21.8.0] Net...

Client IP Address	Name	Lease Expiration	Type	Unique ID
197.21.8.3	WS-111.hospital.net	18.05.2026 20:08:46	DHCP	005079666...
197.21.8.4	WS-121.hospital.net	18.05.2026 20:08:52	DHCP	005079666...
197.21.8.5	HOSPITAL-PC10.ho...	18.05.2026 20:14:58	DHCP	080027336...

Рисунок 3.64 - Перевірка виданих адрес

DHCP

File

Action

View

Help

Address Leases

Reservations

Scope Options

Policies

194.21.8.0/24

Client IP Address	Name	Lease Expiration	Type	Unique ID
198.21.8.3	WS-141.hospital.net	09.06.2026 1:05:51	DHCP	005079666...
198.21.8.4	WS-151.hospital.net	09.06.2026 1:06:02	DHCP	005079666...
198.21.8.5	HOSPITAL-PC13.ho...	09.06.2026 1:48:28	DHCP	080027a74...

Рисунок 3.65 - Перевірка виданих адрес

Всі адреси були правильно видані, переходимо до перевірки зв'язку з маршрутизаторами та робочими станціями (Рисунок 3.66-67).

```

PS C:\Users\Administrator> ping 193.21.8.1

Pinging 193.21.8.1 with 32 bytes of data:
Reply from 193.21.8.1: bytes=32 time=6ms TTL=255

Ping statistics for 193.21.8.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 6ms, Average = 6ms
Control-C
PS C:\Users\Administrator> ping 5.0.0.1

Pinging 5.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 5.0.0.1: bytes=32 time=54ms TTL=253
Reply from 5.0.0.1: bytes=32 time=48ms TTL=253
Reply from 5.0.0.1: bytes=32 time=52ms TTL=253

Ping statistics for 5.0.0.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 48ms, Maximum = 54ms, Average = 51ms
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:
Request timed out.
Reply from 20.0.0.1: bytes=32 time=64ms TTL=253
Reply from 20.0.0.1: bytes=32 time=63ms TTL=253

Ping statistics for 20.0.0.1:
    Packets: Sent = 3, Received = 2, Lost = 1 (33% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 63ms, Maximum = 64ms, Average = 63ms
Control-C
PS C:\Users\Administrator> ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:
Reply from 20.0.0.2: bytes=32 time=41ms TTL=252
Reply from 20.0.0.2: bytes=32 time=33ms TTL=252

Ping statistics for 20.0.0.2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 41ms, Average = 37ms
  
```

Рисунок 3.66 – Перевірка зв'язку з маршрутизаторами

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				62
Змн.	Арк.	№ докум.	Підпис	Дата		

```

PS C:\Users\Administrator> ping 194.21.8.4

Pinging 194.21.8.4 with 32 bytes of data:
Reply from 194.21.8.4: bytes=32 time=3066ms TTL=61
Reply from 194.21.8.4: bytes=32 time=62ms TTL=61
Reply from 194.21.8.4: bytes=32 time=63ms TTL=61
Reply from 194.21.8.4: bytes=32 time=55ms TTL=61

Ping statistics for 194.21.8.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 3066ms, Average = 811ms
PS C:\Users\Administrator> ^C
PS C:\Users\Administrator> ping 195.21.8.4

Pinging 195.21.8.4 with 32 bytes of data:
Reply from 195.21.8.4: bytes=32 time=3058ms TTL=61
Reply from 195.21.8.4: bytes=32 time=62ms TTL=61
Reply from 195.21.8.4: bytes=32 time=56ms TTL=61

Ping statistics for 195.21.8.4:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 56ms, Maximum = 3058ms, Average = 1058ms
Control-C
PS C:\Users\Administrator> ping 196.21.8.4

Pinging 196.21.8.4 with 32 bytes of data:
Reply from 196.21.8.4: bytes=32 time=3032ms TTL=61
Reply from 196.21.8.4: bytes=32 time=39ms TTL=61

Ping statistics for 196.21.8.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 39ms, Maximum = 3032ms, Average = 1535ms
Control-C
PS C:\Users\Administrator> ping 197.21.8.4

Pinging 197.21.8.4 with 32 bytes of data:
Reply from 197.21.8.4: bytes=32 time=3028ms TTL=61
Reply from 197.21.8.4: bytes=32 time=40ms TTL=61

Ping statistics for 197.21.8.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 3028ms, Average = 1534ms

```

Рисунок 3.67 – Перевірка зв'язку з робочими станціями

Всі пристрої пінгуються, тепер перейдемо до перевірки віддаленого доступу до обладнання та серверу (Рисунок 3.68-70).

Рисунок 3.68 – Перевірка SSH маршрутизаторів

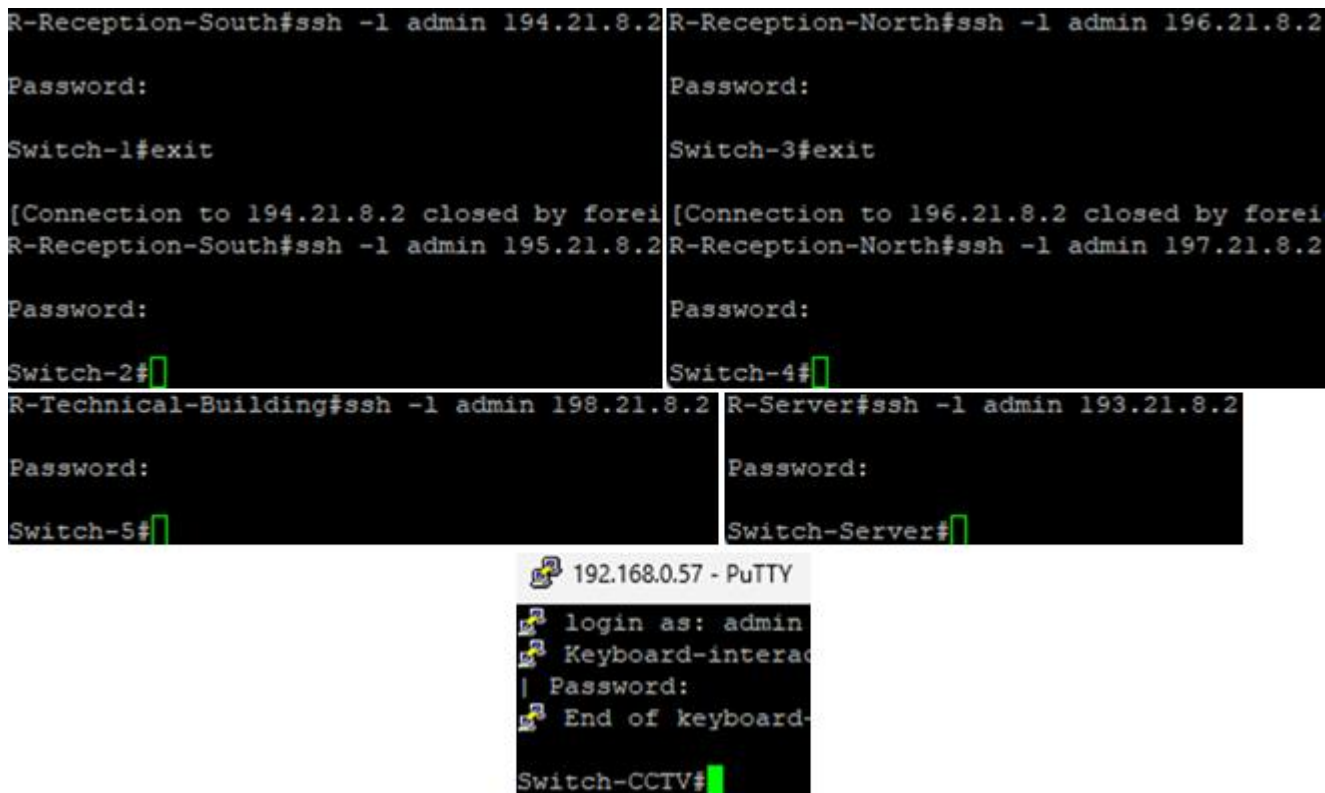


Рисунок 3.69 – Перевірка SSH комутаторів

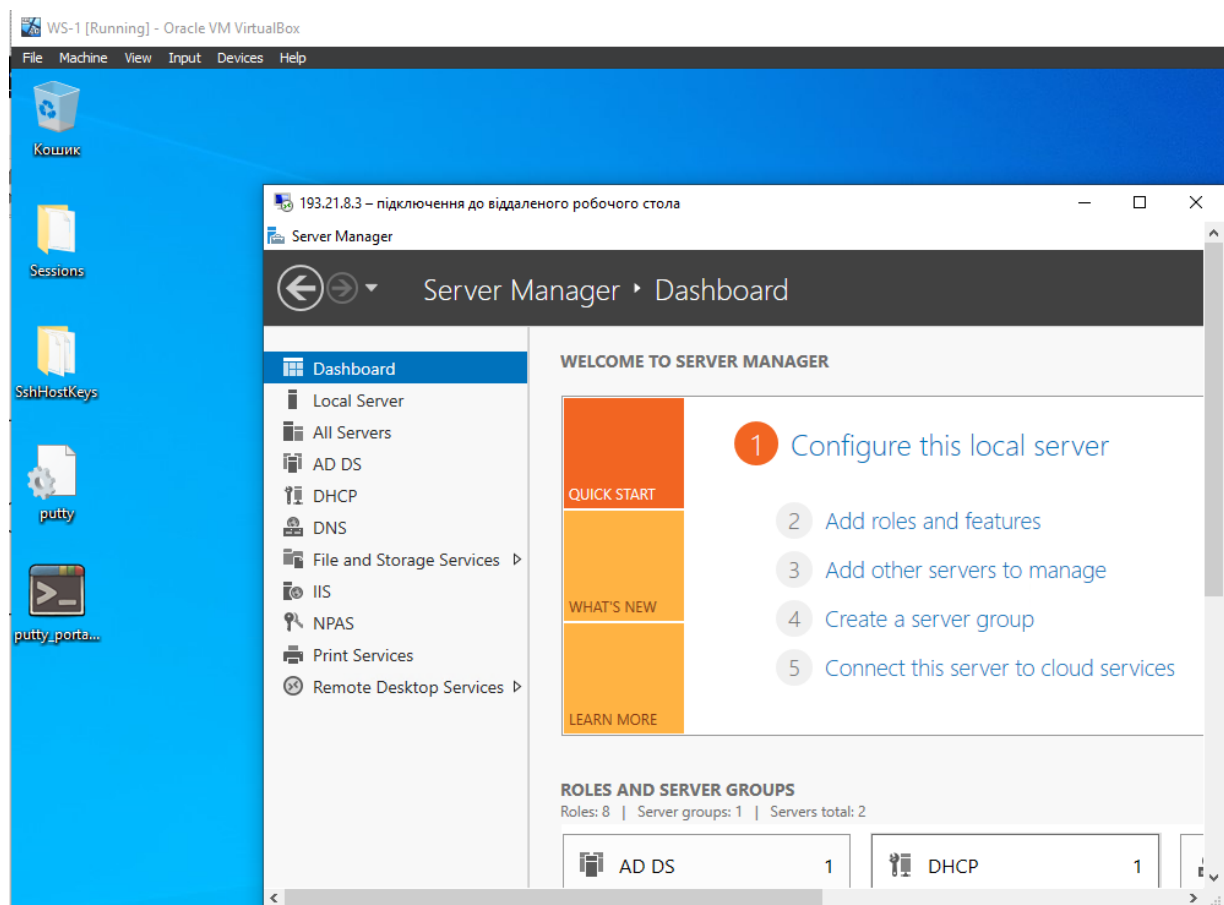


Рисунок 3.70 – Перевірка RDS

Тепер перевірка групових політик на комп'ютері користувача (Рисунок 3.71).

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				64
Змн.	Арк.	№ докум.	Підпис	Дата		

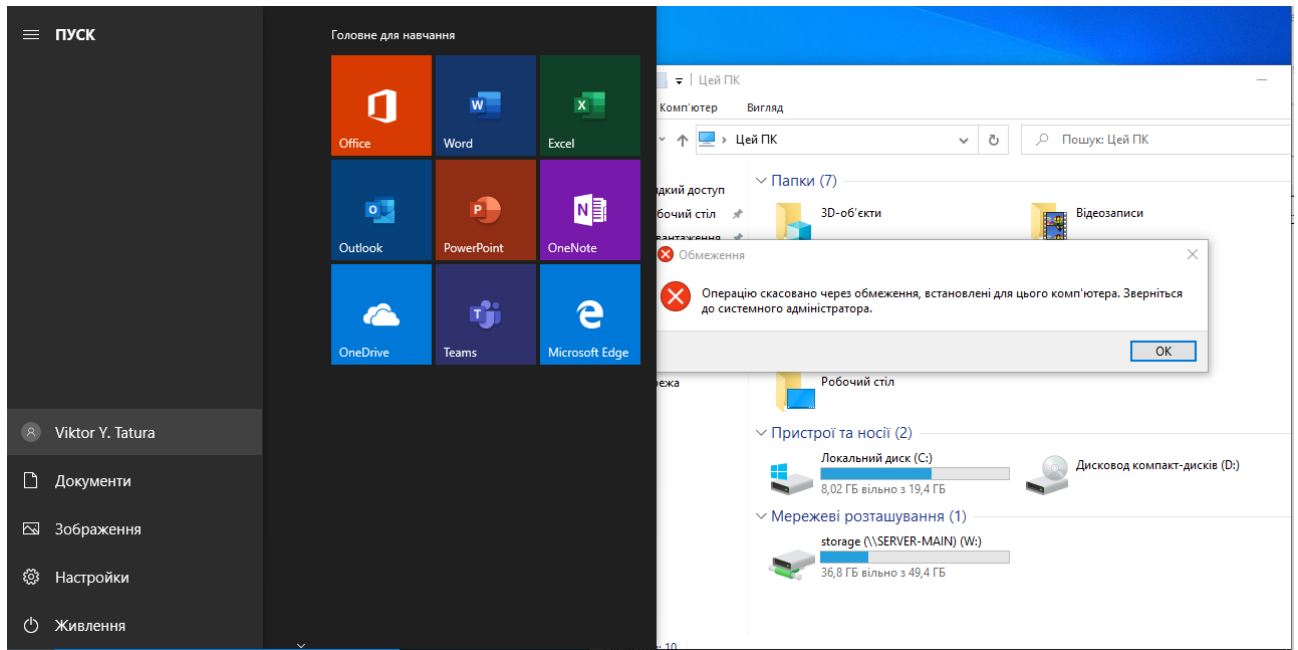


Рисунок 3.71– Перевірка групових політик

Аналіз рисунків підтверджує, що групові політики працюють коректно, а саме користувачі домену не мають доступу до системних налаштувань, флеш накопичувач не відображається, тоді як мережевий диск є доступним. Далі перевіримо функціональність відеоспостереження, зокрема роботу налаштованих подій (Рисунок 3.72-73).

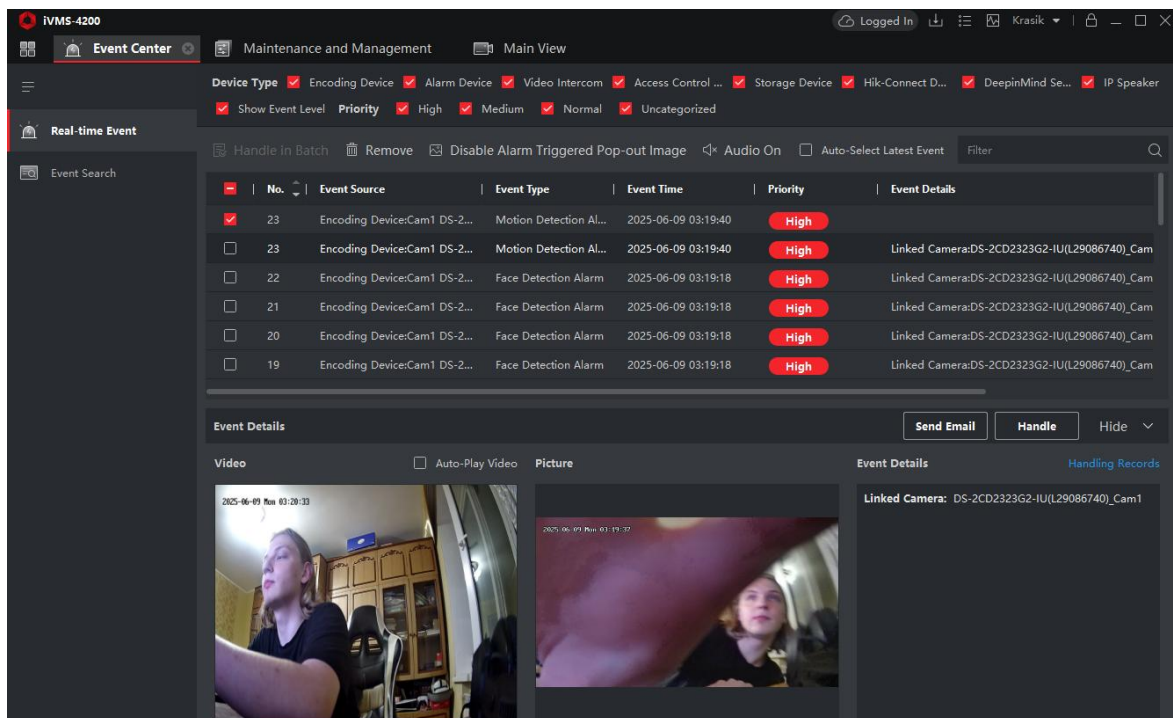


Рисунок 3.72 – Журнал подій

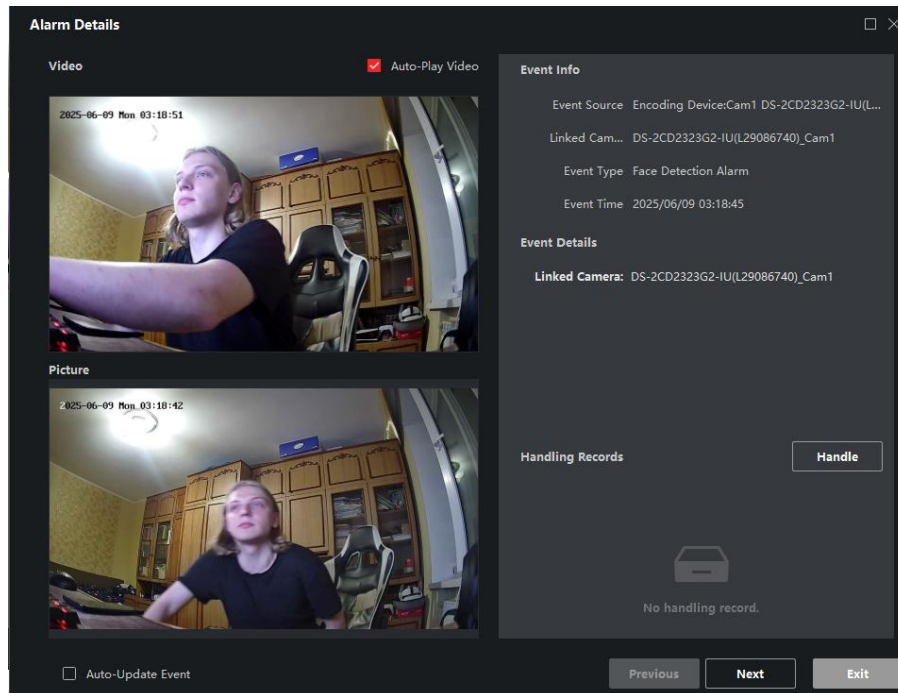


Рисунок 3.73 – Журнал подій

Перевірка системи відеоспостереження підтвердила її повну працездатність та відповідність вимогам проєкту. Камера успішно налаштована, а всі визначені події, включаючи виявлення руху та розумні події, коректно реєструються та зберігаються у сховищі. Таким чином, всі перевірки завершені, і система готова до експлуатації.

3.5 Перспективи розвитку

Проєкт комплексної системи мережевого доступу та безпеки міської лікарні створює міцну основу, проте має значний потенціал для подальшого розширення та модифікації. Перспективи розвитку охоплюють наступні напрямки:

Інтеграція з системами електронного документообігу Helsi: забезпечення безшовної інтеграції з існуючими та майбутніми медичними інформаційними системами та платформами електронного документообігу. Це дозволить оптимізувати обмін даними, прискорити доступ до медичних записів та адміністративної інформації, а також покращити взаємодію між лікарями, пацієнтами та іншими учасниками медичного процесу.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		66

Впровадження хмарних технологій: дослідження можливостей використання гібридних або публічних хмарних рішень для зберігання певних типів даних, резервного копіювання або розміщення некритичних сервісів. Це може забезпечити підвищену гнучкість, масштабованість та економію на апаратній інфраструктурі, з одночасним дотриманням вимог щодо захисту персональних даних пацієнтів.

Підвищення рівня кібербезпеки: Постійне вдосконалення механізмів кібербезпеки шляхом впровадження сучасних методів шифрування для всіх типів передачі даних, багатоетапної автентифікації для всіх користувачів та адміністраторів, розгортання систем виявлення вторгнень та централізованого управління доступом до мережевих ресурсів на основі ролей.

Автоматизація та моніторинг мережі: Впровадження систем автоматизованого моніторингу, таких як Zabbix. Це дозволить здійснювати безперервний контроль за станом мережевого обладнання, серверів та сервісів, своєчасно виявляти аномалії, прогнозувати потенційні проблеми, оптимізувати трафік та проводити профілактичне обслуговування обладнання, мінімізуючи час простою.

Розширення мережевої інфраструктури: У майбутньому можливе органічне розширення мережі шляхом підключення до системи додаткових відділень, корпусів або амбулаторій. Це дозволить створити єдину, централізовано керовану мережу для всього медичного закладу, забезпечуючи уніфікований доступ до ресурсів та сервісів.

Впровадження IoT-технологій: Інтеграція Інтернету речей у медичне середовище. Це може включати підключення до мережі розумних пристроїв, таких як датчики моніторингу стану пацієнтів, системи відстеження медичного обладнання, автоматизацію систем освітлення, клімат-контролю та інших аспектів управління будівлею. Такі технології дозволять значно підвищити якість та швидкість надання медичних послуг, а також оптимізувати використання ресурсів.

Резервування та відновлення даних: Постійне вдосконалення стратегій резервування та відновлення даних. Це включає регулярне створення резервних копій критично важливих медичних та адміністративних даних, а також розробку та тес-

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		67

тування процедур швидкого відновлення в разі збоїв, кібератак чи інших непередбачуваних ситуацій. Це дозволить мінімізувати ризики втрати інформації та забезпечити безперервність роботи лікарні.

Модернізація обладнання: Планове оновлення мережевого обладнання з урахуванням зростаючих потреб у пропускній здатності та нових технологій. Модернізація маршрутизаторів, комутаторів та серверів забезпечить підтримку більш високої пропускної здатності, зниження затримок та стабільну роботу системи в умовах зростання навантажень та впровадження нових сервісів.

Висновок до третього розділу

У цьому розділі ми успішно налаштували мережеві пристрої та повністю розгорнули Microsoft Active Directory, включаючи DHCP, DNS та створення користувачів. Детально конфігурували групові політики для забезпечення безпеки. Також налагоджено систему відеоспостереження з камерою HikVision, включаючи аналітику та використання Hikvision Storage Server для зберігання. Фінальне тестування підтвердило повну працездатність мережі, коректність адресації, надійний зв'язок та ефективність застосованих політик безпеки, свідчаючи про готовність інфраструктури до використання.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				
Змн.	Арк.	№ докум.	Підпис	Дата		68

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було успішно розроблено та протестовано комплексну та безпечну систему мережевого доступу та відеоспостереження для міської лікарні. Метою роботи було створення інтегрованої системи, що забезпечує централізоване управління ресурсами, захист чутливих даних та високу доступність сервісів, враховуючи специфіку медичного середовища.

Проведено комплексний аналіз сучасних технологій, протоколів та обладнання, необхідних для проектування мережевої інфраструктури медичних установ. Було обґрунтовано вибір клієнт-серверної архітектури мережі як найбільш ефективною та безпечною для лікарні, що дозволяє централізовано керувати доступом до ресурсів та інформації.

Особливу увагу було приділено системі Microsoft Active Directory, що була реалізована та налаштована як ключове рішення для адміністрування користувачів, пристроїв та групових політик у корпоративній мережі. Завдяки AD забезпечено централізоване управління правами доступу, що є критично важливим для захисту чутливих медичних даних. Налаштовані групові політики ефективно розмежовують доступ користувачів до ресурсів та функцій операційних систем, підвищуючи загальний рівень безпеки.

Детально розглянуто та реалізовано систему відеоспостереження, використовуючи IP-камеру Hikvision DS-2CD2323G2-IU та програмне забезпечення Hikvision iVMS-4200. Було продемонстровано переваги використання обраного обладнання та ПЗ, включаючи високу якість зображення, інтелектуальні функції відеоаналітики та ефективне зберігання даних за допомогою Storage Server.

У рамках роботи було розроблено логічну топологію мережі для трьох будівель лікарні та детально сплановано схему IP-адресації. Налаштування DHCP-сервера на базі Windows Server забезпечило автоматизоване управління адресами для кінцевих пристроїв, тоді як сервери та ключові мережеві пристрої отримали статичні IP-адреси.

Проведене моделювання та тестування системи в GNS3, а також тестування реалізованої частини відеоспостереження на фізичному обладнанні, підтвердило

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				69
Змн.	Арк.	№ докум.	Підпис	Дата		

повну працездатність та ефективність запропонованих рішень. Було підтверджено коректність IP-адресації, надійність зв'язку між усіма сегментами мережі та функціональність реалізованих політик безпеки.

Таким чином, результати кваліфікаційної роботи демонструють здатність до проектування, розробки та налагодження сучасної, інтегрованої та безпечної комплексної системи мережевого доступу та відеоспостереження для медичних установ. Перспективи подальшого розвитку включають інтеграцію з іншими медичними інформаційними системами, впровадження хмарних технологій, подальше підвищення рівня кібербезпеки та автоматизацію моніторингу мережі, що підкреслює значний потенціал розробленої системи для покращення якості та безпеки медичних послуг.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				70
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cisco Systems. Zero Trust Security in Healthcare Organizations, Cisco White Paper, 2023.
2. Splunk Inc. What is Network Architecture? [Best practices for secure and scalable network design], 2024.
3. National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018.
4. Alturki, J. M., et al. "Security Engineering of Patient-Centered Health Care Information Systems in Peer-to-Peer Networks." Healthcare, 2020.
5. Microsoft. Client-Server Networking Model Overview. Microsoft Learn, 2022.
6. Microsoft Docs. Active Directory Overview. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>, 2025.
7. Microsoft Docs. Group Policy Overview. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview>, 2025.
8. Microsoft Docs. Domain Controller Overview. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>, 2025.
9. Microsoft Docs. Group Policy Management Console (GPMC). URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-policy/group-policy-management-console>, 2025.
10. Microsoft Docs. Managing Active Directory Groups. URL: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/replication/active-directory-replication-concepts>, 2025.
11. Lonnquist K., Lynch J. Windows Server 2016: Active Directory. Wiley, 2017.
12. Chen, J., & Wang, L. Advanced IP Camera Technologies and Their Applications. IEEE Transactions on Multimedia, 2021, 23(4), 982-995.
13. Official documentation of Network Video Recorders (NVR). Dahua Technology, 2021.
14. Dahua Technology. Video Management System Overview, 2021.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				71
Змн.	Арк.	№ докум.	Підпис	Дата		

15. Smith, A. Video Analytics and Security Integration in Modern VMS. Journal of Security Technology, 2021, 15(2), 123-134.
16. Коваленко, І. П. Управління правами доступу у системах відеоспостереження. Безпека інформаційних систем, 2020, 8(3), 45-52.
17. Cisco Systems. Cisco Catalyst 8000 Edge Platform Data Sheet, 2023.
18. Cisco Systems. Cisco 7200 Series Routers Overview, 2022.
19. Cisco Systems. Cisco Catalyst 1000 Series Switches Data Sheet, 2023.
20. Hikvision. DS-2CD2323G2-IU Network Camera Datasheet. Hikvision Official Documentation, 2023
21. Hikvision. AcuSense Technology White Paper. Hikvision Global, 2022.
22. PoE Standards and Applications. IEEE 802.3af/at Overview. IEEE Standards Association, 2021.

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				72
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Красовський В.І.			ККІКБ.КР.Б – 123 – 8 – ПЗ	Арк.
		Шелуха О.О.				73
Змн.	Арк.	№ докум.	Підпис	Дата		

Зведена таблиця IP-адресації

Мережа / Пристрій	Інтерфейс	IP-адреса	Маска	Префікс
Маршрутизатор R-Main-Building	G0/0	5.0.0.2	255.255.255.252	/30
	G1/0	40.0.0.2	255.255.255.252	/30
	G2/0	35.0.0.2	255.255.255.252	/30
	G3/0	25.0.0.1	255.255.255.252	/30
	G4/0	10.0.0.2	255.255.255.252	/30
Маршрутизатор R-Reception-South	G0/0	194.21.8.1	255.255.255.224	/27
	G1/0	195.21.8.1	255.255.255.224	/27
	G2/0	30.0.0.1	255.255.255.252	/30
	G3/0	15.0.0.1	255.255.255.252	/30
	G4/0	10.0.0.1	255.255.255.252	/30
Маршрутизатор R-Reception-North	G0/0	197.21.8.1	255.255.255.224	/27
	G1/0	196.21.8.1	255.255.255.224	/27
	G2/0	35.0.0.1	255.255.255.252	/30
	G3/0	15.0.0.2	255.255.255.252	/30
	G4/0	20.0.0.1	255.255.255.252	/30
Маршрутизатор R-Technical-Building	G0/0	198.21.8.1	255.255.255.224	/27
	G2/0	30.0.0.2	255.255.255.252	/30
	G3/0	25.0.0.2	255.255.255.252	/30
	G4/0	20.0.0.2	255.255.255.252	/30
Маршрутизатор R-Server	G0/0	192.168.0.58	255.255.255.0	/24
	G1/0	40.0.0.1	255.255.255.252	/30
	G2/0	193.21.8.1	255.255.255.224	/27
Маршрутизатор Mikrotik	G0/0	5.0.0.1	255.255.255.252	/30
	G1/0	DHCP		
Мережа А		193.21.8.0	255.255.255.224	/27
Комутатор Switch-Server	Інтерфейс Vlan1	193.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1	-	-
Комутатор Switch-CCTV	Інтерфейс Vlan1	192.168.0.57	255.255.255.0	/24
	Шлюз за замовчуванням	193.21.8.1		
Сервер Srv-Win-Main	Мережний адаптер	193.21.8.3	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1	-	-
Сервер Srv-Win-Reserve	Мережний адаптер	193.21.8.4	255.255.255.224	/27
	Шлюз за замовчуванням	193.21.8.1	-	-

WS-Administrator	Мережний адаптер	DHCP		
CCTV-1	Мережний адаптер	192.168.0.56	255.255.255.0	/24
Мережа B		194.21.8.0	255.255.255.224	/27
Комутатор Switch-1	Інтерфейс Vlan1	194.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	194.21.8.1	-	-
WS-1	Мережний адаптер	DHCP		
WS-2	Мережний адаптер	DHCP		
WS-3	Мережний адаптер	DHCP		
Мережа C		195.21.8.0	255.255.255.224	/27
Комутатор Switch-2	Інтерфейс Vlan1	195.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	195.21.8.1	-	-
WS-4	Мережний адаптер	DHCP		
WS-5	Мережний адаптер	DHCP		
WS-6	Мережний адаптер	DHCP		
Мережа D		196.21.8.0	255.255.255.224	/27
Комутатор Switch-3	Інтерфейс Vlan1	196.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	196.21.8.1	-	-
WS-7	Мережний адаптер	DHCP		
WS-8	Мережний адаптер	DHCP		
WS-9	Мережний адаптер	DHCP		
Мережа E		197.21.8.0	255.255.255.224	/27
Комутатор Switch-4	Інтерфейс Vlan1	197.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	197.21.8.1	-	-
WS-10	Мережний адаптер	DHCP		
WS-11	Мережний адаптер	DHCP		
WS-12	Мережний адаптер	DHCP		
Мережа F		198.21.8.0	255.255.255.224	/27
Комутатор Switch-5	Інтерфейс Vlan1	198.21.8.2	255.255.255.224	/27
	Шлюз за замовчуванням	198.21.8.1	-	-
WS-13	Мережний адаптер	DHCP		
WS-14	Мережний адаптер	DHCP		
WS-15	Мережний адаптер	DHCP		