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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Караськіна Іллі Євгеновича
(ПІБ)
академічної групи 123-19-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(офіційна назва)
на тему "Комп'ютерна система КП «Дніпропетровська обласна клінічна офтальмологічна лікарня» з детальною реалізацією побудови та налаштування корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	проф. Цвіркун Л.І.			
розділів:				
розробка апаратної частини	доц. Бешта Д.О.			
розробка корпоративної мережі	ас. Панферова Я.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

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

"26" січня 2023 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Караськіна Іллі Євгеновича **академічної групи** 123-19-1
(прізвище та ініціали) (шифр)
спеціальності 123 «Комп'ютерна інженерія»
за освітньо-професійною програмою 123 «Комп'ютерна інженерія»
(офіційна назва)
на тему "Комп'ютерна система КП «Дніпропетровська обласна клінічна офтальмологічна лікарня» з детальною реалізацією побудови та налаштування корпоративної мережі"

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	05.06.2023

Завдання видано _____ проф. Цвіркун Л.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 10.02.2023

Дата подання до екзаменаційної комісії 07.06.2023

Прийнято до виконання _____ Караськін І.Є.

РЕФЕРАТ

Пояснювальна записка: 86 с., 34 Рис., 9 Табл., 3 дод., 9 джерел.

СИСТЕМА, МЕРЕЖА, ПІДПРИЄМСТВО, СЕРВЕР, КОМУТАТОР, МАРШРУТИЗАТОР, ПРИСТРІЙ, LAN, VLSM, VLAN, VPN.

Об’єкт розробки: комп'ютерна система КП «Дніпропетровська обласна клінічна офтальмологічна лікарня» з детальною реалізацією побудови та налаштування корпоративної мережі.

Мета: організація корпоративної комп'ютерної мережі КП «Дніпропетровська обласна клінічна офтальмологічна лікарня» із детальним опрацюванням нюансів налаштування апаратно-програмного мережного комплексу для подальшого розгортання цієї мережі та використання її для подальшої роботи підприємства.

Розроблено комп’ютерну систему з можливістю здійснювати програмну та технічну модернізацію системи, орієнтовану на функціонування медичних закладів галузі охорони здоров’я типу лікарня.

Система дозволяє виконувати наступні функції:

– забезпечення доступу медичним працівникам до електронних медичних сервісів;

– здійснення адміністративно-господарської діяльності, пов’язаної з доступом до мережі;

– забезпечення створення, сортування та зберігання даних системи;

– забезпечення роботи мережевих програм підприємства;

– організація зв’язку між працівниками та Internet.

Розробку комп’ютерної мережі було виконано відповідно до завдання на кваліфікаційну роботу бакалавра.

Розроблену схему мережі було реалізовано у вигляді моделі на базі симулятора Cisco Packet Tracer та було перевірено її працездатність.

Результати перевірки у вигляді таблиць, графіків та рисунків були описані і наводяться у пояснювальній записці або додатках.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КП – комунальне підприємство;

ПЗ – програмне забезпечення;

IP – Internet Protocol;

LAN – Local Area Network;

VLAN – Virtual Local Area Network;

WAN – Wide Area Network;

WEB – World Wide Web;

VPN – Virtual Private Network;

NAT – Network Address Translation;

AAA – Authentication, Authorization, Accounting.

ВСТУП

Протягом останніх років в нашій країні активно відбувається медична реформа. У зв’язку с цим впроваджуються нові прогресивні системи електронного зберігання медичних даних, онлайн сервісів запису до лікарів, виписки електронних рецептів та направлень, електронного документообігу. З метою відповідності новим вимогам до галузі охорони здоров’я, підвищення ефективності та зручності медичного обслуговування населення, медичні працівники різних рівнів долучаються до роботи з електронними сервісами, отримують власні облікові записи та електронні підписи. Адміністративно-господарська та управлінська діяльність закладів охорони здоров’я теж активно долучається до користування інформаційними технологіями. Це стосується багатьох напрямків діяльності: використання програмного забезпечення від компанії Microsoft для створення різного роду документів; використання у роботі програмних продуктів для кадрового, бухгалтерського та складського обліку, функціонування планово-економічного відділу та інформаційно аналітичного відділу медичної статистики; проведення процедур публічних закупівель на електронних торгових майданчиках у системі Prozorro; подання звітності до контролюючих органів та обміну юридично значущими первинними документами між контрагентами в електронному вигляді через «M.E.Doc» (My Electronic Document); дистанційне банківське обслуговування; використання у роботі електронних ключів; електронного листування, тощо.

Реалізація такого обсягу заходів та організація ефективної роботи вимагає впровадження на підприємствах галузі охорони здоров’я новітніх інформаційних технологій передачі, обробки та зберігання інформації, оснащення працівників комп’ютерною технікою з можливістю безперебійного доступу до мережі Internet, інтенсивного використання комп'ютерних мереж та серверів.

Для успішної роботи КП «ДОКОЛ» та відповідності усім сучасним вимогам, вкрай необхідне впровадження ефективної комп'ютерної системи.

В даному проекті вирішуються задача створення комп'ютерної системи КП «Дніпропетровська обласна клінічна офтальмологічна лікарня» з детальною реалізацією побудови та налаштування корпоративної мережі, з забезпеченням необхідного рівня комунікацій, функціонування, зберігання та захисту інформації.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умов застосування комп’ютерної системи.

Галузь діяльності підприємства, яке було обрано нами як об’єкт впровадження комп’ютерної системи, – охорона здоров’я. Ця галузь є одним із основоположних елементів соціальної сфери та входить в число найбільш важливих обов’язків нашої держави. Її мета – збереження та зміцнення здоров'я населення за допомогою профілактичної, лікувальної та інших видів діяльності медичних установ.

У наш час в галузі охорони здоров’я широко застосовуються сучасні технології та можливості, що вони надають. Комп’ютерні системи допомагають автоматизувати роботу лікарів та іншого персоналу лікарень, вести електрону звітність ліків, зберігати та працювати з електронними картами пацієнтів. Лікарі отримують змогу працювати з новітнім медичним обладнанням, що гарно сприяє на якість та швидкість отримуваної населенням медичної допомоги.

На даний час саме для медичної галузі має велике значення поглиблення, розширення та покращення доступу до мережі Internet та спеціалізованих систем та сервісів. Так, кожного лікаря, сертифікований державою, зареєстровано в таких інформаційних системах, як Helsi. Вони є активними користувачам цих систем, виписуючи електроні рецепти, направлення до фахівців та багато іншого. Ціж системи дають змогу пацієнтам перегляду медичних послуг та реєстрації на прийом того чи іншого фахівця.

Сучасні комп’ютерні системи також дуже важливі для адміністративно-господарської діяльності медичних закладів. Така діяльність вимагає від працівників реєстрації на електронних торгових майданчиках для проведення закупівель у системі Prozorro згідно із законом України «Про

публічні закупівлі». Також необхідний доступ працівників адміністративно-управлінського персоналу до реєстрації на сервісах НСЗУ (Національної Служби Здоров'я України), до електронної системи MeDoc, податкових та статистичних служб, дистанційного банківського обслуговування та обслуговування працюючих на підприємстві програмних продуктів, тощо.

1.2 Характеристика і структура об'єкта впровадження

Комп'ютерну систему нами буде впроваджено у комунальному підприємстві «Дніпропетровська обласна клінічна офтальмологічна лікарня» (ск. КП «ДОКОЛ») та її відокремленого підрозділу - Криворізька філія комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня» (ск. КФ КП «ДОКОЛ»).

Основний вид діяльності цього підприємства – діяльність лікарняних закладів (код 86.10).

Ця лікарня є унікальною спеціалізованою державною клінікою, яка на найвищому рівні щодня надає весь спектр офтальмологічної допомоги дорослим та дітям.

В ній проводять діагностику та лікування широкого спектру очних захворювань від комп'ютерної діагностики до складних хірургічних втручань, таких як кератопластика за допомогою новітніх лазерних технологій.

Завдяки цьому та багатьом іншим факторам, вона вважається найкращою офтальмологічною клінікою у Дніпропетровській області та однією з провідних офтальмологічних клінік України, в якій працює дуже багато провідних спеціалістів в області хірургії ока.

На даний час це комунальне підприємство також вносить великий вклад в надання медичної допомоги пораненим воїнам ЗСУ.

Об'єкт впровадження комп'ютерної системи має головний підрозділ КП «ДОКОЛ», що знаходиться за адресою: площа Соборна, 14, м. Дніпро, Дніпропетровська область (Рис. 1.1), а також відокремлений підрозділ – КФ

КП «ДОКОЛ», що знаходиться за адресою: вул. Володимира Великого, 21, м. Кривий Ріг, Дніпропетровська область (Рис. 1.2).

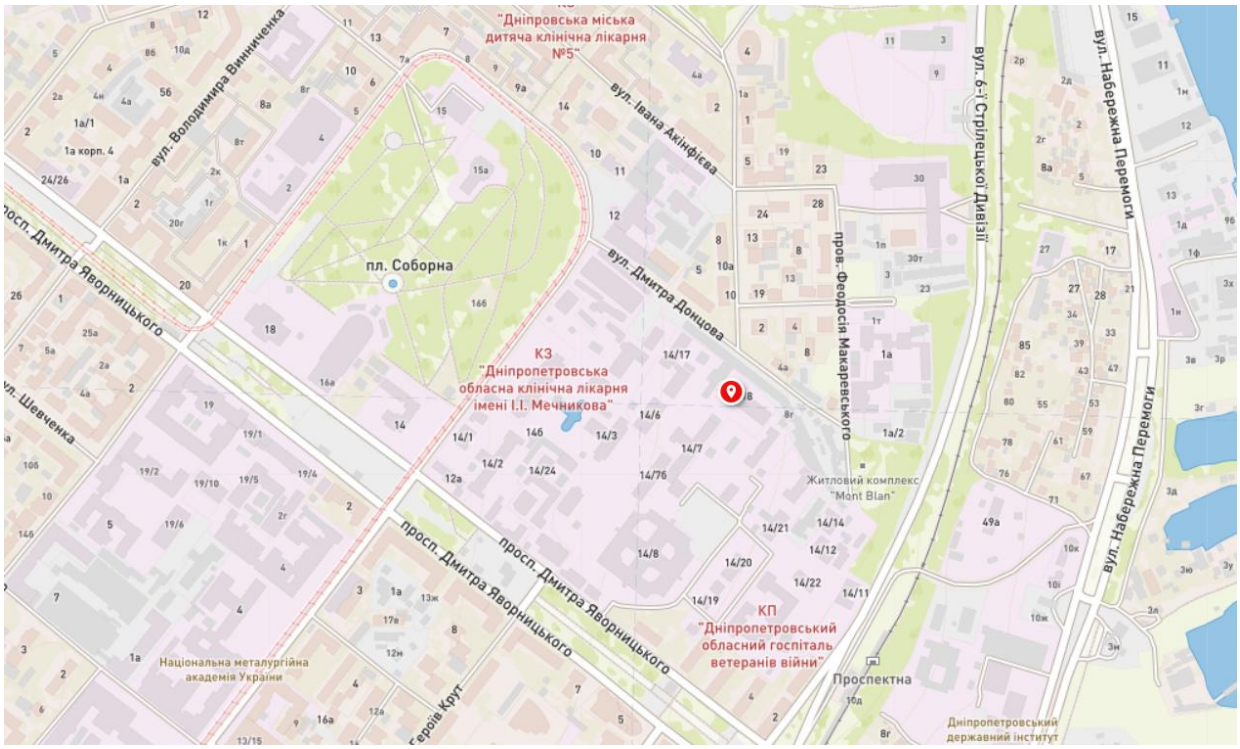


Рисунок 1.1 – Схема гео-позиції КП «ДОКОЛ»

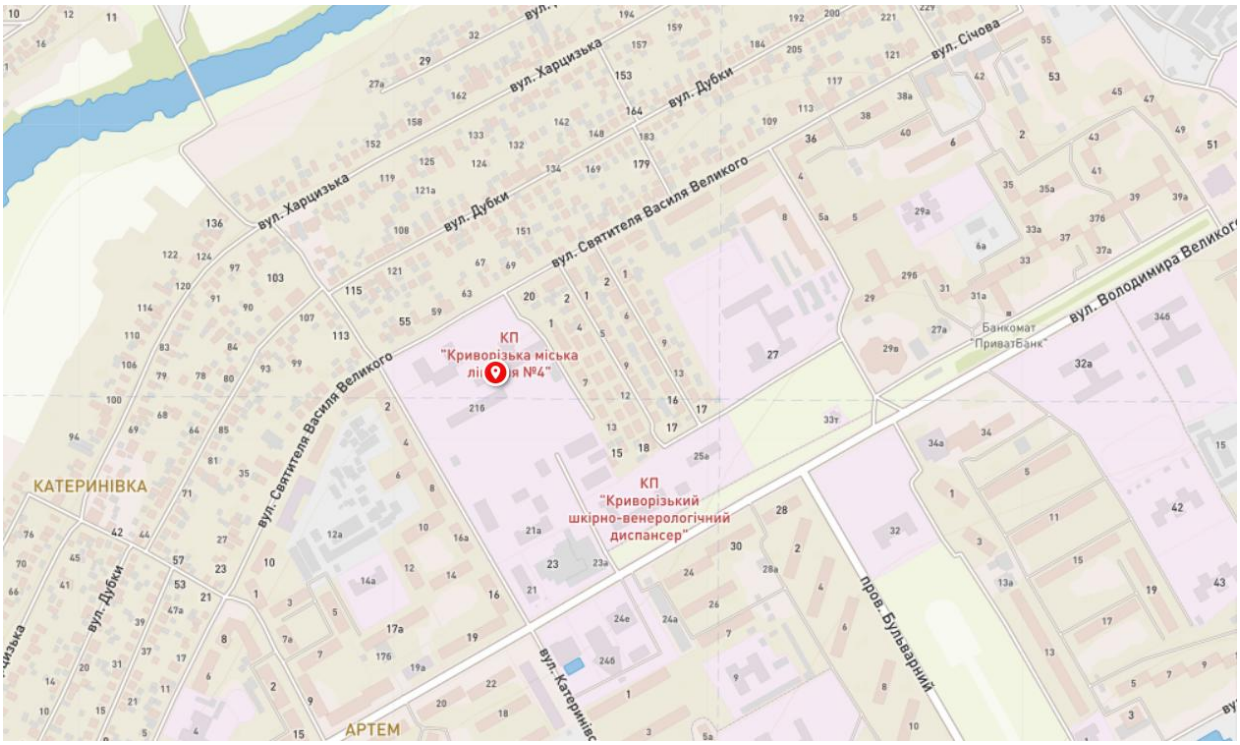


Рисунок 1.2 – Схема гео-позиції КФ КП «ДОКОЛ»

Топологія основного підрозділу комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня», що буде розглядатись нами у цьому проекті, складається з однієї 6-поверхової будівлі.

Структурну схему підприємства нами буде розглянуто на прикладі першого та третього поверхів будівлі, у яких розташовані основні його відділи, що потребують найбільш детального опрацювання комп'ютерною системою. Для цього нами було отримано затверджені схеми цих поверхів підприємства, а саме першого та третього його поверхів (Додаток А), на основі яких нами було побудовано відповідні топологічні схеми.

Топологічні схеми поверхів, представлені на рисунках 1.3 – 1.6, поділеними на дві частини (ліве та праве крило) з наведенням на кожній частині загального для них приміщення холу з метою покращення візуалізації у зв'язку з тим, що план поверху має занадто великий розмір та в повному виді потребує занадто великого масштабування.

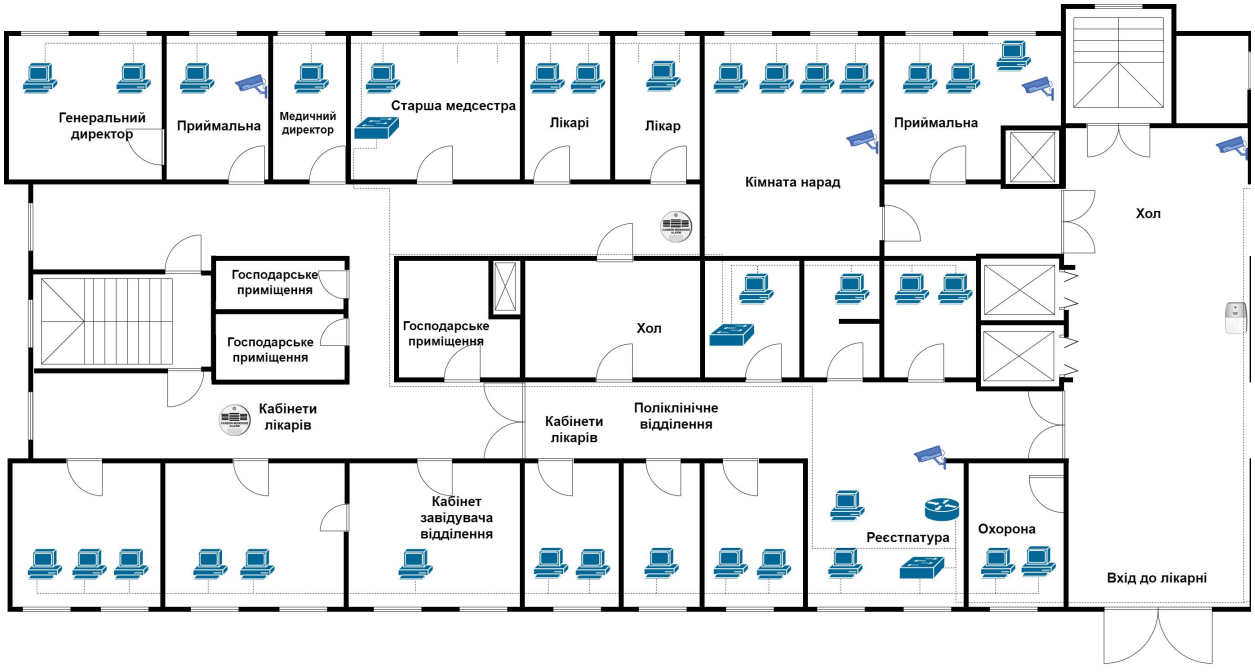


Рисунок 1.3 – Топологічна схема першого поверху (ліве крило)

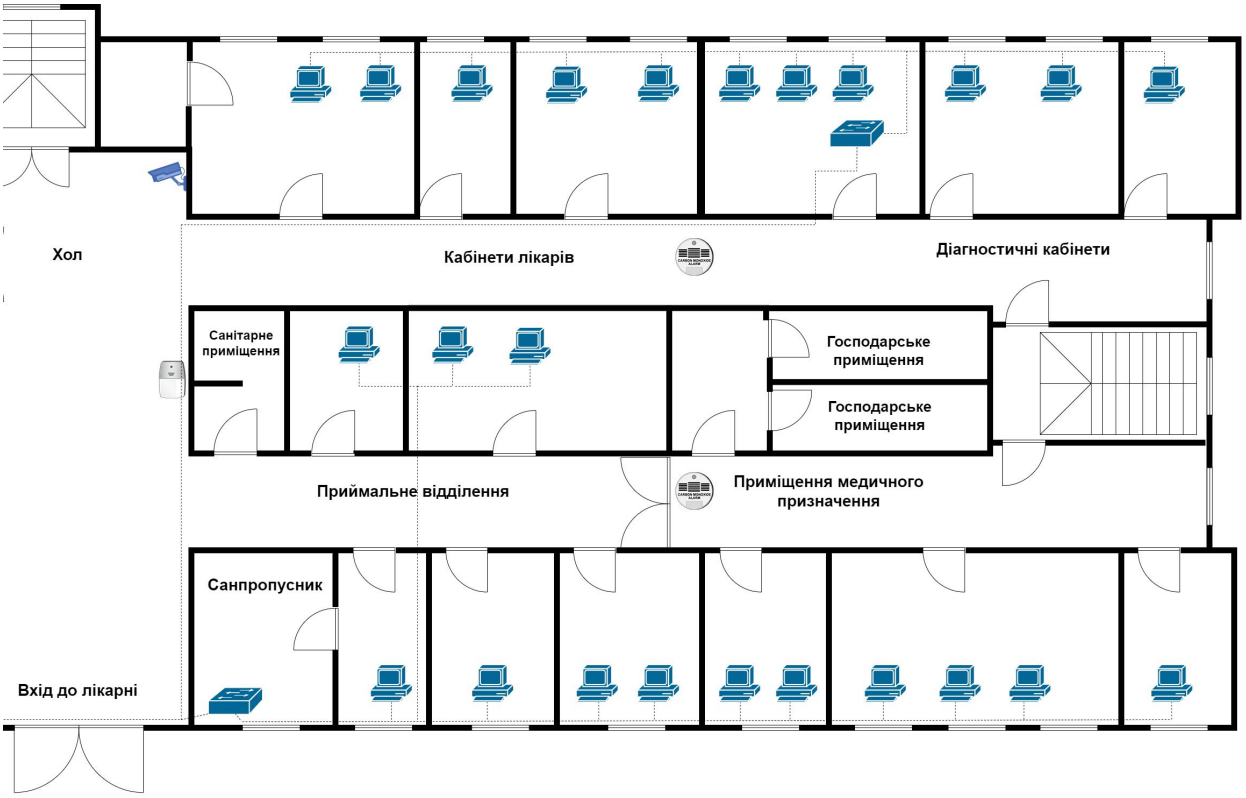


Рисунок 1.4 – Топологічна схема першого поверху (праве крило)

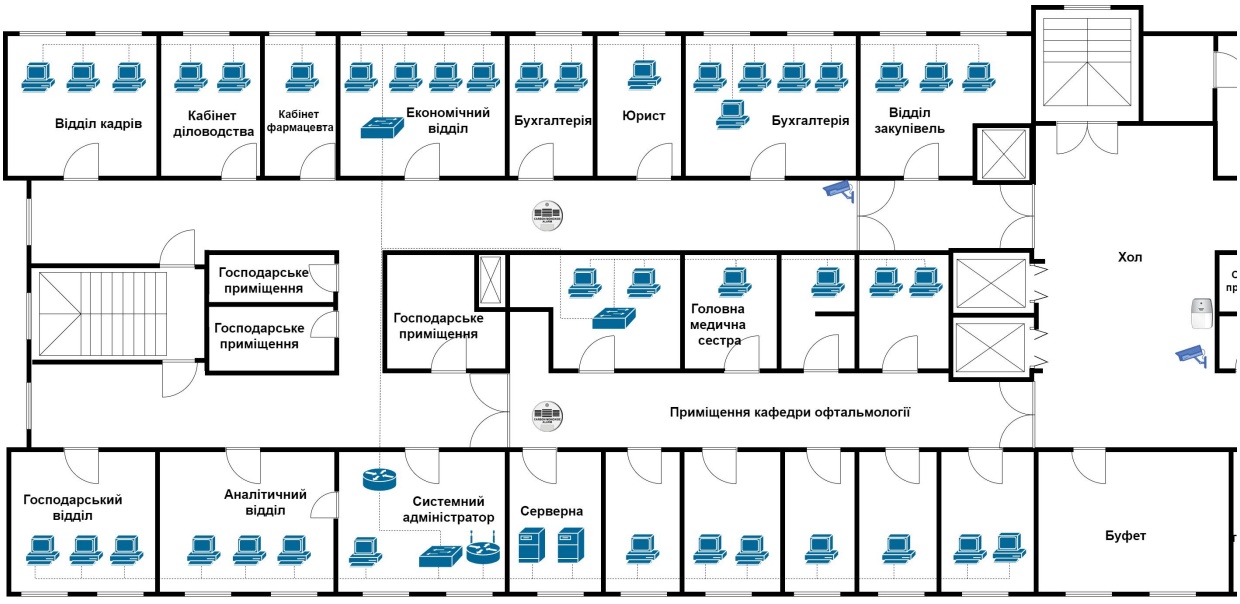


Рисунок 1.5 – Топологічна схема третього поверху (ліве крило)

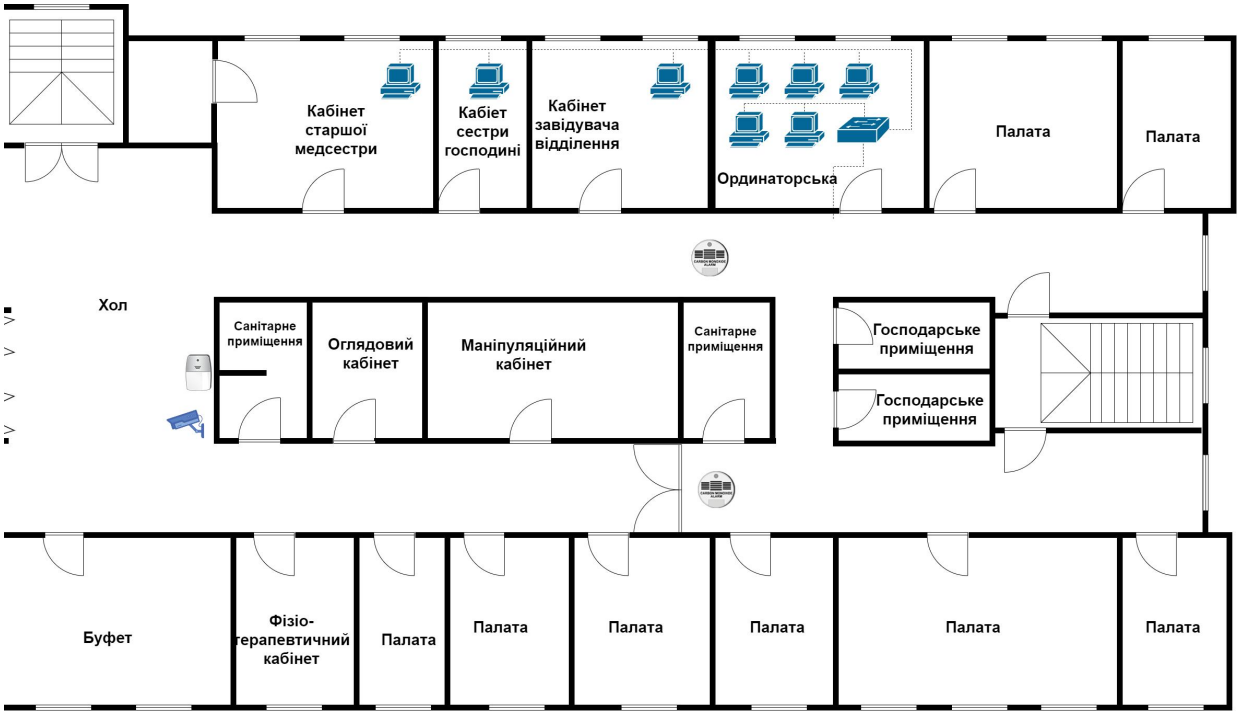


Рисунок 1.6 – Топологічна схема третього поверху (праве крило)

Перший поверх представлений приймальним та поліклінічним відділеннями, та кабінетами керівництва закладу. На третьому поверсі розташовані бухгалтерія, економічний відділ, відділ з організації та проведення публічних закупівель, відділ кадрів, юридичний консультант, аналітично-статистичний відділ та інший адміністративно-господарський персонал, а також одне з стаціонарних відділень лікарні.

1.3 Організаційна структура підприємства

Організаційна структура підприємства – це побудова структури компанії та принципів її роботи з метою досягнення поставлених перед нею цілей. Документом, який відображає організаційну структуру підприємства, розподілення підрозділів та відділів, їх взаємодію та підпорядкованість, є штатний розпис.

Організаційну структуру управління поділяють на декілька типів за критерієм розподілу відповідальності та обов’язків між усіма працівниками підприємства (від керівництва до рядових співробітників). Теоретично,

структура управління підприємством існує двох типів: ієрархічна (вертикальна) та мережева (горизонтальна).

Але на практиці, в реальному житті, організаційна часто структура управління підприємством включає в себе одночасно як елементи вертикальної, так і горизонтальної структур управління. Однак загалом домінує перша. Найбільш поширеними є такі три типи структури: лінійна, функціональна та матрична.

Як і будь-яке інше підприємство чи організація, комунальне підприємство «Дніпропетровська обласна клінічна офтальмологічна лікарня» має власну організаційну структуру (Рис. 1.7).

Рисунок 1.7 – Організаційна структурна підприємства

Наше комунальне підприємство відноситься до функціонального типу організаційної структури. За такої побудови фахівці одного рівня об'єднуються в спеціалізовані підрозділи. Тобто спеціалісти з продажів – у відділ продажів, усі фахівці бухгалтерії – у фінансовий відділ, тощо.

Але, оскільки підприємство має дуже багато відділів, що не стосуються виконуваного нами у цій роботі завдання, нами було вирішено надати на організаційну схему тільки основні відділи підприємства, що необхідні для загального розуміння його організаційної структури, та відділи, що будуть безпосередньо задіяні в процесі впровадження комп’ютерної системи.

1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об’єкта впровадження

Комунальні підприємства сфери охорони здоров’я протягом часу все більш інтенсивно та різнобічно використовують у своїй діяльності можливості, які надають сучасні технічні та інформаційні технології. Серед основних напрямків найбільш необхідних та актуальних у діяльності закладів охорони здоров’я можна зазначити наступні:

1. Комп’ютерне програмне та технічне обслуговування сучасного медичного, діагностичного та функціонального обладнання, з можливістю фіксації, аналізу, сортування та зберігання даних

2. Використання спеціального програмного забезпечення у медичній та адміністративно-господарській діяльності підприємства.

3. Зберігання на серверах та комп’ютерних пристроях даних та електронних документів для забезпечення швидкого доступу до необхідної інформації та безпеки щодо протидії її втрати.

4. Онлайн доступ доступ до електронних таблиць, з метою звітуванням керувальним організаціям.

5. Використання програмних продуктів таких сервісів, як MS Office, для створення і зберігання документів та баз даних.

6. Забезпечення безперебійного електронного документообігу між співробітниками структурних підрозділів шляхом налагодження стабільного мережевого зв’язку технічними та програмними методами.

7. Використання корпоративної електронної пошти з метою комунікації працівників в межах виконання службових обов’язків.

8. Використання бухгалтерських програмних продуктів, працюючих зі складними математичними алгоритмами, для забезпечення автоматизації та вдосконалення роботи працівників.

9. Захист конфіденційної інформації працівників та пацієнтів за допомогою антивірусного програмного забезпечення, шифрування даних, тощо.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації

В медичних установах створюється та регулярно оновлюється велика кількість документів. Вони пов’язані як з медичною діяльністю, так і з господарськими процесами, адміністративно-управлінськими заходами, фінансовою та статистичною звітністю, тощо. Цей факт сприяє виникненню постійній необхідності та попиту на забезпечення можливості для швидкого, зручного та конфіденційного обміну інформацією. Для того, щоб задовольнити цей попит, необхідне використання багатьох існуючих методів обробки та передачі інформації, а саме:

1. Використання серверів для безпечного зберігання інформації, що дозволяє накопичувати великі обсяги інформаційних даних з різних напрямків діяльності закладу. Це надає можливість постійного доступу до них. За необхідністю, з метою контролю конфіденційності та захисту даних, можливе використання систем контролю доступу до даних, їх шифрування та резервне копіювання.

2. Використання хмарних сховищ для зберігання та обміну інформаційними даними, з можливістю контролю доступу до них клієнтському та серверному рівні.

3. Застосування систем Virtual Private Network (VPN) – віртуальної приватної мережі, – з метою організації безпечного доступу до інформаційних даних в незалежності від місця знаходження користувача за допомогою мережі Internet. VPN дозволяє шифрувати трафік та забезпечувати необхідність автентифікації працівника, щоб отримати доступ до інформації.

4. Використання електронних підписів – актуальне та вкрай необхідне в медичній галузі, оскільки всі медичні працівники вищої та середньої ланки повинні бути авторизовані та мати ці підписи для виконання своїх робочих обов’язків. Також поширене їх використання при адміністративно-господарській та фінансовій діяльності закладу. Електронні підписи надають можливість забезпечення автентифікації співпрацівників та підтвердження створених звітів та документів, таких як електронні направлення до лікарів, електронні рецепти, різноманітні звітні форми, банківські документи та багатьох інших.

5. Користування електронною поштою як найпоширенішим засобом обміну інформаційними даними між кореспондентами різних напрямків та рівнів. З метою забезпечення захисту інформації можливе використання шифрування електронної пошти та електронного підпису. Це надає можливість автентифікації кореспондентів з обох боків, а також захисту від сторонніх втручань в процесі передачі інформації.

6. Застосування у роботі відеозв’язку та конференцій, що дозволяє вирішувати організаційні питання, проводити наради, налагоджувати взаємодію між віддаленими підрозділами і працівниками, ефективне та швидке керівництво трудовими процесами незважаючи на відстань. За для безпеки можливе використання шифрування трафіку та контролю доступу користувачів до участі та перегляду конференцій.

Кожен із засобів передачі, обробки та захисту інформаційних даних та комунікації має свої переваги та недоліки, але відіграває важливу роль у функціюванні та діяльності підприємств галузі охорони здоров’я.

1.6 Завдання і мета роботи

Метою роботи є організація корпоративної комп'ютерної мережі комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня» із детальним опрацюванням нюансів

налаштування апаратно-програмного мережного комплексу для подальшого розгортання цієї мережі та використання її для подальшої роботи підприємства.

Для вирішення поставленої мети в роботі вирішуються наступні завдання:

1. Аналіз об'єкта впровадження комп’ютерної системи;
2. Визначення технічних вимог до системи;
3. Вибір мережевої архітектури;
4. Розробка специфікацій системного обладнання;
5. Розробка структури комп’ютерної системи;
6. Розрахунок інтенсивності трафіку найбільшої підмережі;
7. Розробка адресації мережі підприємства;
8. Розробка логічної топології мережі підприємства;
9. Налаштування мережевого обладнання
10. Налаштування безпеки пристроїв мережі від сторонніх втручань;
11. Конфігурація обладнання для налаштування безпечного мережевого зв’язку працівників підприємства;
12. Налаштування роботи серверів підприємства;
13. Аналіз трафіку та роботи системи;
14. Розробка систем відеоспостереження та пожежної тривоги для забезпечення безпеки на підприємстві

Необхідно розробити комп’ютерну мережу комунального підприємства і передбачити негаразди, які можуть статись з нею.

1.7 Визначення можливих напрямків рішення поставлених задач

За для вирішення поставленої перед нами задачі з проектування комп'ютерної системи Комунального підприємства "Дніпропетровська обласна клінічна офтальмологічна лікарня" з детальною реалізацією

побудови та налаштування корпоративної мережі, необхідна робота у наступних напрямках:

1. Здійснення вибору мережевої архітектури корпоративної мережі КП «ДОКОЛ» між централізованою, при якій ресурси та обчислювальні потужності зосереджені в центральному вузлі мережі, та розподіленою, в якій вони розподілені між декількома вузлами.

2. Виконання аналізу трафіку корпоративної мережі, з використанням програмного забезпечення, що реалізує моніторинг та аналіз активності в мережі, а також визначення пріоритетів для різних типів трафіку.

3. Розробка фізичної та логічної топології корпоративної мережі підприємства з застосування як стандартних топологій, так і пристосованих до конкретних індивідуальних потреб підприємства.

4. Вибір типу кабельної системи для фізичної побудови топології корпоративної мережі в залежності від необхідної швидкісної спроможності, дистанції між окремими частинами та/або вузлами мережі та економічної доцільності.

5. Налаштування мережевого обладнання, такого як маршрутизатори, комутатори та сервери, для забезпечення мережевих потреб підприємства та вимог обраної архітектури та побудованих фізичної та логічної топології.

6. Розподіл та налаштування пристроїв для їх взаємодії з мережею підприємства та функціонування.

З урахуванням вказаних вище рішень, буде створена надійна, гнучка, масштабована, безпечна, швидка та детальна корпоративна мережа для Комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня».

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

2.1 Технічні вимоги до Системи

2.1.1 Вимоги до Системи в цілому

2.1.1.1 Вимоги до структури і функціювання Системи

2.1.1.1.1 Перелік підсистем, їхнє призначення й основні характеристики, вимоги до числа рівнів ієрархії та ступені централізації Системи

Комп'ютерна система (далі Система) комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня» (ск. КП «ДОКОЛ») повинна складатись з п'яти підмереж, чотири з яких виділено та розподілено між відділами та поверхами КП «ДОКОЛ», а одна – виділена Криворізькій філії підприємства, згідно із загальною архітектурою мережі підприємства, наданою нам замовником (Додаток А).

Підмережі, виділені КП «ДОКОЛ» у м. Дніпро складаються з:

1. Адміністрація, приймальня та поліклінічне відділення (1 поверх);
2. Дитяче відділення (2 поверх);
3. Адміністративно-господарський персонал (3 поверх);
4. Стаціонарні відділення (4, 5 поверхи)

Повинні бути налаштовані сервери HTTP, DNS, IoT та TFTP, та забезпечено справне функціонування. Сервери повинні бути розташовані наступним чином: сервери HTTP, DNS та IoT мають бути розташовані у КП «ДОКОЛ», сервер TFTP – у його Криворізькій філії.

Для організації безпеки підприємства КП «ДОКОЛ», має бути розроблено системи відеоспостереження та автоматичної пожежної сигналізації, доступ та керування якою матимуть тільки відповідальні особи. Цей доступ має здійснюватись за допомогою спеціального серверу із сервісом IoT та виділеного додатково маршрутизатору бездротового зв'язку з усіма пристроями цього компоненту системи.

Розміщення камер відеоспостереження передбачене таким чином: 1 поверх – 5 штук, на інших чотирьох поверхах – по 2 штуки.

Розміщення детекторів чадного газу та сирен відбувається наступним чином: по чотири датчики чадного газу на поверсі, по одному на кожен коридор, та одна сирена у холі.

2.1.1.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами Системи

Можливість доступу користувачами до розробленої мережі повинна забезпечуватись на базі як персональних комп’ютерів або ноутбуків, так і мобільних пристроїв, підключених до мережі.

Користувачі з головної мережі КП «ДОКОЛ» та її філії повинні мати зв’язок між собою, а саме:

1. В своїх підмережах за допомогою динамічної адресації їх пристроїв та призначенню шлюзів на їх маршрутизаторах;

2. В основній мережі підприємства – за допомогою WAN зв’язку між маршрутизаторами та динамічній адресації за протоколом RIP для прокладання шляху від однієї підмережі до іншої;

3. Між адміністрацією підприємства та Криворізькою філією за допомогою налаштування приватного site-to-site VPN між основною мережею та віддаленою.

Має бути налаштовано вихід до мережі Internet для кожного працівника підприємства з використанням технології NAT та шифруванням його IP-адреси, що полягає в заміні внутрішньої адреси пристрою користувача на зовнішню з діапазону 209.165.200.5 - 209.165.200.30 для основної мережі, та на адреси з діапазону 209.165.200.5 - 209.165.200.30 для віддаленої.

Також, при використанні NAT, має бути налаштовано окремі зовнішні статичні адреси для DNS та HTTP серверів, щоб користувачі Internet мали змогу переглядати WEB сторінку КП «ДОКОЛ».

Зв’язок між вузлами Системи має здійснюватись за допомогою інтерфейсу Ethernet з використанням кабелів. Обмін інформацією між компонентами Системи має відбуватись згідно зі стандартними протоколами на рівні програмного забезпечення.

2.1.1.1.3 Вимоги до діагностування Системи

Для діагностування Системи на наявність та тип проблем, має бути передбачена можливість для адміністратора системи переглядати поточні налаштування мережевих та інших пристроїв. У випадку виявлення проблем мережевого характеру, слід здійснювати послідовне надсилання ехо-запитів з пристрою організації з одночасним відстеженням шляху проходження пакетів, їх типу, трансформацій за різними критеріями та пошуком аномалій.

2.1.1.1.4 Перспективи розвитку, модернізації Системи.

При розподіленні виділеної провайдером для організації мережі на її підмережі, слід враховувати можливі перспективи розвитку щодо додавання нових вузлів у вже створену комп’ютерну мережу в майбутньому. Для цього виділений список адрес для підмереж має передбачати запас для зарезервованих адрес (таких як адреси мережевого обладнання та сервери) та додатково не менш ніж 20 адрес у кожній підмережі для можливого додавання нових користувачів та їх пристроїв у Систему.

2.1.1.2 Вимоги до показників призначення

Комп’ютерній системі необхідно забезпечувати умови функціонування обладнання відповідно з умовами технологічного процесу, зокрема серверу, на якому зберігаються дані комунального підприємства. Комп’ютерна система повинна забезпечувати доступ до цих даних у мережі підприємства та захист їх від втрати при збоях, нештатних ситуаціях та кібератаках.

Комп’ютерна система має дозволяти користувачам у підприємстві підключатись до мережі Internet для виконання своїх робочих обов’язків, таких як надання електронних медичних рецептів та направлень, надсилання звітів керуючим організаціям, тощо.

Комп’ютерна система повинна дозволяти об’єднувати користувачів відділів в межах окремо функціонуючих програмних продуктів.

2.1.1.3 Вимоги до експлуатації, технічного обслуговування ремонту і зберігання компонентів системи

2.1.1.3.1 Умови і регламент експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) Системи з заданими технічними показниками

Всі приміщення у будівлі підприємства, в яких знаходяться техніка, повинні мати вентиляцію та відповідати наступним умовам:

1. За температури від 21 до 28 градусів Цельсія та вологість повітря повинна бути від 75% до 55% відповідно, в залежності від періоду року;

2. Швидкість руху повітря в робочій зоні має не перевищувати 0.1 або 0.2 м/с в залежності від періоду року;

3. Атмосферний тиск 740-770 мм.рт.ст;

4. Повинні бути в наявності засоби протипожежної безпеки на випадок нештатних ситуацій пов’язаних із займанням компонентів апаратної частини комп’ютерної системи та електричної мережі, до якої вони під’єднані.

У зв’язку зі специфікою роботи лікарських закладів, певна кількість персоналу завжди знаходиться на робочих місцях або має ненормований робочий день. Тому технічне забезпечення має надавати можливість працівникам доступу до Системи в будь-який час.

2.1.1.3.2 Вимоги до параметрів мереж енергопостачання (живлення та заземлення)

До кожного робочого місця повинно бути підведена електрична мережа, розташовані розетки 220В, 50Гц з заземлювальним контактом.

Забезпечення безперебійного енергопостачання технічними та організаційними засобами для запобігання екстреного вимкнення компонентів Системи, такими як блоки безперебійного живлення, резервні генератори електропостачання, тощо.

2.1.1.3.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу і режимам його роботи

Обов’язкова наявність одного системного адміністратора, що матиме бакалаврський ступінь вищої освіти за спеціальністю «Комп’ютерна інженерія». У його обов’язки входитиме забезпечення підтримки функціонування впровадження Системи. Створення конкретного графіку, який передбачатиме перевірку та підтримку системним адміністратором працездатності усіх компонентів системи, а також здійснення позапланових заходів по налагодженню роботи Системи згідно з заявками користувачів про її некоректну роботу.

Обов’язкова наявність робітника з обслуговування електроустаткування. У його обов’язки входить підтримка в робочому стані електричних мереж та устаткування підприємства, здійснення термінового ремонту згідно до заяв користувачів.

2.1.1.3.4 Вимоги до складу, розміщенню й умовам збереження комплекту запасних виробів і приладів

У апаратного забезпечення (кабелів, комутаторів, тощо) має бути в наявності додаткова кількість запасних частин/пристроїв на складі для забезпечення термінової необхідності заміни тих, що вийшли з ладу або

стали непридатними для подальшого використання. Або у комунального підприємства має бути можливість своєчасного придбання необхідних запчастин або пристроїв для термінового відновлення працездатності Системи.

2.1.1.3.5 Вимоги до регламенту обслуговування

Періодичне технічне обслуговування і тестування технічних засобів повинні включати в себе обслуговування і тестування всіх використовуваних технічних засобів в кожному відділі згідно з розробленим графіком або за необхідністю чи за вимогою користувача Системи.

Графік такого тестування має передбачати проведення його не рідше ніж раз на місяць.

В рамках проведення періодичного технічного огляду та обслуговування компонентів Системи, повинні проводитися зовнішній і внутрішній огляд, чистка апаратних компонентів, перевірка контактних з'єднань, перевірка параметрів налаштувань працездатності технічних засобів, тестування їх взаємодії, перевірка програмних компонентів на наявність вразливостей, неполадок та оновлень, перевірка працездатності мережевих налаштувань та інших необхідних конфігурацій в залежності від типу компонента Системи.

Перебої з енергопостачанням можуть призвести до виходу з ладу компонентів Системи. У випадку таких перебоїв потрібно додати до обов'язків відповідального співробітника регулярну перевірку (не рідше, ніж раз на тиждень) апаратної частини Системи підприємства та її обслуговування за необхідністю.

2.1.1.4 Вимоги до патентної чистоти

Використовуване обладнання і програмне забезпечення повинно мати патентну чистоту і бути сертифіковано (якщо потрібно) для роботи у використовуваних режимах.

2.1.1.5 Додаткові вимоги

2.1.1.5.1 Вимоги до Системи, пов'язані з особливими умовами її експлуатації

У зв’язку із воєнним станом та перебоями з електропостачанням, підприємство повинно бути обладнане власним генератором, а також необхідна наявність фахівця з обслуговування генератору, електричних мереж та устаткування підприємства.

2.1.1.5.2 Вимоги до активного обладнання

Для налаштування ефективного функціонування Системи, необхідна наявність наступних елементів системи:

1. Маршрутизатори з трьома портами Gigabit Ethernet для підключення підмереж, з двома або з чотирма Serial портами для зв’язку маршрутизаторів між собою та з мережею провайдеру.

2. Комутатори з двома портами Gigabit Ethernet для виходу у мережу та 24 портами Fast Ethernet для підключення пристроїв та серверів, а також забезпечення певного запасу для можливого розширення відділів;

3. Сервери з портами Fast Ethernet RJ-45 та підтримкою сервісів HTTP, DNS, TFTP, AAA, IoT для забезпечення виконання задач, поставлених підприємством перед системою;

4. Стаціонарні комп’ютери та ноутбуки зі стандартними портами, в тому числі, Fast Ethernet RJ-45 для забезпечення зв’язку з мережею підприємства.

2.1.1.5.3 Вимоги до кабель-каналів та електричних розеток (тип, розмір, варіант розміщення)

Для забезпечення пожежної безпеки та естетичного вигляду, кабелі у приміщеннях підприємства повинні бути захищені кабель-каналами. Для проведення кабелів у підприємстві мають використовуватись пластикові настінні та підлогові кабель-канали.

Електричні розетки повинні повинні розміщуватись на висоті 15 – 30 см від плінтусу, якщо це не заперечує вимогам та обмеженням електричної та пожежної безпеки. Розетки повинні мати заземлення, режим напруги 220 Вольт, ступінь захисту не менш ніж IP20 та бути типу F (європейський тип розеток із заземленням). Також, розетка повинна мати не менш ніж два гнізда.

2.1.1.5.4 Вимоги до комунікаційного обладнання і його розташування

При створенні Системи, для з'єднання пристроїв, слід використовувати мідні кабелі наскрізного та перехресного типів.

Необхідний технічний та фізичний захист комунікаційного обладнання Системи:

1. Розташування комунікацій та кабелів має відбуватись таким чином, що запобігатиме їх випадковому фізичному контакту з людьми, який може призвести до розриву зв’язку, знеструмленню, пошкодженню техніки, фізичного травмуванню персоналу та пацієнтів, тощо. За фізичною можливістю, вони повинні бути прокладені вздовж стін та надійно закріплені. У випадку перетинання кімнат або коридорів, вони повинні бути також надійно закріплені та додатково покриті спеціальним кабельним захистом (такими як напільний кабельний канал, тощо).

2. При прокладенні кабельних систем крізь стіни підприємства, враховувати товщину несущих стін 27 см, не несущих стін 10 см, висоту поверху 2.8 м. Матеріал будівлі – цегла.

3. На самих пристроях Системи необхідно дотримуватись кабель-менеджменту.

4. Необхідно організувати безпечне розташування технічних засобів (стаціонарних комп’ютерів, комутаторів, маршрутизаторів, серверів, тощо) на спеціально пристосованих поверхнях (столах робітників, спеціальних підставках, тощо).

5. Наявність блоків безперебійного живлення з часом роботи не менше 1 хвилини при повному навантаженні для запобігання аварійного вимикання пристроїв підприємства.

6. Камери мають бути розташовані на стелях із забезпеченням максимального кута огляду приміщень, за якими ведеться відеоспостереження. Детектори чадного газу повинні бути розташовані в середині стелі кожного коридору поверху. Сирени мають бути розташовані у холі кожного поверху з можливістю доступу для ручного вимкнення. Перераховані у цьому пункті пристрої мають бути надійно закріпленими та забезпечені електроенергією для безперебійного функціонування.

2.1.1.5.5 Вимоги до однорідності

Для мережі повинні використовуватись якісні високооднорідні LAN-кабелі з номінальним значенням параметру робочої ємності ланцюга, що не перевищує 50 нФ/км.

2.1.2 Вимоги до налаштувань та функцій, які виконує Система

За для роботи Системи, необхідно здійснити наступні кроки з налаштування маршрутизаторів та комутаторів Системи:

1. Призначити системні найменування кожному пристрою за правилом *Karaskin_тип пристрою_номер пристрою* та розробити банер MOTD, а також доменне ім’я, що повторює ім’я цього пристрою;

2. Призначити пароль *cisco* до консольних та vty ліній на всіх пристроях та пароль *class* для доступу до привілейованого режиму. Ці паролі мають бути зберігатись у зашифрованому вигляді за допомогою ключа RSA завдовжки 1024 біт;

3. Призначити використання протоколу ssh на всіх vty лініях;

4. Створити користувача *123191_Karaskin* з паролем *admincisco* на всіх пристроях;

5. Встановити значення тактової частоти на DCE-інтерфейсах маршрутизаторів 128000;

6. На serial-інтерфейсах має бути призначено пропускна спроможність, що дорівнює 128 Кб/с;

7. Призначити адреси інтерфейсам маршрутизаторів;

8. Налаштувати роботу протоколу маршрутизації RIP, оголосивши підключені до нього мережі;

9. Задати на граничних маршрутизаторах статичні маршрути для доступу у мережу Internet та мережі провайдеру, та поширити цій маршрути на інші маршрутизатори мережі підприємства;

10. Налаштувати підтримку служби AAA на всіх маршрутизаторах за допомогою локальної бази даних користувачів для підключення до vty ліній та протоколу RADIUS для доступу у консоль

11. Налаштувати RADIUS-сервер так, щоб в якості облікового запису користувачів використовувались ім’я пристрою та пароль *admin123*, а ключовим словом було *radius123;*

12. Забезпечити захист інформації в Системі шляхом впровадження та налаштування VLAN на маршрутизаторі, що відповідає за роботу адміністративно-управлінського персоналу;

13. Налаштувати функції безпеки портів на комутаторах, під’єднаних до серверів так, щоб тільки двом унікальним пристроям було надано дозівл на доступ до порту, їх MAC-адреси динамічно розпізнавались, а під час

порушення системи безпеки з’являлось повідомлення, а порт залишався включеним.

Функції, що повинна виконувати Система:

1. Забезпечення безперебійної, своєчасної та швидкої комунікації користувачів комп'ютерної системи підприємства між собою;

2. Забезпечення можливості користувачам безпечного доступу до мережі Інтернет, отримання інформації звідси та обміну нею між собою;

3. Збереження та резервне копіювання інформації на серверах та захист її від зовнішніх та внутрішніх негараздів;

4. Забезпечення захисту компонентів системи від зовнішніх втручань, таких як віруси, шпигунське ПЗ та т.і.;

5. Забезпечення шифрування IP-адрес пристроїв при їх виході у мережу Internet;

6. Заборона доступу до пристроїв комп’ютерної системи зі сторонніх вузлів;

7. Підтримка загальнодоступної web-сторінки підприємства як для користувачів комп’ютерної системи, так і для користувачів з мережі інтернет;

8. Розділення підмереж підприємства на відділи, у разі необхідності, для сегментування праці, ПЗ, тощо;

9. Підтримка постійного контролю за пожежною безпекою та відеоспостереження.

2.1.3 Вимоги до видів забезпечення системи

2.1.3.1 Вимоги до інформаційного забезпечення

Система збереження даних має бути представлена у зручній для користувачів формі з можливістю комфортного доступу, формування тематичної вибірки та вивантаження даних в заданій програмі користувачем формі. Бази даних мають бути структуровані та зберігатись на пристроях та сервері.

Зберігання даних про конфігурацію Системи та її пристроїв відбувається як на самих пристроях, так і на спеціально налаштованому для цього сервері.

Програмне забезпечення повинно мати можливість вивантаження даних користувача у редактори Word та Exel від компанії Microsoft Office.

Дані від камер відеоспостереження мають зберігатися на сервері визначений користувачем термін.

2.1.3.2 Вимоги до лінгвістичного забезпечення системи

Система повинна мати змогу обробляти та видавати інформацію на українській та англійській мовах за вибором користувача.

2.1.3.3 Вимоги для технічного забезпечення системи

Інтерфейс Системи має бути пристосованим для використання клавіатури та миші.

Інтерфейс Системи повинен бути максимально зрозумілим і зручним для працівників.

Також інтерфейс Системи повинен бути максимально лагідним для очей працівників, у зв’язку з їх тривалим використанням комп’ютеру під час робочого часу, з метою зменшення втомлюваності та навантаження на очі. Для цього монітори комп’ютерів та пристроїв працівників повинні мати роздільну здатність екрану не менш ніж 1280×720 px та мати величину яскравості в діапазоні від 100 до 200 nit, в залежить від ступеню освітленості приміщення.

Обладнання, що буде використовуватись для створення та впровадження Системи на підприємстві замовника, буде закуповуватись через систему Prozzorro згідно з технічними вимогами щодо специфікації обладнання, заданими до закупівлі. Виробник обладнання та його торгова марка будуть відомі після визначення переможця у тендері.

2.1.3.4 Вимоги до організаційного забезпечення

Основна функція контролю за працездатністю комп'ютерної системи покладена на системного адміністратора підприємства. Система має як відокремлених користувачів, так і об'єднані одним програмним продуктом відділи. На мережевому рівні, об'єднання таких відділів відбувається завдяки виділенню віртуальних локальних мережі в рамках вже існуючих підмереж організації, що мають змогу взаємодіяти як між собою, так і з зовнішніми вузлами. В таких відділах мають бути призначені відповідальні особи, що контролюють коректність роботи системи та контактують із системним адміністратором у випадку негараздів в її роботі.

Обов'язкове проведення технічного інструктажу та навчання персоналу для забезпечення коректної роботи з мережею підприємства, програмним забезпеченням та обладнанням, а також стосовно правил безпечного користування мережею Internet з метою кібербезпеки.

У користувачів не повинно бути можливості виходу користувача з системи без його прямого на те волевиявлення. Система повинна передбачати уточнення чи дійсно користувач бажає покинути систему та запропонувати, у разі дійсної відповіді, можливість зберегти поточні дані, з метою запобігання випадкового чи незапланованого виходу користувача з системи та втрати інформації.

2.1.3.5 Вимоги до методичного забезпечення

Наданий підприємству замовнику проект має супроводжуватись наступною методичною документацією:

1. Загальна архітектура мережі підприємства;
2. Структурна схема комплексу технічних засобів для реалізації комп'ютерної системи підприємства з демонстрацією кількості вузлів, мережевих рівнів та типів використовуваних пристроїв;

3. Специфікацію обладнання, необхідного для закупівлі та подальшого впровадження та функціонування комп’ютерної системи;

4. Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства;

5. Таблиці адресації мережі підприємства та інтерфейсів пристроїв, необхідних для функціонування мережі та системи;

6. Схеми логічної топології мережі підприємства;

7. Інструкція та правила налаштування мережевих, системних та IoT пристроїв.

2.2 Розробка апаратного частини комп’ютерної системи

2.2.1 Обстеження об’єкту розробки та аналізу способів доступу до інфраструктурі мережі

Комунальне підприємство «Дніпропетровська обласна клінічна офтальмологічна лікарня» займає п’ять поверхів у шестиповерховій будівлі. Його мережа поділяється на підмережі за структурною схемою, представленою на рисунку 2.1. Цю схему було побудовано на основі даних про загальну архітектуру мережі підприємства КП «ДОКОЛ» (Додаток А), кількості підмереж та вузлів в них, розташування серверів, камер відеоспостереження, детекторів чадного газу та сирен, та розробленої схеми організаційної структури підприємства (Рис. 1.7).

Структурна схема комплексу технічних засобів Системи КП «ДОКОЛ» передбачає розділення мережі на п’ять підмереж, чотири з яких розподілені між відділами головної мережі підприємства, а п’ята є віддаленою підмережею, що належить криворізькій філії підприємства.

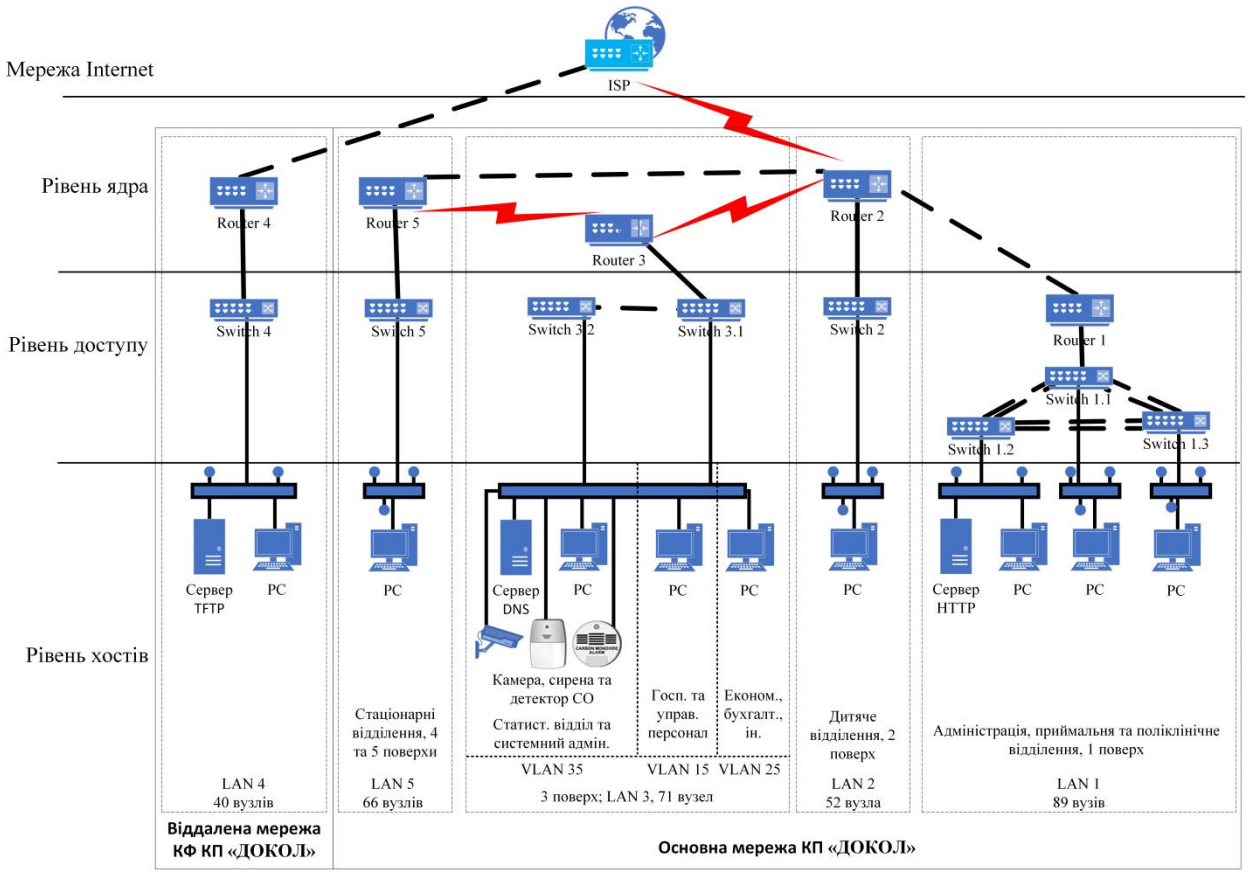


Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи КП «ДОКОЛ»

Зв’язок між підмережами здійснюється за допомогою кабелів Serial, Gigabit та Fast Ethernet, які пов’язують між собою комутатори та маршрутизатори у локальних підмережах підприємства. Вони також використовуються для зв’язку підмереж з провайдером для доступу у Internet.

Пересилання трафіку між маршрутизаторами здійснюється за протоколом RIP, оскільки мережа підприємства є невеликою та не потребує великої кількості переходів між підмережами.

Також, для взаємодії комп’ютерів, за бажанням замовника, нами було використано систему VLAN на комутаторах однієї з підмереж підприємства.

2.2.2 Розробка специфікації апаратних засобів комп'ютерної системи

Оскільки закупівля необхідної апаратури буде відбуватись через систему публічних закупівель «Prozorro», спрогнозувати конкретну марку та модель пристроїв, з яких буде побудовано корпоративну комп'ютерну мережу, не є можливим, тому будуть завдані лише конкретні технічні вимоги до закупівлі на прикладі абстрактних пристроїв з необхідними технічними характеристиками, що матимуть змогу забезпечити роботу мережі підприємства. Необхідні для подальшого проведення комунальним підприємством тендеру через систему «Prozorro» технічні характеристики та кількість використаних пристроїв при побудові комп'ютерної мережі підприємства наводяться у таблиці 2.1.

Таблиця 2.1 – ТХ пристроїв, використаних при побудові Системи підприємства КП «ДОКОЛ»

Позиція	Тип прострію	Необхідні ТХ	Необхідна кількість за такими ТХ
1.	Комп'ютер (PC)	Процесор: 4-6 ядерний, 3.7 - 4.2 ГГц; Оперативна пам'ять: 8 ГБ; Тип пам'яті: SSD, 240 ГБ або більше; Графічний адаптер: AMD Radeon Vega 7 або східний за характеристиками; Підтримка LAN; Предустановлена ОС: Windows 11.	318
2.	Комутатор	Керований комутатор з 24 фіксованими 10/100 Fast Ethernet портами та 2 портами 10/100/1000 Gigabit Ethernet, встановлене ПЗ - LAN Base. Інтегровані функції безпеки, включаючи контроль доступу в мережу. Розширені можливості управління якістю обслуговування (QoS) і забезпечення відмовостійкості Інтелектуальні сервіси на кордоні мережі.	18

Продовження таблиці

3.	Маршрутизатор	Тип обладнання: маршрутизатор; Стандарт: 802.11 b/g/n Вбудовані порти: RJ45 x3, Serial x4 Швидкість на вбудованих портах: 10/100/1000 Мбіт/с.	1
		Тип обладнання: маршрутизатор; Стандарт: 802.11 b/g/n Вбудовані порти: RJ45 x3 Швидкість на вбудованих портах: 10/100/1000 Мбіт/с.	1
		Тип обладнання: маршрутизатор; Стандарт: 802.11 b/g/n Вбудовані порти: RJ45 x2, Serial x2 Швидкість на вбудованих портах: 10/100/1000 Мбіт/с.	2
		Тип обладнання: маршрутизатор; Стандарт: 802.11 b/g/n Вбудовані порти: RJ45 x2 Швидкість на вбудованих портах: 10/100/1000 Мбіт/с.	1
4.	Сервер	Процессор: 2 шт x Intel Xeon E5-2650 v2; або східний за характеристиками; Оперативна пам’ять: 16 GB; Тип ОП: DDR3 (2 x 8 GB); Мережевий контролер: 2 порти 1Gb Ethernet.	4
5.	Камера відеоспостереження	Тип зв’язку: Бездротовий; Роздільна здатність камери: не менше ніж 3 Мп; Слот для карток пам'яті: MicroSD; Максимальний обсяг картки пам'яті: не менш ніж 64 Гб; Розмір матриці: 1/3" або краще.	13
6.	Детектор чадного газу	Тип зв’язку: бездротовий; Тип монтажу: стельовий; Тип сенсора диму: фотоелектричний.	

Кінець таблиці 2.1

7.	Сирена	Тип зв’язку: бездротовий; Тип сповіщення; звуковий або світлозвуковий; Гучність сирени: від 80 до 100 Дб.	

З урахуванням системи публічних закупівель Prozzorro, кількості пристроїв, що вказані у таблиці 2.1, топологічних схем КП «ДОКОЛ» (Рис. 1.3 – 1.6), плану першого поверху будівлі підприємства (Додаток Б), на якому вказані її розмірні характеристики, та вимог до комунікаційного обладнання та його розташування, викладених у підпункті 2.1.1.5.4, нами було визначено специфікацію структурованої кабельної системи, яку наведено у таблиці 2.2. При поданні кількісної характеристики у таблиці 2.2, береться до уваги необхідність забезпечення можливості підключення додаткових периферійних пристроїв, збільшення кількості робочих місць та інших не передбачуваних моментів.

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Тип	Необхідні ТХ	Необхідна кількість за такими ТХ
1.	Кабельний канал, настінний	Матеріал: Пластик (ПВХ) Розміри: 40х40 мм Довжина: 2 м	200
2.	Кабельний канал, напільний	Матеріал: Пластик (ПВХ) Розміри: 50х10 мм Довжина: 2 м	35
3.	Розетка електроживлення	Заземлення: є Режим напруги: 220 Вольт Ступінь захисту: IP20 або краще Тип розетки: F Кількість гнізд: 2 або більше	200

Кінець таблиці 2.2

4.	Кабель живлення	Тип: ПВС Кількість жил: 3 Площа перетину жил: 1.5 мм^2 Довжина: 2 м або більше	20
5.	Комутаційна коробка	Розміри: 80x80x40 мм Ступінь захисту: IP20 або краще	10
6.	LAN кабель	Тип: патч-корд Тип інтерфейсу: RJ-45 Категорія: Cat 5e Довжина: від 2 – 4 метри	400
7.	Комп'ютерна розетка	Тип інтерфейсу: RJ-45 Кількість портів: 2 або більше Ступінь захисту: IP20 або краще Вид монтажу: прихований Категорія: UTP	100

2.2.3 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Вихідний трафік маршрутизується в лінію з пропускною здатністю, що становить 1000 Мбіт/с.

Щоб уникнути перенавантаження на маршрутизаторі, швидкість находження пакетів до нього повинна буде менше швидкості їх відправлення.

Середня інтенсивність трафіку μ = 111 кадрів/с, середня довжина повідомлення складає 650 байт.

Теоретично припустимо, що всі користувачі найбільшої підмережі (LAN1, що складається з 89 вузлів) одночасно використовують мережу. В такому разі, пропускна здатність на рівні доступу буде дорівнювати:

$$P_{р.р.} = \mu * L_{пов} * N * 8 = 111 * 650 * 89 * 8 = 51{,}37 \text{ Мбіт/с} \quad (2.1)$$

де $L_{пов}$ – середня довжина повідомлення;

N – кількість вузлів в мережі.

Отриманий результат не перевищуватиме заданих параметрів мережі по вихідному каналу, отже перенавантажень не трапиться.

Комутатор рівня доступу також передає трафік до маршрутизатора зі швидкістю 1000 Мбіт/с. Отже, загальне навантаження на комутатор не повинно перевищувати:

$$\mu_{вих} = 10^9 / (650 * 8) = 192\ 307 \text{ пакетів/с} \quad (2.2)$$

Оскільки в середньому, кожне джерело виробляє 111 пакетів/с, то маршрутизатор обмежений кількістю приєднань, яку ми можемо дізнатись наступним чином:

$$N = \mu_{вих} / \mu = 192307 / 111 = 1732{,}5 \approx 1732 \text{ джерела} \quad (2.3)$$

Ця кількість задовольняє кількості вузлів у найбільшій нашій локальній мережі, до якої входить 89 ПК.

Кожен з 89 ПК посилає потік заявок з інтенсивністю у 111 кадрів/с. Звідси, можем розрахувати інтенсивність вихідного трафіку:

$$\lambda = N * \mu = 89*111 = 9879 \text{ пакетів/с.} \quad (2.4)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{9879}{192\ 307} = 0{,}05 \quad (2.5)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0{,}05}{1-0{,}05} = 0{,}053 \quad (2.6)$$

Середня затримка кадру, пов’язана з чергою M/M/1, дорівнює:

$$T = \frac{1}{(\mu-\lambda)} = \frac{1}{(192307 - 9879)} = 5{,}48 \text{ мкс} \quad (2.7)$$

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0.05^2}{1-0.05} = 0.0026 \quad (2.8)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}026}{9879} = 0{,}26 \text{ мкс} \quad (2.9)$$

Це значення задовольняє нашим вимогам, оскільки є меншим, ніж 6 мс.

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації комп’ютерної мережі

Згідно з нашим завданням, отриманим від замовника, блок адрес та кількість вузлів, які нами буде використано у подальшій розробці комп’ютерної системи, виглядає наступним чином (таблиця 3.1):

Таблиця 3.1 - Блок адрес та кількість вузлів у підмережах підприємства.

Блок адрес	LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
10.23.32.0 /22	89	52	71	40	66

Отже, перед нами поставлено задачу розробити модель комп’ютерної мережі, до якої входить п’ять підмереж та 318 вузлів.

Також підприємством-замовником нам було надано мережеву архітектуру підприємства (див. Рис. 2.1), в рамках якої нами буде впроваджено комп’ютерну систему та розроблено модель комп’ютерної мережі у програмі Cisco Packet Tracer.

Отже, перед нами поставлена задача, використовуючи дані, отримані від замовника, створити комп’ютерну мережу, шляхом розбиття наданого блоку адрес на 5 підмереж, одна з яких (LAN 4) є віддаленою та знаходиться у філіалі підприємства в іншому місті, а також враховуючи необхідність виділити окремі невеликі блоки адрес для зв’язку між самими підмережами.

Для розбиття мережі на підмережі нами був використовуваний метод VLSM – маска змінної довжини, – який розподіляє IP-адресацію мережі не використовуючи рамки класової адресації. Це дозволяє нам більш економно розподілити IP-адреси за нашими підмережам, ніж якщо ми б стали використовувати маски постійної довжини.

Також, при розбитті, нами було враховано, що кожна з підмереж матиме декілька зарезервованих адрес, що вимагає від нас виділяти блоки

адрес дещо більші, ніж в ній знаходиться вузлів. Це необхідно, щоб ми мали запас для зарезервованих адрес (таких як багатомовна адреса, адреса шлюзу, зарезервовані при dhcp-адресації та т.і.), а також на випадок, якщо у підприємства-замовника виникне необхідність додати деяку кількість нових вузлів у якусь з підмереж. Запас адрес дозволить уникнути зайвої роботи з перерозподіляння адрес та переналаштування мережі.

Оскільки метод VLSM дозволяє виділяти підмережі розміру у ступінь двійки, в нашому прикладі будемо ділити діапазон таким чином, що одна з підмереж, яку, згідно з вимогами підприємства, потрібно буде поділити на три відділи, кожний зі своїми віртуальними локальними мережами, буде мати пул адрес 256, а інші чотири, щоб виділити їм надійний запас IP-адрес у пулах, отримають пули по 128 адрес.

Для виділення підмереж з мережі, виділеної провайдером на наше комунальне підприємство, переведемо адресу мережі в двійковий вид і відокремимо вже зафіксовану маскою частину. Частину IP-адреси мережі, що незадіяна у операціях, переводити у двійковий вид не будемо.

Для зручності розрахунків за методом VLSM, почнемо ділити мережу з найбільшого блоку в 256 адрес, що дорівнює 2^8. Отже отримуємо, що нам необхідно відрізати справа 8 біт:

10.23.00100000.|00000000

Щоб отримати кінець діапазону, заповнюємо відокремлену частину одиницями:

10.23.00100000.|11111111

Звідси, отримуємо підмережу 10.23.32.0/24 з діапазоном IP-адрес хостів 10.23.32.1 – 10.23.32.255 розміром у 255 адреси, одна з яких, – 10.23.32.255 – широкомовна адреса, яку не можна привласнити якомусь з вузлів, оскільки вона розсилає пакети одразу на всі підключені вузли своєї підмережі.

Наступними розрахуємо підмережі, яким ми виділили блоки 128 адрес, для чого збільшуємо останню отриману адресу мережі на одиницю та знову виділяємо окрему частину, але вже розміром у 7 біт, оскільки 128 дорівнює 2^7:

10.23.00100001.0|0000000

10.23.00100001.0|1111111

Звідси, отримуємо підмережу 10.23.33.0/25 з діапазоном IP-адрес хостів 10.23.33.1 – 10.23.33.126 розміром у 126 адрес та широкомовною адресою – 10.23.33.127.

Таким самим чином розраховуємо і інші підмережі з блоками по 128 адрес.

Збільшуємо останню отриману адресу мережі на одиницю та знову виділяємо блок адрес 128 виділяємо відокремлюючи 7 біт:

10.23.00100001.1|0000000

10.23.00100001.1|1111111

Звідси, отримуємо підмережу 10.23.33.128/25 з діапазоном IP-адрес хостів 10.23.33.129 – 10.23.33.254 розміром у 126 адрес та широкомовною адресою – 10.23.33.255.

Збільшуємо останню отриману адресу мережі на одиницю та виділяємо блок адрес 128 виділяємо відокремлюючи 7 біт:

10.23.00100010.0|0000000

10.23.00100010.0|1111111

Звідси, отримуємо підмережу 10.23.34.0/25 з діапазоном IP-адрес хостів 10.23.34.1 – 10.23.34.126 розміром у 126 адрес та широкомовною адресою – 10.23.34.127.

Збільшуємо останню отриману адресу мережі на одиницю та виділяємо блок адрес 128 виділяємо відокремлюючи 7 біт:

10.23.00100010.1|0000000

10.23.00100010.1|1111111

Звідси, отримуємо підмережу 10.23.34.128/25 з діапазоном IP-адрес хостів 10.23.34.129 – 10.23.34.254 розміром у 126 адрес та широкомовною адресою – 10.23.34.255.

Таким чином, у таблиці 3.2 можна побачити результат розподілу адрес для нашої майбутньої комп'ютерної мережі.

Таблиця 3.2 – Адресація мережі КП "ДОКОЛ"

Назва мережі	Кількість вузлів	Номер мережі	Маска	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN1	89	10.23.33.0	/25	10.23.33.1	10.23.33.126
LAN2	52	10.23.33.128	/25	10.23.33.129	10.23.33.254
LAN3	71	10.23.32.0	/24	10.23.32.1	10.23.32.254
LAN4	40	10.23.34.128	/25	10.23.34.129	10.23.34.254
LAN5	66	10.23.34.0	/25	10.23.34.1	10.23.34.126
ISP	2	209.165.201.0	/28	209.165.201.1	209.165.201.14

Також до таблиці було включено адресацію підмережі провайдеру та використовується ним для зв'язку з мережею нашого підприємства і використовується у подальшому моделюванні мережі.

Крім того нами також було розроблено схему IP-адресації між маршрутизаторами нашої мережі, користуючись тим самим методом, що і при розподілі адрес для підмереж. Згідно з вимогами, для зв'язку між маршрутизаторами нами було використано блок адрес 10.0.5.0 /24. Розбиття

на підмережі зв’язку маршрутизаторів мережі, а також дані IP адресації зв’язку нашої мережі з провайдером можна побачити у таблиці 3.3.

Таблиця 3.3 – Адресація між маршрутизаторами мережі

Назва підме-режі	Необхідна кількість вузлів	Адрес підмережі та маска	Діапазон допустимих IP-адрес	Багатомовна адреса
WAN1	4	10.0.5.12 255.255.255.248	10.0.5.13 - 10.0.5.16	10.0.5.17
WAN2	2	10.0.5.0 255.255.255.252	10.0.5.1 - 10.0.5.2	10.0.5.3
WAN3	2	10.0.5.4 255.255.255.252	10.0.5.5 - 10.0.5.6	10.0.5.7
WAN4	2	10.0.5.8 255.255.255.252	10.0.5.9 - 10.0.5.10	10.0.5.11
ISP1	2	209.165.202.0 255.255.255.252	209.165.202.1- 209.165.202.2	209.165.202.3
ISP2	2	64.100.13.0 255.255.255.252	64.100.13.1- 64.100.13.2	64.100.13.3

3.2 Розрахунок схеми адресації пристроїв

Після розрахунку IP-адресації наших підмереж, нами було розподілено адреси для інтерфейсів маршрутизаторів мережі підприємства та маршрутизатору провайдера, враховуючи налаштування, які будуть нами виконані у наступних підрозділах. Розподіл адрес інтерфейсам маршрутизаторів приведено у таблиці 3.4. За вимогами підприємства-замовника, інтерфейсам маршрутизаторів, що виступають як шлюз для однієї з підмереж, було виділено перші можливі адреси с пулів цих підмереж.

Таблиця 3.4 – Адресація інтерфейсів маршрутизаторів

Назва пристрою	Назва інтерфейсу	IP-адреса	Маска	№VLAN
Karaskin_Router_1	G0/0	10.23.33.1	255.255.255.128	-
	S0/0/1	10.0.5.13	255.255.255.248	-
Karaskin_Router_2	G0/0	10.23.33.129	255.255.255.128	-
	Se0/0/0	209.165.202.1	255.255.255.252	-
	Se0/0/1	10.0.5.5	255.255.255.252	-
	Se0/1/0	10.0.5.1	255.255.255.252	-
	Se0/1/1	10.0.5.14	255.255.255.248	-
Karaskin_Router_3	G0/1.15	10.23.32.1	255.255.255.192	15
	G0/1.25	10.23.32.65	255.255.255.192	25
	G0/1.35	10.23.32.129	255.255.255.192	35
	G0/1.99	10.23.32.193	255.255.255.192	99
	Se0/0/0	10.0.5.9	255.255.255.252	-
	Se0/0/1	10.0.5.6	255.255.255.252	-
Karaskin_Router_4	G0/1	64.100.13.1	255.255.255.252	-
	G0/0	10.23.34.129	255.255.255.128	-
Karaskin_Router_5	G0/1	10.23.34.1	255.255.255.128	-
	Se0/0/0	10.0.5.10	255.255.255.252	-
	Se0/0/1	10.0.5.2	255.255.255.252	-
Karaskin_ISP	G0/1	64.100.13.2	255.255.255.252	-
	Se0/0/0	209.165.202.2	255.255.255.252	-
	G0/0	209.165.201.1	255.255.255.240	-

Наступним кроком нами було розраховано та статично розподілено IP-адреси серверів нашого підприємства (Табл. 3.5) за умовою, що вони

отримуватимуть п’ятнадцяту з допустимих IP-адрес підмережі, у якій вони знаходяться.

Таблиця 3.5 – Адресація інтерфейсів серверів

Назва пристрою	Назва інтер-фейсу	IP-адреса	Маска	Шлюз	VLAN
Karaskin_Server_HTTP	Fa0	10.23.33.15	/25	10.23.33.1	-
Karaskin_Server_DNS	Fa0	10.23.32.143	/26	10.23.32.129	35
Karaskin_Server TFTP	Fa0	10.23.34.143	/25	10.23.34.129	-

Останніми нами було розподілено IP-адреси SVI-інтерфейсам комутаторів наших підмереж (Табл. 3.6), які, згідно з вимогою підприємства-замовника, отримали IP-адреси, починаючи с другої допустимої адреси у пулі своїй підмережі.

Таблиця 3.6 – Адресація інтерфейсів комутаторів

Назва пристрою	IP-адреса SVI-інтерфейсу	Маска	Шлюз	№ VLAN
Karaskin_Switch_LAN1_1	10.23.33.2	/25	10.23.33.1	1
Karaskin_Switch_LAN1_2	10.23.33.3	/25	10.23.33.1	1
Karaskin_Switch_LAN1_3	10.23.33.4	/25	10.23.33.1	1
Karaskin_Switch_LAN1_4	10.23.33.5	/25	10.23.33.1	1
Karaskin_Switch_LAN1_5	10.23.33.6	/25	10.23.33.1	1
Karaskin_Switch_LAN2_1	10.23.33.130	/25	10.23.33.129	1
Karaskin_Switch_LAN2_2	10.23.33.131	/25	10.23.33.129	1

Кінець таблиці 3.6

Karaskin_Switch_LAN2_3	10.23.33.132	/25	10.23.33.129	1
Karaskin_Switch_LAN3_Core	10.23.32.194	/26	10.23.32.193	99
Karaskin_Switch_LAN3_1	10.23.32.195	/26	10.23.32.193	99
Karaskin_Switch_LAN3_2	10.23.32.196	/26	10.23.32.193	99
Karaskin_Switch_LAN3_3	10.23.32.197	/26	10.23.32.193	99
Karaskin_Switch_LAN4_1	10.23.34.130	/25	10.23.34.129	1
Karaskin_Switch_LAN4_2	10.23.34.131	/25	10.23.34.129	1
Karaskin_Switch_LAN5_1	10.23.34.2	/25	10.23.34.1	1
Karaskin_Switch_LAN5_1	10.23.34.3	/25	10.23.34.1	1
Karaskin_Switch_LAN5_1	10.23.34.4	/25	10.23.34.1	1
Karaskin_Switch_LAN5_1	10.23.34.5	/25	10.23.34.1	1

3.3 Налаштування моделі комп’ютерної системи корпоративної мережі

Розроблені схему комп’ютерної мережі КП «ДОКОЛ» та розраховану схему адресації пристроїв і мереж, що представлені у таблицях 3.2 – 3.6, нами було перенесено для перевірці на моделі комп’ютерної системи у програму Cisco Packet Tracer. Результат переносу логічної топології мережі можна побачити на рисунку 3.1.

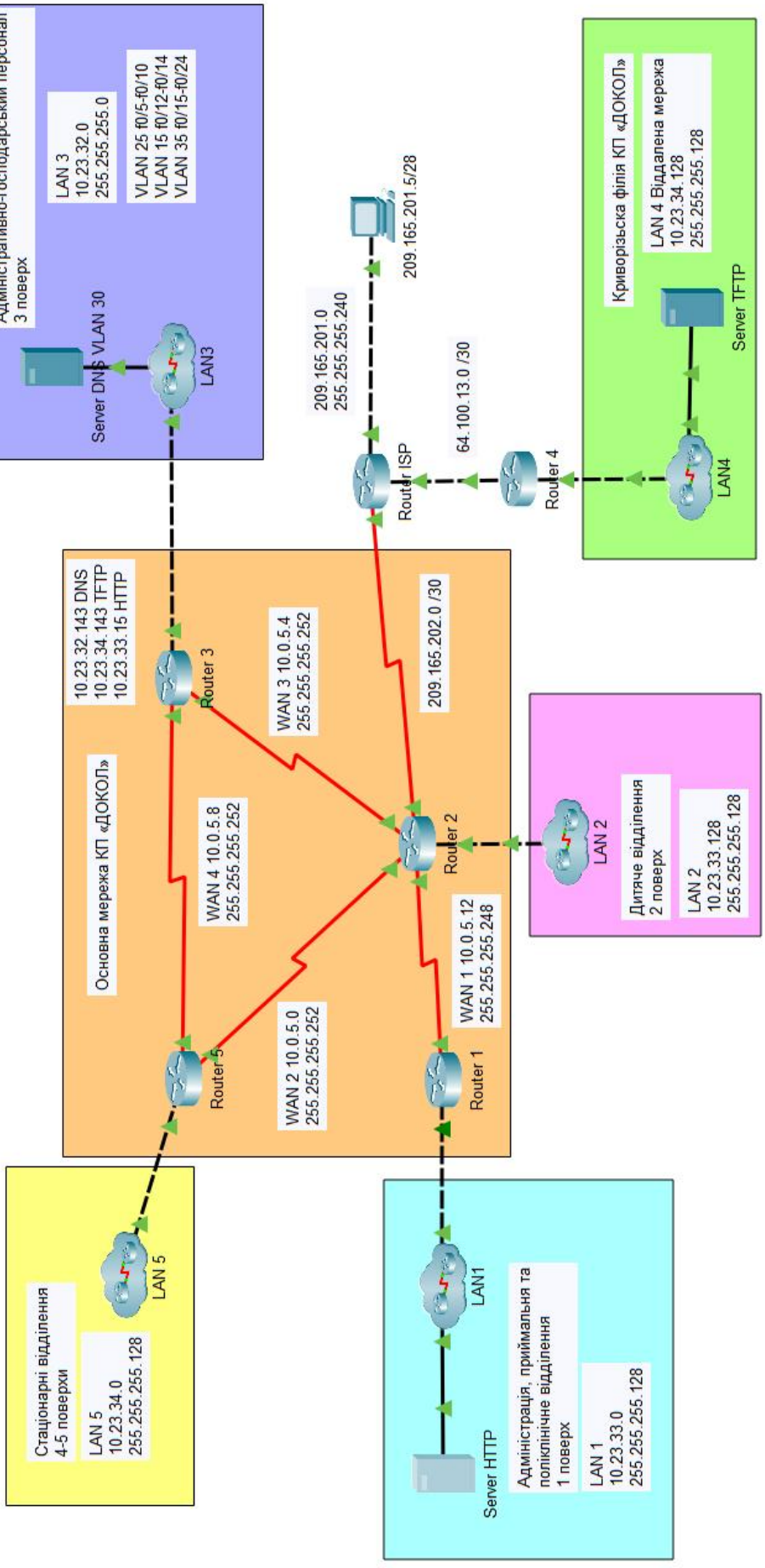


Рисунок 3.1 – Логічна топологія мережі КП «ДОКОЛ»

3.4.1 Базове налаштування конфігурації пристроїв

Перш, ніж приступати до програмування майбутньої мережі, нами було виконано базові налаштування конфігурації пристроїв мережі для їх захисту від несанкціонованого доступу. Проведені налаштування розглянемо на прикладі маршрутизатору підмережі LAN1:

Router>en //перехід до привелейованого режиму користувача

Router#conf t //перехід у режим глобальної конфігурації

Router(config)#hostname Karaskin_Router_1 //встановлення назви маршрутизатора згідно з його розташування у підмережі LAN1

Karaskin_Router_1(config)#line console 0

Karaskin_Router_1(config-line)#password cisco //встановлення паролю до консольної лінії

Karaskin_Router_1(config-line)#login

Karaskin_Router_1(config-line)#line vty 0 15

Karaskin_Router_1(config-line)#password cisco //встановлення паролю до ліній vty

Karaskin_Router_1(config-line)#login

Karaskin_Router_1(config-line)#enable secret class //встановлення паролю для входу у привелейований режим користувача на маршрутизаторі

Karaskin_Router_1(config)#service password-encryption //вмикання шифрування паролів

Karaskin_Router_1(config)#banner motd "Hi! I'm Karaskin_Router_1. Let's do it!" //Налаштування привітального повідомлення при запуску консолі на маршрутизаторі

Karaskin_Router_1(config)#ip domain-name Karaskin_Router_1 //Встановлення доменного імені

Karaskin_Router_1(config)#crypto key generate rsa //вмикання шифрування паролів за протоколом rsa

How many bits in the modulus [512]: 1024 //Задання кількості біт, які використовуються для шифрування протоколом rsa

Karaskin_Router_1(config)#username 123191_Karaskin password admincisco //задання локального користувача

Також нами було увімкнено використання протоколу ssh на всіх vty лініях:

Karaskin_Router_1(config)#line vty 0 15

Karaskin_Router_1(config-line)#transport input ssh

Karaskin_Router_1(config-line)#login local

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для того, щоб налаштувати зв’язок між нашими користувачами та пристроями у мережі, на маршрутизаторах були налаштовані відповідні IP-адреси на інтерфейсах, після чого нами було налаштовано таблицю маршрутизації на кожному з них таким чином, щоб кожен пристрій з однієї підмережі мав змогу встановити зв’язок с будь-яким іншим у своїй або іншій підмережі підприємства.

Для створення таблиці маршрутизації нами було використано протокол RIP (Routing Information Protocol). Це універсальний протокол, який може бути налаштовано майже на будь-яких марках маршрутизаторів.

Що стосується його характеристик, то він забезпечує доставку всієї таблиці маршрутизації на всі активні інтерфейси кожні 30 секунд, що дещо сповільнює протокол RIP в порівнянні з його більш сучасними аналогами. Також з мінусів можна виділити обмеження за кількістю переходів між маршрутизаторами – 15.

Але його простота розгортання у мережі і універсальність, порівняно з такими протоколами, як EIGRP, що може використовуватись тільки на маршрутизаторах компанії Cisco, роблять RIP зручним та оптимальним протоколом для невеликих мереж, що нам і потрібно.

Також, в процесі створення таблиць маршрутизації, нами буде використано статичну маршрутизацію на наших граничних маршрутизаторах для доступу основної мережі та віддаленої між собою, а також налаштування виходу пристроїв мережі підприємства в інтернет.

Налаштування протоколу RIP на прикладі маршрутизатора мережі LAN2, а саме налаштування самого протоколу:

Karaskin_Router_2(config)#router rip

Karaskin_Router_2(config-router)#version 2

Karaskin_Router_2(config-router)#network 10.23.33.128

Karaskin_Router_2(config-router)#network 10.0.5.12

Karaskin_Router_2(config-router)#network 10.0.5.0

Karaskin_Router_2(config-router)#network 10.0.5.4

Karaskin_Router_2(config-router)#exit

Та додавання статичного маршруту до мережі інтернет, після чого його було розповсюджено через оновлення інформації протоколом RIP на інші маршрутизатори мережі:

Karaskin_Router_2(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.2

Karaskin_Router_2(config)#router rip

Karaskin_Router_2(config-router)#redistribute static

Також додаємо статичний маршрут, щоб був доступ з локальної мережі підприємства до мережі провайдера ISP:

Karaskin_Router_2(config)#ip route 209.165.201.0 255.255.255.240 209.165.202.2

Крім того, згідно з вимогами, задаємо пропускну спроможність та тактову частоту на serial-інтерфейсах маршрутизаторів:

Karaskin_Router_1(config-if)#clock rate 128000

Karaskin_Router_1(config-if)#bandwidth 128

Також на всіх маршрутизаторах нами було налаштовано підтримку служби AAA таким чином:

Karaskin_Router_3(config)#aaa new-model //Увімкнення служби

Karaskin_Router_3(config)#radius-server host 10.23.32.143 auth-port 1645 key radius123 //Вказуємо AAA Radius сервер.

Для доступу до консолі створюємо аутентифікацію на основі протоколу RADIUS, а на випадок відсутності зв'язку з сервером AAA створюємо локальну базу даних:

Karaskin_Router_3(config)#aaa authentication login CONSOLE group radius local

Karaskin_Router_3(config)#line console 0

Karaskin_Router_3(config-line)#login authentication CONSOLE

Karaskin_Router_3(config-line)#exit

Для перевірки підключень до VTY ліній на маршрутизаторі створимо локальну базу даних користувачів:

Karaskin_Router_3(config)#aaa authentication login default local

Karaskin_Router_3(config)#username Karaskin_Router_3 password admin123

Karaskin_Router_3(config)#line vty 0 15

Karaskin_Router_3(config-line)#login authentication default

Karaskin_Router_3(config-line)#exit

Karaskin_Router_3(config)#do wr

Також, щоб сервіс AAA почав свою роботу, нами були зроблені відповідні налаштування на самому AAA-сервісі, функції якого ми поклали на DNS-сервер, на якому нами, крім DNS, було налаштовано сервіс AAA, як показано на рисунку 3.2, було додано кожен маршрутизатор до серверу radius, а також створено єдиного користувача, якого ми реєстрували на кожному маршрутизаторі.

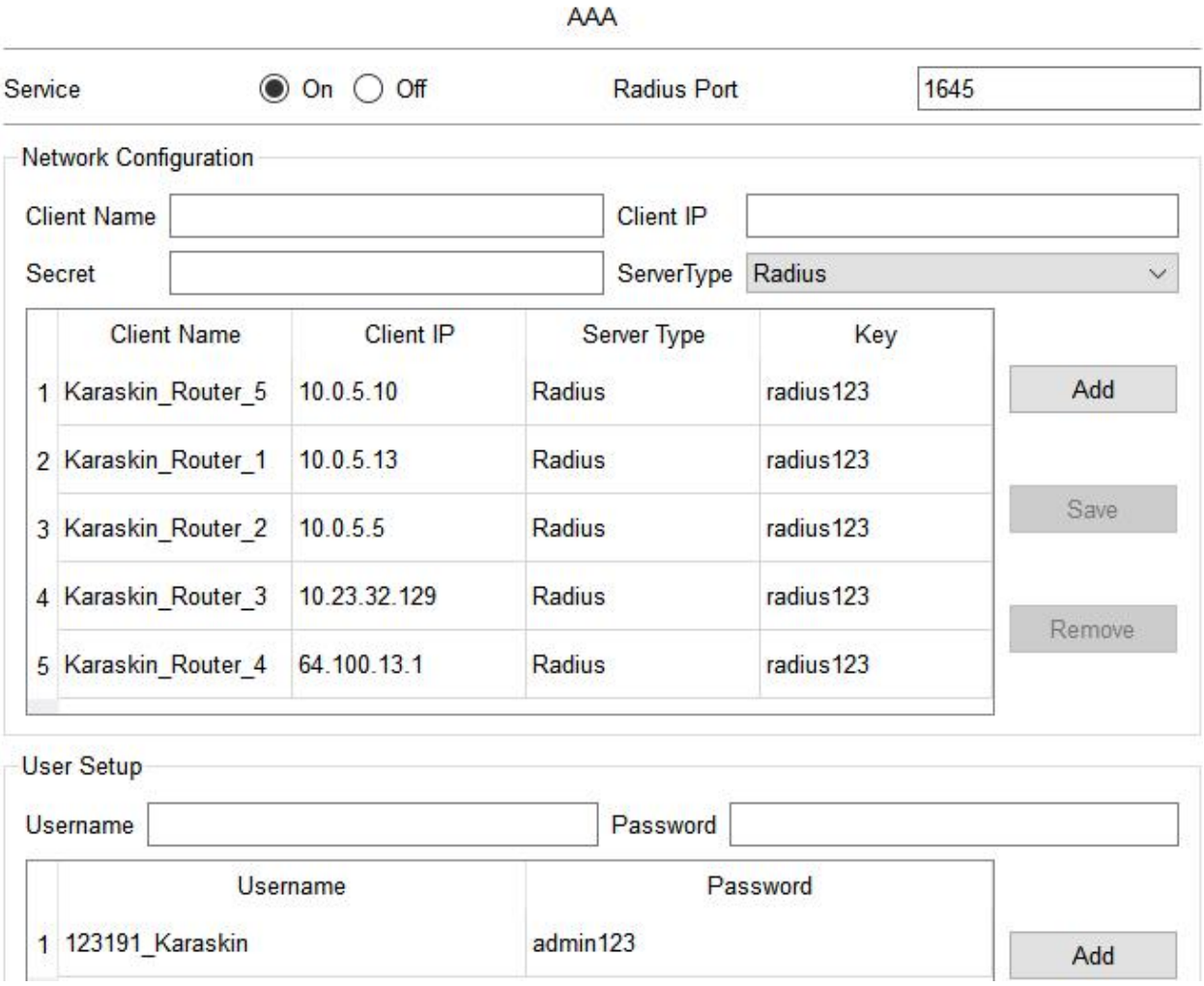


Рисунок 3.2 – Налаштування сервісу AAA на сервері

Крім того, кожен з маршрутизаторів було налаштовано на динамічне розподілення адрес вузлам, що входять до його підмережі. Для цього нами було створено dhcp пули адрес на кожному з них, що виключатимуть перші 10 адрес для резервування для шлюзу, комутаторів та інших можливих потреб, що можуть з’явитись у працівників в майбутньому. Також окремо були виключені адреси серверів підприємства, якщо вони входять до підмережі, для якої створюється пул адрес.

Налаштування такого пулу приведемо на прикладу LAN1:

Karaskin_Router_1(config)#ip dhcp pool poolLAN1

Karaskin_Router_1(dhcp-config)#network 10.23.33.0 255.255.255.128

Karaskin_Router_1(dhcp-config)#default-router 10.23.33.1

Karaskin_Router_1(dhcp-config)#dns-server 10.23.32.143

Karaskin_Router_1(dhcp-config)#exit

Karaskin_Router_1(config)#ip dhcp excluded-address 10.23.33.1 10.23.33.10

Karaskin_Router_1(config)#ip dhcp excluded-address 10.23.33.15

3.4.3 Налаштування роботи Інтернет

Для налаштування доступу до мережі Інтернет нами було встановлено одного провайдера послуг ISP. Для виходу пристроїв наших підмереж в Інтернет, нами було налаштовано динамічний NAT на граничному маршрутизаторі мережі, використовуючи заданий згідно з вимогами пул адрес: з 209.165.200.5 по 209.165.200.30.

Для налаштування, нами було створено розширений список доступу NAT5, що забороняє трафік з нашої основної мережі до віддаленої, та дозволяє весь інший:

Karaskin_Router_2(config)#ip access-list extended NAT5

Karaskin_Router_2(config-ext-nacl)#deny ip 10.23.32.0 0.0.0.255 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#deny ip 10.23.33.0 0.0.0.127 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#deny ip 10.23.33.128 0.0.0.127 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#deny ip 10.23.34.0 0.0.0.127 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#deny ip 10.0.5.0 0.0.0.255 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.32.0 0.0.0.255 any

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.33.0 0.0.0.127 any

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.33.128 0.0.0.127 any

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.34.0 0.0.0.127 any

Karaskin_Router_2(config-ext-nacl)#permit ip 10.0.5.0 0.0.0.255 any

Наступним кроком, користуючись цим списком, нами було налаштовано інтерфейси на взаємодію з NAT:

Karaskin_Router_2(config)#int s0/0/1

Karaskin_Router_2(config-if)#ip nat inside

Karaskin_Router_2(config-if)#int s0/1/1

Karaskin_Router_2(config-if)#ip nat inside

Karaskin_Router_2(config-if)#int s0/1/0

Karaskin_Router_2(config-if)#ip nat inside

Karaskin_Router_2(config-if)#int g0/0

Karaskin_Router_2(config-if)#ip nat inside

Karaskin_Router_2(config-if)#int s0/0/0

Karaskin_Router_2(config-if)#ip nat outside

Останнім кроком в налаштуванні NAT створення пулу Internet з адресами, вказаними на початку цього пункту, та призначення його для маскування IP-адрес пристроїв локальної мережі при виході їх у зовнішню мережу.

Karaskin_Router_2(config)#ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224

Karaskin_Router_2(config)#ip nat inside source list NAT5 pool Internet

Окремо нами було додано два статичні NAT для шифрування DNS та HTTP серверів відповідно. Це необхідно для того, щоб сторонній користувач мав змогу за адресою http://123.dnipro.ua переглянути WEB-сторінку нашого підприємства:

Karaskin_Router_2(config)#ip nat inside source static 10.23.32.143 209.165.200.4

Karaskin_Router_2(config)#ip nat inside source static 10.23.33.15 209.165.200.3

Таким самим чином, нами було налаштовано NAT на маршрутизаторі віддаленої мережі, але в пулі зовнішніх адрес для пристроїв використовувався діапазон від 209.165.200.37 до 209.165.200.62 з маскою 255.255.255.224.

Раніше нами було заборонено зв’язок через Інтернет з віддаленою мережею підприємства. Для налаштування, вже безпечного, зв’язку між ними, нами буде використано віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку. Для її створення, на граничному маршрутизаторі та віддаленої мережі нами було активовано модуль securityk9:

Karaskin_Router_2(config)#license boot module c2900 technology-package securityk9

Далі нами було створено нові списки доступу – VPN15, що на відміну від списків NAT15, дозволятимуть проходження трафіку між основною мережею та віддаленою:

Karaskin_Router_2(config)#ip access-list extended VPN5

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.32.0 0.0.0.255 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.33.0 0.0.0.127 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.33.128 0.0.0.127 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#permit ip 10.23.34.0 0.0.0.127 10.23.34.128 0.0.0.127

Karaskin_Router_2(config-ext-nacl)#permit ip 10.0.5.0 0.0.0.255 10.23.34.128 0.0.0.127

Наступним кроком на граничних маршрутизаторах додано властивості крипто-графічної політики ISAKMP 10 та створено загальний ключ шифрування karas:

Karaskin_Router_2(config)#crypto isakmp policy 10

Karaskin_Router_2(config-isakmp)#encr

Karaskin_Router_2(config-isakmp)#encryption 3des

Karaskin_Router_2(config-isakmp)#hash md5

Karaskin_Router_2(config-isakmp)#auth

Karaskin_Router_2(config-isakmp)#authentication pre-share

Karaskin_Router_2(config-isakmp)#group 2

Karaskin_Router_2(config-isakmp)#crypto isakmp key karas address 64.100.13.1

Karaskin_Router_2(config)#crypto ipsec transform-set dokol esp-3des esp-md5-hmac

Karaskin_Router_2(config)#crypto map DMAP 10 ipsec-isakmp

Karaskin_Router_2(config-crypto-map)#

Karaskin_Router_2(config-crypto-map)#set peer 64.100.13.1

Karaskin_Router_2(config-crypto-map)#set transform-set dokol

Karaskin_Router_2(config-crypto-map)#match address VPN5

Karaskin_Router_2(config-crypto-map)#exit

Останнім кроком у налаштуванні нами було прив’язано створене криптографічне зіставлення DMAP до вихідного інтерфейсу граничного маршрутизатору:

Karaskin_Router_2(config)#int s0/0/0

Karaskin_Router_2(config-if)#crypto map DMAP

*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON

З останнього повідомлення бачимо, що наш VPN-зв’язок було запущено успішно.

3.4.4 Захист інформації в комп'ютерній або кіберфізичній системі від несанкціонованого доступу

Для захисту інформації в системі від несанкціонованого доступу та розділення користувачів мережі на декілька підрозділів за виконуваними ними функціями, мережу LAN3 було розділено на чотири VLAN (віртуальні локальні мережі), три з яких, в свою чергу, належатимуть окремим відділам підприємства, а четверта – відповідати за управління пристроями мережі (Табл.3.7).

Створення VLAN та призначення їм імен на прикладі центрального комутатору мережі LAN3:

```
Karaskin_Switch_LAN3_Core(config)#vlan 15
Karaskin_Switch_LAN3_Core(config-vlan)#name VLAN15
Karaskin_Switch_LAN3_Core(config-vlan)#vlan 25
Karaskin_Switch_LAN3_Core(config-vlan)#name VLAN25
Karaskin_Switch_LAN3_Core(config-vlan)#vlan 35
Karaskin_Switch_LAN3_Core(config-vlan)#name VLAN35
Karaskin_Switch_LAN3_Core(config-vlan)#vlan 99
Karaskin_Switch_LAN3_Core(config-vlan)#name MANAGE
Karaskin_Switch_LAN3_Core(config-vlan)#vlan 100
Karaskin_Switch_LAN3_Core(config-vlan)#name NATIVE
```

Таблиця 3.7 – список мереж VLAN

Номер VLAN	Ім'я VLAN	Примітка	Розподілення портів
1	default	Не використовується	–
15	VLAN15	Господарський та управлінський персонал	f0/12 – f0/14

Кінець таблиці 3.7

25	VLAN25	Економічний відділ, бухгалтерія та відділ кадрів	f0/5 – f0/10
35	VLAN35	Медичні працівники, відділ статистики та системний адміністратор	f0/15 – f0/24
99	MANAGEMENT	Управління пристроями	–
100	NATIVE	Зв’язок між іншими VLAN підмережі	Switch_Core: f0/1-3 та g0/1 Інші комутатори: f0/1

Далі нами було VLAN налаштовано порти доступу для кожної з користувацьких віртуальних мереж та транкові для мережі NATIVE:

Karaskin_Switch_LAN3_Core(config-vlan)#int r f0/5-10
Karaskin_Switch_LAN3_Core(config-if-range)#switchport mode access
Karaskin_Switch_LAN3_Core(config-if-range)#switchport access vlan 25
Karaskin_Switch_LAN3_Core(config-if-range)#int r f0/12-14
Karaskin_Switch_LAN3_Core(config-if-range)#switchport mode access
Karaskin_Switch_LAN3_Core(config-if-range)#switchport access vlan 15
Karaskin_Switch_LAN3_Core(config-if-range)#int r f0/15-24
Karaskin_Switch_LAN3_Core(config-if-range)#switchport mode access
Karaskin_Switch_LAN3_Core(config-if-range)#switchport access vlan 35
Karaskin_Switch_LAN3_Core(config-if-range)#int r f0/1-3
Karaskin_Switch_LAN3_Core(config-if-range)#switchport mode trunk
Karaskin_Switch_LAN3_Core(config-if-range)#switchport trunk native vlan 100

Окремо налаштовуємо як транковий порт, що відповідає за зв’язок з маршрутизатором:

```
Karaskin_Switch_LAN3_Core(config)#int g0/1
Karaskin_Switch_LAN3_Core(config-if)#switchport mode trunk
Karaskin_Switch_LAN3_Core(config-if)#switchport trunk native vlan 100
```

Далі нами було зроблено налаштування маршрутизатору, а саме виділено чотири підінтерфейси під кожну з задіяних VLAN та призначено їм відповідну інкапсуляцію та шлюз (на прикладі інкапсуляції для vlan 15):

```
Karaskin_Router_3(config-if)#int g0/1.15
Karaskin_Router_3(config-subif)#encapsulation dot1Q 15
Karaskin_Router_3(config-subif)#ip address 10.23.32.1 255.255.255.192
Karaskin_Router_3(config-subif)#no sh
```

Також цей маршрутизатор, що здійснює маршрутизацію між VLAN, як і інші у минулому пункті, було налаштовано як dhcp сервер. Пули, створені на ньому, отримали назву за принципом pollvlan№ та з виключенням перших 10 адрес з пулу допустимих для розподілення. Також, у VLAN35 знаходиться сервер із статичною адресою, яку ми також виключили з пулів. Синтаксис команд описаних дій:

```
Karaskin_Router_3(config)#ip dhcp pool poolvlan15
Karaskin_Router_3(dhcp-config)#network 10.23.32.0 255.255.255.192
Karaskin_Router_3(dhcp-config)#default-router 10.23.32.1
Karaskin_Router_3(dhcp-config)#dns-server 10.23.32.143
Karaskin_Router_3(config)#ip dhcp pool poolvlan25
Karaskin_Router_3(dhcp-config)#network 10.23.32.64 255.255.255.192
Karaskin_Router_3(dhcp-config)#default-router 10.23.32.65
Karaskin_Router_3(dhcp-config)#dns-server 10.23.32.143
Karaskin_Router_3(config)#ip dhcp pool poolvlan35
Karaskin_Router_3(dhcp-config)#network 10.23.32.128 255.255.255.192
Karaskin_Router_3(dhcp-config)#default-router 10.23.32.129
```

Karaskin_Router_3(dhcp-config)#dns-server 10.23.32.143

Karaskin_Router_3(config)#ip dhcp excluded-address 10.23.32.1 10.23.32.10

Karaskin_Router_3(config)#ip dhcp excluded-address 10.23.32.65 10.23.32.75

Karaskin_Router_3(config)#ip dhcp excluded-address 10.23.32.129 10.23.32.139

Karaskin_Router_3(config)#ip dhcp excluded-address 10.23.32.143

Для комутаторів були налаштовані SVI-інтерфейси, призначивши їм IP адреси з таблиці 3.6:

Karaskin_Switch_LAN3_Core(config)#int vlan99

Karaskin_Switch_LAN3_Core(config-if)#ip address 10.23.32.194 255.255.255.192

Karaskin_Switch_LAN3_Core(config-if)#ip default-gateway 10.23.32.193

Для забезпечення безпеки серверів, на порти комутаторів, підключених до них, було налаштовано функцію безпеки портів, а саме дозволяємо доступ до порту тільки двом унікальним пристроям, налаштовуємо динамічне розпізнавання MAC-адрес та додавання їх в поточну конфігурацію та щоб у разі порушення безпеки, з’являлось повідомлення:

Karaskin_Switch_LAN3_3(config)#int f0/24

Karaskin_Switch_LAN3_3(config-if)#switchport mode access

Karaskin_Switch_LAN3_3(config-if)#switchport port-security maximum 2

Karaskin_Switch_LAN3_3(config-if)#switchport port-security mac-address sticky

Karaskin_Switch_LAN3_3(config-if)#switchport port-security violation restrict

Згідно з цими налаштуваннями VLAN, наша підмережа набуває наступного топологічного вигляду, що можна побачити на рисунку 3.3

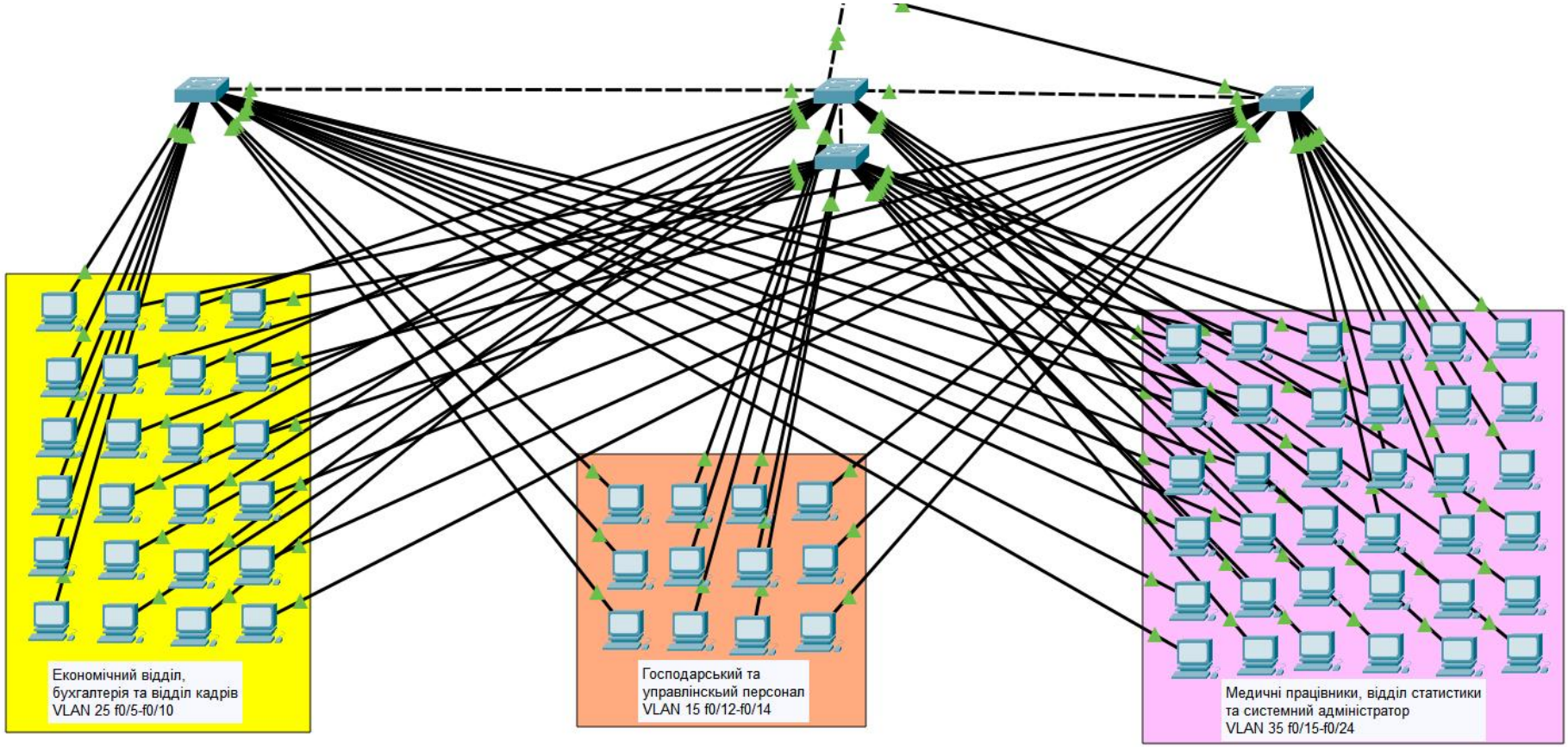


Рисунок 3.3 – Логічна топологія підмережі LAN3 КП «ДОКОЛ»

3.5 Перевірка роботи моделі комп'ютерної системи

Для перевірки базових налаштувань пристроїв та працездатності AAA сервісу, спробуємо зробити вхід до якогось з маршрутизаторів (Рис. 3.4):

```
Hi! I'm Karaskin_Router_2. Let's do it!

User Access Verification

Username: 123191_Karaskin
Password:
Karaskin_Router_2>en
Password:
Karaskin_Router_2#
```

Рисунок 3.4 – Вхід до граничного маршрутизатора мережі

Наступним кроком перевіримо таблицю маршрутизації, щоб переконатись в її вірному налаштуванні, на прикладі того ж маршрутизатору, оскільки він є граничним, та спробуємо надіслати exo-запит з різних кінців мережі в рамках головної мережі (Рис. 3.5):

Successful	PC8	PC4	ICMP	0.000	N	1

Рис. 3.5 – Таблиця маршрутизації граничного маршрутизатору

PC8 належить до мережі LAN3, в той час як PC4 знаходить у LAN1.

Наступним кроком перевіримо можливість пристроїв мережі виходити у інтернет. Для цього на PC4 відправимо exo-запит на адресу 0.0.0.0 (Рис. 3.6).

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 0.0.0.0

Pinging 0.0.0.0 with 32 bytes of data:

Ping statistics for 0.0.0.0:
    Packets: Sent = 4, Received = 219, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1427ms, Average = 390ms
```

Рисунок 3.6 – Перевірка можливості пристроїв вийти у Internet

Наступним кроком перевіримо налаштування NAT на граничному маршрутизаторі основної та віддаленої мереж. Для цього знову відправимо ехо-запити з пристроїв цих мереж до пристрою провайдеру, після чого за допомогою спеціальної команди переглянемо характеристики трансляції через на граничних маршрутизаторах (Рис. 3.7 – 3.9).

Successful	PC4	209.165.201.5/28	ICMP		0.000	N
Successful	PC11	209.165.201.5/28	ICMP		0.000	N
Failed	209.165.201.5/28	PC4	ICMP		0.000	N
Failed	209.165.201.5/28	PC11	ICMP		0.000	N

Рисунок 3.7 – Ехо-запити з пристроїв підприємства та провайдеру

```
Karaskin_Router_4#sh ip nat tran
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.37:4  10.23.34.140:4     209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.37:5  10.23.34.140:5     209.165.201.5:5    209.165.201.5:5
```

Рисунок 3.8 – Ехо-запит з віддаленої мережі до пристрою провайдера

```
Karaskin_Router_2#sh ip nat tran
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.5:11  10.23.33.12:11     209.165.201.5:11   209.165.201.5:11
---  209.165.200.3     10.23.33.15        ---                ---
---  209.165.200.4     10.23.32.143       ---                ---
```

Рисунок 3.9 – Ехо-запит з основної мережі до пристрою провайдера

Як бачимо, ехо-запити до провайдеру пройшли успішно, в той час, як запити від провайдеру були не допущені до внутрішньої мережі, що задовільняє виконаним налаштуванням. Також, з рисунку 3.9 можна побачити, що при відстежуванні nat, також враховуються статичні NAT адреси, що ми призначили нашим DNS та HTTP серверам. Отже, перевіримо доступність сайту КП «ДОКОЛ» з пристрою провайдера та його наповнення, що має включати тему, мету та завдання дипломного (Рис. 3.10).

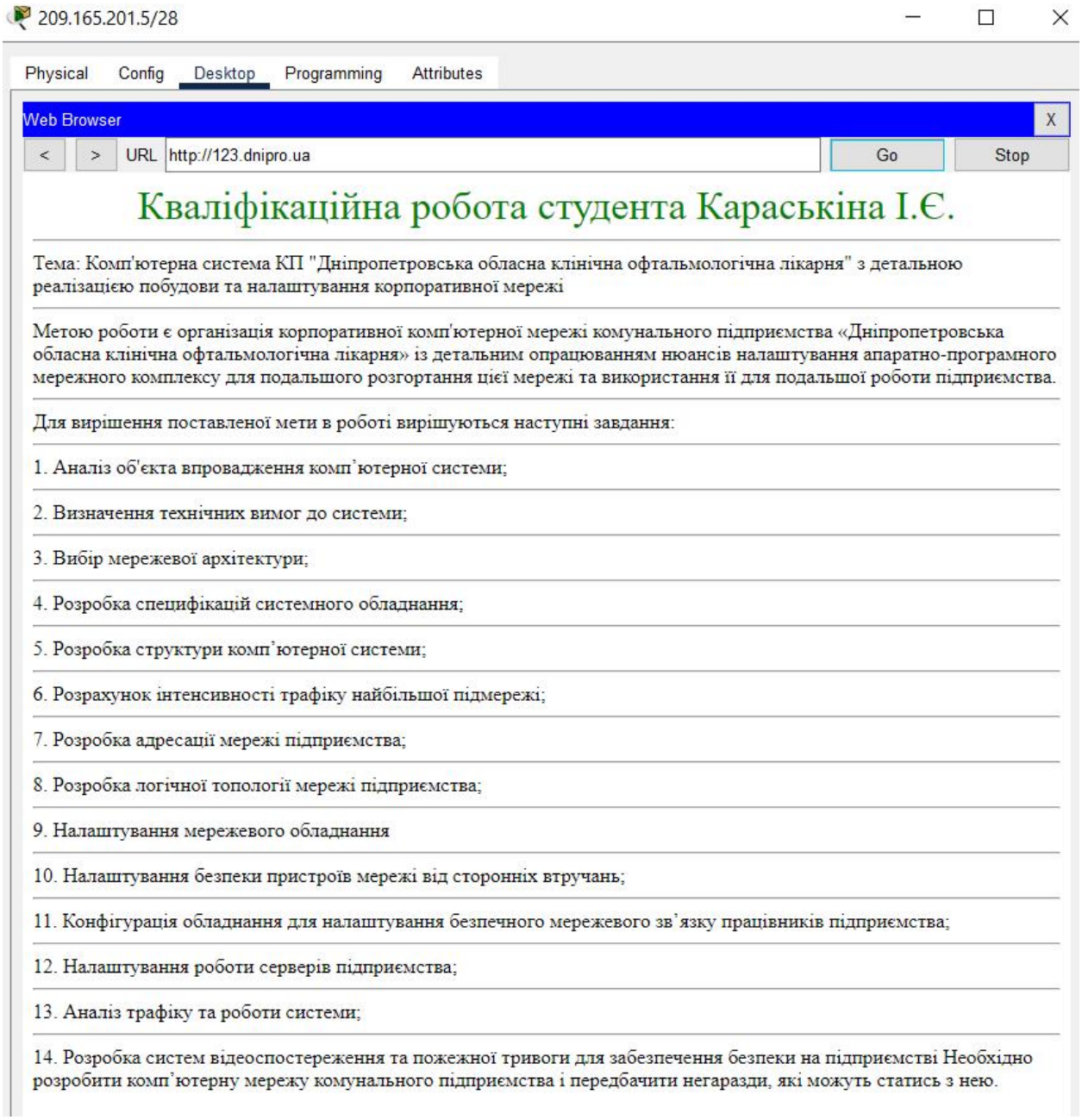


Рисунок 3.10 – Доступність сайту підприємства з пристрою провайдера

Для перевірки встановлення VPN зв'язку між основною та віддаленою мережею підприємства, відправимо ехо-запити між пристроями цих мереж (Рис. 3.11) та переконаємось, що вони проходять саме через налаштований VPN тунель (Рис. 3.12).

```
C:\> ping 10.23.34.140

Pinging 10.23.34.140 with 32 bytes of data:

Request timed out.
Reply from 10.23.34.140: bytes=32 time=14ms TTL=125
Reply from 10.23.34.140: bytes=32 time=2ms TTL=125
Reply from 10.23.34.140: bytes=32 time=2ms TTL=125

Ping statistics for 10.23.34.140:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 14ms, Average = 6ms

C:\> ping 10.23.34.140

Pinging 10.23.34.140 with 32 bytes of data:

Reply from 10.23.34.140: bytes=32 time=3ms TTL=125
Reply from 10.23.34.140: bytes=32 time=2ms TTL=125
Reply from 10.23.34.140: bytes=32 time=21ms TTL=125
Reply from 10.23.34.140: bytes=32 time=2ms TTL=125

Ping statistics for 10.23.34.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 21ms, Average = 7ms
```

Рисунок 3.11 – Ехо-запит з пристрою у мережі LAN5 до віддаленої

```
local  ident (addr/mask/prot/port): (10.23.34.0/255.255.255.128/0/0)
remote  ident (addr/mask/prot/port): (10.23.34.128/255.255.255.128/0/0)
current_peer 64.100.13.1 port 500
 PERMIT, flags={origin_is_acl,}
#pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
#pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0
```

Рисунок 3.12 – Інформація про проходження пакетів по тунелю VPN

Для перевірки працездатності побудованої VLAN, переконаємось в доступності вузлів з однієї VLAN до іншої, зробивши ехо-запит (Рис. 3.13).

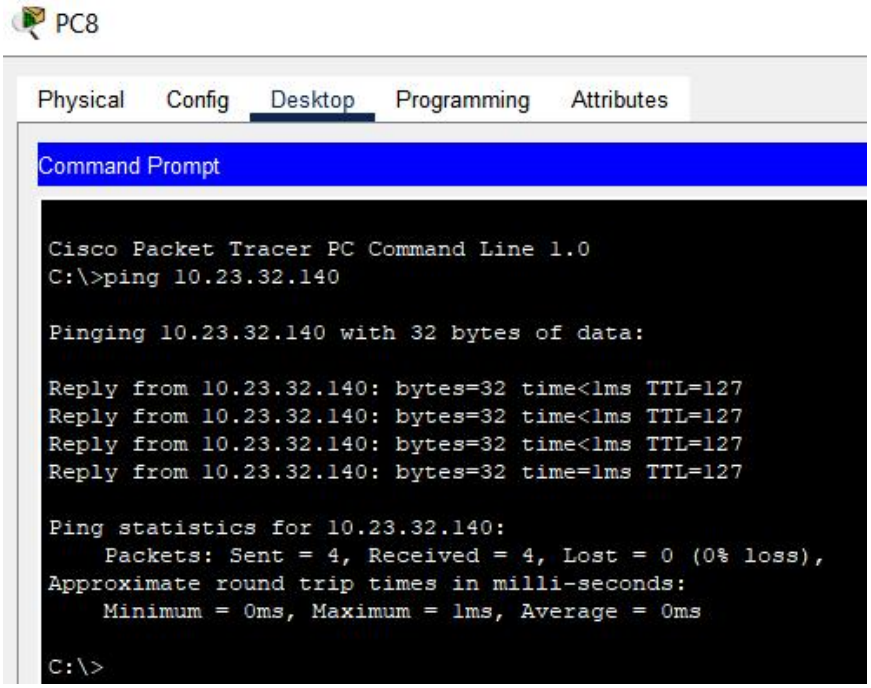


Рисунок 3.13 – Ехо-запит між вузлами різних VLAN

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Об’єкт та тип впроваджуваного компоненту системи

Для Комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня», згідно з вимогами, було розроблену системи відеоспостереження та попередження про пожежну небезпеку для кожного поверху основної будівлі підприємства.

4.2 Застосовані технології IoT

В рамках проекту комп’ютерної системи, а саме розробки інтернету речей, нами була використана технологія хмарних обчислень.

За цією технологією, надання обчислювальних ресурсів за запитом відбувається через мережу інтернет. В якості ресурсів для таких обчислень можуть виступати сервери, мережі передачі даних, системи зберігання, ПЗ, тощо.

В нашому випадку, обчислення відбуватимуться на спеціально відведеному для цього сервері IoT в мережі підприємства, що фізично розташований поряд з сервером DNS та входить до тієї ж віртуальної локальної мережі VLAN35 для спрощення доступу до нього системного адміністратора. Цей сервер буде використано для керування камерами відеоспостереження у будівлі підприємства та системою попередження про пожежну небезпеку.

4.3 Розробка адресації та топології компоненту системи

Для функціонування описаних компонентів, нами було додатково налаштовано нашу топологію мережі, додавши до неї сервер IoT, пристрої, що виконуватимуть функції веб-камер, пристрої, необхідні для функціонування системи попередження про пожежну небезпеку, а також пристрій типу Home Gateway. Останній буде забезпечувати бездротове під’єднання до IoT пристроїв з одного боку, а з іншого також матиме підключення до мережі підприємства у VLAN35. Логічну топологію отриманої мережі з розподіленням пристроїв за поверхами розташування, можна побачити на рисунку 4.1.

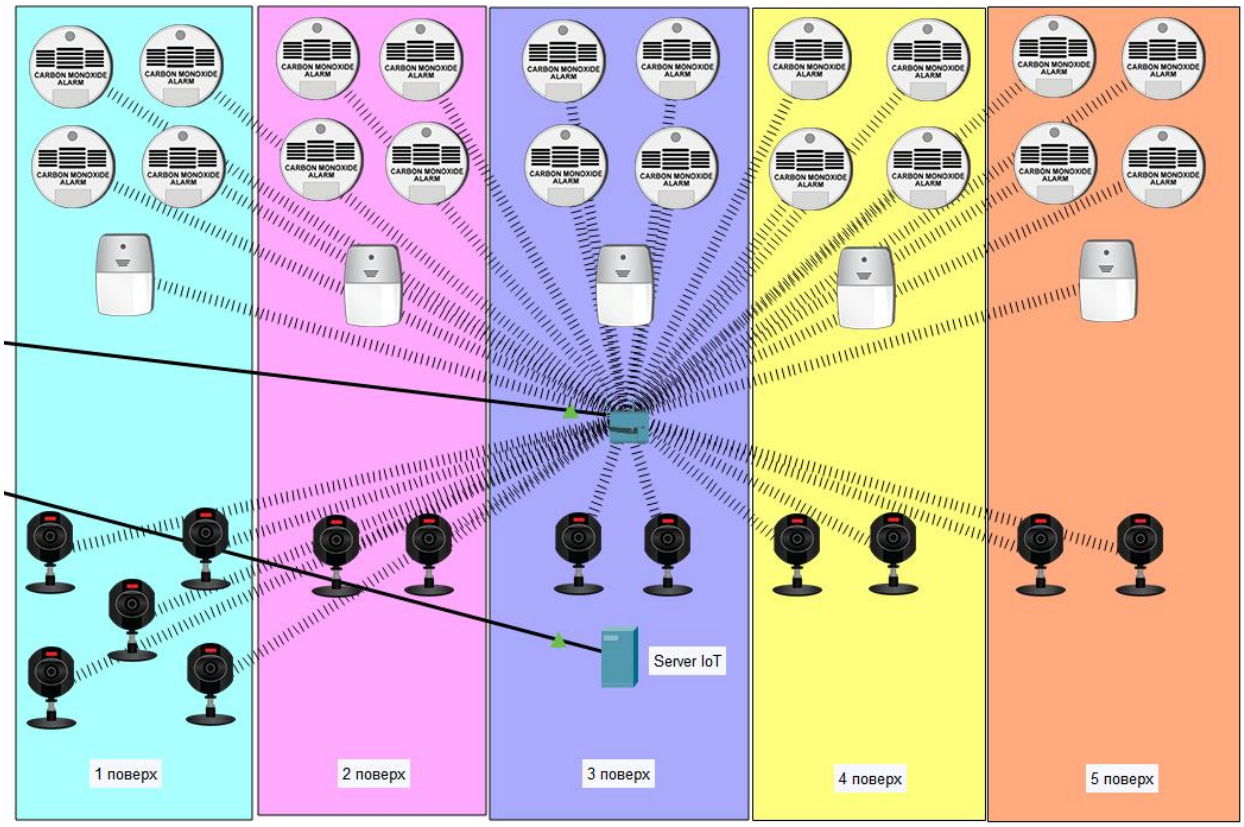


Рисунок 4.1 – Логічна топологія IoT пристроїв

Для виконання подальших налаштувань, нами було розроблено окрему таблицю адресації для нових пристроїв, необхідних для функціонування системи, яку наведено у таблиці 4.1.

Таблиця 4.1 – IP-адресація пристроїв компоненту системи

Назва пристрою	Назва інтер-фейсу	IP-адреса	Маска	Шлюз	VLAN
Karaskin_Serve_IoT	Fa0	10.23.32.139	/26	10.23.32.129	35
Karaskin_IoT_Gateway	Internet	10.23.32.138	/26	10.23.32.129	35

Адреси пристроям були виділені статично, користуючись закладеним у підрозділі 3.4.4 при налаштуванні у VLAN dhcp пулів запасом у 10 адрес на кожну VLAN.

4.4 Налаштування зв'язку IoT пристроїв компоненту системи

Для виконання налаштувань та керування IoT пристроями, по-перше, необхідно налаштувати їх зв'язок з сервером IoT, що ми розташували у віртуальній мережі VLAN35.

Для цього було увімкнено сервіс IoT на сервері, а на сервері DNS додано новий домен – iot.dokol.ua за адресою 10.23.32.138.

Наступним кроком, налаштовуємо маршрутизатор Karaskin_IoT_Gateway, що буде об'єднувати всі пристрої IoT та надавати їм доступ до відповідного серверу. Ці налаштування можна побачити на рисунках 4.2–4.4. На рисунку 4.2 нами було привласнено адресу та шлюз для маршрутизатору. На рисунку 4.3 – внутрішній шлюз для пристроїв, що під'єднуються зсередини, а також це налаштування відповідає за можливу динамічну адресацію внутрішніх пристроїв, якщо увімкнути цю опцію на них. На рисунку 4.4 було зроблено мережеві налаштування, а саме введено власний SSID мережі – Security, а також встановлено протокол автентифікації WPA2-PSK з паролем karabaskin. Це надає деякий захист від підключень до цієї мережі та робить її приватною.

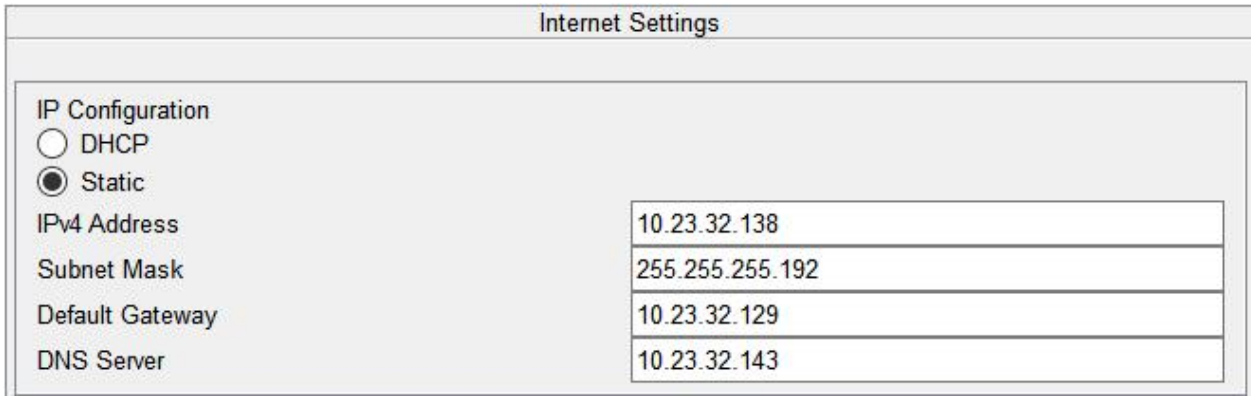


Рисунок 4.2 – Адресація для доступу у мережу на Karaskin_IoT_Gateway

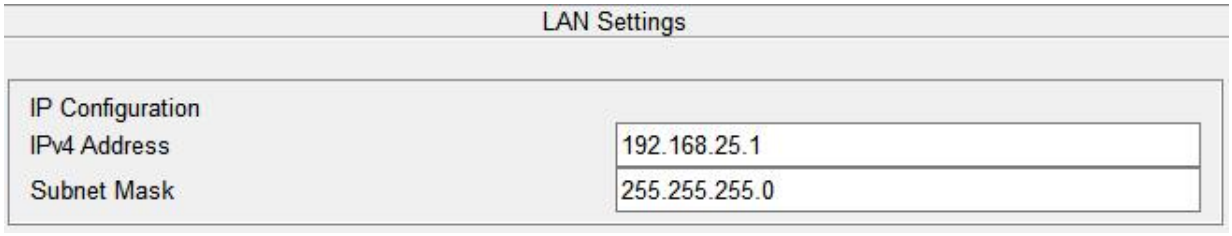


Рисунок 4.3 – Налаштування внутрішньої мережі Karaskin_IoT_Gateway

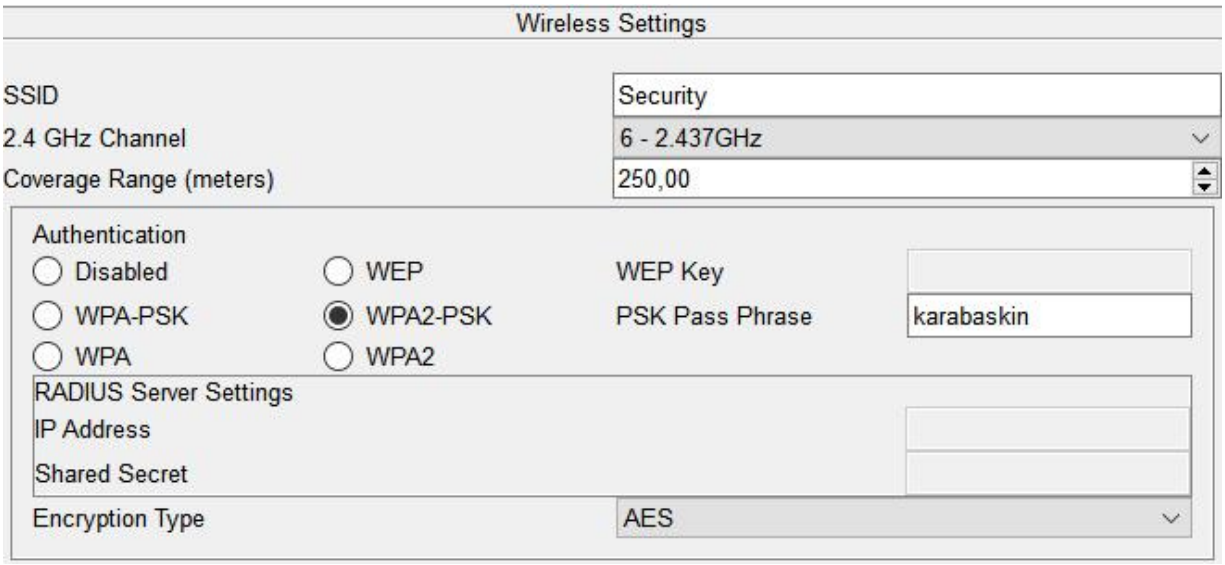


Рисунок 4.4 – Налаштування бездротового зв’язку Karaskin_IoT_Gateway

Останнє, що нам було необхідно зробити перед налаштуванням вже самих IoT пристроїв – увійти з будь-якого ПК мережі підприємства до серверу через домен iot.dokol.ua та створити нового користувача з логіном та паролем admin12319 (Рис. 4.5). Після цього, увійшовши за цим логіном і паролем, ми зможемо переглядати, налаштовувати та керувати підключеними IoT пристроями.

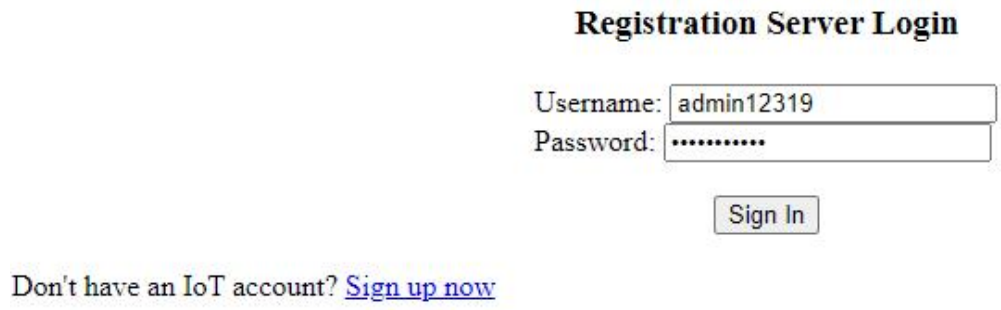


Рисунок 4.5 – Вхід користувача на IoT сервер

За даним акаунтом будуть додаватись всі IoT пристрої до нашого серверу. Без наявності логіну та паролю від акаунту, доступ до налаштувань або перегляду цих пристроїв через сервер буде неможливим.

Принцип налаштування зв'язку з сервером у нашому випадку єдиний для всіх пристроїв, оскільки ми використовуємо хмарні обчислення і всі пристрої підключаються бездротовим способом через однаковий шлюз.

Тож, розглянемо ці налаштування на прикладі камери відеоспостереження 1.1, що розташована на першому поверху підприємства. У налаштуваннях бездротового зв'язку (Рис. 4.6) було вказано SSID та пароль протоколу WPA2-PSK, які нами було вказано на IoT шлюзі, а також обрано dhcp адресацію, щоб шлюз сам надав пристрою IP-адресу.

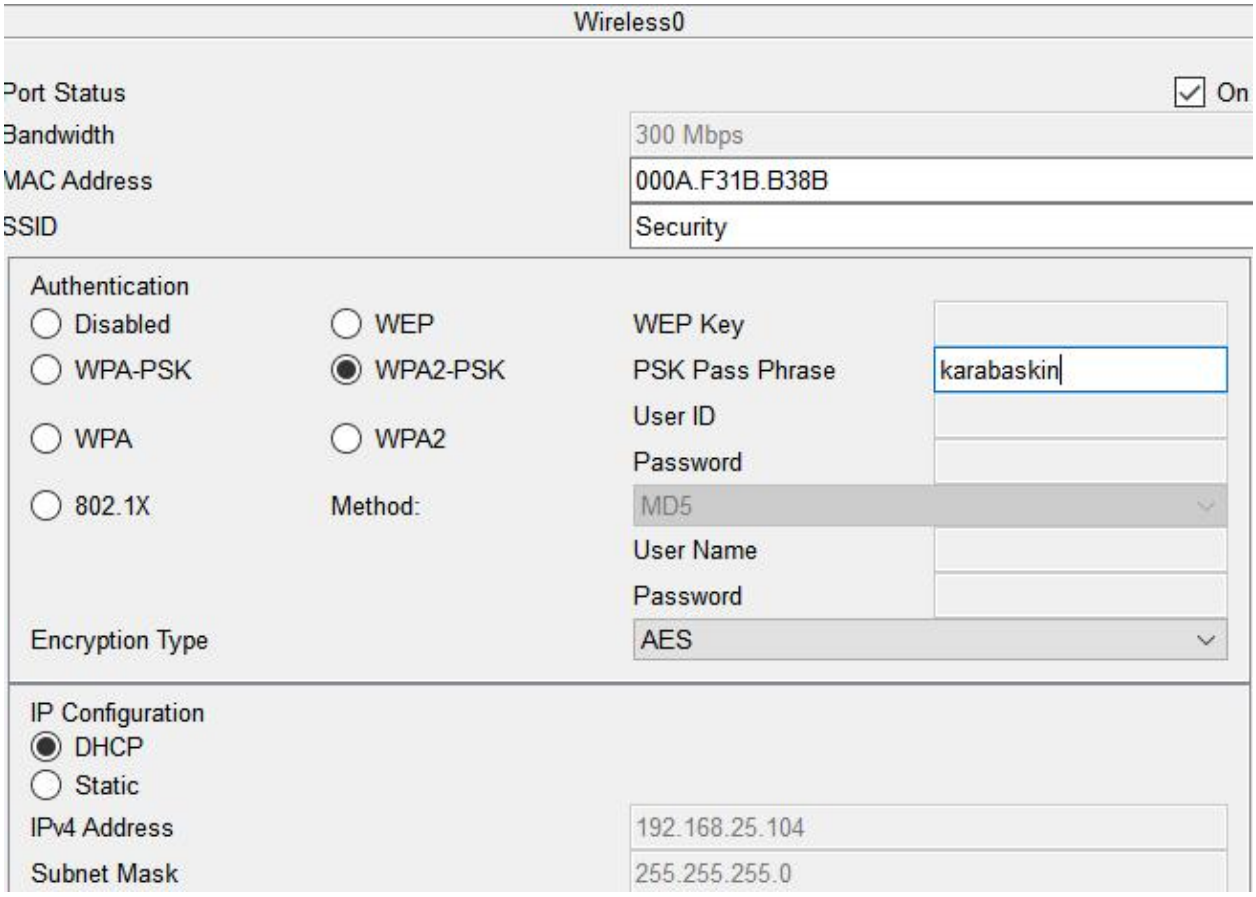


Рисунок 4.6 – Бездротові налаштування пристроїв IoT

У глобальних налаштуваннях кожного IoT пристрою (Рис. 4.7), нами було призначено їм індивідуальні імена, що відповідають їх роду діяльності, та пронумеровано індексами, перша цифра якого означає належність до поверху будівлі підприємства, а друга – порядковий номер на цьому поверсі.

Рисунок 4.7 – Базові налаштування пристрою IoT

Також, на кожному пристрої IoT, нами було внесено дані, щодо IoT серверу для цих пристроїв, та акаунту, на які вони будуть зареєстровані та відображатимуться у списку при вході до цього акаунту користувачем з мережі підприємства. Ці налаштування можна побачити на рисунку 4.8.

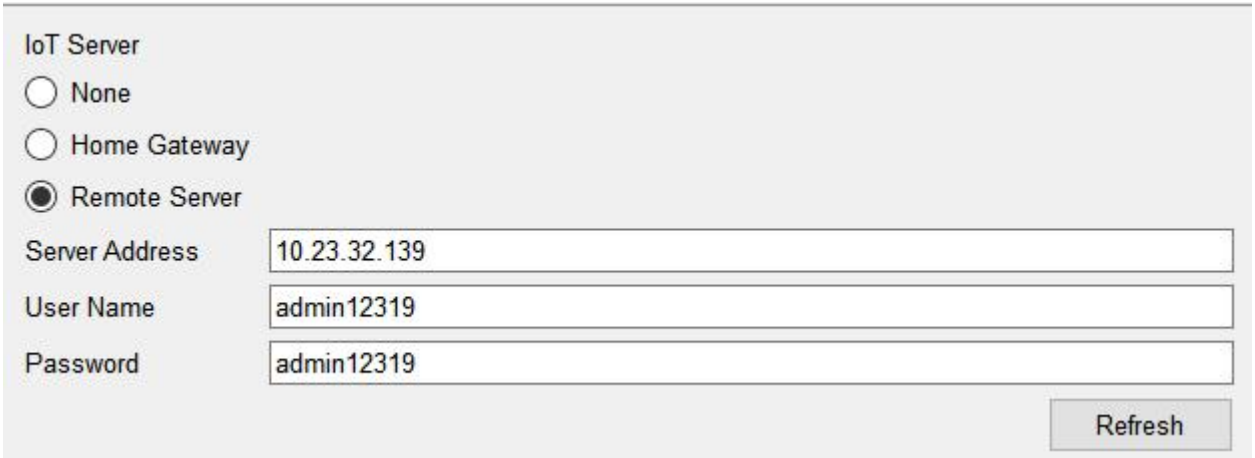


Рисунок 4.8 – Налаштування зв’язку з IoT сервером на пристрої

4.5 Налаштування роботи IoT пристроїв компоненту системи

Для налаштування та керування пристроями IoT, увійдемо з будь-якого ПК мережі підприємства до нашого акаунту на IoT сервері (Рис. 4.9). Там ми побачимо список всіх під'єднаних пристроїв, їх статус та матимемо можливість, якщо це активний пристрій (в нашому випадку це камери відеоспостереження та сирени) вручну керувати їх станом.

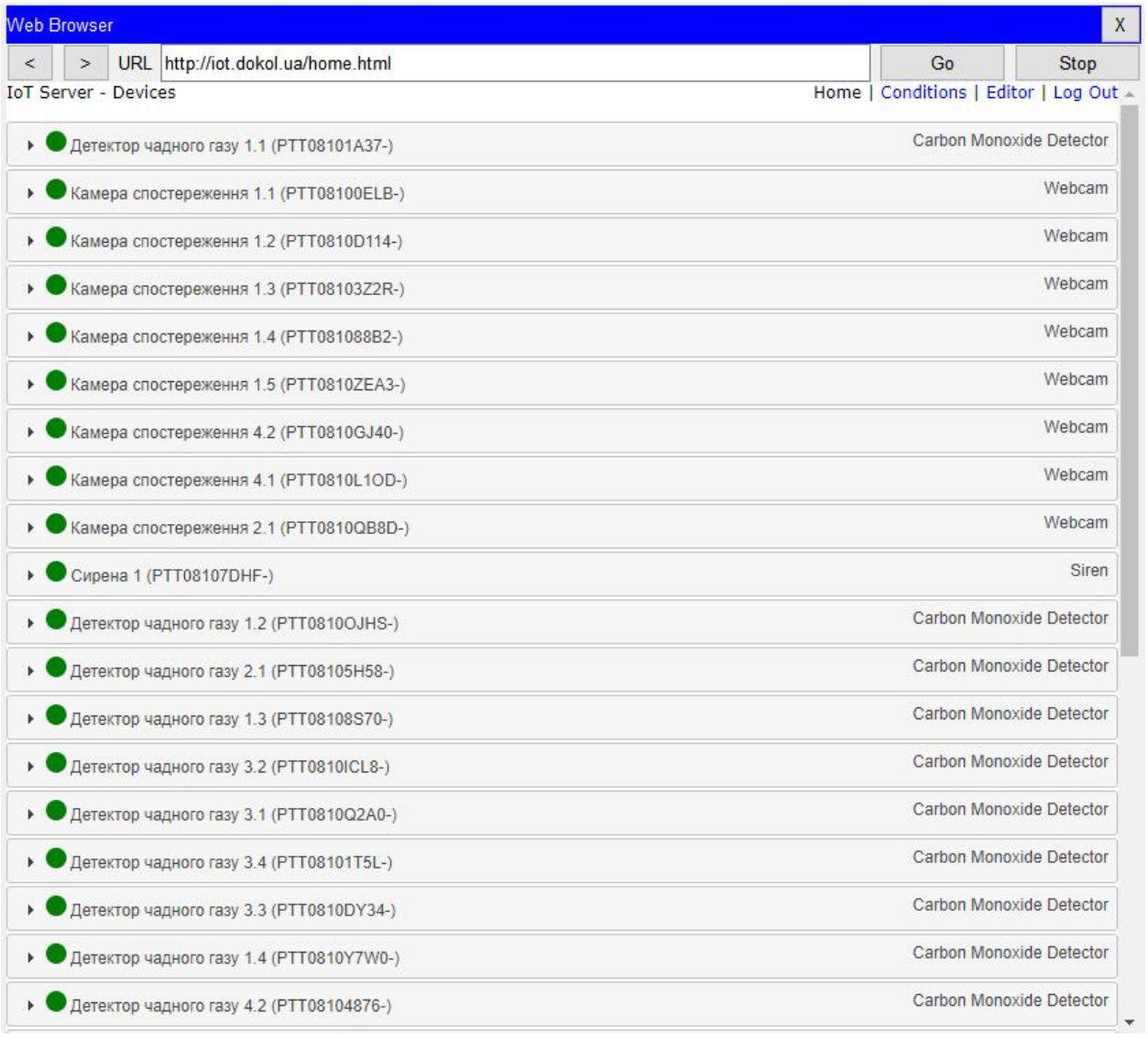


Рисунок 4.9 – Підключені та функціонуючі до IoT серверу пристрої

Якщо у випадку з камерами відеоспостереження нас влаштовує їх підключення, перегляд картинки з них та можливість ручного вмикання та

вимикання їх за необхідністю, то система пожежної тривоги вимагає додаткового налаштування.

Для цього налаштування, на сторінці IoT серверу з головної сторінки із списком пристроїв перейдемо до сторінки Conditions, де нами було створено два типу правил. Перше (Рис. 4.10) – сирена вмикається, якщо хоча б один датчик на поверсі фіксує загрозливий для життя людини рівень чадного газу у повітрі. Друге (Рис. 4.11) – сирена вимикається тільки за умовою, що всі датчики не фіксують загрозливої концентрації газу у повітрі.

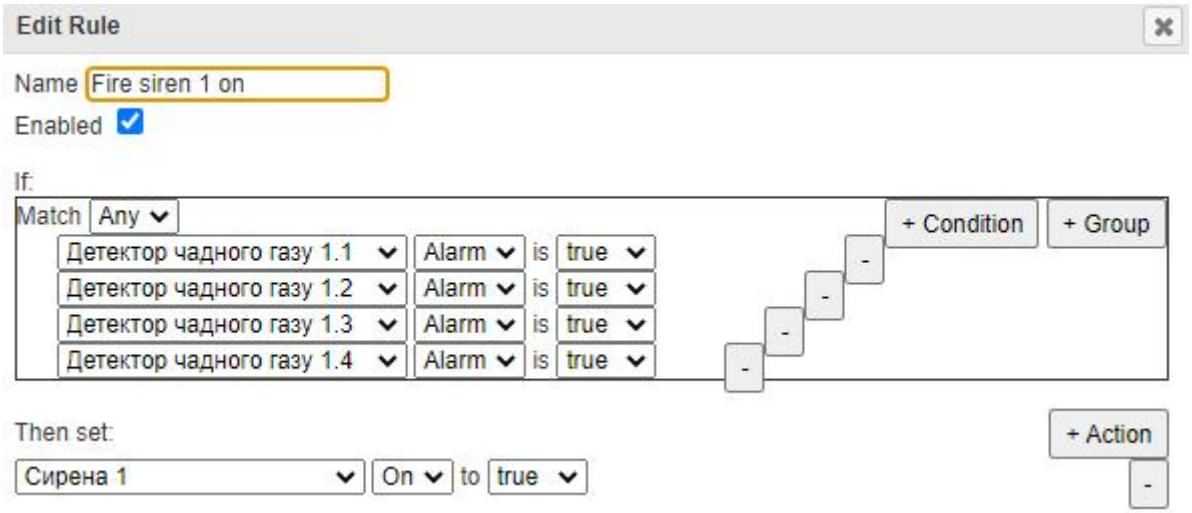


Рисунок 4.10 – Умови для увімкнення сирени пожежної небезпеки

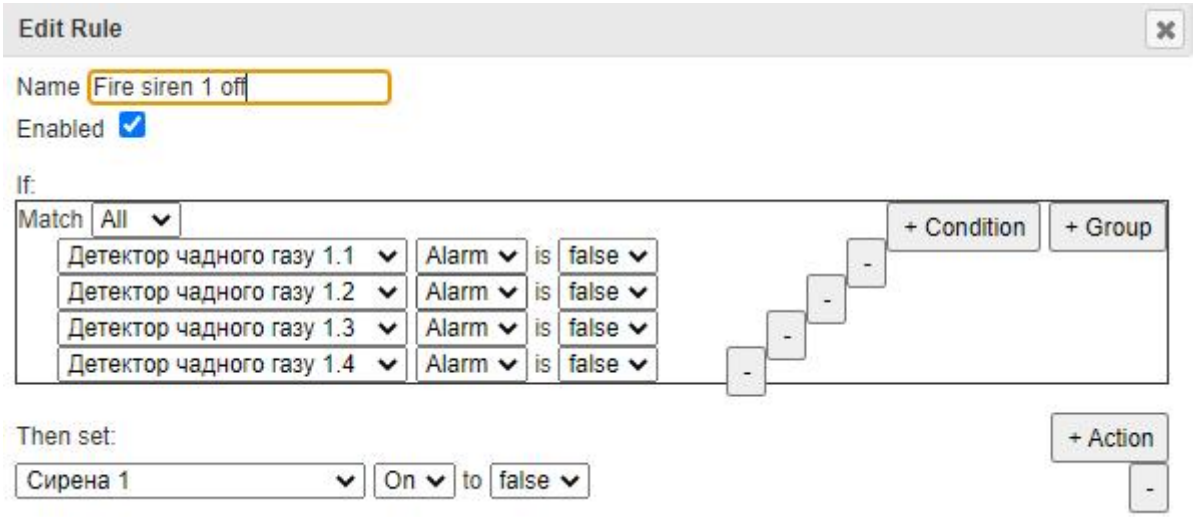


Рисунок 4.11 – Умови для вимкнення сирени пожежної небезпеки

Сумарно було створено 10 правил роботи сигналізації про пожежну небезпеку, по 2 правили для кожного поверху що можна побачити на рисунках 4.12 та 4.13.

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Fire siren 1 on	Match any: • PTT08101A37- Alarm is true • Детектор чадного газу 1.2 Alarm is true • Детектор чадного газу 1.3 Alarm is true • Детектор чадного газу 1.4 Alarm is true	Set Сирена 1 On to true
Edit Remove	Yes	Fire siren 1 off	Match all: • PTT08101A37- Alarm is false • Детектор чадного газу 1.2 Alarm is false • Детектор чадного газу 1.3 Alarm is false • Детектор чадного газу 1.4 Alarm is false	Set Сирена 1 On to false
Edit Remove	Yes	Fire siren 2 on	Match any: • Детектор чадного газу 2.1 Alarm is true • Детектор чадного газу 2.2 Alarm is true • Детектор чадного газу 2.4 Alarm is true • Детектор чадного газу 2.3 Alarm is true	Set Сирена 2 On to true
Edit Remove	Yes	Fire siren 2 off	Match all: • Детектор чадного газу 2.1 Alarm is false • Детектор чадного газу 2.2 Alarm is false • Детектор чадного газу 2.4 Alarm is false • Детектор чадного газу 2.3 Alarm is false	Set Сирена 2 On to false
Edit Remove	Yes	Fire siren 3 on	Match any: • Детектор чадного газу 3.1 Alarm is true • Детектор чадного газу 3.2 Alarm is true • Детектор чадного газу 3.3 Alarm is true • Детектор чадного газу 3.4 Alarm is true	Set Сирена 3 On to true
Edit Remove	Yes	Fire siren 3 off	Match all: • Детектор чадного газу 3.1 Alarm is false • Детектор чадного газу 3.2 Alarm is false • Детектор чадного газу 3.3 Alarm is false • Детектор чадного газу 3.4 Alarm is false	Set Сирена 3 On to false
Edit Remove	Yes	Fire siren 4 on	Match any: • Детектор чадного газу 4.1 Alarm is true • Детектор чадного газу 4.3 Alarm is true • Детектор чадного газу 4.2 Alarm is true • Детектор чадного газу 4.4 Alarm is true	Set Сирена 4 On to true

Рисунок 4.12 – Правила спрацьовування сирени (початок)

Edit Remove	Yes	Fire siren 4 off	Match all: • Детектор чадного газу 4.1 Alarm is false • Детектор чадного газу 4.2 Alarm is false • Детектор чадного газу 4.3 Alarm is false • Детектор чадного газу 4.4 Alarm is false	Set Сирена 4 On to false
Edit Remove	Yes	Fire siren 5 on	Match any: • Детектор чадного газу 5.1 Alarm is true • Детектор чадного газу 5.2 Alarm is true • Детектор чадного газу 5.3 Alarm is true • Детектор чадного газу 5.4 Alarm is true	Set Сирена 5 On to true
Edit Remove	Yes	Fire siren 5 off	Match all: • Детектор чадного газу 5.1 Alarm is false • Детектор чадного газу 5.2 Alarm is false • Детектор чадного газу 5.3 Alarm is false • Детектор чадного газу 5.4 Alarm is false	Set Сирена 5 On to false

Рисунок 4.13 – Правила спрацьовування сирени (кінець)

ВИСНОВКИ

В даному дипломному проекті нами було розроблено комп’ютерну систему для Комунального підприємства «Дніпропетровська обласна клінічна офтальмологічна лікарня» з детальною реалізацією побудови та налаштування корпоративної мережі, а також здійснено налаштування систем відеоспостереження та попередження про пожежну небезпеку.

За результатами виконання проекту, розроблена система повністю відповідає поставленим перед нами задачами по побудові та опрацюванню апаратно-програмного мережного комплексу, що сприятиме підвищенню ефективності роботи підприємства в цілому.

В рамках виконання даного проекту були успішно вирішені задачі з аналізу об’єкту впровадження комп’ютерної системи, визначення технічних вимог до системи, з обрання мережевої архітектури, розробки специфікацій системного обладнання та комп’ютерної системи, розрахунку інтенсивності трафіку найбільшої підмережі, розробки адресації та логічної топології мережі підприємства, з налаштування мережевого обладнання та безпеки пристроїв мережі від сторонніх втручань; було виконано налаштування безпечного мережевого зв’язку працівників та роботи серверів підприємства. Крім того, були здійснені аналіз трафіку та роботи системи за допомогою спеціального програмного забезпечення з моделювання комп’ютерних мереж Cisco Packet Tracer та розроблені системи відеоспостереження та пожежної тривоги для забезпечення безпеки на підприємстві.

В проекті була обґрунтована важливість та необхідність застосування даних заходів по модернізації систем як у КП «ДОКОЛ», так і в цілому у закладах галузі охорони здоров’я. Були розраховані можливі технічні рішення та створені можливі специфікації обладнання для їх впровадження.

Дипломний проект повністю відповідає темі та завданню, оформлений згідно з нормативними документами та вимогами методичного керівництва. Поставлені перед проектом цілі були досягнуті в повному обсязі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 65 с.

2. ДСТУ 1.5:2015. Правила розроблення, викладання та оформлення національних нормативних документів – К.: Держстандарт, 2015. – 65 с.

3. Постанова № 42 від 01.12.99 «Про санітарні норми мікроклімату виробничих приміщень» ДСН 3.3.6.042-99 / Міністерство охорони здоров'я України, головний державний санітарний лікар України.

4. Закон України «Про публічні закупівлі» від 25.12.2015 № 922-VIII (чинний) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/922-19#Text (дата звернення 17.05.2023р.)

5. Vkursi Pro. Інформація про організацію, що виступила об'єктом дослідження [Електронний ресурс] – Режим доступу: https://vkursi.pro/card/kp-dokol-26508184 (дата звернення 04.05.2023р.)

6. Школа Бізнесу Нова Пошта. Як організувати структуру підприємства: актуальні види і формати [Електронний ресурс] – Режим доступу: https://online.novaposhta.education/blog/yak-organizuvati-strukturu-pidpriyemstva-aktualni-vidi-i-formati (дата звернення 06.05.2023р.)

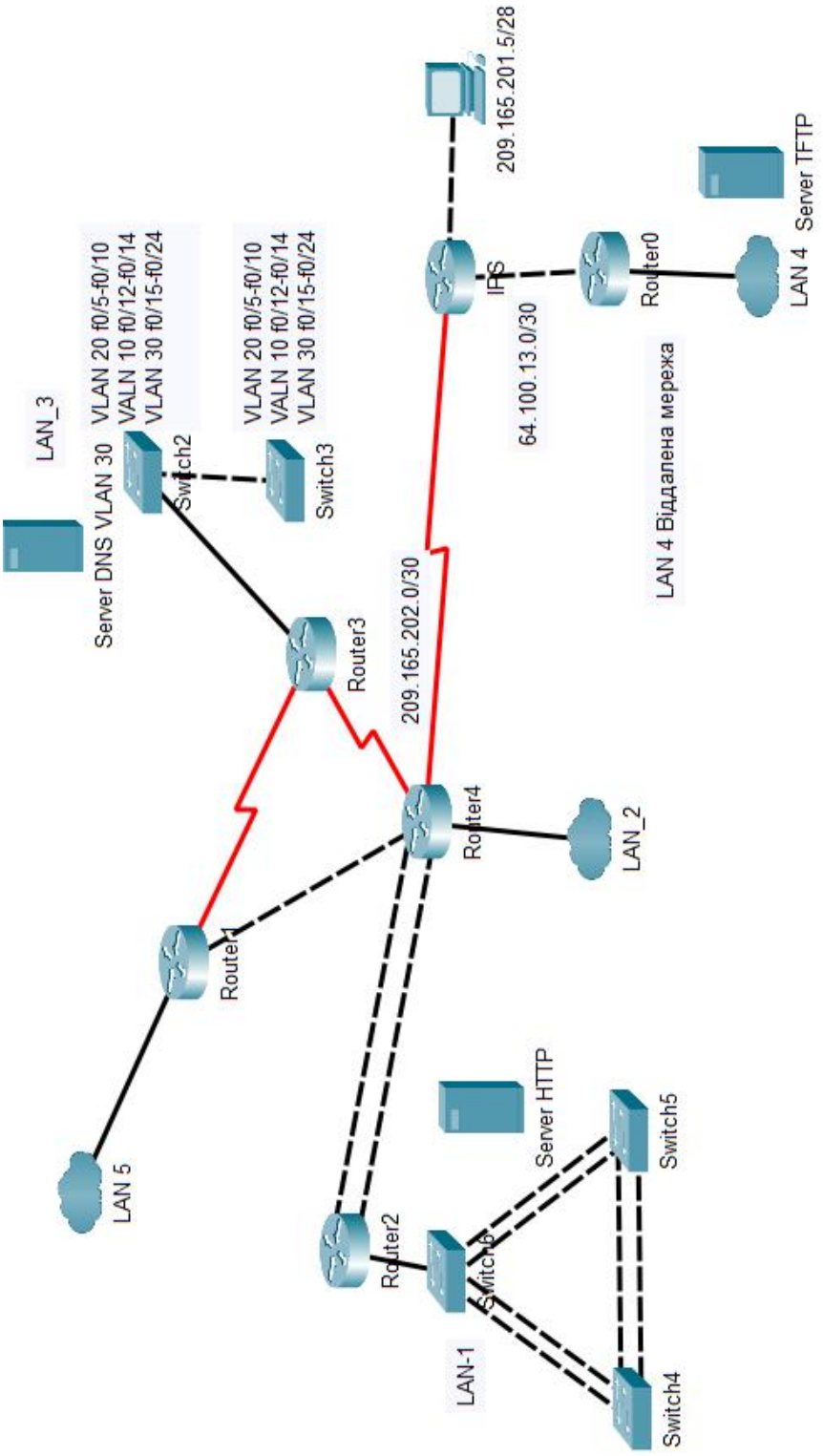
7. Комп'ютерна академія Cisco [Електронний ресурс] – Режим доступу: https://www.netacad.com (дата звернення 19.05.2023р.)

8. Проектування та монтаж локальних комп'ютерних мереж: [навчальний посібник] / І. М. Журавська. – Миколаїв : Видавництво ЧДУ ім. Петра Могили, 2016. – 396 с.

9. Технічні характеристики обладнання впроваджуваної системи [Електронний ресурс] – Режим доступу: https://rozetka.com.ua (дата звернення 30.05.2023р.)

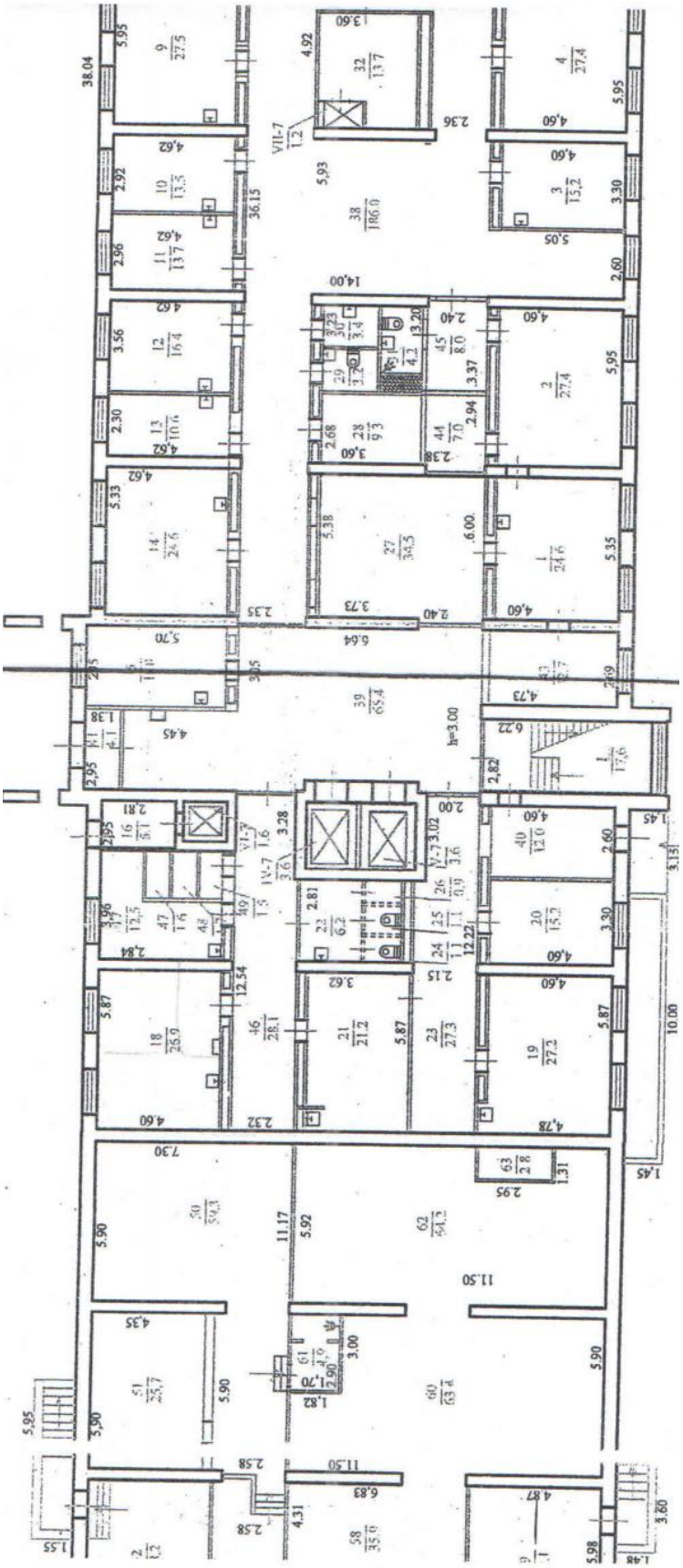
Додаток А

Загальна архітектура мережі КП «ДОКОЛ»



Додаток Б

План першого поверху будівлі КП «ДОКОЛ»



Додаток В

Текст програми налаштування корпоративної мережі

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23005-01 12 01

Листів 13

2023

АНОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи.

Ця програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену та ssh доступу до комп’ютерної системи на маршрутизаторах.

ЗМІСТ

1. Налаштування маршрутизатора Karaskin_Router_2

```
Current configuration : 3496 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
//Шифрування паролів
service password-encryption
!
//Ім’я пристрою
hostname Karaskin_Router_2
!
//Пароль до привілейованого режиму
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
// 1.4 Налаштування DHCP
ip dhcp excluded-address 10.23.33.129 10.23.33.139
!
ip dhcp pool poolLAN2
network 10.23.33.128 255.255.255.128
default-router 10.23.33.129
dns-server 10.23.32.143
!
//Налашутвання AAA сервісу
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
```

```
no ip cef
no ipv6 cef
!
//Створення користувача з логіном та паролем
username 123191_Karaskin password 7 082048430017061E010803
username Karaskin_Router_2 password 7 082048430017544541
!
//Підключення технології securityk9
license udi pid CISCO2901/K9 sn FTX15242CPI-
license boot module c2900 technology-package securityk9
!
//Створення та налаштування VPN
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key karas address 64.100.13.1
!
crypto ipsec transform-set dokol esp-3des esp-md5-hmac
!
crypto map DMAP 10 ipsec-isakmp
set peer 64.100.13.1
set transform-set dokol
match address VPN5
!
//Створення доменного імені
ip domain-name Karaskin_Router_2
```

```
spanning-tree mode pvst
!
//Налаштування інтерфейсів маршрутизатора
interface GigabitEthernet0/0
ip address 10.23.33.129 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.165.202.1 255.255.255.252
ip nat outside
clock rate 128000
crypto map DMAP
!
interface Serial0/0/1
bandwidth 128
ip address 10.0.5.5 255.255.255.252
ip nat inside
clock rate 128000
!
interface Serial0/1/0
bandwidth 128
```

```
ip address 10.0.5.1 255.255.255.252
ip nat inside
clock rate 128000
!
interface Serial0/1/1
bandwidth 128
ip address 10.0.5.14 255.255.255.252
ip nat inside
!
interface Vlan1
no ip address
shutdown
!
//Налаштування протоколу маршрутизації
router rip
version 2
redistribute static
network 10.0.0.0
no auto-summary
!
//Налаштування NAT
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224
ip nat inside source list NAT5 pool Internet
ip nat inside source static 10.23.32.143 209.165.200.4
ip nat inside source static 10.23.33.15 209.165.200.3
ip classless
//Налаштування виходу до мережі провайдеру та Internet
ip route 0.0.0.0 0.0.0.0 209.165.202.2
ip route 209.165.201.0 255.255.255.240 209.165.202.2
```

```
ip route 10.23.34.128 255.255.255.128 209.165.202.2
!
ip flow-export version 9
!
//Налаштування розширених ACL списків
ip access-list extended VPN5
permit ip 10.23.32.0 0.0.0.255 10.23.34.128 0.0.0.127
permit ip 10.23.33.0 0.0.0.127 10.23.34.128 0.0.0.127
permit ip 10.23.33.128 0.0.0.127 10.23.34.128 0.0.0.127
permit ip 10.23.34.0 0.0.0.127 10.23.34.128 0.0.0.127
permit ip 10.0.5.0 0.0.0.255 10.23.34.128 0.0.0.127
ip access-list extended NAT5
deny ip 10.23.34.0 0.0.0.127 10.23.34.128 0.0.0.127
deny ip 10.23.32.0 0.0.0.255 10.23.34.128 0.0.0.127
deny ip 10.23.33.0 0.0.0.127 10.23.34.128 0.0.0.127
deny ip 10.23.33.128 0.0.0.127 10.23.34.128 0.0.0.127
deny ip 10.0.5.0 0.0.0.255 10.23.34.128 0.0.0.127
permit ip 10.23.32.0 0.0.0.255 any
permit ip 10.23.33.128 0.0.0.127 any
permit ip 10.23.33.0 0.0.0.127 any
permit ip 10.23.34.0 0.0.0.127 any
permit ip 10.0.5.0 0.0.0.255 any
!
//Налаштування привітання при вмиканні командного рядку
banner motd ^CHi! I'm Karaskin_Router_2. Let's do it!^C
!
//Налаштування RADIUS серверу
radius server 10.23.32.143
address ipv4 10.23.32.143 auth-port 1645
```

```
key radius123
!
//Налаштування консольних та vty ліній
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
end
```

2. Налаштування маршрутизатора Karaskin_Router_3

```
Current configuration : 2461 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Karaskin_Router_3
```

```
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
ip dhcp excluded-address 10.23.32.1 10.23.32.10
ip dhcp excluded-address 10.23.32.65 10.23.32.75
ip dhcp excluded-address 10.23.32.129 10.23.32.139
ip dhcp excluded-address 10.23.32.143
!
ip dhcp pool poolvlan15
network 10.23.32.0 255.255.255.192
default-router 10.23.32.1
dns-server 10.23.32.143
ip dhcp pool poolvlan25
network 10.23.32.64 255.255.255.192
default-router 10.23.32.65
dns-server 10.23.32.143
ip dhcp pool poolvlan35
network 10.23.32.128 255.255.255.192
default-router 10.23.32.129
dns-server 10.23.32.143
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
no ip cef
no ipv6 cef
!
```

```
username 123191_Karaskin password 7 082048430017061E010803
username Karaskin_Router_3 password 7 082048430017544541
!
license udi pid CISCO2901/K9 sn FTX1524063O-
!
ip domain-name Karaskin_Router_3
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/1.15
encapsulation dot1Q 15
ip address 10.23.32.1 255.255.255.192
!
interface GigabitEthernet0/1.25
encapsulation dot1Q 25
ip address 10.23.32.65 255.255.255.192
!
interface GigabitEthernet0/1.35
```

```
encapsulation dot1Q 35
ip address 10.23.32.129 255.255.255.192
!
interface GigabitEthernet0/1.99
encapsulation dot1Q 99
ip address 10.23.32.193 255.255.255.192
!
interface Serial0/0/0
bandwidth 128
ip address 10.0.5.9 255.255.255.252
!
interface Serial0/0/1
ip address 10.0.5.6 255.255.255.252
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
mac-address 0090.0c1c.a101
no ip address
!
router rip
version 2
network 10.0.0.0
no auto-summary
!
ip classless
!
```

```
ip flow-export version 9
!
banner motd ^CHi! I'm Karaskin_Router_3. Let's do it!^C
!
radius server 10.23.32.143
address ipv4 10.23.32.143 auth-port 1645
key radius123
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
end
```