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 Ширмакова Леоніда Олеговича
(ПІБ)

Академічної групи 123-20ск-1
(шифр)

Спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)

За освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

На тему «Комп'ютерна система ДП «Антонов» з реалізацією побудови, налаштування та безпеки корпоративної мережі з підтримкою IP-телефонії»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
Кваліфікаційної Роботи	проф. Цвіркун Л.І.			
Розділів:				
Розробка апаратної частини	доц. Ткаченко С.М.			
Розробка корпоративної мережі	ас. Бешта Л.В.			

Рецензент				

Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро
2023

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних технологій
та комп'ютерної інженерії
(повна назва)

(підпис) Гнатушенко В.В. (прізвище, ініціали)

" " *2023 року*

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента Ширмакова Л.О (прізвище та ініціали) **академічної групи** 123-20ск-1 (шифр)

спеціальності 123 «Комп'ютерна інженерія»

за освітньо-професійною програмою 123 «Комп'ютерна інженерія» (офіційна назва)

на тему «Комп'ютерна система ДП «Антонов» з реалізацією побудови, налаштування та безпеки корпоративної мережі з підтримкою IP-телефонії»

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	22.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	29.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	12.06.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	26.06.2023

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

Дата видачі 16.05.2023

Дата подання до екзаменаційної комісії 13.07.2023

Прийнято до виконання Ширмаков Л.О.

РЕФЕРАТ

Пояснювальна записка: 85 с., 40 рис., 14 табл., 8 джерел.

Об’єктом розробки є комп'ютерна мережа Державного підприємства «Антонов».

Мета роботи полягає в розробці, налаштуванні та забезпеченні безпеки корпоративної мережі ДП «Антонов» з підтримкою IP-телефонії у зв'язку з перенесенням базового аеропорту ДП «Антонов» з міста Гостомель до аеропорту Leipzig/Halle Airport у місті Лейпциг через воєнну агресію російської федерації проти України, головною метою є створення надійного каналу зв'язку між головним офісом ДП «Антонов» у Києві та аеропортом Leipzig/Halle Airport у Лейпцигу. Одночасно необхідно забезпечити безпеку цього зв'язку шляхом впровадження VPN тунелю, що гарантуватиме захищений обмін даними між об'єктами та забезпечить конфіденційність, цілісність та доступність інформації.

Комп'ютерна мережа підприємства працює на основі кількох технологічних рішень, які забезпечують надійність, швидкість та безпеку передачі даних. Основні технологічні характеристики мережі включають:

– топологія – дерево, яка дозволяє ефективно організувати підключення різних пристроїв до мережі.

– використовуються стандартні протоколи зв'язку, зокрема набір протоколів TCP/IP, які забезпечують гарантовану передачу даних в мережі.

– мережа підтримує швидкість передачі даних на рівні 100 мегабіт в секунду (100 Мбіт/с). Це дозволяє швидко та ефективно обмінюватись інформацією між пристроями в мережі.

– у кабельній інфраструктурі використовуються кабелі категорії 5e (Cat 5e), які забезпечують високу пропускну здатність і стійкість до зовнішніх впливів.

– мережа використовує різноманітні механізми захисту для забезпечення безпеки даних. Вона використовує VLAN для розділення мереж на

логічні сегменти, ACL для керування доступом до ресурсів мережі, VPN для захищеної передачі даних через публічні мережі. Також встановлюються зашифровані паролі для захисту від несанкціонованого доступу. Для централізованого управління доступом використовується сервер AAA (Radius). Віддалене керування мережевими пристроями здійснюється за допомогою захищеного протоколу SSH.

Моделювання мережевої системи підприємства було виконано за допомогою програмного забезпечення Cisco Packet Tracer. Це дозволило створити віртуальну модель мережі та провести тестування різних сценаріїв її роботи.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

ДП – Державне підприємство

КМ – Корпоративна мережа

КС – Комп'ютерна система

IP – (англ. Internet Protocol) Інтернет протокол

IP-АТС – Автоматична телефонна станція

VPN – (англ. Virtual Private Network) Віртуальна приватна мережа

ВСТУП

У сучасному цифровому світі, ефективна комунікація та надійний зв'язок є невід'ємною складовою успіху будь-якої організації. Комп'ютерні мережі стають основним інструментом для забезпечення швидкого та безперебійного обміну інформацією між співробітниками, а також співпрацюючими підприємствами та клієнтами. У цьому контексті кваліфікаційна робота має на меті розробку та впровадження сучасної мережевої інфраструктури для забезпечення найвищого рівня комунікаційних можливостей організації.

У сучасному бізнес-середовищі, ефективна комунікація та обмін інформацією є ключовими факторами для ефективної роботи будь-якої організації. Побудова корпоративної мережі з підтримкою IP-телефонії може значно покращити комунікаційні можливості ДП «Антонов», забезпечуючи швидкий та надійний обмін даними між співробітниками.

Впровадження такої корпоративної мережі дозволить забезпечити безперебійний обмін інформацією між співробітниками ДП «Антонов», незалежно від їхнього місця роботи. Це стане основним інструментом для швидкої та ефективної комунікації, сприяючи координації роботи та прийняттю стратегічних рішень.

Крім того, корпоративна мережа з підтримкою IP-телефонії надасть можливість здійснювати голосові телефонні виклики за допомогою Інтернету, що знизить витрати на телефонію та забезпечить ефективне використання ресурсів організації.

Актуальність даної теми ґрунтується на сучасних викликах, перед якими стоїть ДП «Антонов». Зокрема, в контексті воєнної агресії та неможливості використання базового аеропорту в Україні, існує необхідність перемістити базовий аеропорт Авіаліній Антонова до Німеччини, що, в свою чергу, створює необхідність налагодження каналу зв’язку між віддаленими підрозділами.

Забезпечення належного функціонування ДП «Антонов» та авіакомпанії «Авіалінії Антонова» може сприяти зближенню з європейськими ринками,

розширенню співпраці з міжнародними партнерами та залученню нових можливостей для розвитку. Такий крок дозволяє ДП «Антонов» не лише відповісти на складні життєві виклики, але й проявити свою спроможність ефективного керування у кризових ситуаціях. Вміння адаптуватись до змінного геополітичного контексту та змінювати стратегічну орієнтацію компанії важливе для підвищення репутації не лише самої компанії, але й України в цілому.

Мета роботи полягає у створенні й налагодженні корпоративної мережі з використанням IP-телефонії для налагодження комунікації між географічно віддаленими органами підприємства.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика галузі та умов застосування КС

Авіація сприяє розвитку сучасного світу. Мережа авіакомпаній, аеропортів і організацій управління повітряним рухом цілодобово з'єднує великі міста та невеликі громади з дедалі досконалими літаками. Якби авіація була країною, це була б 17-та найбільша економіка у світі, яка підтримувала б 87,7 мільйонів робочих місць і майже 3,5 трильйона доларів економічного впливу [1]. Авіаційне сполучення дозволяє швидко та гарантовано переміщуватися світом, що дозволяє налагоджувати взаємодію у міжнародному бізнесі та подорожувати у приватних цілях. Не менше 58% усіх міжнародних туристів подорожуючи віддають перевагу літакам [2]. Оскільки глобальна економіка стає все більш взаємопов'язаною, авіація є важливим фактором її розвитку.

Окрім пасажироперевезення, авіація відіграє значну роль у доставці товарів, оскільки перевагою авіаперевезень є коротші терміни транспортування, порівняно з автомобільним та морським транспортом. Недоліком такого методу порівняно з наведеними альтернативами є обмеження за об'ємом та вагою, звідки випливає найвища вартість перевезення. Однак, більш дешевий морський транспорт також має слабкі місця. 23 березня 2021 сталася блокада Суецького каналу контейнеровозом EVER GIVEN що викликало катастрофічні наслідки для світової економіки, з огляду на те, що 30% світових контейнерних перевезень затримались [3], можна уявити колосальний економічний ефект. Збитки, спровоковані цією подією, Allianz оцінив у 10 мільярдів доларів на тиждень.

Літальні апарати відіграють особливу роль в Україні, оскільки вони застосовні як для аграрних потреб [4], (наприклад, запилення сільськогосподарських культур добривами, посів та моніторинг росту врожаю) так і для військових [5]. Наявність власного виробництва літальних апаратів сприяє технологічній перевазі, що впливає на репутацію країни на міжнародній арені та оборонну міць.

Застосування комп'ютерних систем у сфері авіації відіграє важливу роль у поліпшенні ефективності та безпеки авіаційних операцій. Ось деякі умови застосування комп'ютерних мереж у цій галузі:

– Авіаційні системи управління трафіком: Комп'ютерні мережі використовуються для забезпечення ефективного управління повітряним рухом. Це включає системи наземного контролю повітряного руху, автоматичну систему керування повітряним рухом, системи зв'язку між повітряними суднами та наземними контролерами.

– Авіаційні системи безпеки: Комп'ютерні мережі використовуються для моніторингу та забезпечення безпеки авіаційних операцій. Наприклад, системи виявлення перешкод, системи контролю польоту, системи розпізнавання ідентифікації повітряних суден та інші системи безпеки.

– Авіаційні системи диспетчерського керування: Комп'ютерні мережі використовуються для диспетчерського керування авіаційними процесами. Це включає системи планування маршрутів, диспетчерські системи зв'язку, системи моніторингу польотів та інші системи для забезпечення ефективного керування авіаційними операціями.

– Авіаційна безпека та кібербезпека: Комп'ютерні мережі використовуються для забезпечення безпеки авіаційних систем і захисту від кібератак. Це включає застосування систем виявлення та запобігання вторгнень, шифрування даних, захисту мережевих пристроїв та інші заходи для забезпечення безпеки авіаційних мереж та інфраструктури.

– Управління обслуговуванням літаків: Комп'ютерні мережі використовуються для управління та моніторингу обслуговування літаків. Це включає системи планування технічного обслуговування, системи діагностики та виявлення несправностей, системи управління запасними частинами та інші системи, що допомагають забезпечити безперебійну експлуатацію літаків.

Ці умови відображають загальні застосування комп'ютерних мереж у сфері авіації. В реальності, використання комп'ютерних мереж може бути більш

розгалуженим та включати багато інших аспектів, залежно від конкретних потреб та вимог авіаційного підприємства.

1.2 Характеристика і структура об’єкта впровадження

Державне підприємство «Антонов» є об'єктом для впровадження комп'ютерної мережі. Це підприємство володіє всіма необхідними ресурсами для здійснення повного циклу створення сучасних літаків, включаючи проєктування, будівництво, випробування, експлуатацію та обслуговування. Конструкторське бюро «Антонов» відоме своїми значними досягненнями у галузі авіації, включаючи створення видатних серійних та вантажних літаків.

Згідно з законодавством України, а саме Законом «Про розвиток літакобудівної промисловості» авіаційна промисловість є пріоритетною галуззю економіки України [6].

Мета ДП «Антонов» – задовільнити потреби у сфері пасажиро- та вантажоперевезеннях, створення надійних, сучасних конкурентноздатних літальних апаратів, компетентний супровід та надання якісних послуг з технічного обслуговування та ремонту літаків на сучасному рівні [7].

Враховуючи складність технологічного процесу, фінансові затрати та трудомісткість виготовлення авіаційної техніки, підприємства цієї галузі вимагають значної державної підтримки.

Організаційна структура ДП «Антонов» подана на рисунку 1.1.

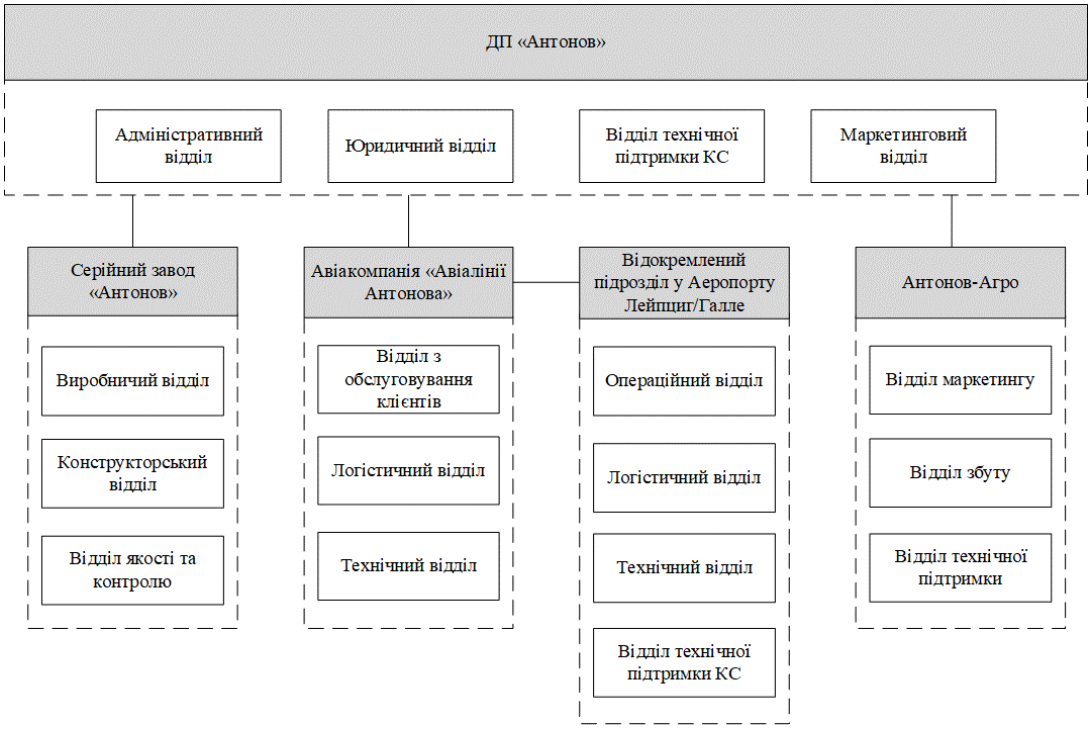


Рисунок 1.1 – Організаційна структура підприємства

Комп'ютерна система, що розглядається, має прямий зв'язок з діяльністю головного офісу ДП «Антонов», авіакомпанії «Авіалінії Антонова» та відокремленого підрозділу у Лейпцигу [8]. Відомості про діяльність Серійного заводу «Антонов» та «Антонов Агро» не ввійшли до даної теми, оскільки вони не є прямо пов'язаними з об'єктом дослідження.

Опис організаційної структури ДП «Антонов»

Адміністративний відділ в головному офісі ДП Антонов відповідає за ефективну організацію та керування різними аспектами адміністративної діяльності. Його головна мета – забезпечити функціонування офісу та підтримку всіх адміністративних процесів. Відділ займається плануванням та координацією роботи офісу, управлінням постачаннями, організацією авіаперевезень, контроль за фінансами та бухгалтерський облік та іншими адміністративними обов'язками.

Юридичний відділ головного офісу ДП «Антонов» відповідає за всі юридичні аспекти діяльності підприємства. Він забезпечує правову підтримку та консультування усіх відділів компанії з питань законодавства, угод, контрактів

та регуляторної сфери. Юридичний відділ також відповідає за ведення правової документації, урегулювання спорів та взаємодію з правовими органами та зовнішніми сторонами.

Маркетинговий відділ головного офісу ДП «Антонов» відповідає за розробку та впровадження маркетингових стратегій та акцій компанії. Його завдання включає аналіз ринку, визначення цільової аудиторії, планування та виконання маркетингових кампаній, рекламу та просування продуктів або послуг. Маркетинговий відділ також займається вивченням конкурентного середовища, визначенням позиціонування компанії на ринку та забезпеченням ефективного використання маркетингових ресурсів.

Відділ технічної підтримки КС в ДП «Антонов» відповідає за надання високоякісної технічної підтримки, включаючи встановлення, налаштування та ремонт комп'ютерного обладнання, забезпечення безперебійної роботи корпоративної мережі.

План приміщень та розташування пристроїв головного офісу ДП «Антонов» подано у додатках А та Б.

Опис організаційної структури «Авіаліній Антонова»

Відділ з обслуговування клієнтів авіакомпанії «Авіалінії Антонова» відповідає за підтримку та задоволення потреб клієнтів, які користуються вантажоперевезеннями. Головна мета відділу – забезпечити високий рівень обслуговування клієнтів, відповідати на їхні запити та вирішувати проблеми. Відділ займається прийомом та обробкою запитів, наданням інформації про вантажоперевезення та післяпродажною підтримкою.

Логістичний відділ: Логістичний відділ авіакомпанії «Авіалінії Антонова» відповідає за організацію логістичних процесів та оптимізацію вантажних перевезень. Відділ займається плануванням, координацією та моніторингом транспортування вантажів, управлінням складськими операціями, вибором оптимальних маршрутів та співпрацею зі зовнішніми логістичними партнерами.

Основна мета відділу – забезпечити ефективну та надійну доставку вантажів відправникам та одержувачам.

Технічний відділ відповідає за консультування щодо технічних питань при вирішенні проблем та надає підтримку віддаленим ремонтним бригадам. Відділ приймає участь у плануванні та керуванні проектами, пов'язаними з технічними аспектами авіакомпанії. Це може включати створення графіків ремонтних робіт, контроль виконання завдань, оновлення проектної документації тощо. Відділ займається проведенням аналізу технічних даних, спостереження за параметрами обладнання, перевірки відповідності документації та інші аналітичні завдання. Також відділ відповідає за оновлення та управління програмним забезпеченням, що використовується для керування технічними процесами, аналізу даних, комунікації, роботи вузлів та агрегатів літальних апаратів, тощо.

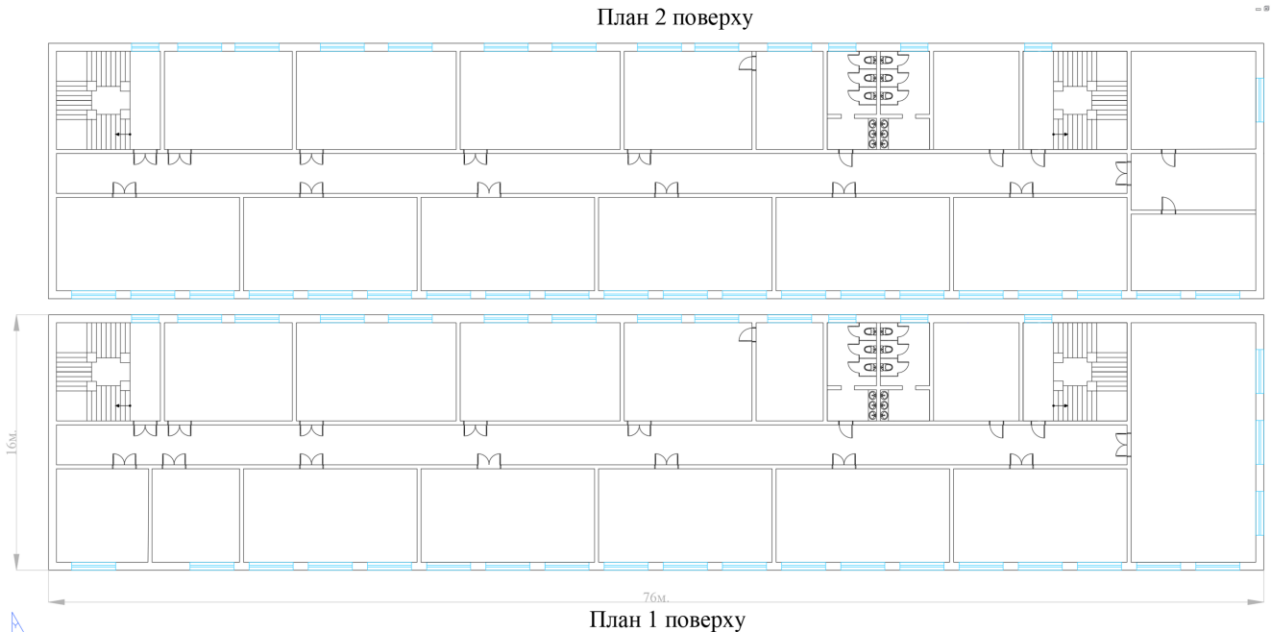


Рисунок 1.2 – План приміщень головного офісу ДП «Антонов»

Опис організаційної структури відокремленого підрозділу авіакомпанії «Авіалінії Антонова» у аеропорту Лейпциг/Галле.

Логістичний відділ відповідає за координацію та планування вантажних операцій, взаємодію з клієнтами та перевізниками, організацію та контроль над вантажними потоками та ресурсами для забезпечення ефективного перевезення вантажів.

Операційний відділ відповідає за координацію та управління операційними процесами, пов'язаними з взаємодією з аеропортовими службами, вирішення питань, пов'язаних з посадкою, вильотом, технічним обслуговуванням літаків, контролем вантажу та багажу, а також забезпеченням дотримання вимог безпеки та виконання регуляторних норм. Операційний відділ забезпечує безперебійну та ефективну роботу аеропорту, співпрацюючи з різними відділами та службами, які діють у складі аеропорту.

Технічний відділ забезпечує виконання планового обслуговування, діагностики та ремонту літаків, їхніх систем та компонентів згідно з встановленими технічними стандартами, виконання графіка технічних робіт, встановлення пріоритетів, забезпечення вчасного та ефективного виконання робіт. Співпрацюючи з іншими відділами забезпечується безперебійна експлуатація літаків. Технічний відділ відповідальний за проведення систематичних спостережень, вимірювань та аналізу параметрів обладнання, систем та компонентів літаків чим забезпечується вчасне виявлення потенційних проблем, несправностей та прийняття заходів для їх вирішення. Технічний відділ виконує перевірки та контроль за якістю проведених технічних робіт.

Зона відповідальності відділу технічної підтримки КС у віддаленому підрозділі належить до надання технічної підтримки та розв'язання проблем комп'ютерних систем в межах сегменту корпоративної мережі, що знаходиться в офісі у Лейпцизі.

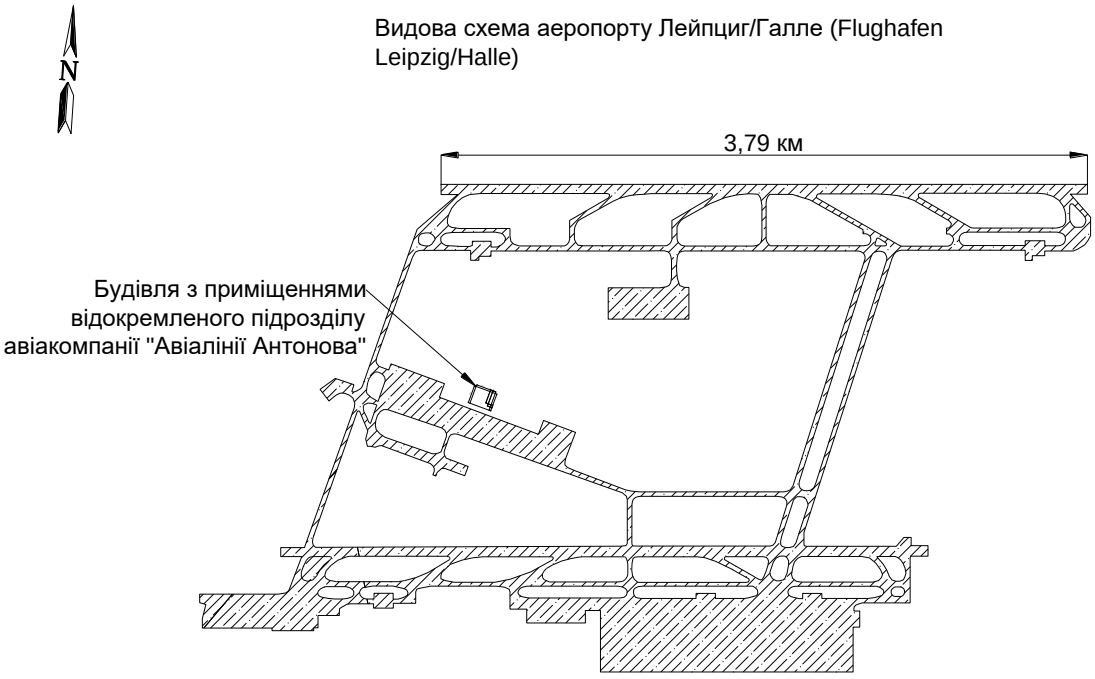


Рисунок 1.3 – Видова схема аеропорту Лейпциг

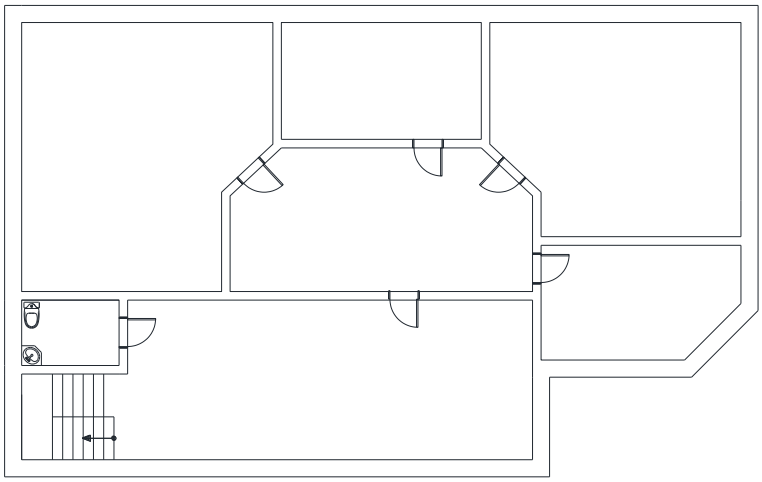


Рисунок 1.4 – План приміщень відокремленого підрозділу ДП «Антонов» у Лейпцигу

1.3 Завдання і мета роботи

Мета роботи створити і налаштувати комп'ютерну систему в ДП «Антонов» з реалізацією побудови, налаштування та безпеки корпоративної мережі з підтримкою IP-телефонії з метою забезпечення безпеки та надійного

зв'язку між ДП «Антонов» у Києві та аеропортом Leipzig/Halle Airport у Лейпцигу. Основні цілі включають:

Впровадити безпечний канал зв'язку між об'єктами для забезпечення надійного обміну даними і комунікації.

Забезпечити конфіденційність та цілісність передачі даних шляхом використання VPN-тунелю.

Захистити мережу від можливих кібератак і несанкціонованого доступу до даних.

Забезпечити ефективний і безперебійний зв'язок між ДП «Антонов» у Києві та аеропортом Leipzig/Halle Airport у Лейпцигу для оптимальної роботи організації під час перенесення базового аеропорту.

Завдання роботи провести детальний аналіз потреб і вимог ДП «Антонов» щодо корпоративної мережі, розглянути можливість створення прямого каналу зв'язку для забезпечення ефективної та безпечної взаємодії між географічно віддаленими відділеннями.

Розробити архітектуру корпоративної мережі, враховуючи специфіку ДП «Антонов» та особливості створення каналів зв'язку між Києвом та Лейпцигом. Визначити оптимальний тип з'єднання для забезпечення безпечного та стабільного зв'язку.

Обрати мережеве обладнання (маршрутизатори, комутатори, мережеві екрани тощо) для побудови корпоративної мережі з врахуванням специфічних потреб ДП «Антонов». Провести встановлення та налаштування мережевого обладнання.

Розгорнути сервіс IP-телефонії, використовуючи відповідні системи та протоколи, які забезпечують якість звуку та надійність зв'язку між розташованими в різних локаціях підрозділами.

1.4 Основні особливості та проблематика впровадження

Створення корпоративної мережі для ДП «Антонов» та тимчасового базового аеропорту залежить від кількох основних особливостей та стикається з

проблемами, враховуючи їх фізичну віддаленість та забезпечення безпеки зв'язку. Основні аспекти, які слід враховувати, включають наступне:

Фізична віддаленість: Відокремлений підрозділ розташований у віддаленому місці, що може вимагати встановлення довгих зв'язків інфраструктури, наприклад, використання додаткових комунікаційних ліній або використання віртуальних приватних мереж (VPN) для з'єднання місць розташування.

Безпека: У зв'язку з суттєвою відстанню між об’єктами відсутня можливість побудувати окремий канал зв’язку, тому виникає необхідність передачі конфіденційної інформації між ДП «Антонов» та відокремленим підрозділом посередництвом мережі Інтернет, тому важливо забезпечити захист даних та безпеку зв'язку. Це може включати використання шифрування, мережевих екранів та інших заходів безпеки.

Стійкість зв'язку: Забезпечення надійності та стабільності зв'язку між ДП Антонов та відокремленим підрозділом вимагає розгляду питань, пов'язаних з резервуванням ліній зв'язку, резервними джерелами живлення та іншими технічними аспектами, які забезпечують безперебійну роботу мережі.

Проблематика впровадження корпоративної мережі з телефонією між ДП «Антонов» та відокремленим підрозділом включає складнощі, пов'язані з фізичною віддаленістю, вибором технологій та систем, забезпеченням безпеки та стійкості зв'язку. Крім того, важливо враховувати витрати на інфраструктуру, обладнання, підтримку та навчання персоналу. Розробка детального плану впровадження та вирішення цих проблем можуть допомогти забезпечити успішне функціонування корпоративної мережі та зв'язку між ДП Антонов та відокремленим підрозділом.

1.5 Аналіз існуючої топології та пропозиції щодо поліпшення корпоративної мережі

Корпоративна мережа підприємства ДП «Антонов» має наступну архітектуру:

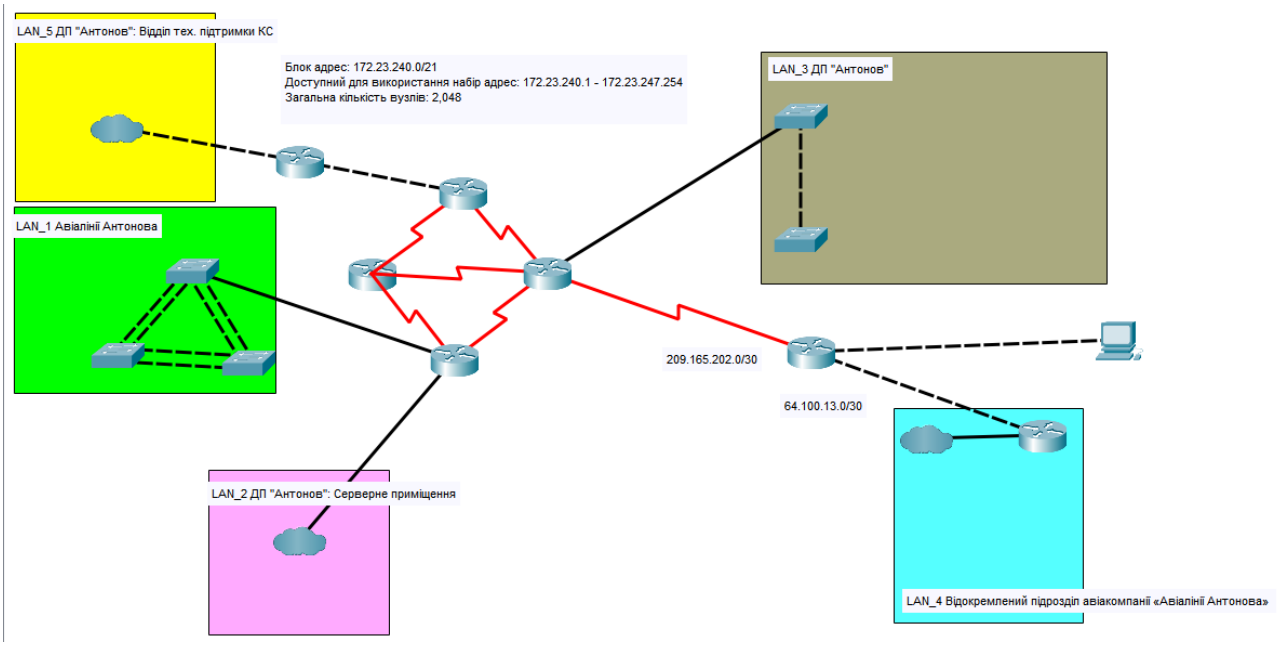


Рисунок 1.5 – Логічна структура корпоративної мережі

Виходячи з даних на поданій схемі, в головному офісі ДП «Антонов» існують чотири підмережі дві з яких використовуються ДП «Антонов» та дві були виділені для авіакомпанії «Авіалінії Антонова». Надлишковість мережевої системи забезпечена наявністю дублюючих компонентів, резервних з'єднань, запасних маршрутизаторів та комутаторів, які призначені для гарантування безперебійної роботи системи навіть у разі виникнення несправностей або втрати певних ресурсів. Найбільш критичною вірогідною точкою відмови, що може призвести до повної втрати зв’язку між головним офісом та відокремленим відділом є використання одного каналу для зв’язку з мережею Інтернет.

В якості потенційного шляху вирішення поставленої задачі запропоновано поділити мережу ДП «Антонов», авіакомпанії «Авіалінії Антонова» та відокремленого підрозділу авіакомпанії «Авіалінії Антонова» на підмережі за допомогою технології віртуальних мереж для кожного з їх структурних відділів, створити IP-АТС для роботи IP-телефонії, створити відокремлений канал зв’язку між головним офісом ДП та відокремленим підрозділом шляхом створення VPN тунелю, передбачити резервне підключення до мережі Інтернет. У процесі

модернізації мережі необхідно звернути особливу увагу на дотримання правил безпеки, зокрема налаштування паролів, шифрування для маршрутизаторів та інших мережевих пристроїв.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Призначення створюваної системи

Комп'ютерна система ДП «Антонов» призначена для надання необхідних інструментів та ресурсів для збору, обробки та аналізу даних, що дозволить керівництву та співробітникам ДП «Антонов» приймати обґрунтовані та ефективні рішення.

Метою створення корпоративної мережі на забезпечити співробітникам доступ до інформації, документів, баз даних та інших ресурсів. Цей доступ дозволяє проводити аналіз даних, проводити дослідження та прогнозування ринкових тенденцій, оцінки поточної ситуації, а також прогнозування майбутніх подій, трендів або результатів. Крім того, IP-телефонія в рамках мережі сприятиме швидкому обміну інформацією між співробітниками у режимі реального часу, що підтримує оперативне прийняття рішень та покращує комунікацію в організації.

2.2 Вимоги до структури і функціональним можливостям системи

Комп'ютерна система ДП «Антонов» має забезпечити підприємству швидку та надійну комунікацію між співробітниками шляхом комп'ютерних мереж. що підвищує продуктивність співробітників та допомагає ефективно виконувати робочі завдання. Система має об'єднати робочі станції співробітників та інші пристрої такі як принтери, файлові сервери, баз даних тощо в єдину мережу. Це дозволяє спільно використовувати ресурси, що спрощує спільну роботу та обмін інформацією. Водночас це дозволятиме підприємству забезпечити захист конфіденційної інформації.

Комп'ютерна мережа має об'єднати наступні відділи:

1. ДП «Антонов» охоплює відділи: Адміністративний відділ, Юридичний відділ, Маркетинговий відділ, Відділ технічної підтримки КС, Серверне приміщення;

2. Авіалінії Антонова охоплює відділи: Логістичний відділ, Технічний відділ, Відділ обслуговування клієнтів;

3. Відокремлений підрозділ авіакомпанії «Авіалінії Антонова» охоплює відділи: Логістичний відділ, Технічний відділ, Операційний відділ, Відділ технічної підтримки КС;

Розміщення відділів на кожному поверсі зображено у плані розташування відділів підприємства, що наведений на рисунку 2.1.

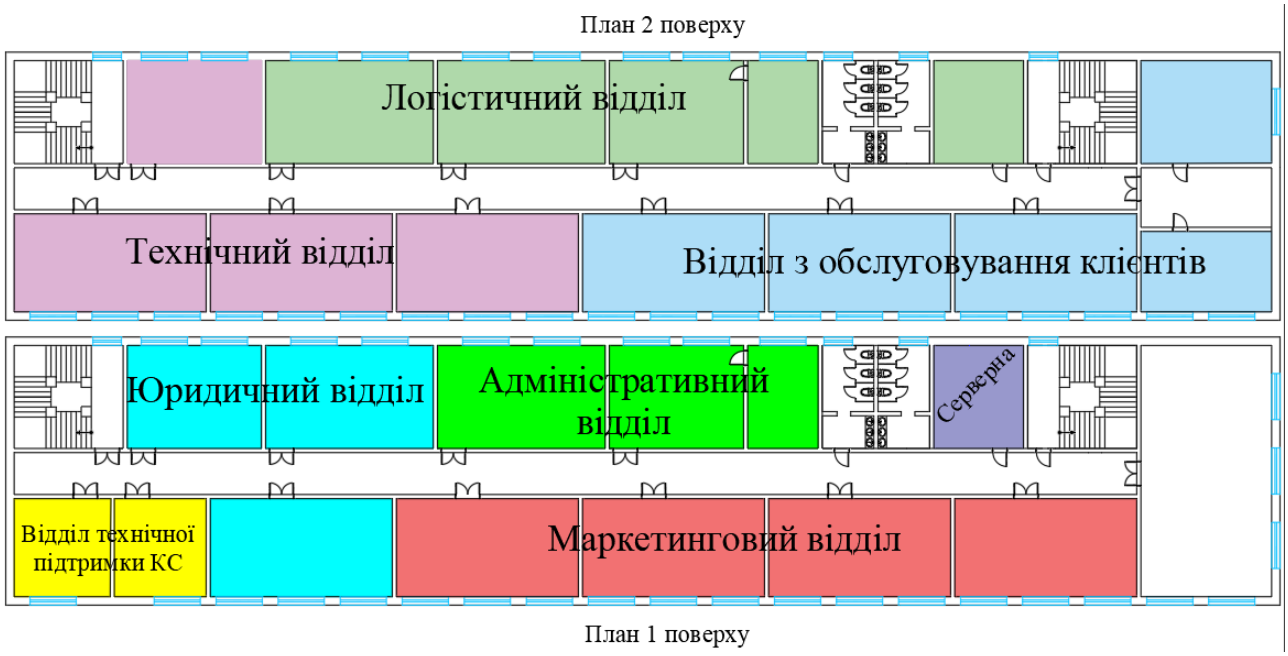


Рисунок 2.1 – План розташування відділів підприємства у головному офісі

Система IP-телефонії:

– встановлення та налаштування IP-телефонного сервера з підтримкою стандартів VoIP.

– забезпечення роботи різноманітних типів телефонів, таких як стаціонарні телефони, мобільні телефони, комп'ютери, а також спеціалізовані IP-телефони.

Система безпеки:

– обмеження доступу до ресурсів

– резервне копіювання конфігураційних файлів мережевого обладнання та серверів IP-телефонії.

– використання сильних паролів та механізмів аутентифікації для доступу до системи.

Управління мережею: Реалізація системи управління мережею, яка дозволяє моніторинг, діагностику, конфігурацію та керування пристроями у мережі, включаючи IP-телефони, комутатори, маршрутизатори тощо.

Резервне копіювання та відновлення даних: Забезпечення системи резервного копіювання та відновлення даних, щоб забезпечити безперебійну роботу мережі та збереження важливої інформації.

Масштабованість: Забезпечення можливості розширення мережі з урахуванням зростання бізнесу та потреб користувачів.

2.2.1 Вимоги до чисельності та кваліфікації персоналу, який обслуговує систему і режим його роботи

Таблиця 2.1 – Вимоги до чисельності та кваліфікації обслуговуючого персоналу корпоративної мережі

№ п/п	Посада	Кількість	Кваліфікаційний рівень	Режим роботи
Головний офіс				
1	Мережний адміністратор	2	Бакалавр або магістр в галузі комп'ютерних наук, інформаційних технологій або суміжних спеціальностей.	1 зміна
2	Спеціаліст з IP-телефонії	1	Бакалавр або магістр в галузі телекомунікацій, комп'ютерних наук, електроніки або суміжних спеціальностей.	1 зміна
3	Системний адміністратор	2	Бакалавр або магістр в галузі комп'ютерних наук, інформаційних технологій або суміжних спеціальностей.	1 зміна

Кінець таблиці 2.1.

№ п/п	Посада	Кількість	Кваліфікаційний рівень	Режим роботи
4	Спеціаліст кібербезпеки	1	Бакалавр або магістр в галузі комп'ютерних наук, інформаційної безпеки або суміжних спеціальностей.	1 зміна
5	Спеціаліст з технічної підтримки	5	Ступінь молодшого спеціаліста у галузі комп'ютерних наук, інформаційних технологій або суміжних спеціальностей.	1 зміна
Відокремлений підрозділ				
6	Мережний адміністратор	1	Бакалавр або магістр в галузі комп'ютерних наук, інформаційних технологій або суміжних спеціальностей.	1 зміна
7	Системний адміністратор	1	Бакалавр або магістр в галузі комп'ютерних наук, інформаційних технологій або суміжних спеціальностей.	1 зміна
8	Спеціаліст з технічної підтримки	2	Ступінь молодшого спеціаліста у галузі комп'ютерних наук, інформаційних технологій або суміжних спеціальностей.	1 зміна

Мережний адміністратор повинен мати досвід роботи з побудовою, налаштуванням та підтримкою корпоративних мереж, знання мережевих протоколів (TCP/IP, DNS, DHCP і т. д.), вміння конфігурувати та управляти мережевим обладнанням (комутатори, маршрутизатори, мережеві екрани), здатність виявляти та вирішувати проблеми мережі.

Спеціаліст з IP-телефонією повинен мати досвід роботи побудови, налаштування та підтримки IP-телефонних систем, знання протоколів VoIP (SIP, H.323), здатність конфігурувати IP-телефони, налаштовувати систему маршрутизації дзвінків, вміти вирішувати проблеми зі зв'язком та якістю звуку.

Системний адміністратор повинен мати досвід роботи з побудовою, налаштуванням та підтримкою серверів і операційних систем, знання апаратної та програмної частини серверів, вміння встановлювати та налаштовувати

серверне програмне забезпечення (операційні системи, бази даних, електронна пошта тощо), здатність виявляти та вирішувати проблеми з серверами та програмним забезпеченням.

Спеціаліст кібербезпеки повинен мати досвід роботи з налаштуванням та моніторингом системи безпеки мережі, знання методів захисту мережевих ресурсів (мережеві екрани, VPN, шифрування), здатність виявляти та врегулювати потенційні загрози безпеці мережі.

Спеціаліст з технічної підтримки повинен мати досвід роботи з підтримкою користувачів, вміння проводити діагностику та усувати неполадки з комп'ютерами, операційними системами, програмним забезпеченням та мережами. Крім того, він повинен мати глибокі знання мережевих протоколів, системного адміністрування, управління користувачами та забезпечення безпеки інформації. Здатність до ефективного комунікації з користувачами та навички ведення документації також є важливими для спеціаліста з технічної підтримки.

2.2.2 Вимоги до показників призначення

Забезпечення швидкості передачі даних до 100 Мбіт на всіх мережевих компонентах.

Пропускна здатність мережі: Система повинна мати достатню пропускну здатність для обробки одночасних голосових і даних потоків у мережі. Максимальну кількість одночасних дзвінків – 80. Пропускна здатність залежить від використовуваного кодеку:

Таблиця 2.2 – Розрахунок пропускної здатності для одного користувача

Канал	**Вхідна пропускна здатність**	**Вихідна пропускна здатність**	**Вхідна пропускна здатність**	**Вихідна пропускна здатність**
IP	7.81 Кбіт/с	7.81 Кбіт/с	7.81 Кбіт/с	7.81 Кбіт/с
UDP	3.13 Кбіт/с	3.13 Кбіт/с	3.13 Кбіт/с	3.13 Кбіт/с
RTP	4.69 Кбіт/с	4.69 Кбіт/с	4.69 Кбіт/с	4.69 Кбіт/с
Аудіо кодек:	g.711		g.726	

Кінець таблиці 2.2.

Канал	**Вхідна пропускна здатність**	**Вихідна пропускна здатність**	**Вхідна пропускна здатність**	**Вихідна пропускна здатність**
	64.00 Кбіт/с		32.00 Кбіт/с	
Вх/Вих	79.63 Кбіт/с	79.63 Кбіт/с	47.63 Кбіт/с	47.63 Кбіт/с
Загалом	159.26 Кбіт/с		95.26 Кбіт/с	

Для 80 одночасних дзвінків має забезпечуватись пропускна здатність у 12,740 кілобіт у секунду.

2.2.3 Вимоги до надійності системи

– Система повинна функціонувати надійно та стабільною, забезпечуючи мінімальний рівень відмови, також у випадках збою у одному з сегментів мережі, робота системи не повинна припинятися на інших сегментах.

– Забезпечити безперебійну роботу мережі шляхом використання резервних шляхів застосовуючи механізми динамічної маршрутизації OSPF та надлишковості використовуючи технологію агрегації каналів LACP.

– Забезпечення відновлення системи протягом встановленого проміжку часу після збою. Час відновлення системи повинен бути в межах від 10 до 60 секунд.

– У разі аварії або глобальної відмови система повинна мати час відновлення, що залежить від складності проблеми, від 10 хвилин, але не довше ніж 30 хвилин.

2.2.4 Вимоги до захисту інформації від несанкціонованого доступу

– Застосування механізмів автентифікації та авторизації для контролю доступу до системи та її ресурсів за допомогою протоколу RADIUS.

– Використання сучасних алгоритмів шифрування, таких як Advanced Encryption Standard (AES), для захисту конфіденційної інформації під час передачі каналами зв’язку.

– Застосування заходів для захисту обладнання від стихійних лих, таких як пожежа, повінь або землетрус, включаючи встановлення пожежних систем, водонепроникних оболонок та стійких конструкцій.

– Визначення обмежень доступу для користувачів системи/ресурсів відповідно до їхніх обов'язків та потреб за допомогою ACL списків.

– Забезпечення регулярного оновлення паролів та використання сильних парольних політик.

– Проведення навчання користувачів щодо захисту інформації та відповідального використання системи.

2.2.5 Вимоги до ергономіки робочих місць

Столи та крісла операторів ПК повинні бути розташовані таким чином, щоб користувач міг зайняти природну та комфортну позицію під час роботи. Це означає правильне підтримання спини, рук і ніг, а також належне розташування клавіатури, миші та монітора. Робочі місця повинні мати можливість регулювання для відповідності різним фізичним параметрам та потребам користувачів. Це включає регулювання висоти столу та крісла, нахилу спинки, нахилу та висоти монітора тощо. Згідно до пункту 2.3 Державних санітарних правил і норм роботи 3.3.2.007-98, на одне робоче місце оператора ПК площа має становити не менше ніж 6,0 м^2.

2.2.6 Вимоги до застосунку керування сервером IP-телефонії

– Інтерфейс програмного забезпечення керування сервером IP-телефонії повинен бути зрозумілим та логічним для користувачів, дозволяти інтуїтивно взаємодіяти без необхідності глибокого знання системи. Система повинна бути легкою у навчанні нових користувачів. Забезпечення сумісності та підтримки різних типів пристроїв: комп'ютери, планшети, смартфони на різних операційних системах, таких як Windows, macOS, Linux тощо.

– Застосунок повинен надавати можливість додавати нові номери для користувачів телефонної системи та видаляти номери користувачів, які більше не потрібні або були заблоковані.

– Застосунок має забезпечувати підтримку різних мов, зокрема української, англійської, французької та німецької. Це означає, що інтерфейс користувача має бути локалізований і застосунок має автоматично визначати мову користувача залежно від налаштувань системи.

– Застосунок має надавати можливість переглядати поточний стан сервера IP-телефонії.

– Застосунок повинен надавати інтерфейс для перегляду інформації про клієнтів телефонії. Це включає статус доступності клієнтів, інформацію про їхнє з'єднання.

– Застосунок повинен забезпечувати можливість керування обліковими записами адміністраторів, додавання та видалення таких облікових записів.

2.2.7 Вимоги до збереження інформації при аваріях

– Забезпечення регулярного резервного копіювання даних на серверах та важливих мережевих компонентах не рідше одного разу на 3 години для поточних документів, раз на тиждень для конфігурацій серверів.

– Застосування системи збереження даних, мережевого сховища даних для централізованого збереження та відновлення інформації.

2.2.8 Вимоги до патентної чистоти

– Перевірка та дотримання вимог щодо патентної чистоти при використанні програмного забезпечення, апаратного забезпечення та технологій.

– Використання ліцензійного програмного забезпечення та обладнання, які не порушують інтелектуальну власність та патентні права.

2.2.9 Вимоги до функцій системи, часові регламенти

– Передбачити застосування резервних джерел живлення (UPS) для запобігання втрати даних у випадку відключення електроенергії.

– Сегментування мережі на віртуальні LAN-підмережі (VLAN) для гарантування безпеки та зменшення широкомовного трафіку.

– Створення зашифрованого каналу зв’язку з корпоративною мережею для працівників віддалених відділень, за допомогою віртуальних приватних мереж (VPN).

– Використання активного мережевого обладнання, такого як маршрутизатори та комутатори, з підтримкою відповідних мережевих протоколів таких як, TCP/IP, VLAN, OSPF, IPSec, VoIP.

– QoS (Quality of Service): Налаштування механізмів QoS для забезпечення надійної передачі голосу в мережі, приділяючи пріоритетний обсяг пропускної здатності для IP-телефонії та запобігаючи затримки і втрати пакетів.

– Забезпечити налагодження відокремленого каналу зв’язку між головним офісом та відокремленим підрозділом використовуючи VPN тунель, що передбачає використання існуючої інфраструктури провайдера зв'язку замість необхідності прокладати фізичний кабель.

– Маршрутизація та комутація дзвінків: Система повинна забезпечувати ефективну маршрутизацію та комутацію голосових дзвінків в мережі з мінімальною затримкою і високою якістю зв'язку. Система повинна реагувати на дзвінки або запити користувачів протягом декількох секунд, не більше ніж 3-5 секунд.

– Керування користувачами та розподіл ресурсів: Система повинна мати можливість управляти користувачами, надавати їм доступ до необхідних послуг та розподіляти ресурси мережі для забезпечення оптимального функціонування IP-телефонії.

– Години роботи: Система повинна бути доступною для користувачів протягом робочого часу компанії ДП «Антонов». З понеділка по п'ятницю з 9:00 до 18:00.

– Для регламентних робіт, таких як технічне обслуговування, оновлення програмного забезпечення та системних компонентів, часовий проміжок не рідше ніж раз на квартал. Конкретний час для проведення таких робіт може бути визначений відповідно до вимог і графіку роботи компанії ДП «Антонов». Забезпечення проведення регламентних робіт кожного останнього вівторка кварталу з 18:00 до 22:00. Важливо попередньо повідомляти користувачів про заплановані регламентні роботи та можливі тимчасові обмеження в доступності послуг під час цих робіт. Таким чином, можна забезпечити ефективну підтримку системи, понижуючи ризик перешкоджання її нормальному функціонуванню.

2.3 Додаткові вимоги

При створенні кабельної системи використовувати кабель типу «кручена пара» категорії 5е, які забезпечують максимальну швидкість передачі даних до 1000 Мбіт/с, що відповідає вимозі показників призначення, а саме пропускній здатності каналів до 100 Мбіт/с.

При розрахунку фізичних параметрів використовуваних кабель-каналів керуватися стандартом TIA/EIA-569-B, згідно якому заповнення кабель-каналів не має перевищувати 40 відсотків.

2.4 Розробка апаратної частини комп’ютерної системи

Маршрутизатор Cisco ISR4331/K9 відповідає вимогам, описаних у попередніх пунктах. Він має ряд функцій і можливостей, які дозволяють задовольнити потреби, пов'язані з маршрутизацією та мережевим управлінням.

Основні характеристики маршрутизатора Cisco ISR4331/K9 включають:

– Підтримку протоколу OSPF (Open Shortest Path First), що дозволяє маршрутизатору ефективно обчислювати шляхи найкоротшого шляху у мережі.

– Наявність функції Dynamic NAT (Network Address Translation), яка забезпечує автоматичне перетворення IP-адрес між приватними та глобальними IP-адресами.

– Підтримку VPN IPSec (IP Security), що дозволяє безпечно передавати дані по відкритим мережам шляхом шифрування та аутентифікації.

– Можливість створення та конфігурування VLAN (Virtual Local Area Network), що дозволяє фізичну мережу розділити на логічні сегменти з метою керування трафіком та забезпечення безпеки.

– Наявність ACL (Access Control Lists), що дозволяє налаштовувати правила фільтрації трафіку для контролю доступу до ресурсів мережі.

– Маршрутизатор Cisco ISR4331/K9 також підтримує аутентифікацію, авторизацію та облік (AAA) зокрема за допомогою протоколу RADIUS (Remote Authentication Dial-In User Service). Протокол RADIUS є стандартом для централізованої аутентифікації, авторизації та обліку у мережевих середовищах.

Маршрутизатор Cisco ISR 2811 відповідає вимогам завдяки наступним характеристикам:

– Cisco ISR 2811 підтримує OSPF (Open Shortest Path First), що є одним з протоколів маршрутизації, використовуваних для обміну маршрутною інформацією у мережах. Завдяки підтримці OSPF, маршрутизатор може ефективно обмінюватись маршрутною інформацією з іншими маршрутизаторами та обчислювати найкоротші шляхи до призначення.

– Дозволяє налаштовувати VLAN (Virtual Local Area Network), що дозволяє логічно розділити мережу на окремі сегменти з різними налаштуваннями та безпекою. Це дає можливість створювати віртуальні мережі в рамках одного фізичного мережевого пристрою.

– Підтримує ACL (Access Control Lists), що дозволяє налаштовувати правила фільтрації трафіку на основі різних параметрів, таких як IP-адреса, порти, протоколи тощо. ACL дозволяє контролювати доступ до ресурсів мережі та забезпечувати безпеку та обмеження доступу для користувачів.

– Має підтримку AAA (Authentication, Authorization, and Accounting) та RADIUS (Remote Authentication Dial-In User Service) для централізованого управління автентифікацією, авторизацією та обліком користувачів.

Комутатор Cisco Catalyst 2960-24TC-L є задовільним варіантом для використання у даній мережі, оскільки він відповідає усім зазначеним вимогам. Особливості цього комутатора включають:

– Cisco Catalyst 2960-24TC-L є керованим комутатором, що дозволяє налаштовувати його під конкретні потреби.

– Cisco Catalyst 2960-24TC-L дозволяє створювати та керувати віртуальними локальними мережами (VLAN), що дозволяє розділити мережу на логічні сегменти для гнучкого управління трафіком, зменшення широкомовного простору та гарантування безпеки мережі.

– Комутатор підтримує технологію агрегації каналів (Link Aggregation), яка дозволяє об'єднати кілька фізичних портів в один логічний канал, забезпечуючи збільшену пропускну здатність та відмовостійкість.

– Віддалене керування: Комутатор підтримує можливість віддаленого керування, що дозволяє адміністраторам налаштовувати та керувати комутатором з віддаленого місця за допомогою протоколів керування мережею, таких як SSH.

Загалом, Cisco Catalyst 2960-24TC-L є надійним та функціональним комутатором, який задовольняє вказані вимоги і може бути ефективним в розробці комп'ютерної системи.

Таблиця 2.3 – Специфікація обладнання

№	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
Мережеве обладнання					
1	Маршрутизатор	Cisco ISR4331/K9	од.	2	SFP Ge, RJ-45 Ge
2	Маршрутизатор	Cisco CISCO2811	од.	4	RJ-45 Ge
3	SFP модуль	SFP OnisNetworks GLC-BX-20D-сумісний	од.	2	Модуль підключення оптоволоконного кабелю
4	SFP модуль	Alistar SFP 1000BASE-T SFP-1G-T	од.	6	Модуль підключення кабелю типу кручена пара
5	Модуль розширення	HWIC-1GE-SFP	од.	6	Блок розширення SFP
6	Комутатор	Cisco Catalyst 2960-24TC-L	од.	8	24x Fa/2x Ge інтерфейси
Робочі станції					
7	Настільний комп'ютер	RIM 2000	од.	121	Intel Core i3-10105, 8GB, SSD 512GB
Сервери					
8	Сервер	RIM 2000 Patriot Server (R1250.10)	од.	2	Xeon E-2234 4 ядра 3,6 ГГц, 2x1TB RAID 1/32GB DDR4-2666
Телефонія					
9	IP-телефон	Cisco IP Phone 7821 Series	од.	121	–
Периферійні пристрої					
10	Миша	Logitech B100	од.	121	–

Кінець таблиці 2.3

11	Клавіатура	Dell 580-AHHE	од.	121	–
12	Принтер	HP LaserJet Tank 2602sdn	од.	36	–
13	Монітор	Acer V247YBIPV	од.	121	–

2.5 Структурна схема обладнання

Після проведення аналізу технічних вимог була розроблена структурна схема обладнання комп'ютерної системи з урахуванням потреб і особливостей проекту. Схема включає наступні рівні:

Рівень ядра: На цьому рівні розташовані основні компоненти інфраструктури, включаючи центральні сервери, дата-центри та системи зберігання даних. Це серце системи, яке забезпечує надійну та швидку обробку даних, забезпечує високу доступність та масштабованість.

Рівень доступу: На цьому рівні розташовані мережеві пристрої, такі як маршрутизатори та комутатори. Вони забезпечують передачу даних між різними сегментами мережі, керують трафіком і забезпечують безпеку мережі. Також на цьому рівні можуть бути розташовані файерволи, проксі-сервери та інші пристрої для забезпечення безпеки та контролю доступу.

Кінцеві пристрої: Цей рівень включає робочі станції, ноутбуки, планшети, смартфони та інші пристрої, які використовуються користувачами для доступу до мережі та виконання різних завдань. Також до кінцевих пристроїв можуть відноситись IP-телефони, які використовуються для здійснення голосових комунікацій.

Цей програмно-апаратний комплекс базується на розгорнутій мережі і включає різноманітне обладнання. До складу мережевого обладнання входять маршрутизатори, комутатори, серверне обладнання, а також робочі станції та IP-телефони. Кожен компонент має свою функціональність і спрямований на

задоволення вимог проекту, забезпечуючи надійну та ефективну роботу всієї системи.

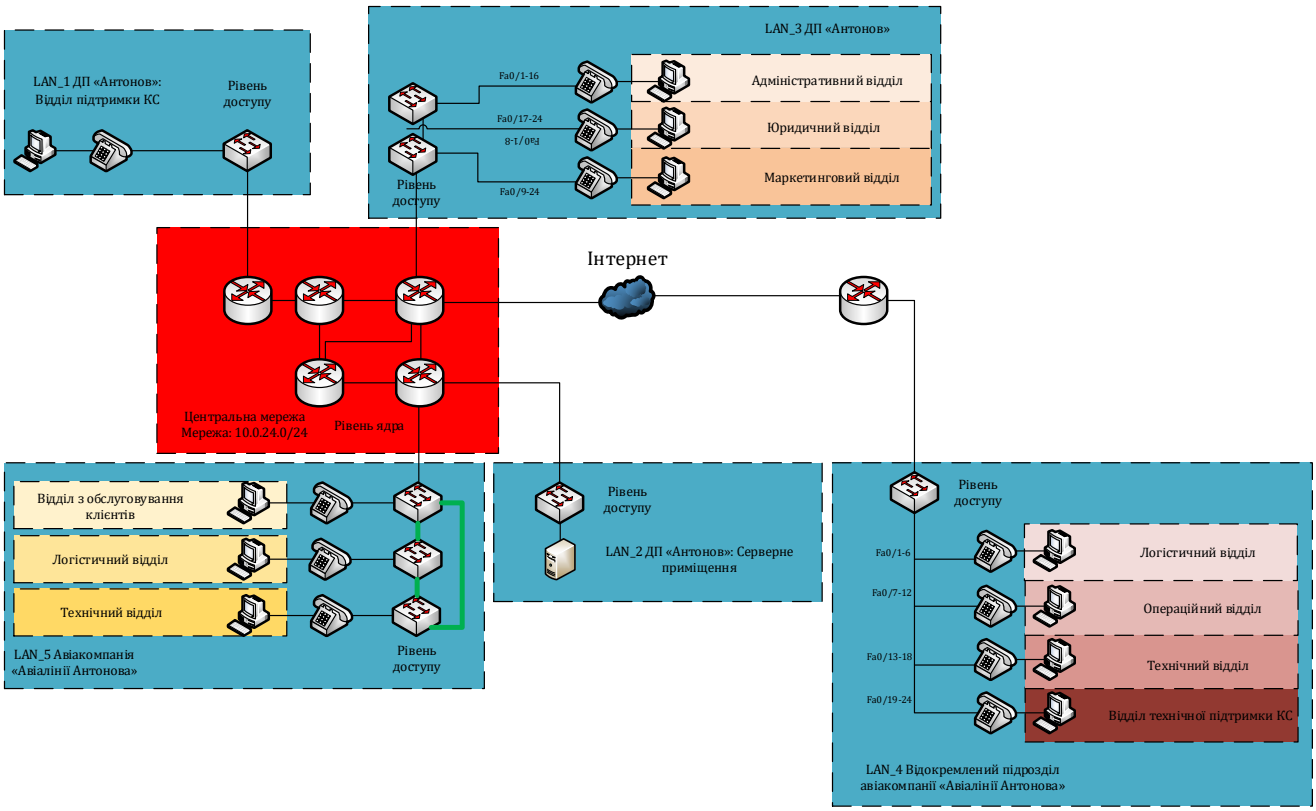


Рисунок 2.2 – Структурна схема обладнання

2.6 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі

Найбільшою мережею підприємства є підмережа ДП «Антонов», тобто LAN_3. Для розрахунку інтенсивності вхідного трафіку дані наступні значення:

N = 74 (одиниць); – кількість вузлів в мережі;

μ = 106 (кадрів/секунду) – середня інтенсивність трафіку;

l = 650 (байт) – середня довжина повідомлення становить;

n = 24 (одиниць) – кількість портів комутатора.

Затримка передачі пакету не повинна перевищувати 6 мс.

При розрахунку пропускної здатності мережі на рівні доступу використано формулу (2.1).

$$P_{\text{р.р}} = \mu * l * n, \quad (2.1)$$

де $P_{\text{р.р}}$ – пропускна здатність мережі, біт/с;

μ – інтенсивність обслуговування, кадрів/с;

l – середня довжина повідомлення, байт;

n – кількість портів комутатора.

Розрахунок пропускної здатності мережі на рівні доступу:

μ = 106 (кадрів/секунду);

При проведенні розрахунку довжину кадра необхідно навести у бітах.

l = 650 байт = 5200 (біт);

n = 24 одиниць;

$P_{\text{р.р}}$ = 106 * 5200 * 24 = 13 228 800 (біт/секунду) ≈ (13.2 Мбіт/секунду)

При розрахунку значення інтенсивності виходу використано формулу (2.2).

$$\mu_{\text{вих}} = C / l, \quad (2.2)$$

де

C – пропускна здатність лінії, біт/с;

l – середня довжина повідомлення байт.

Розрахунок значення інтенсивності виходу:

C = 100 000 000 (біт/секунду);

l = 650 байт = 5200 (біт).

$\mu_{\text{вих}}$ = 100 000 000 / 5200 = 19 230 (пакетів/секунду)

Для розрахунку максимальної кількості вузлів, яку можна приєднати до комутатора рівня розподілу на основі заданої середньої інтенсивності трафіку, використано формулу (2.3).

$$N = \mu_{вих} / \mu, \quad (2.3)$$

де N – кількість вузлів, яку можна приєднати;

$\mu_{вих}$ – інтенсивність виходу, пакетів/с;

μ – середня інтенсивність трафіку, пакетів/с.

Розрахунок максимальної кількості вузлів, яку можна приєднати до комутатора рівня розподілу:

$\mu_{вих}$ = 19 230 (пакетів/секунду);

μ = 106 (кадрів/секунду);

N = 19 230 / 106 ≈ 181 (одиниць)

Максимальна кількість вузлів, яку можна приєднати, складатиме 181.

Для розрахунку загальної інтенсивності трафіку від всіх користувачів використано формулу (2.4).

$$\lambda = x * \mu, \quad (2.4)$$

де λ – загальна інтенсивність трафіку, пакетів/секунду;

x – коефіцієнт, який представляє кількість користувачів або вузлів в мережі, одиниць;

μ - середня інтенсивність трафіку, пакетів/секунду.

Розрахунок загальної інтенсивності трафіку від всіх користувачів:

x = 74 (одиниць);

μ = 106 (кадрів/секунду);

$\lambda = 74*106 = 7\ 844$ (пакетів/секунду).

Для розрахунку коефіцієнту затримки на рівні розподілу, використано формулу (2.5):

$$\rho = \lambda / \mu_{вих}, \quad (2.5)$$

де ρ – коефіцієнт затримки на рівні розподілу;

λ – загальна інтенсивність трафіку від всіх користувачів;

$\mu_{вих}$ – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

Розрахунок коефіцієнту затримки на рівні розподілу:

$\lambda = 7\ 844$ (пакетів/секунду);

$\mu_{вих} = 19\ 230$ (пакетів/секунду);

$\rho = 7\ 844 / 19\ 230 \approx 0{,}4079$.

Для розрахувати коефіцієнт зайнятості комутатора на рівні розподілу, використано формулу (2.6).

$$r = \rho / (1 - \rho), \quad (2.6)$$

де r – коефіцієнт зайнятості комутатора;

ρ – коефіцієнт затримки на рівні розподілу.

Розрахунок коефіцієнту зайнятості комутатора:

$\rho \approx 0{,}4079$;

$r = 0{,}4079 / (1 - 0{,}4079) \approx 0{,}6889$.

Для розрахунку середньої затримки кадру, використано формулу (2.7).

$$T = 1 / (\mu_{вих} - \lambda), \quad (2.7)$$

де T – середня затримка кадру;

λ – загальна інтенсивність трафіку від всіх користувачів;

$\mu_{вих}$ – інтенсивність виходу, яка вказує на кількість пакетів, що виходять з комутатора за одиницю часу.

Розрахунок середньої затримки кадру:

λ = 7 844 (пакетів/секунду);

$\mu_{вих}$ = 19 230 (пакетів/секунду);

$T = 1 / (19\,230 - 7\,844) \approx 8{,}78 * 10^{-5}$ (секунд) = 0,09 (мілісекунд).

Для розрахунку середньої довжини черги використано формулу (2.8).

$$L_{черги} = \rho^2 / (1 - \rho), \quad (2.8)$$

де $L_{черги}$ – середня довжина черги;

ρ – коефіцієнт затримки на рівні розподілу.

Розрахунок середньої довжини черги:

$\rho \approx 0{,}4079$;

$L_{черги} = (0{,}4079)^2 / (1 - 0{,}4079) \approx 0{,}281$ пакетів.

Значення $L_{черги}$ менше за одиницю, що означає високу продуктивність сегменту.

Для розрахунку середнього часу перебування пакета в черзі використано формулу (2.9).

$$T_{очік} = L_{черги} / \lambda, \quad (2.9)$$

де $T_{очік}$ – середній час перебування пакета в черзі;

$L_{черги}$ – середня довжина черги;

λ – загальна інтенсивність трафіку від всіх користувачів.

Розрахунок середнього часу перебування пакета в черзі:

$L_{черги} \approx 0{,}281$ (пакетів);

$\lambda = 7\ 844$ (пакетів/секунду);

$T_{очік} = 0{,}281 / 7\ 844 = 3{,}582*10^{-5}$ (секунди) $\approx 0{,}04$ (мілісекунди)

Отримане значення $T_{очік}$ задовольняє вимоги.

Розрахунок пропускної здатності каналу можна виконати за формулою (2.9).

$$b = \lambda * l, \tag{2.9}$$

де b – пропускна здатність каналу, біт/с;

λ – інтенсивність трафіку, пакетів/с;

l – середня довжина пакету, байт.

Розрахунок пропускної здатності каналу:

$\lambda = 7844$ (пакетів/секунду);

$l = 650$ байт $= 5200$ (біт);

$b = 7844 * 5200 = 40\ 788\ 800$ біт/с $\approx 40{,}7$ Мбіт/с.

Розрахункова пропускна здатність каналу не перевищує заплановану пропускну здатність.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Виходячи зі структурної схеми, топологія мережі є дворівневою і складається з рівнів ядра та рівня доступу.

На рівні ядра задіяні маршрутизатори, які забезпечують маршрутизацію і даних між підмережами та зовнішніми мережами. Рівень ядра відповідає за централізоване керування мережею, виконання функцій маршрутизації та контролю доступу.

З вихідного адресного простору мережі маршрутизації 10.0.24.0/24 було виділено шість сегментів по 6 адрес кожний для призначення каналам між маршрутизаторами.

Таблиця 3.1 – Розподіл вихідного адресного простору

Назва мережі	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
WAN_1	6	10.0.24.0/29	10.0.24.1-10.0.24.6	10.0.24.7
WAN_2	6	10.0.24.8/29	10.0.24.9-10.0.24.14	10.0.24.15
WAN_3	6	10.0.24.16/29	10.0.24.17-10.0.24.22	10.0.24.23
WAN_4	6	10.0.24.24/29	10.0.24.25-10.0.24.30	10.0.24.31
WAN_5	6	10.0.24.32/29	10.0.24.33-10.0.24.38	10.0.24.39
WAN_6	6	10.0.24.40/29	10.0.24.41-10.0.24.46	10.0.24.47

Рівень доступу включає комутатори, які підключаються безпосередньо до клієнтських пристроїв (комп'ютери, принтери, IP-телефони тощо). Цей рівень відповідає за надання прямого доступу користувачам до мережевих ресурсів і забезпечення локальної комутації даних в межах підмережі.

З вихідного адресного простору корпоративної мережі 172.23.240.0/21 було виділено п’ять сегментів на кожен з наведених нижче об’єктів згідно потребам у адресному просторі.

Мережа_1 – ДП «Антонов»: Відділ підтримки КС

Мережа_2 – ДП «Антонов»: Сервери

Мережа_3 – ДП «Антонов»

Мережа_4 – Відокремлений підрозділ авіакомпанії «Авіалінії Антонова»

Мережа_5 – Авіакомпанія «Авіалінії Антонова»

Таблиця 3.2 – Кількість вузлів у мережах

	Мережа_1	Мережа_2	Мережа_3	Мережа_4	Мережа_5
Кількість вузлів	15	15	74	48	58

Враховуючи надану інформацію, було прийнято рішення розділити вихідну мережі на подані вище мережі, та додатково виділити адресні простори на потреби IP-телефонії та віддалене керування мережевими пристроями.

Результат розподілу вихідного адресного простору корпоративної мережі наведено у таблиці 3.3.

Таблиця 3.3 – Розподіл вихідного адресного простору

Назва мережі	Розмір	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
Телефонія	216	254	172.23.240.0/24	172.23.240.1 - 172.23.240.254	172.23.240.255
Мережа_3 ДП «Антонов»	74	126	172.23.241.0/25	172.23.241.1 - 172.23.241.126	172.23.241.127
Мережа_5 «Авіалінії Антонова»	58	62	172.23.241.128/26	172.23.241.129 - 172.23.241.190	172.23.241.191
Мережа_4 Відокремлений підрозділ «Авіалінії Антонова»	48	62	172.23.241.192/26	172.23.241.193 - 172.23.241.254	172.23.241.255
Мережа_1 ДП «Антонов»: Відділ технічної підтримки КС	15	30	172.23.242.0/27	172.23.242.1 - 172.23.242.30	172.23.242.31
Мережа_2 «ДП Антонов» Серверне приміщення	15	30	172.23.242.32/27	172.23.242.33 - 172.23.242.62	172.23.242.63
Керування мережевими пристроями	15	30	172.23.242.64/27	172.23.242.65 - 172.23.242.94	172.23.242.95

Отриманий адресний простір IP-телефонії розподілено між мережами усіма мережами, за винятком мережі з серверами. Результат розподілу адресного простору для IP-телефонії подано у таблиці 3.4.

Таблиця 3.4 – Розподіл адресного простору телефонії

Назва підмережі	Розмір	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
Мережа_3 ДП «Антонов»	56	62	172.23.240.0/26	172.23.240.1 - 172.23.240.62	172.23.240.63
Мережа_5 «Авіалінії Антонова»	37	62	172.23.240.64/26	172.23.240.65 - 172.23.240.126	172.23.240.127
Мережа_4 Відокремлений підрозділ «Авіалінії Антонова»	35	62	172.23.240.128/26	172.23.240.129 - 172.23.240.190	172.23.240.191
Мережа_1 ДП «Антонов»: Відділ технічної підтримки КС	15	30	172.23.240.192/27	172.23.240.193 - 172.23.240.222	172.23.240.223

Для обмеження широкомовного трафіку та ізоляції відділів підприємства одне від одного використано технологію VLAN, яка використовується для розділу мережі на підмережі та шляхом логічного розділення фізичної мережі на окремі віртуальні сегменти.

Кожен віртуальний сегмент VLAN відповідає конкретному відділу або функціональному призначенню, такі як IP-телефонія або керування мережевими пристроями. Розділ мережі на підмережі за допомогою VLAN дозволяє забезпечити ефективну організацію і гнучке керування мережевим трафіком, зменшити широкомовний трафік і гарантувати безпеку даних.

Адресні простори підприємств «Антонов», «Авіаліній Антонова» та її відокремленого підрозділу були розділені для кожного з їх відділів наведених у організаційній структурі підприємства згідно потребам у адресному просторі наведеним у таблиці 3.5. Так само, кожному з відділів призначений ідентифікатор віртуальної локальної мережі.

Таблиця 3.5 – Кількість вузлів у підмережах

Назва підприємства	Назва відділу	VLAN	Кількість вузлів, одиниць
ДП «Антонов»	Маркетинговий відділ	34	26
	Адміністративний відділ	44	18
	Юридичний відділ	54	12
Авіакомпанія «Авіалінії Антонова»	Відділ з обслуговування клієнтів	34	15
	Технічний відділ	44	12
	Логістичний відділ	54	10
Відокремлений підрозділ авіакомпанії «Авіалінії Антонова»	Операційний відділ	34	12
	Логістичний відділ	44	10
	Технічний відділ	54	8
	Відділ технічної підтримки КС	64	5

Результати розподілу адресних просторів підприємств наведено у таблицях 3.6-3.9.

Таблиця 3.6 – Розподіл адресного простору на відділи ДП «Антонов»

Назва підмережі	Розмір	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
Маркетинговий відділ	26	30	172.23.241.0/27	172.23.241.1 - 172.23.241.30	172.23.241.31
Адміністративний відділ	18	30	172.23.241.32/27	172.23.241.33 - 172.23.241.62	172.23.241.63
Юридичний відділ	12	14	172.23.241.64/28	172.23.241.65 - 172.23.241.78	172.23.241.79

Таблиця 3.7 – Розподіл адресного простору на відділи авіакомпанії «Авіалінії Антонова»

Назва підмережі	Розмір	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
Відділ з обслуговування клієнтів	15	30	172.23.241.128/27	172.23.241.129 - 172.23.241.158	172.23.241.159
Технічний відділ	12	14	172.23.241.160/28	172.23.241.161 - 172.23.241.174	172.23.241.175
Логістичний відділ	10	14	172.23.241.176/28	172.23.241.177 - 172.23.241.190	172.23.241.191

Таблиця 3.8 – Розподіл адресного простору на відділи відокремленого підрозділу авіакомпанії «Авіалінії Антонова»

Назва підмережі	Розмір	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
Операційний відділ	12	14	172.23.241.192/28	172.23.241.193 - 172.23.241.206	172.23.241.207
Логістичний відділ	10	14	172.23.241.208/28	172.23.241.209 - 172.23.241.222	172.23.241.223
Технічний відділ	8	14	172.23.241.224/28	172.23.241.225 - 172.23.241.238	172.23.241.239
Відділ технічної підтримки КС	5	6	172.23.241.240/29	172.23.241.241 - 172.23.241.246	172.23.241.247

Таблиця 3.9 – Розподіл адресного простору керування мережевими пристроями

Назва підмережі	Розмір	Виділений розмір	Адреса	Діапазон доступних адрес	Широкомовлення
LAN_5 «Авіалінії Антонова»	4	6	172.23.242.64/29	172.23.242.65 - 172.23.242.70	172.23.242.71
LAN_4 Відокремлений підрозділ «Авіалінії Антонова»	3	6	172.23.242.72/29	172.23.242.73 - 172.23.242.78	172.23.242.79
LAN_3 ДП «Антонов»	3	6	172.23.242.80/29	172.23.242.81 - 172.23.242.86	172.23.242.87
LAN_1 ДП «Антонов»: Відділ технічної підтримки КС	2	2	172.23.242.88/30	172.23.242.89 - 172.23.242.90	172.23.242.91
LAN_2 «ДП Антонов» Серверне приміщення	2	2	172.23.242.92/30	172.23.242.93 - 172.23.242.94	172.23.242.95

Було проведено налаштування мережевих комутаторів та маршрутизаторів, відповідно до наведених вище таблиць з адресними просторами. Результати конфігурації пристроїв наведена у таблиці 3.10.

Таблиця 3.10 – Налаштування адресації мережевих пристроїв

Пристрій	Інтерфейс	Суб-інтерфейс	IP-адреса	Маска	VLAN	Шлюз
Shyrmakov_Router_0	Se0/1/1 DCE	–	10.0.24.1	/29	–	–
	Se0/2/0 DCE	–	10.0.24.9	/29	–	–
	Se0/2/1 DCE	–	10.0.24.17	/29	–	–

Кінець таблиці 3.10

Пристрій	Інтерфейс	Суб-інтерфейс	IP-адреса	Маска	VLAN	Шлюз
	Ge0/0/0	GE0/0/0.24	172.23.240.1	/26	24	–
		GE0/0/0.34	172.23.241.33	/27	34	–
		GE0/0/0.44	172.23.241.65	/28	44	–
		GE0/0/0.54	172.23.241.1	/27	54	–
		GE0/0/0.99	172.23.242.81	/29	99	–
	GE0/0/2	–	209.165.202.2	/27	–	–
Shyrmakov_Router_1	GE0/0/0	–	172.23.242.33	/27	–	–
		GE0/0/0.99	172.23.242.93	/30	99	–
	GE0/0/1	GE0/0/1.24	172.23.240.65	/26	24	–
		GE0/0/1.34	172.23.241.129	/27	34	–
		GE0/0/1.44	172.23.241.177	/28	44	–
		GE0/0/1.54	172.23.241.161	/28	54	–
		GE0/0/1.99	172.23.242.65	/29	99	–
	Se0/1/0 DTE	–	10.0.24.18	/29	–	–
	Se0/1/1 DCE	–	10.0.24.33	/29	–	–
Shyrmakov_Router_2	Se0/1/0 DTE	–	10.0.24.10	/29	–	–
	Se0/1/1 DTE	–	10.0.24.26	/29	–	–
	Se0/2/0 DTE	–	10.0.24.34	/29	–	–
Shyrmakov_Router_3	GE0/0/0	–	10.0.24.41	/29	–	–
	Se0/1/0	–	10.0.24.2	/29	–	–
	Se0/1/1	–	10.0.24.25	/29	–	–
Shyrmakov_Router_4	GE0/0/0	–	10.0.24.42	/29	–	–
	GE0/0/1	–	172.23.242.1	/27	–	–
		GE0/0/1.24	172.23.240.193	/27	24	–
		GE0/0/1.99	172.23.242.89	/30	99	–
Shyrmakov_Switch_0	VLAN 99	–	172.23.242.83	/29	99	172.23.242.81
Shyrmakov_Switch_1	VLAN 99	–	172.23.242.82	/29	99	172.23.242.81
Shyrmakov_Switch_2	VLAN 99	–	172.23.242.66	/29	99	172.23.242.65
Shyrmakov_Switch_3	VLAN 99	–	172.23.242.67	/29	99	172.23.242.65
Shyrmakov_Switch_4	VLAN 99	–	172.23.242.68	/29	99	172.23.242.65
Shyrmakov_Switch_5	VLAN 99	–	172.23.242.94	/30	99	172.23.242.93
Shyrmakov_Switch_6	VLAN 99	–	172.23.242.90	/30	99	172.23.242.89
Shyrmakov_Switch_7	VLAN 99	–	172.23.242.74	/29	99	172.23.242.73

Після розробки таблиць адресації створено мережеву діаграму для візуалізації структури мережі та зв'язків між пристроями. Мережева діаграма є графічним зображенням, що включає компоненти, такі як комп'ютери, сервери, маршрутизатори, комутатори, а також мережеві сегменти.

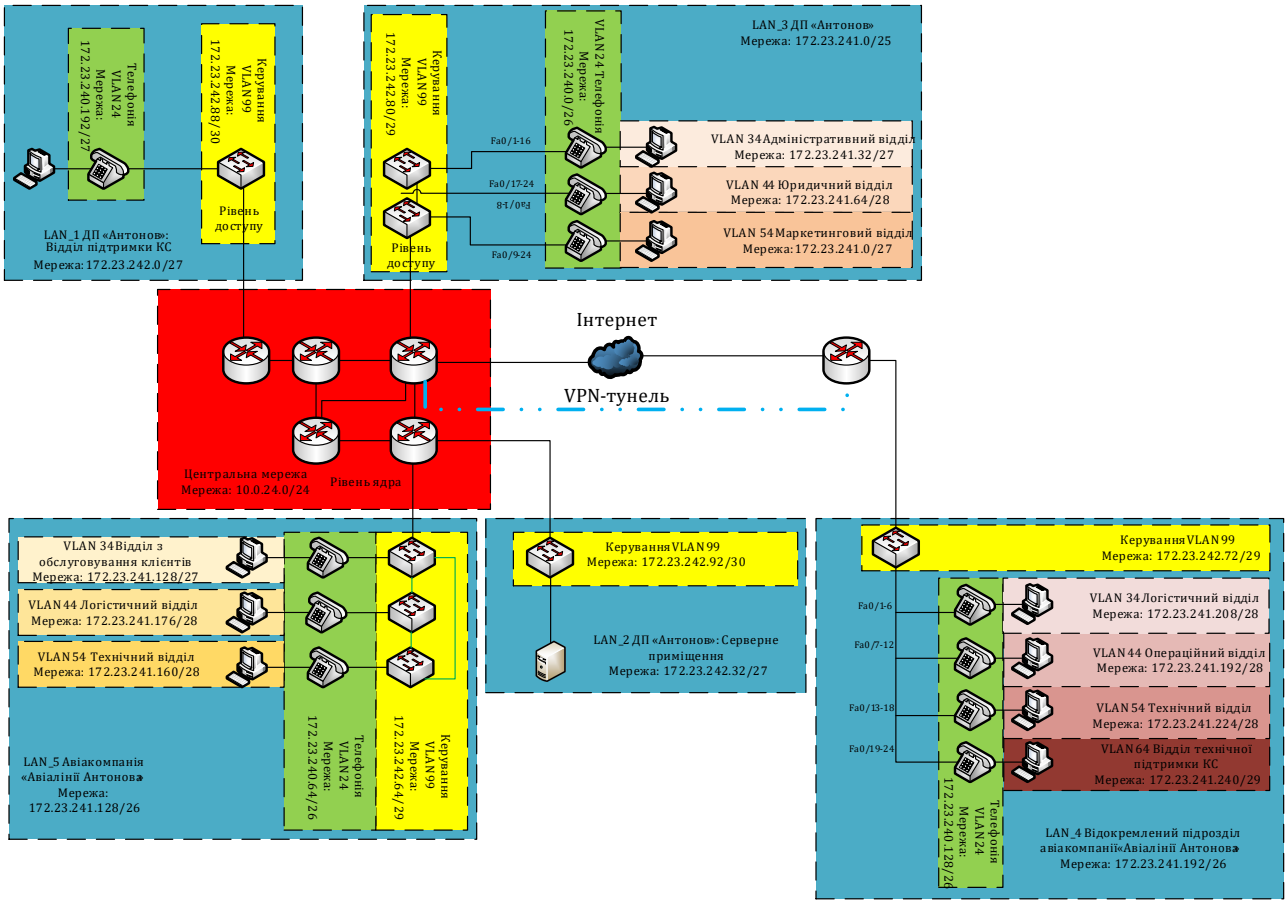


Рисунок 3.1 – Діаграма корпоративної мережі

3.2 Проєктування структурованої кабельної системи

Відповідно до умов, зазначених у плані розташування кінцевих пристроїв наведеному у додатку А, плану розміщення відділів наведеному на рисунку 2.1, проведено проєктування структурованої кабельної системи, результат якої наведений у додатку Б. Це включало визначення оптимального розташування мережевих розеток та кабельної інфраструктури, а також розрахунок довжини найбільшого сегмента мережевого кабелю.

Проєктована структурована кабельна система передбачає використання крученої пари категорії 5 (Cat 5e) для забезпечення з'єднання між мережевими пристроями. Кручена пара Cat 5e є стандартним типом кабелю, який широко використовується для передачі даних в локальних мережах. Такий кабель здатний забезпечити пропускну здатність кабелю, яка становить до 1000 Мбіт/с,

таким чином, повністю задовольняє вимогу, забезпечуючи необхідну швидкість передачі даних.

Під час планування враховано важливу характеристику, а саме довжину найдовшого сегмента мережевого кабелю. Згідно плану найбільша відстань від серверної стійки до найвіддаленішої комп'ютерної розетки становить 96,80 метрів, що не перевищує рекомендовану максимальну відстань у 100 метрів між активними мережевими пристроями при використанні кабелю Cat 5e.

Площа перерізу кабелю категорії 5e становить 5 мм. кв.

При проєктуванні СКС використані кабель-канали:

– Кабель-канал 100*40мм до 64 одиниць кабелів категорії 5e;
– Кабель-канал 30*20мм до 9 одиниць кабелів категорії 5e.

Таблиця 3.11 – Таблиця відповідності підключень розеток та інтерфейсів мережевого обладнання.

Поверх будівлі	Відділ підприємства	Номер комутаційної розетки	Ім'я пристрою	Інтерфейс
I	ДП «Антонов»: Адміністративний відділ	P1.1.10-P1.1.19	Shyrmakov_Switch_0	Fa0/1-16
	ДП «Антонов»: Юридичний відділ	P1.1.1-P1.1.9; P1.1.47-P1.1.54	Shyrmakov_Switch_0	Fa0/17-24
			Shyrmakov_Switch_1	Fa0/1-8
	ДП «Антонов»: Маркетинговий відділ	P1.1.21-46	Shyrmakov_Switch_1	Fa0/9-24
	ДП «Антонов»: Відділ технічної підтримки КС	P1.1.55-60	Shyrmakov_Switch_6	Fa0/1-24
II	Авіакомпанія «Авіалінії Антонова»: Логістичний відділ	P1.2.5-P1.2.21	Shyrmakov_Switch_3	Fa0/5-24

Кінець таблиці 3.11.

Поверх будівлі	Відділ підприємства	Номер комутаційної розетки	Ім’я пристрою	Інтерфейс
II	Авіакомпанія «Авіалінії Антонова»: Відділ з обслуговування клієнтів	P1.2.22-P1.2.42	Shyrmakov_Switch_2	Fa0/5-24
	Авіакомпанія «Авіалінії Антонова»: Технічний відділ	P1.2.1-P1.2.4; P1.2.48-P1.2.62	Shyrmakov_Switch_4	Fa0/5-24

3.3 Розробка моделі комп’ютерної мережі

Побудовано модель мережі згідно діаграми на рисунку 3.1.

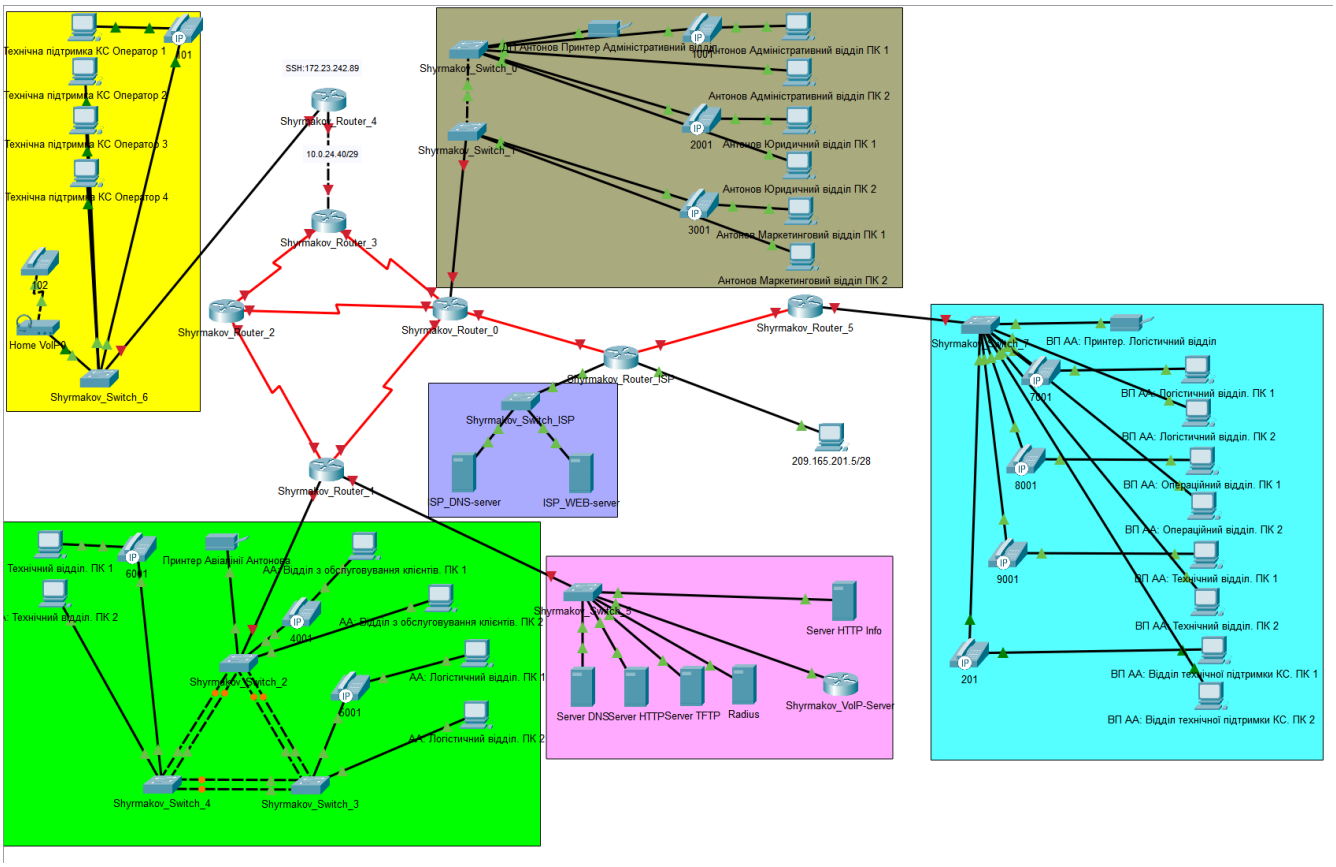


Рисунок 3.2 – Неконфігурована модель мережі

3.3.1 Проведення базового налаштування мережевих пристроїв

Базова конфігурація пристроїв включає:

– налаштування адрес інтерфейсів пристроїв;

– встановлення ідентифікаторів (назв) та доменних імен для кожного мережевого пристрою;

– налаштування банеру повідомлення дня (MOTD);

– налаштування тактової частоти DCE-інтерфейсах маршрутизаторів.

Приклад налаштування IP-адрес інтерфейсів, тактової частоти послідовних портів, банеру повідомлення дня та імені пристрою для Shyrmakov_Router_0:

```
Router_0(config)#hostname Shyrmakov_Router_0
Shyrmakov_Router_0(config)#banner motd #
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED
You must have explicit, authorized permission to access
or configure this device.
Unauthorized attempts and actions to access or use this
system may result in civil and/or
criminal penalties.
All activities performed on this device are logged and
monitored.
#
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.24
 Shyrmakov_Router_0(config-subif)#encapsulation dot1Q 24
 Shyrmakov_Router_0(config-subif)#ip address 172.23.240.1
255.255.255.192
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.34
 Shyrmakov_Router_0(config-subif)#encapsulation dot1Q 34
 Shyrmakov_Router_0(config-subif)#ip address 172.23.241.33
255.255.255.224
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.44
 Shyrmakov_Router_0(config-subif)#encapsulation dot1Q 44
 Shyrmakov_Router_0(config-subif)#ip address 172.23.241.65
255.255.255.240
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.54
 Shyrmakov_Router_0(config-subif)#encapsulation dot1Q 54
 Shyrmakov_Router_0(config-subif)#ip address 172.23.241.1
255.255.255.224
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.99
 Shyrmakov_Router_0(config-subif)#encapsulation dot1Q 99
 Shyrmakov_Router_0(config-subif)#ip address 172.23.242.81
255.255.255.248
```

```
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/2
 Shyrmakov_Router_0(config-if)#media-type sfp
 Shyrmakov_Router_0(config-if)#ip address 209.165.202.2
255.255.255.224
 Shyrmakov_Router_0(config-if)#exit
Shyrmakov_Router_0(config)#interface Serial0/1/1
 Shyrmakov_Router_0(config-if)#ip address 10.0.24.1
255.255.255.248
 Shyrmakov_Router_0(config-if)#clock rate 128000
 Shyrmakov_Router_0(config-if)#exit
Shyrmakov_Router_0(config)#interface Serial0/2/0
 Shyrmakov_Router_0(config-if)#ip address 10.0.24.9
255.255.255.248
 Shyrmakov_Router_0(config-if)#clock rate 128000
 Shyrmakov_Router_0(config-if)#exit
Shyrmakov_Router_0(config)#interface Serial0/2/1
 Shyrmakov_Router_0(config-if)#ip address 10.0.24.17
255.255.255.248
 Shyrmakov_Router_0(config-if)#clock rate 128000
```

3.3.2 Налаштування протоколів маршрутизації та динамічної конфігурації вузлів корпоративної мережі

Конфігурація протоколів маршрутизації включає:

– налаштування статичних маршрутів;

– налаштування протоколів динамічної маршрутизації;

– налаштування серверу динамічної конфігурації вузлів.

При налаштуванні OSPF, визначено мережі анонсовані в OSPF-процесі, для скорочення кількості анонсованих маршрутів, що полегшить обробку маршрутів в мережі та зменшить розмір OSPF-таблиць маршрутизації, застосована агрегація маршрутів.

Також за протоколом OSPF оголошується статичний маршрут в мережу інтернет.

Приклад налаштування статичного маршруту та протоколу динамічної маршрутизації OSPF для маршрутизатора Shyrmakov_Router_0:

```
Shyrmakov_Router_0(config)#ip route 0.0.0.0 0.0.0.0 209.165.202.1
Shyrmakov_Router_0(config)#router ospf 1
 Shyrmakov_Router_0(config-router)#passive-interface
GigabitEthernet0/0/0.24
 Shyrmakov_Router_0(config-router)#passive-interface
GigabitEthernet0/0/0.34
```

```
 Shyrmakov_Router_0(config-router)#passive-interface
GigabitEthernet0/0/0.44
 Shyrmakov_Router_0(config-router)#passive-interface
GigabitEthernet0/0/0.54
 Shyrmakov_Router_0(config-router)#passive-interface
GigabitEthernet0/0/0.99
 Shyrmakov_Router_0(config-router)#network 10.0.24.0 0.0.0.15 area
0
 Shyrmakov_Router_0(config-router)#network 10.0.24.16 0.0.0.7 area
0
 Shyrmakov_Router_0(config-router)#network 172.23.241.0 0.0.0.127
area 0
 Shyrmakov_Router_0(config-router)#network 172.23.240.0 0.0.0.63
area 0
 Shyrmakov_Router_0(config-router)#network 172.23.242.80 0.0.0.7
area 0
 Shyrmakov_Router_0(config-router)#default-information originate
```

На маршрутизаторах Shyrmakov_Router_0 та Shyrmakov_Router_5 (для мережі LAN_4) створено простори динамічної конфігурації вузлів для мереж згідно таблиці для підмереж:

LAN_1 Авіакомпанія «Авіалінії Антонова»:

– Відділ з обслуговування клієнтів;
– Логістичний відділ;
– Технічний відділ;
– Телефонія.

LAN_3 ДП «Антонов»:

– Адміністративний відділ;
– Юридичний відділ;
– Маркетинговий відділ;
– Телефонія.

LAN_4 Відокремлений підрозділ авіакомпанії «Авіалінії Антонова»:

– Логістичний відділ;
– Операційний відділ;
– Технічний відділ;
– Відділ технічної підтримки КС;
– Телефонія.

LAN_5 ДП «Антонов»: Відділ технічної підтримки КС;

Телефонія для LAN_5 ДП «Антонов»: Відділ технічної підтримки КС.

Приклад налаштування протоколу динамічної конфігурації вузлів для маршрутизатора Shyrmakov_Router_0:

```
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.241.33
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.241.65
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.242.41
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.242.1
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.240.193
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.240.65
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.241.129
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.241.177
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.241.161
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.240.1
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.240.89
Shyrmakov_Router_0(config)#ip dhcp excluded-address 172.23.241.1
Shyrmakov_Router_0(config)#ip dhcp pool DpAntonov_34
Shyrmakov_Router_0(dhcp-config)#network 172.23.241.32
255.255.255.224
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.241.33
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
Shyrmakov_Router_0(config)#ip dhcp pool DpAntonov_44
Shyrmakov_Router_0(dhcp-config)#network 172.23.241.64
255.255.255.240
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.241.65
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
Shyrmakov_Router_0(config)#ip dhcp pool DpAntonov_54
Shyrmakov_Router_0(dhcp-config)#network 172.23.241.0
255.255.255.224
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.241.1
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
Shyrmakov_Router_0(config)#ip dhcp pool DpAntonov_Tel
Shyrmakov_Router_0(dhcp-config)#network 172.23.240.0
255.255.255.192
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.240.1
Shyrmakov_Router_0(dhcp-config)#option 150 ip 172.23.242.37
Shyrmakov_Router_0(config)#ip dhcp pool DpAntonov_CSSupport
Shyrmakov_Router_0(dhcp-config)#network 172.23.242.0
255.255.255.224
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.242.1
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
Shyrmakov_Router_0(config)#ip dhcp pool Tel_DpAntonov_CSSupport
Shyrmakov_Router_0(dhcp-config)#network 172.23.240.192
255.255.255.224
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.240.193
Shyrmakov_Router_0(dhcp-config)#option 150 ip 172.23.242.37
Shyrmakov_Router_0(config)#ip dhcp pool Tel_AntonovAir
Shyrmakov_Router_0(dhcp-config)#network 172.23.240.64
255.255.255.192
```

```
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.240.65
Shyrmakov_Router_0(dhcp-config)#option 150 ip 172.23.242.37
Shyrmakov_Router_0(config)#ip dhcp pool AntonovAir_34
Shyrmakov_Router_0(dhcp-config)#network 172.23.241.128
255.255.255.224
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.241.129
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
Shyrmakov_Router_0(config)#ip dhcp pool AntonovAir_44
Shyrmakov_Router_0(dhcp-config)#network 172.23.241.176
255.255.255.240
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.241.177
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
Shyrmakov_Router_0(config)#ip dhcp pool AntonovAir_54
Shyrmakov_Router_0(dhcp-config)#network 172.23.241.160
255.255.255.240
Shyrmakov_Router_0(dhcp-config)#default-router 172.23.241.161
Shyrmakov_Router_0(dhcp-config)#dns-server 172.23.242.34
```

Маршрутизатори, які не мають власного сервера DHCP, повинні мати посилання на зовнішній сервер DHCP для кожного з інтерфейсів. Це необхідно для забезпечення розподілу IP-адрес та інших мережевих налаштувань усім пристроям в мережі. Приклад налаштування посилань на сервер динамічної конфігурації вузлів у маршрутизатора Shyrmakov_Router_4:

```
Shyrmakov_Router_4(config)#interface GigabitEthernet0/0/1
Shyrmakov_Router_4(config-if)#ip address 172.23.242.1
255.255.255.224
Shyrmakov_Router_4(config-if)#ip helper-address 10.0.24.1
Shyrmakov_Router_4(config-if)#ip helper-address 10.0.24.9
Shyrmakov_Router_4(config-if)#ip helper-address 10.0.24.17
```

3.3.3 Налаштування роботи Інтернет

Налаштування роботи з мережею Інтернет включає:

– налаштування трансляції приватних адрес за допомогою NAT;

– налаштування DNS-сервера.

Налаштування NAT на Shyrmakov_Router_0 передбачає використання динамічного NAT з набором адрес з 209.165.200.5 по 209.165.200.30. Для статичного перетворення адреси веб-серверу використовується адреса 209.165.200.3.

Для цього створено розширений список доступу з назвою «NATInternet», де вказано правила для перетворення адресів IP. Правило «deny» відхиляє трафік

між двома мережами 172.23.240.0/21. Правило "permit" дозволяє весь трафік з підмережі 172.23.240.0/21 до будь-якого місцевого IP-адресу. Створено пул IP-адрес з назвою «NATPool» з наведеним вище діапазоном. Налаштовано перетворення NAT для пакетів, використовуючи створений розширений список доступу «NATInternet» та пул IP-адрес «NATPool». Крім того, здійснено статичне перетворення NAT, де IP-адреса 172.23.242.39 перетворюється на 209.165.202.3. Для кожного внутрішнього інтерфейсу (GigabitEthernet0/0/0.24, GigabitEthernet0/0/0.34, GigabitEthernet0/0/0.44, GigabitEthernet0/0/0.54, Serial0/1/1, Serial0/2/0, Serial0/2/1) налаштовано параметр «ip nat inside», щоб позначити ці інтерфейси як внутрішні інтерфейси, від яких буде відбуватись перетворення NAT. Інтерфейс «GigabitEthernet0/0/2» визначено як зовнішній інтерфейс, за яким буде здійснюватись зв'язок зі зовнішніми мережами.

Приклад налаштування NAT для маршрутизатора Shyrmakov_Router_0:

```
Shyrmakov_Router_0(config)#ip access-list extended NATInternet
Shyrmakov_Router_0(config-ext-nacl)#deny ip 172.23.240.0 0.0.7.255
172.23.240.0 0.0.7.255
Shyrmakov_Router_0(config-ext-nacl)#permit ip 172.23.240.0
0.0.7.255 any
Shyrmakov_Router_0(config)#ip nat pool NATPool 209.165.202.5
209.165.202.30 netmask 255.255.255.224
Shyrmakov_Router_0(config)#ip nat inside source list NATInternet
pool NATPool
Shyrmakov_Router_0(config)#ip nat inside source static
172.23.242.39 209.165.202.3
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.24
 Shyrmakov_Router_0(config-subif)#ip nat inside
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.34
 Shyrmakov_Router_0(config-subif)#ip nat inside
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.44
 Shyrmakov_Router_0(config-subif)#ip nat inside
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/0.54
 Shyrmakov_Router_0(config-subif)#ip nat inside
 Shyrmakov_Router_0(config-subif)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/2
 Shyrmakov_Router_0(config-if)#ip nat outside
 Shyrmakov_Router_0(config-if)#exit
Shyrmakov_Router_0(config)#interface Serial0/1/1
 Shyrmakov_Router_0(config-if)#ip nat inside
 Shyrmakov_Router_0(config-if)#exit
```

```
Shyrmakov_Router_0(config)#interface Serial0/2/0
 Shyrmakov_Router_0(config-if)#ip nat inside
 Shyrmakov_Router_0(config-if)#exit
Shyrmakov_Router_0(config)#interface Serial0/2/1
 Shyrmakov_Router_0(config-if)#ip nat inside
```

На маршрутизаторі Shyrmakov_Router_5 налаштовано перевантажений NAT, також відомий як PAT.

Проведено налаштування корпоративного серверу DNS. Налаштовано доменну адресу веб-сервера та адресу сервера DNS відповідального за область .UA.

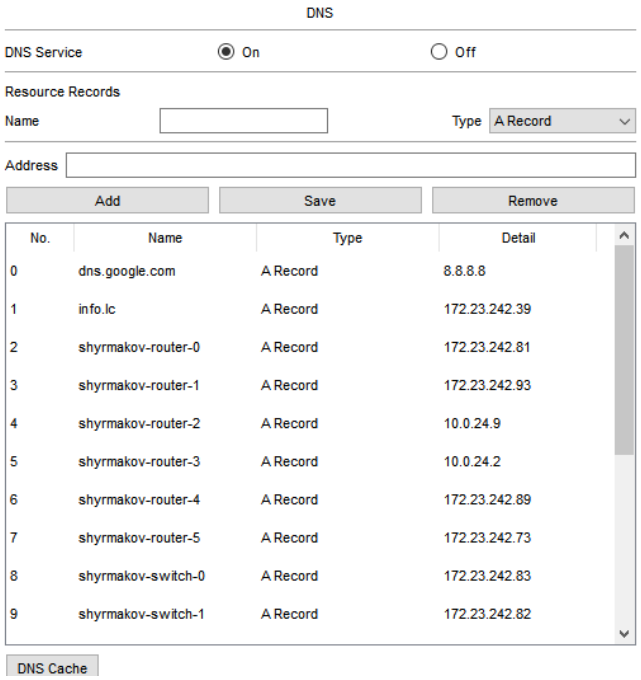


Рисунок 3.3 – Налаштування DNS-сервера підприємства

3.3.4 Заходи безпеки для запобігання несанкціонованому доступу до інформації в комп'ютерній системі

Конфігурація безпеки пристроїв включає:

– встановлення паролів для входу в пристрої через віртуальні термінали (vty) та консоль;

– налаштування паролів для входу в привілейований режим;

– застосування шифрування до збережених паролів для їхнього захисту;

– створення RSA-ключа довжиною 1024 біта для шифрування даних;

– забезпечення використання протоколу SSH на всіх лініях vty;

– створення безпечного VPN-тунелю між головним офісом та віддаленим підрозділом;

– розділення мереж на віртуальні сегменти;

– налаштування списків керування доступом для обмеження доступу до ресурсів;

– впровадження механізму централізованого керування автентифікацією, авторизацією та обліком.

Приклад налаштування паролів входу в пристрої через віртуальні термінали (vty) та консолі, входу в привілейований режим, застосування шифрування збережених паролів, забезпечення роботи протоколу SSH на всіх лініях vty та створення VPN-тунелю на маршрутизаторі Shyrmakov_Router_0:

Приклад налаштування IP-адрес інтерфейсів для віртуальних мереж для Shyrmakov_Router_0 наведено у пункті 3.3.1.

Приклад налаштування безпекових параметрів та віртуальних мереж на комутаторі Shyrmakov_Switch_0:

```
Shyrmakov_Switch_0(config)#username 12320sk1_Shyrmakov privilege
15 password shyrmakovpassword
Shyrmakov_Switch_0(config)#enable secret
Shyrmakov_Switch_0(config)#ip domain-name shyrmakov-switch-0
Shyrmakov_Switch_0(config)#ip ssh version 2
Shyrmakov_Switch_0(config)#ip ssh time-out 60
Shyrmakov_Switch_0(config)#ip ssh authentication-retries 3
Shyrmakov_Switch_0(config)#crypto key generate rsa 1024
Shyrmakov_Switch_0(config)#interface range fastethernet0/1-16
Shyrmakov_Switch_0(if-range)#switchport mode access
Shyrmakov_Switch_0(if-range)#switchport access vlan 34
Shyrmakov_Switch_0(if-range)#switchport voice vlan 24
Shyrmakov_Switch_0(if-range)#exit
Shyrmakov_Switch_0(config)#interface range fastethernet0/16-24
Shyrmakov_Switch_0(if-range)#switchport mode access
Shyrmakov_Switch_0(if-range)#switchport access vlan 44
Shyrmakov_Switch_0(if-range)#switchport voice vlan 24
Shyrmakov_Switch_0(if-range)#exit
Shyrmakov_Switch_0(config)#interface range GigabitEthernet0/1-2
Shyrmakov_Switch_0(if-range)#switchport mode trunk
Shyrmakov_Switch_0(if-range)#exit
Shyrmakov_Switch_0(config)#interface Vlan99
```

```
Shyrmakov_Switch_0(config-if)#ip address 172.23.242.83
255.255.255.248
Shyrmakov_Switch_0(config-if)#exit
Shyrmakov_Switch_0(config)#ip default-gateway 172.23.242.81
Shyrmakov_Switch_0(config)#enable secret en_shyrmakov
Shyrmakov_Switch_0(config)#line console 0
Shyrmakov_Switch_0(config-line)#password ln_shyrmakov
Shyrmakov_Switch_0(config-line)#login local
Shyrmakov_Switch_0(config-line)#transport input ssh
Shyrmakov_Switch_0(config-line)#exit
Shyrmakov_Switch_0(config)#line vty 0 15
Shyrmakov_Switch_0(config-line)#password ln_shyrmakov
Shyrmakov_Switch_0(config-line)#login local
Shyrmakov_Switch_0(config-line)#transport input ssh
Shyrmakov_Switch_0(config-line)#exit
```

На мережевих пристроях активовано модель аутентифікації AAA, встановлено аутентифікацію для входу на консоль та віртуальні термінали з використанням централізованих та локальних баз даних. Створено розширені списки доступу (ACL) для керування трафіком, зокрема VPN-Tunnel для виявлення цікавого трафіку VPN-тунелю, NATInternet для визначення необхідності трансляції адрес, CSSMgmt для обмеження доступу до мережі керування, SSH, та DenyNetworkAccess для обмеження доступу між відділами. Створено VPN-тунель між віддаленими об’єктами. Приклад налаштування механізму централізованого керування автентифікацією, авторизацією та обліком, списками доступу на маршрутизаторі та VPN-тунелю на маршрутизаторі Shyrmakov_Router_0:

```
Shyrmakov_Router_0(config)#aaa new-model
Shyrmakov_Router_0(config)#aaa authentication login default group
radius local
Shyrmakov_Router_0(config)#radius server RAD
Shyrmakov_Router_0(config-radius-server)#address ipv4
172.23.242.38
Shyrmakov_Router_0(config-radius-server)#key radius123
Shyrmakov_Router_0(config-radius-server)#exit
Shyrmakov_Router_0(config)#line console 0
Shyrmakov_Router_0(config-line)#login authentication default
Shyrmakov_Router_0(config-line)#line vty 0 15
Shyrmakov_Router_0(config-line)#login authentication default
Shyrmakov_Router_0(config-line)#exit
Shyrmakov_Router_0(config)#ip access-list extended VPN-Tunnel
Shyrmakov_Router_0(config-ext-nacl)#permit ip 172.23.240.0
0.0.7.255 172.23.240.0 0.0.7.255
Shyrmakov_Router_0(config-ext-nacl)#exit
```

```
Shyrmakov_Router_0(config)#ip access-list extended NATInternet
Shyrmakov_Router_0(config-ext-nacl)#deny ip 172.23.240.0 0.0.7.255
172.23.240.0 0.0.7.255
Shyrmakov_Router_0(config-ext-nacl)#permit ip 172.23.240.0
0.0.7.255 any
Shyrmakov_Router_0(config-ext-nacl)#exit
Shyrmakov_Router_0(config)#ip access-list extended CSSMgmt
Shyrmakov_Router_0(config-ext-nacl)#permit ip 172.23.242.0
0.0.0.31 172.23.242.64 0.0.0.31
Shyrmakov_Router_0(config-ext-nacl)#permit ip host 172.23.242.38
172.23.242.64 0.0.0.31
Shyrmakov_Router_0(config-ext-nacl)#deny ip any 172.23.242.64
0.0.0.31
Shyrmakov_Router_0(config-ext-nacl)#exit
Shyrmakov_Router_0(config)#ip access-list extended SSH
Shyrmakov_Router_0(config-ext-nacl)#permit tcp 172.23.242.0
0.0.0.31 172.23.242.64 0.0.0.31 eq 22
Shyrmakov_Router_0(config-ext-nacl)#permit tcp 172.23.242.0
0.0.0.31 10.0.24.0 0.0.0.255 eq 22
Shyrmakov_Router_0(config-ext-nacl)#deny tcp any any eq 22
Shyrmakov_Router_0(config-ext-nacl)#permit ip any any
Shyrmakov_Router_0(config-ext-nacl)#exit
Shyrmakov_Router_0(config)#ip access-list extended
DenyNetworkAccess
Shyrmakov_Router_0(config-ext-nacl)#permit ip any 172.23.242.0
0.0.0.31
Shyrmakov_Router_0(config-ext-nacl)#permit ip any 172.23.242.32
0.0.0.31
Shyrmakov_Router_0(config-ext-nacl)#deny ip any 172.23.240.0
0.0.7.255
Shyrmakov_Router_0(config-ext-nacl)#permit ip any any
Shyrmakov_Router_0(config)#crypto isakmp policy 1
Shyrmakov_Router_0(config-isakmp)#encr aes
Shyrmakov_Router_0(config-isakmp)#authentication pre-share
Shyrmakov_Router_0(config-isakmp)#group 2
Shyrmakov_Router_0(config-isakmp)#exit
Shyrmakov_Router_0(config)#crypto isakmp key cisco address
64.100.13.2
Shyrmakov_Router_0(config)#crypto ipsec transform-set TS esp-aes
esp-sha-hmac
Shyrmakov_Router_0(config)#crypto map CMAP 10 ipsec-isakmp
Shyrmakov_Router_0(config-crypto-map)#set peer 64.100.13.2
Shyrmakov_Router_0(config-crypto-map)#set transform-set TS
Shyrmakov_Router_0(config-crypto-map)#match address VPN-Tunnel
Shyrmakov_Router_0(config-crypto-map)#exit
Shyrmakov_Router_0(config)#interface GigabitEthernet0/0/2
Shyrmakov_Router_0(config-if)#crypto map CMAP
Shyrmakov_Router_0(config-if)#interface GigabitEthernet0/0/0.34
Shyrmakov_Router_0(config-if)#ip access-group DenyNetworkAccess in
Shyrmakov_Router_0(config-if)#interface GigabitEthernet0/0/0.44
Shyrmakov_Router_0(config-if)#ip access-group DenyNetworkAccess in
Shyrmakov_Router_0(config-if)#interface GigabitEthernet0/0/0.54
```

```
Shyrmakov_Router_0(config-if)#ip access-group DenyNetworkAccess in
```

На сервері Radius вказані мережеві налаштування клієнтів, такі як: ім'я клієнту, IP-адреса клієнту, тип сервера та секретний ключ.

Створений користувач shyrmakov з паролем shyrmakov_aaa.

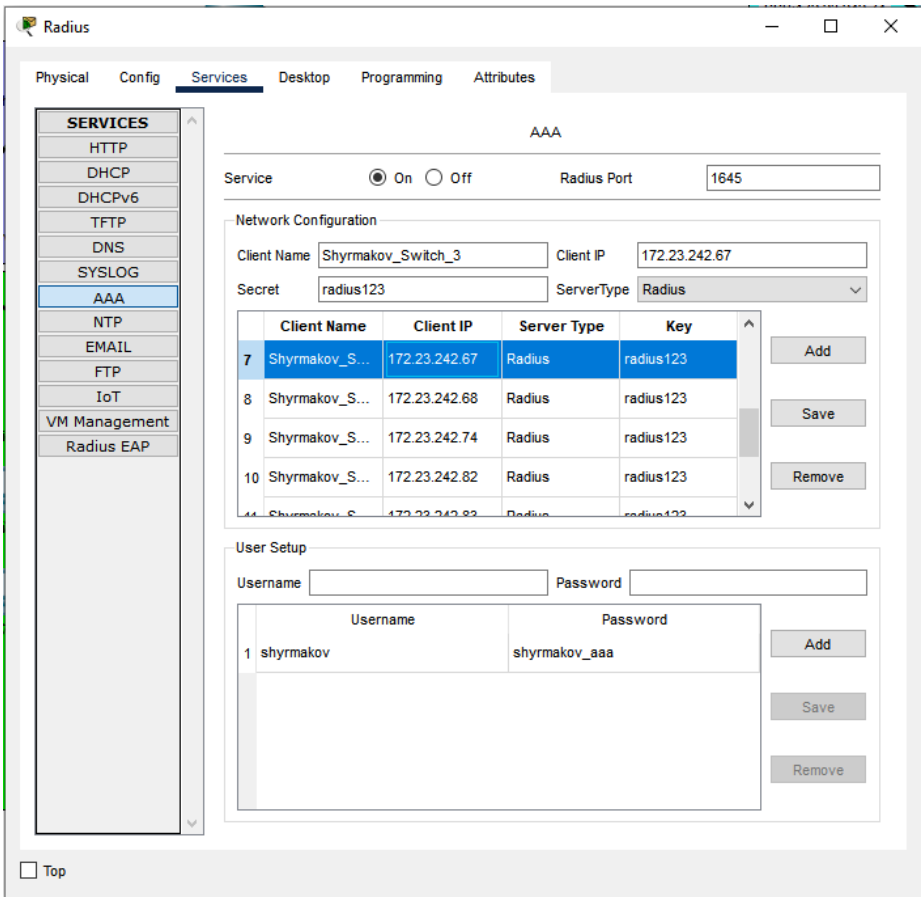


Рисунок 3.4 – Налаштування RADIUS-сервера

3.3.5 Налаштування сервісу телефонії

Налаштування серверу IP-телефонії:

```
Router0(config)#hostname Shyrmakov_VoIP-Server
Shyrmakov_VoIP-Server(config)#interface FastEthernet0/0
Shyrmakov_VoIP-Server(config-if)#ip address 172.23.242.37
255.255.255.224
Shyrmakov_VoIP-Server(config-if)#exit
Shyrmakov_VoIP-Server(config)#ip default-gateway 172.23.242.33
Shyrmakov_VoIP-Server(config)#ip route 0.0.0.0 0.0.0.0
172.23.242.33
Shyrmakov_VoIP-Server(config)#telephony-service
Shyrmakov_VoIP-Server(config-telephony)#no auto-reg-ephone
Shyrmakov_VoIP-Server(config-telephony)#max-ephones 40
Shyrmakov_VoIP-Server(config-telephony)#max-dn 140
```

```
Shyrmakov_VoIP-Server(config-telephony)#ip source-address
172.23.242.37 port 5060
Shyrmakov_VoIP-Server(config-telephony)#exit
Shyrmakov_VoIP-Server(config)#ephone-dn 1
Shyrmakov_VoIP-Server(config-ephone-dn)#number 101
Shyrmakov_VoIP-Server(config-ephone-dn)#exit
Shyrmakov_VoIP-Server(config)#ephone 1
Shyrmakov_VoIP-Server(config-ephone)#device-security-mode none
Shyrmakov_VoIP-Server(config-ephone)#mac-address 00E0.B098.2081
Shyrmakov_VoIP-Server(config-ephone)#type 7960
Shyrmakov_VoIP-Server(config-ephone)#button 1:1
```

3.3.6 Перевірка роботи комп’ютерної системи

Перевірка роботи комп'ютерної мережі є важливим етапом в налаштуванні та підтримці мережевої інфраструктури. Її мета полягає в перевірці функціональності, доступності та стабільності мережевих з'єднань, протоколів, сервісів та пристроїв. Перевірка роботи комп'ютерної мережі дозволяє переконатись, що всі компоненти працюють належним чином і забезпечують необхідну функціональність.

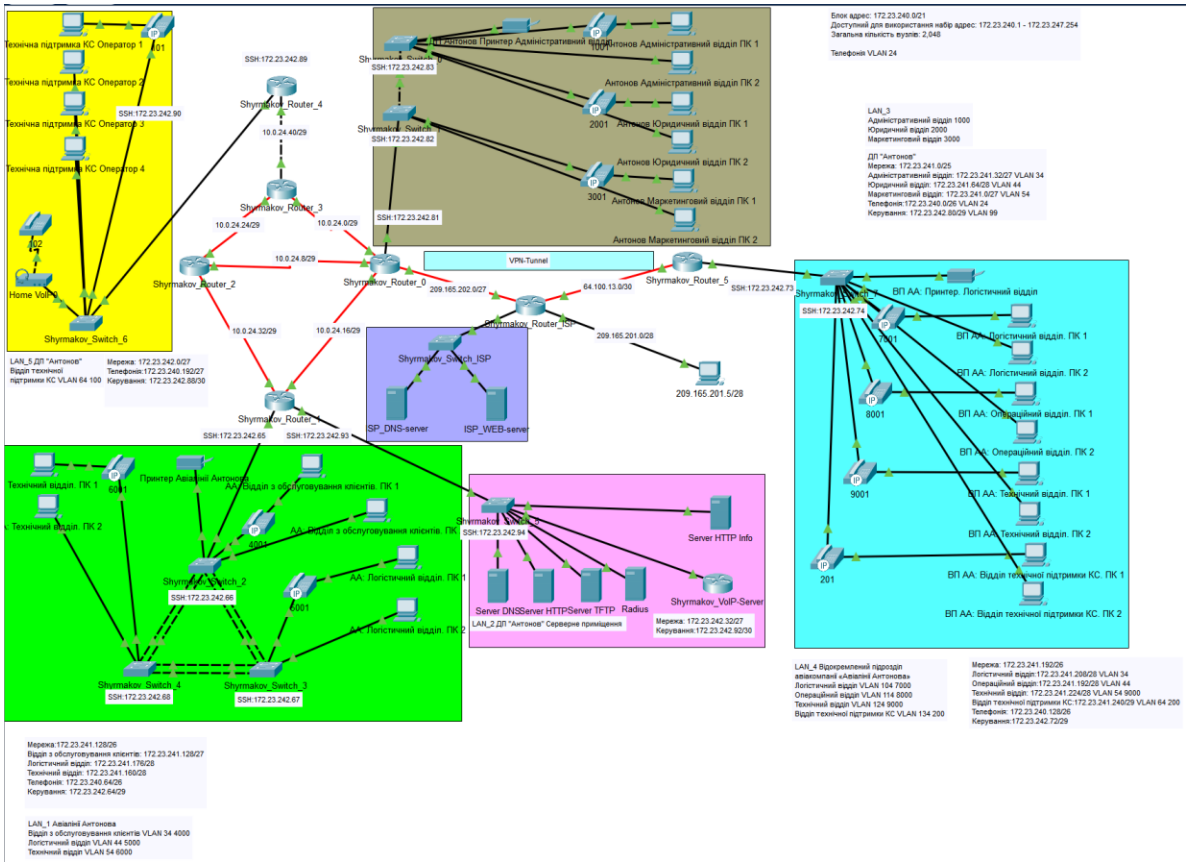


Рисунок 3.5 – Завершена модель мережі

Ознайомившись з рисунком можна можна підтвердити, що на фізичному рівні всі кабелі правильно підключені та мають належний стан. Індикатори підтверджують наявність активного з'єднання, всі пристрої знаходяться в стабільному стані і готові до передачі даних.

На мережевому рівні можна підтвердити, що адреси всіх вузлів налаштовані правильно. Це означає, що кожен вузол мережі має унікальну IP-адресу, яка відповідає розробленій адресаційній схемі. Також, якщо в мережі застосовується протокол DHCP, можна переконатись, що процес надання IP-адрес працює належним чином і кожен вузол отримує коректну адресу від DHCP-сервера.

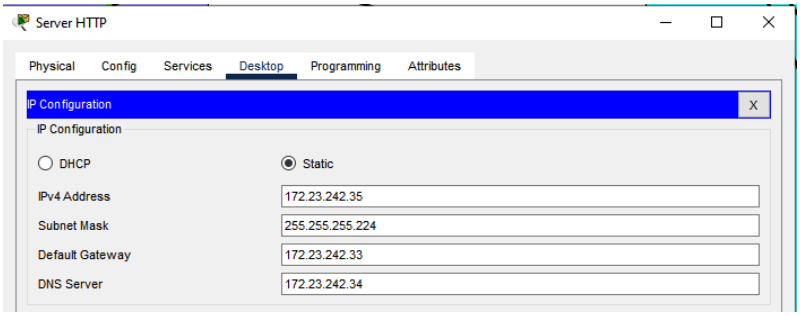


Рисунок 3.6 – Налаштовані параметри IP веб-сервера.

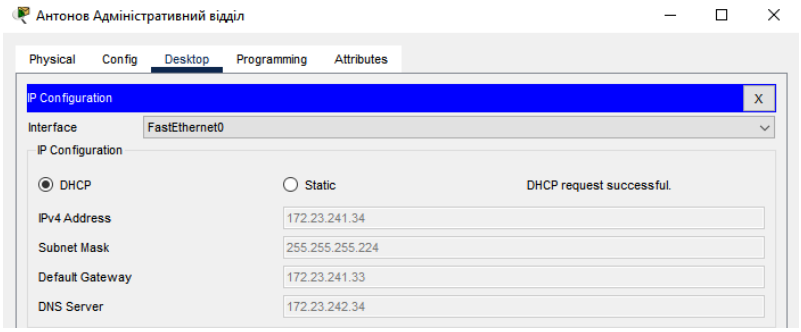


Рисунок 3.7 – IP-адреса отримана за протоколом DHCP

Здійснено перевірку зв’язку між комп’ютерами, що знаходяться в одному відділі. Результатом перевірки стало успішне виконання відправки пакетів між вузлами.

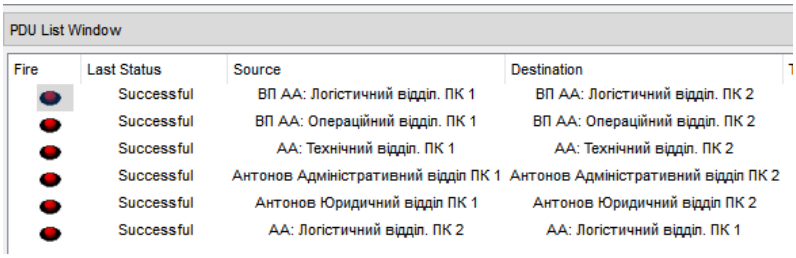


Рисунок 3.8 – Перевірка зв'язку між комп'ютерами в межах відділу

Здійснено перевірку зв'язку між комп'ютерами, що знаходяться в різних відділах, а також комп'ютерами технічної підтримки та комп'ютерами решти відділів. Результатом перевірки стало успішне виконання відправки пакетів між комп'ютерами технічної підтримки та комп'ютерами відділів. Відправка пакетів між вузлами відділів, що не належать до технічної підтримки було відхилено, згідно налаштованих списків керування доступом.

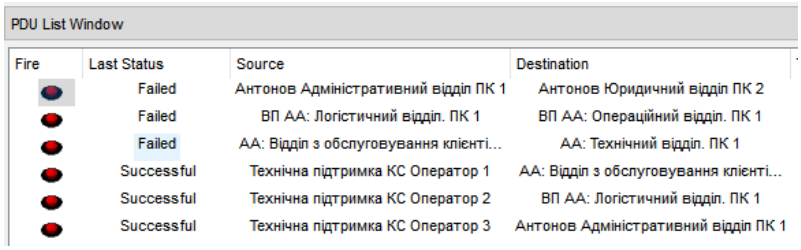


Рисунок 3.9 – Перевірка зв'язку між комп'ютерами в різних відділах

Проведено перевірку доступу до спільних ресурсів, зокрема до веб-серверу та роботи VPN-тунелю, всі пакети надіслані успішно.

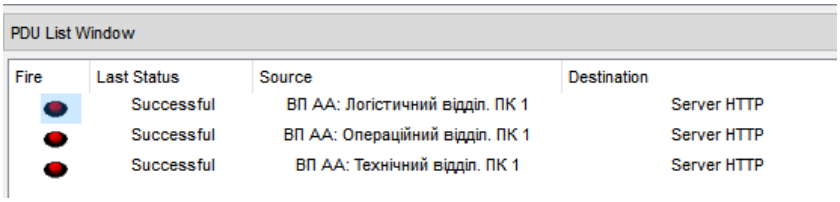


Рисунок 3.10 – Перевірка зв'язку між віддаленим відділом та веб-сервером через VPN-тунель

Виходячи з результату перегляду статистики VPN-тунелю, він налаштований коректно, функціонує без помилок.

```
Shyrmakov_Router_0#show crypto ipsec sa

interface: GigabitEthernet0/0/2
    Crypto map tag: CMAP, local addr 209.165.202.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.23.240.0/255.255.248.0/0/0)
   remote  ident (addr/mask/prot/port): (172.23.240.0/255.255.248.0/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 472, #pkts encrypt: 472, #pkts digest: 0
   #pkts decaps: 485, #pkts decrypt: 485, #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 0, #recv errors 0
```

Рисунок 3.11 – Перегляд статистики роботи VPN-тунелю

Проведено перевірку доступу до мережевих компонентів, зокрема комутаторів, з вузлів працівників рядових відділів та відділу технічної підтримки. Результат перевірки демонструє, що доступ до мережі мережевих компонентів мають лише співробітники технічної підтримки КС.

PDU List Window

Fire	Last Status	Source	Destination
	Failed	Антонов Адміністративний відділ ПК 1	Shyrmakov_Switch_6
	Failed	ВП АА: Логістичний відділ. ПК 1	Shyrmakov_Switch_7
	Failed	АА: Логістичний відділ. ПК 1	Shyrmakov_Switch_3
	Successful	Технічна підтримка КС Оператор 1	Shyrmakov_Switch_0
	Successful	Технічна підтримка КС Оператор 2	Shyrmakov_Switch_7
	Successful	Технічна підтримка КС Оператор 3	Shyrmakov_Switch_3
	Successful	Технічна підтримка КС Оператор 4	Shyrmakov_Switch_5

Рисунок 3.12 – Перевірка зв’язку між комп’ютерами та мережевими пристроями

Проведена перевірка доступу по протоколу SSH підтвердила, що співробітник рядового відділу не має прав доступу по SSH до мережевих пристроїв. Правила доступу до SSH були досягнуті завдяки застосуванню списків управління доступом (ACL) на мережевих пристроях. Впроваджений механізм гарантує, що лише співробітники технічної підтримки комп’ютерних систем мають можливість встановлювати SSH-з'єднання з мережевими

компонентами, забезпечуючи таким чином високий рівень безпеки і обмежуючи доступ до керування мережевими ресурсами на необхідному рівні.

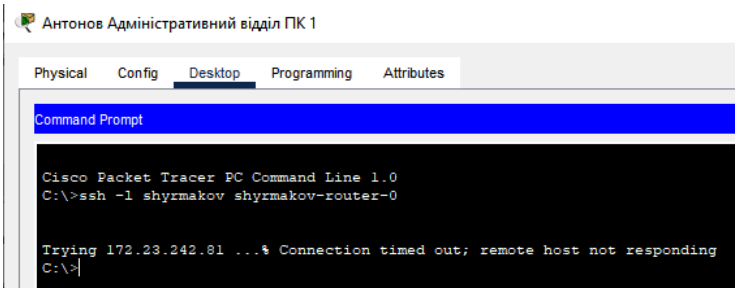


Рисунок 3.13 – Спроба підключення за протоколом SSH з комп'ютера працівника

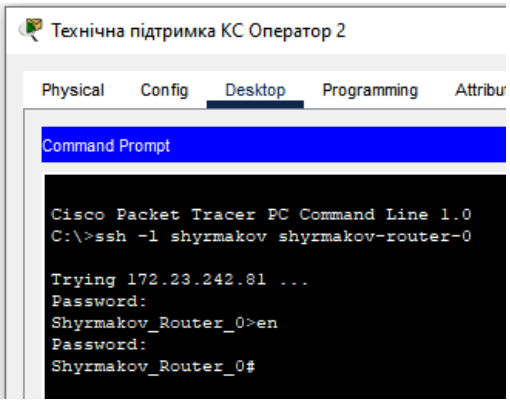


Рисунок 3.14 – Спроба підключення за протоколом SSH з комп'ютера оператора технічної підтримки

Проведено перевірку роботи сервера доменних імен (DNS) шляхом відображення веб-сторінки antonov.ua. Результат свідчить про коректну роботу сервера DNS, оскільки веб-сторінка була успішно відображена. Таким чином додатково було перевірено, чи відправляє сервер DNS запити на інший DNS-сервер, який відповідає за домен з розширенням «.ua». Під час цієї перевірки серверу DNS вдалося переслати запит на інший DNS-сервер та отримати відповідь. Це свідчить про правильне налаштування і функціонування серверів DNS, забезпечуючи надійну роботу системи доменних імен для домену з розширенням «.ua».

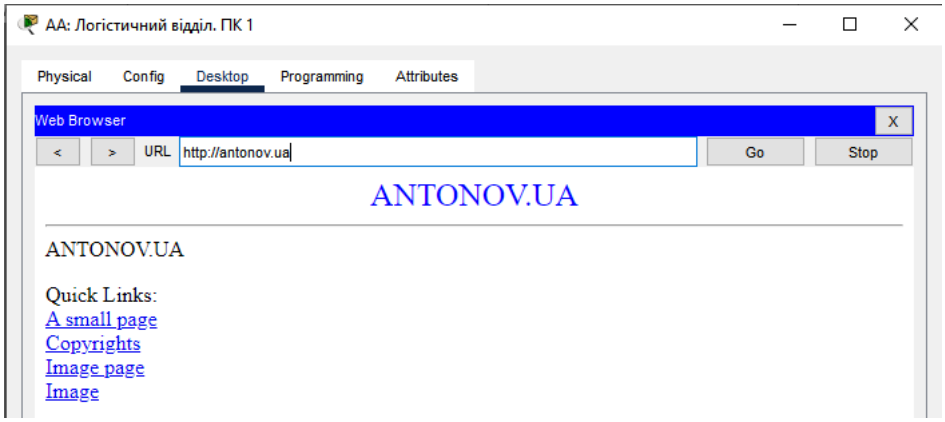


Рисунок 3.15 – Відображена веб-сторінка antonov.ua

При відкритті веб-сторінки antonov.ua було здійснено звернення до зовнішнього веб-сервера. З огляду на використання технології Network Address Translation (NAT) на граничному маршрутизаторі, успішне відображення веб-сторінки свідчить про коректну роботу NAT. Здійснено перегляд перетворень NAT на маршрутизаторі Shyrmakov_Router_0.

```
Shyrmakov_Router_0#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
udp 209.165.202.5:1025 172.23.242.34:1025 8.8.8.8:53         8.8.8.8:53
---  209.165.202.3     172.23.242.39      ---                ---
tcp 209.165.202.6:1026 172.23.241.36:1026 8.8.8.9:80         8.8.8.9:80

Shyrmakov_Router_0#
```

Рисунок 3.16 – Перегляд таблиці трансляцій адрес

Для перевірки функціональності телефонії було здійснено дзвінок з віддаленої мережі до головної мережі. Цей тестовий дзвінок продемонстрував правильну роботу телефонної системи між віддаленими мережами через VPN-тунель. Результати перевірки демонструють, що вдалося успішно здійснити з'єднання, дзвінок пройшов без перешкод.

Рисунок 3.17 – Результат перевірки системи IP-телефонії

В результаті розробки корпоративної мережі було досягнуто успішного впровадження та налаштування необхідних компонентів. Система працює стабільно і надійно, відповідає всім вимогам і задачам, що були поставлені.

Адресація мережі була налаштована коректно, що дозволяє ефективно управляти IP-адресами та забезпечувати взаємозв'язок між різними пристроями. Впроваджено службу DHCP, що автоматично надає IP-адреси для клієнтів.

Використання VLAN дозволило ефективно розділити мережу на логічні сегменти, що забезпечує ізоляцію між відділами та забезпечує безпеку та ефективну роботу.

Сервери доступні клієнтам і забезпечують необхідні сервіси та функціональні можливості. Клієнти з різних відділів мають обмежений доступ одне до одного та до мережевого обладнання, що забезпечує безпеку і приватність даних. Однак, відділи технічної підтримки КС мають необхідний рівень доступу до всіх компонентів мережі за допомогою ACL.

Функція NAT працює належним чином, забезпечуючи доступ до Інтернету для всіх користувачів. Це дозволяє здійснювати зовнішні комунікації та обмін даними з іншими мережами.

Встановлений VPN-тунель дозволяє забезпечити безпечний і зашифрований доступ до ресурсів мережі з віддалених місць, забезпечуючи конфіденційність та захист даних.

Система IP-телефонії була успішно реалізована та налаштована в рамках корпоративної мережі.

Загалом, розробка корпоративної мережі була успішною, і всі поставлені завдання були досягнуті. Система готова до експлуатації, забезпечуючи ефективну комунікацію та роботу між різними відділами та користувачами компанії.

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Опис концепту розроблюваної системи керування сервером телефонії

Згідно вимог, застосунок для керування сервером IP-телефонії має бути розроблений урахуванням декількох ключових принципів.

Перш за все, інтерфейс програмного забезпечення повинен бути зрозумілим та логічним для користувачів, що дозволяє їм інтуїтивно взаємодіяти з системою навіть без глибокого знання її принципів. Застосунок має бути легким у навчанні нових користувачів, забезпечуючи їм швидкий старт в роботі з системою.

Кросплатформність в контексті застосунку забезпечується шляхом розробки веб-сайту як основного інтерфейсу користувача. Замість створення окремих додатків для різних платформ, веб-сайт розробляється з урахуванням сумісності з різними операційними системами та пристроями.

Використання веб-сайту як основного інтерфейсу має кілька переваг для досягнення кросплатформеності:

Веб-сайт може бути відкритим у будь-якому веб-браузері, незалежно від операційної системи на пристрої. Це означає, що користувачі з різних платформ, таких як Windows, macOS, Linux, а також мобільні пристрої на iOS та Android, можуть отримати доступ до застосунку.

Застосунок на веб-сайті можна оновлювати централізовано без потреби оновлювати окремі додатки на кожній платформі. Це забезпечує швидке розгортання оновлень та забезпечує користувачам завжди актуальну версію.

Веб-сайти зазвичай мають інтуїтивний та зрозумілий інтерфейс, що спрощує навчання нових користувачів. Основні функції та операції можуть бути легко доступні через веб-сторінки, що полегшує використання системи без глибоких знань щодо платформи чи операційної системи.

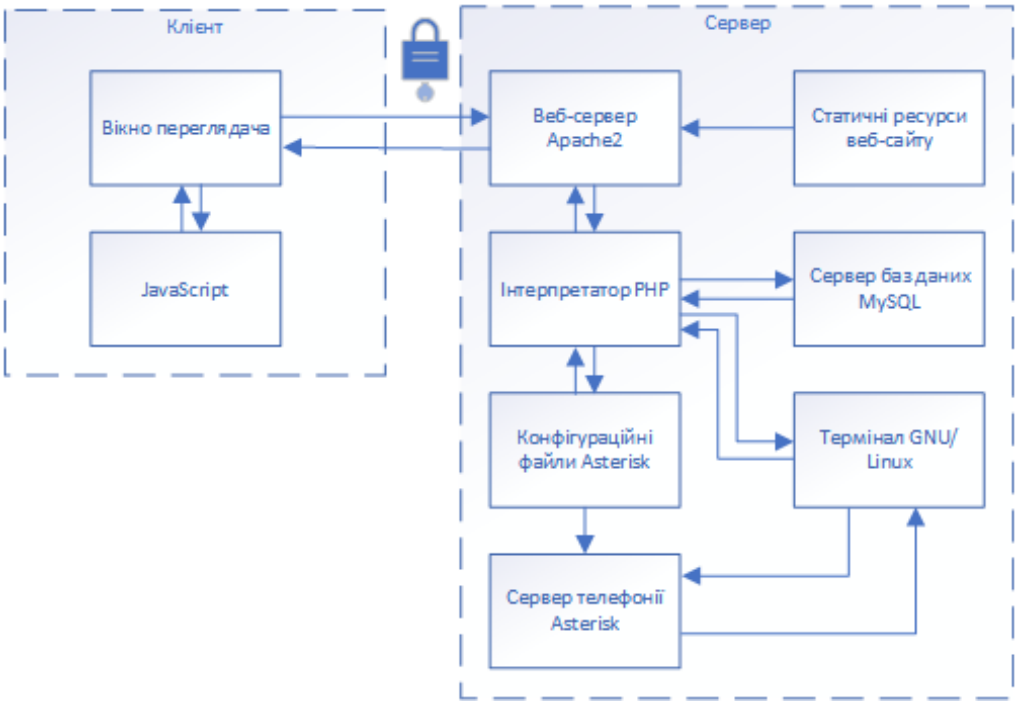


Рисунок 4.1 – Принципова схема веб-додатку керування сервером IP-телефонії

При розробці застосовано наступні компоненти та їх взаємодію:

Веб-сервер Apache2 для хостингу веб-сайту, що забезпечує доступ до інтерфейсу управління сервером IP-телефонії. Apache2 обробляє запити від клієнтів і надсилає веб-сторінки та ресурси до браузерів користувачів.

PHP: Використовується для обробки запитів на стороні сервера. PHP взаємодіє з базою даних MySQL для роботи системи автентифікації, отримує дані від користувача, редагує конфігураційні файли серверу телефонії та здійснює інші операції на стороні сервера.

Сервер телефонії Asterisk забезпечує функціонування системи телефонії, маршрутизацію дзвінків, та інші функції, необхідні для роботи IP-телефонної системи.

HTML і CSS використовуються для створення веб-сторінок, стилізації їх зовнішнього вигляду. HTML відповідає за структуру та розмітку сторінок, а CSS – за їх дизайн і візуальне оформлення.

MySQL: Використовується для функціонування системи ідентифікації та автентифікації, де зберігаються дані про облікові записи адміністраторів телефонної системи.

Bash використовується для керування сервером телефонії, зокрема для виконання різних дій, таких як перезавантаження сервера, перегляд стану процесів і т.д.

JavaScript забезпечує взаємодію з користувачем дозволяючи створювати динамічні елементи на сторінці, обробляти події та реагувати на них.

Це дозволяє реалізовувати:

– інтерактивні інтерфейси, які забезпечують більш покращену взаємодію з користувачем.

– здійснювати формування запитів до сервера виконавши асинхронні запити до сервера без перезавантаження сторінки. За допомогою AJAX, ведеться взаємодія з сервером, передаються дані та отримуються відповіді. Це дозволяє виконувати функції без повного перезавантаження сторінки.

– проводити валідацію та контроль введення даних введених користувачем в форми. Також JavaScript використовується у локалізації додатку, де текстові рядки перекладаються на різні мови в залежності від налаштувань користувача.

Взаємодія між сервером і клієнтом при використанні застосунку здійснюється за допомогою захищеного протоколу HTTPS (HTTP Secure). Цей протокол додає шар шифрування до звичайного протоколу HTTP, забезпечуючи конфіденційність та цілісність переданих даних. Використовуються механізми шифрування, такі як TLS (Transport Layer Security) або SSL (Secure Sockets Layer), які перетворюють дані в зашифрований формат, що запобігає можливості перехоплення або прочитання їх третіми особами. Крім того, захищене з'єднання HTTPS впроваджує механізм, який підтверджує ідентичність сервера і забезпечують довіру між сервером і клієнтом використовуючи сертифікати SSL/TLS. Це забезпечує безпечну комунікацію між обома сторонами, зменшуючи ризик несанкціонованого доступу до переданих даних.

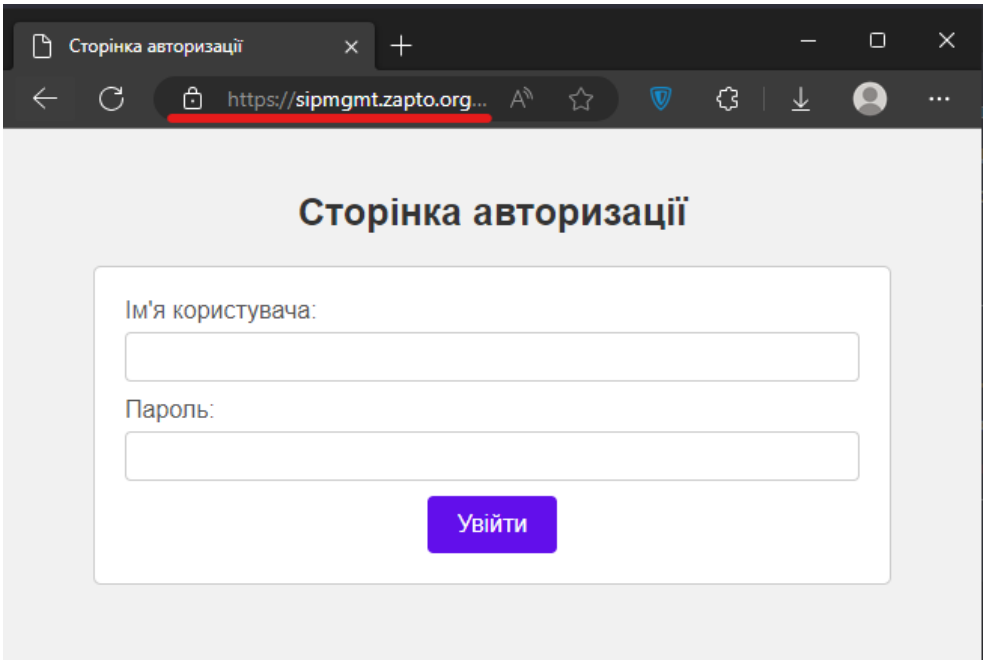


Рисунок 4.2 – Встановлене захищене з’єднання

4.2 Огляд функціональності та особливостей додатку

При запуску Android додатку, користувачу надається можливість ввести адресу сервера. Окрім того, застосунок зберігає останню введену адресу. Це дозволяє зручно використовувати додаток, оскільки користувачу не потрібно вводити адресу кожного разу при наступному запуску.

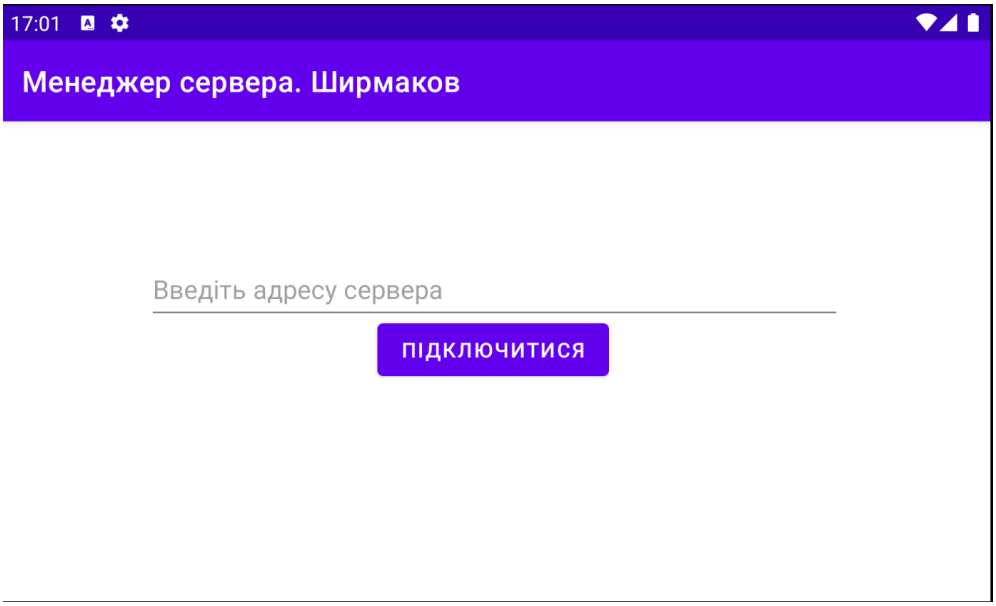


Рисунок 4.3 – Вікно вводу адреси серверу

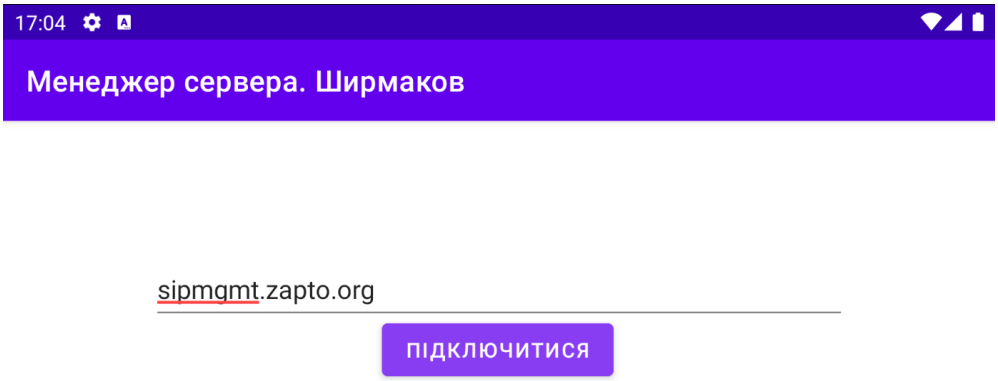


Рисунок 4.4 – Введена адреса серверу у поле адреси

При успішному підключенні до сервера, користувач буде перенаправлений на сторінку авторизації. На цій сторінці він зможе ввести свої облікові дані, такі як ім'я користувача та пароль, для отримання доступу до функціональності додатку. Сторінка авторизації забезпечує захищений доступ до додатку та контролює права доступу для кожного користувача.

У випадку введення неправильного логіна та/або пароля, відсутності зв’язку з базою даних буде виведено відповідні повідомлення.

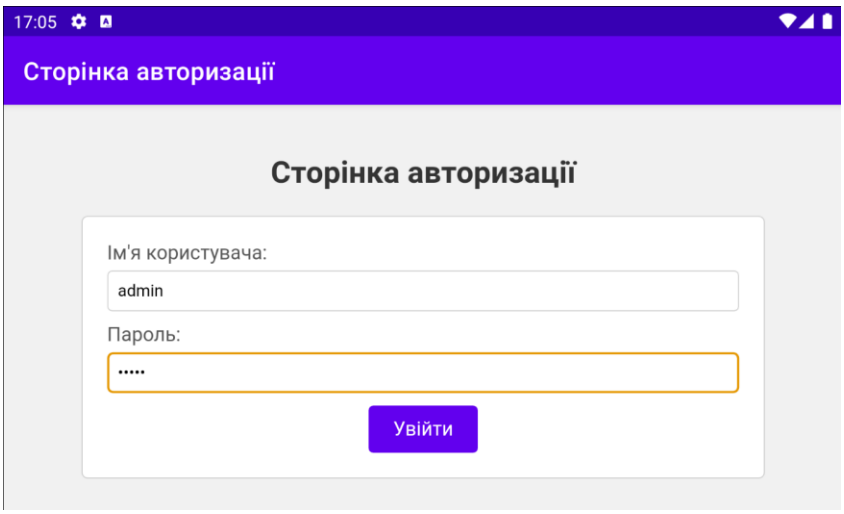


Рисунок 4.5 – Сторінка авторизації у систему керування сервером

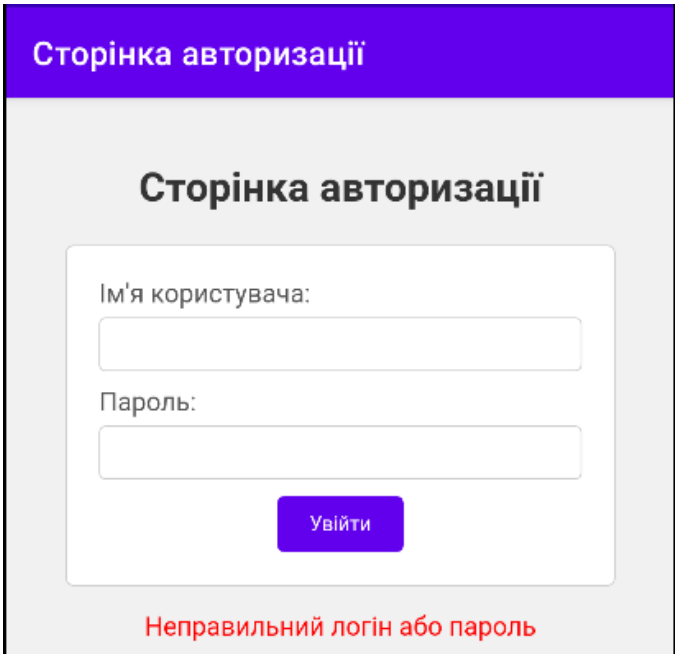


Рисунок 4.6 – Повідомлення про неправильний логін або пароль

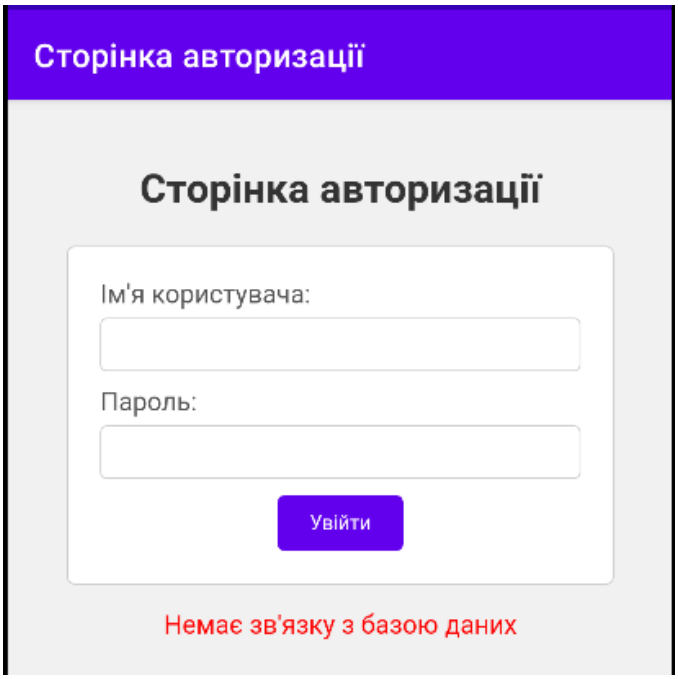


Рисунок 4.7 – Повідомлення про відсутність зв’язку з базою даних

Після успішної авторизації користувач отримає повний доступ до функцій та може почати використовувати додаток для своїх потреб.

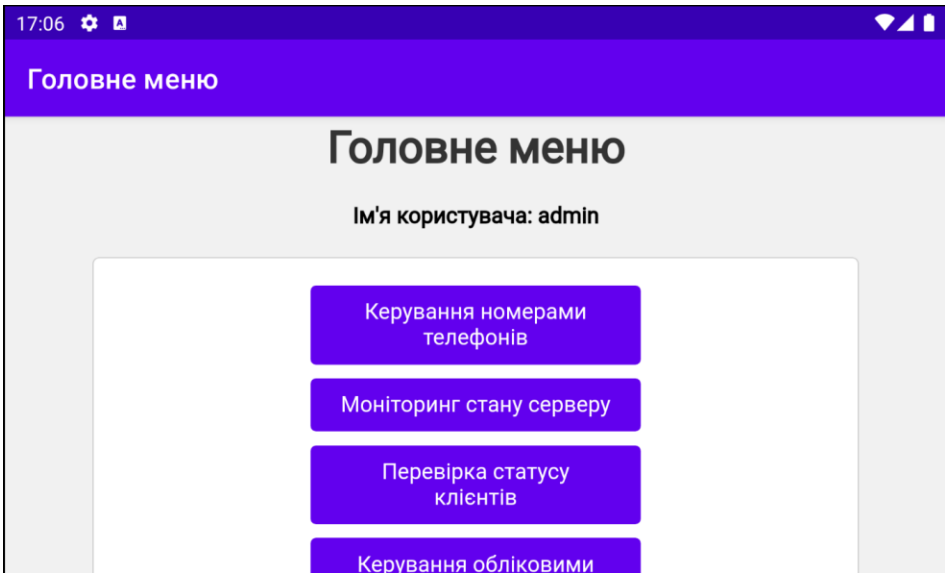


Рисунок 4.8 – Головне меню

На сторінці керування номерами телефонів, функціонал розділяється на два основних блоки: «Створення нового абонента» та «Список абонентів».

У блоку «Створення нового абонента» користувач може створити новий номер телефону. В цьому розділі відображається форма для введення необхідних даних, таких як номер телефону, пароль та вказати чи знаходиться абонент за NAT. Користувач може заповнити ці поля та натиснути на кнопку «Створити користувача», щоб додати новий номер до системи. Після створення нових абонентів обов'язково потрібно натиснути кнопку «Застосувати зміни» для того, щоб перезавантажити конфігураційний файл серверу телефонії.

У блоку «Список абонентів» відображаються всі існуючі номери телефонів. Користувач може переглядати список абонентів, який містить інформацію про кожен номер телефону, його тип та чи знаходиться він за NAT. Крім того, користувач може видалити існуючі номери з системи, якщо вони більше не потрібні або були помилково створені.

Ця структура дозволяє користувачеві зручно керувати номерами телефонів, забезпечуючи можливість створення нових номерів та перегляду/видалення існуючих зручним та логічним способом.

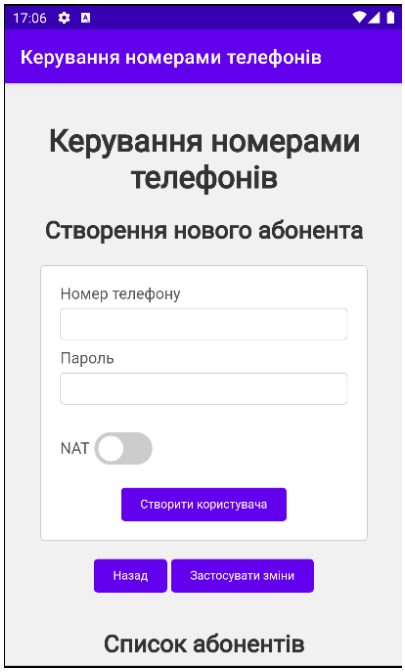


Рисунок 4.9 – Сторінка керування номерами телефонів

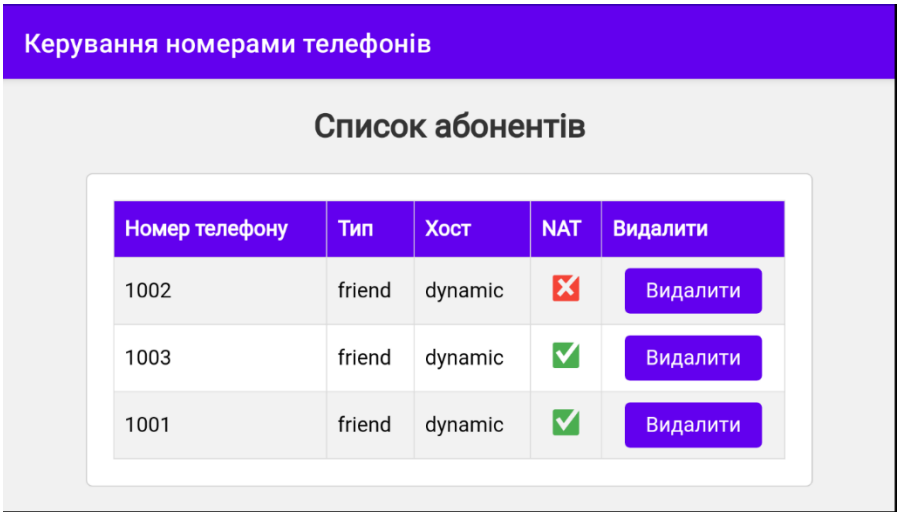


Рисунок 4.10 – Список створених абонентів

При спробі створити користувача, застосунок виконує перевірку чи існує абонент та проводить додаткову перевірку безпеки. Якщо користувач існує, буде виведено відповідне повідомлення. Наступним кроком аналізує введений пароль та перевіряє його складність. Якщо виявлено, що пароль не відповідає встановленим критеріям безпеки (пароль має складатися хоча б з однієї літери, цифри та спеціального символу, та не повинен бути коротшим за 8 символів), застосунок виводить повідомлення про необхідність обрати сильніший пароль.

Це зроблено з метою забезпечення безпеки системи та захисту користувачів від можливих атак та несанкціонованого доступу.

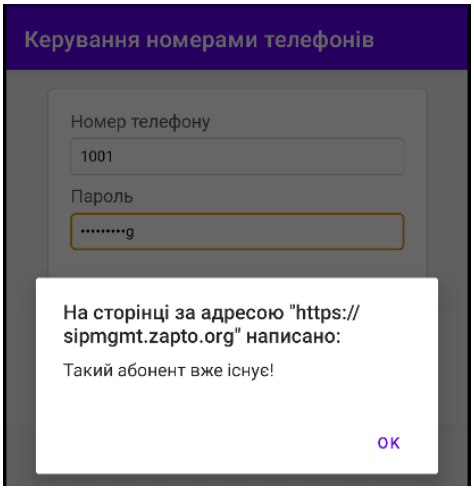


Рисунок 4.11 – Спроба створення існуючого абонента

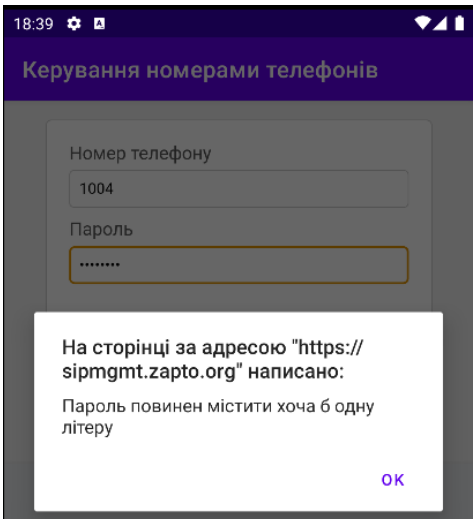


Рисунок 4.12 – Спроба створення абонента зі слабким паролем

На сторінці моніторингу виводиться результат команди терміналу systemctl status asterisk. Ця веб-сторінка відображає статус Asterisk PBX, системи цифрової телефонії. На сторінці наведена інформація про поточний стан служби Asterisk. Наводяться основні деталі про службу, такі як назва служби, робоча директорія, час активності, посилання на документацію, основний PID, використання пам'яті та використання процесора.

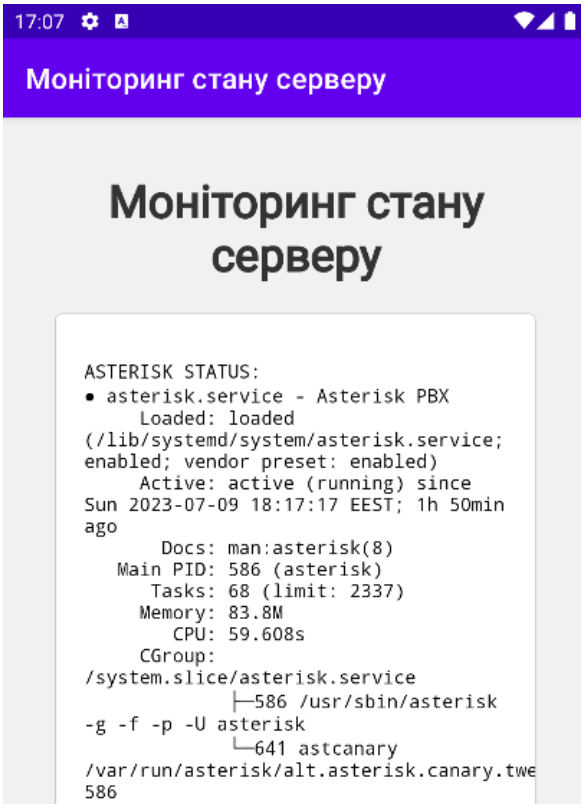


Рисунок 4.13 – Сторінка перегляду стану серверу телефонії

На веб-сторінці перегляду стану SIP клієнтів подається інформація про статус кожного номера, який підключений до системи. Статус може бути одним з наступних:

– Unreachable: номер недоступний або не зареєстрований у системі.

– Lagged: номер може мати деякі затримки або проблеми з підключенням, але все ще зареєстрований.

– OK: номер належним чином зареєстрований і має стабільне підключення.

Крім того, для кожного номера вказується його IP-адреса.

Ця сторінка надає зручний спосіб контролювати статус і доступність SIP номерів у системі, дозволяючи вам вчасно виявляти проблеми з підключенням і вживати необхідних заходів для їх вирішення.

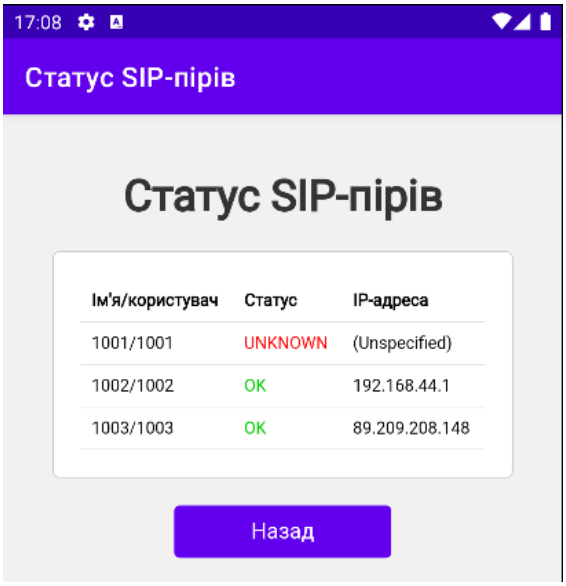


Рисунок 4.14 – Сторінка перегляду стану клієнтів

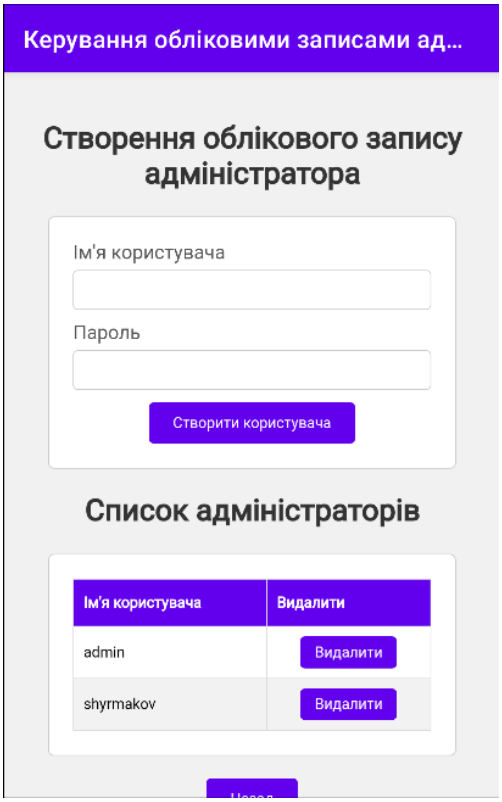


Рисунок 4.15 – Сторінка керування обліковими записами адміністраторів

Додаток автоматично визначає мову інтерфейсу залежно від налаштувань мови системи на пристрої Android. Це забезпечує зручну та інтуїтивно зрозумілу взаємодію для користувачів з різних країн. Незалежно від того, чи використовується додаток на пристрої Android або веб-версія через веб-

переглядач, мова інтерфейсу автоматично пристосовується до мови системи або мови веб-переглядача. Таким чином, користувачам забезпечується зручне та персоналізоване використання додатку відповідно до їхніх мовних налаштувань.

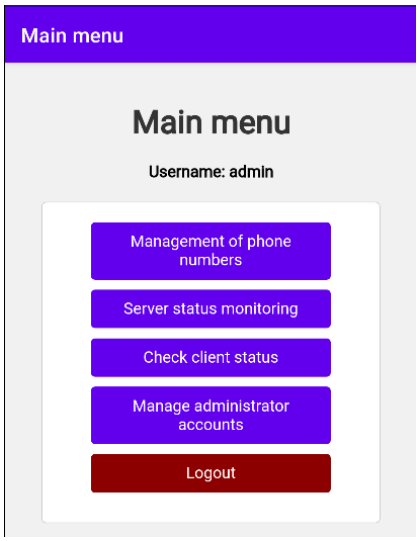


Рисунок 4.16 – Користувацький інтерфейс англійською мовою

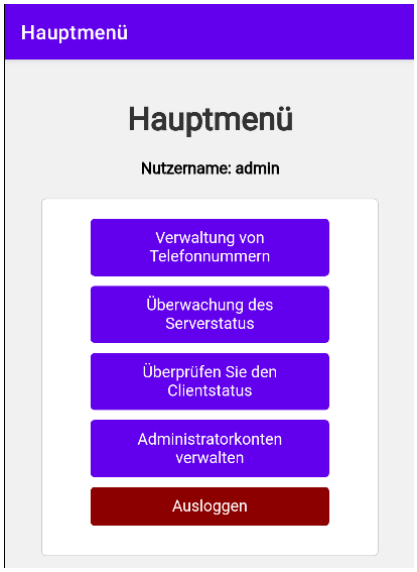


Рисунок 4.17 – Користувацький інтерфейс німецькою мовою

ВИСНОВКИ

В ході кваліфікаційної роботи на тему «Комп’ютерна система ДП «Антонов» з реалізацією побудови, налаштування та безпеки корпоративної мережі з підтримкою IP-телефонії» був проведений огляд підприємства, розроблена модель комп'ютерної мережі та створений додаток для керування сервером IP-телефонії. Результатом роботи є розроблена система, яка відповідає потребам ДП «Антонов» та сприяє ефективному функціонуванню його корпоративної мережі.

Під час огляду підприємства були визначені вимоги та особливості комп'ютерної системи, що відображають його поточну інфраструктуру, обсяг роботи та вимоги до безпеки. З цими даними була розроблена модель комп'ютерної мережі, яка відображає інфраструктурну архітектуру та налаштування мережевих компонентів.

Важливим етапом проекту було створення додатка для керування сервером IP-телефонії, який відповідає вимогам та дозволяє ефективно керувати різними аспектами сервера.

Крім того, додаток має потенціал для подальшого розвитку і вдосконалення. З можливістю додавання нових функціональних можливостей і розширення можливостей керування, додаток може відповідати зростаючим потребам і вимогам користувачів з часом.

Загальний висновок полягає в тому, що розроблена комп'ютерна система ДП «Антонов» з реалізацією корпоративної мережі та IP-телефонії відповідає потребам підприємства і забезпечує надійну та безпечну інфраструктуру з ефективним управлінням та підтримкою користувачів. Результати роботи можуть бути використані для подальшого розвитку та оптимізації системи, щоб забезпечити ще більшу продуктивність та задоволення користувачів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Авіація є ключовим драйвером глобального економічного розвитку [Електронний ресурс] // Режим доступу: https://aviationbenefits.org/economic-growth/

2. Стаття «Всесвітня туристична організація: 58% усіх міжнародних туристів подорожували літаком у 2018 році» | CAPA [Електронний ресурс] // Режим доступу: https://centreforaviation.com/news/unwto-58-of-all-international-tourists-travelled-by-air-in-2018-933705/

3. EVER GIVEN: Всесвітній збиток – GrECo Risk Management [Електронний ресурс] // Режим доступу: https://greco.services/a-world-loss-event-and-its-far-reaching-consequences-ever-given/

4. Поле на крилі, або історія сільгоспавіації в Україні [Електронний ресурс] // Режим доступу: https://agravery.com/uk/posts/show/pole-na-krili-abo-istoria-silgospaviacii-v-ukraini

5. Повітряні Сили Збройних Сил України [Електронний ресурс] // Режим доступу: https://www.mil.gov.ua/ministry/sklad-zbrojnix-sil-ukraini/povitryani-sili/

6. Закон України «Про розвиток літакобудівної промисловості» [Електронний ресурс] // Режим доступу: https://zakon.rada.gov.ua/laws/show/2660-14#Text

7. Послуги ДП «Антонов» [Електронний ресурс] // Режим доступу: https://www.antonov.com/services

8. База «Антонова» працює у Лейпцигу [Електронний ресурс] // Режим доступу: https://www.wing.com.ua/content/view/33076/37/

ДОДАТОК А

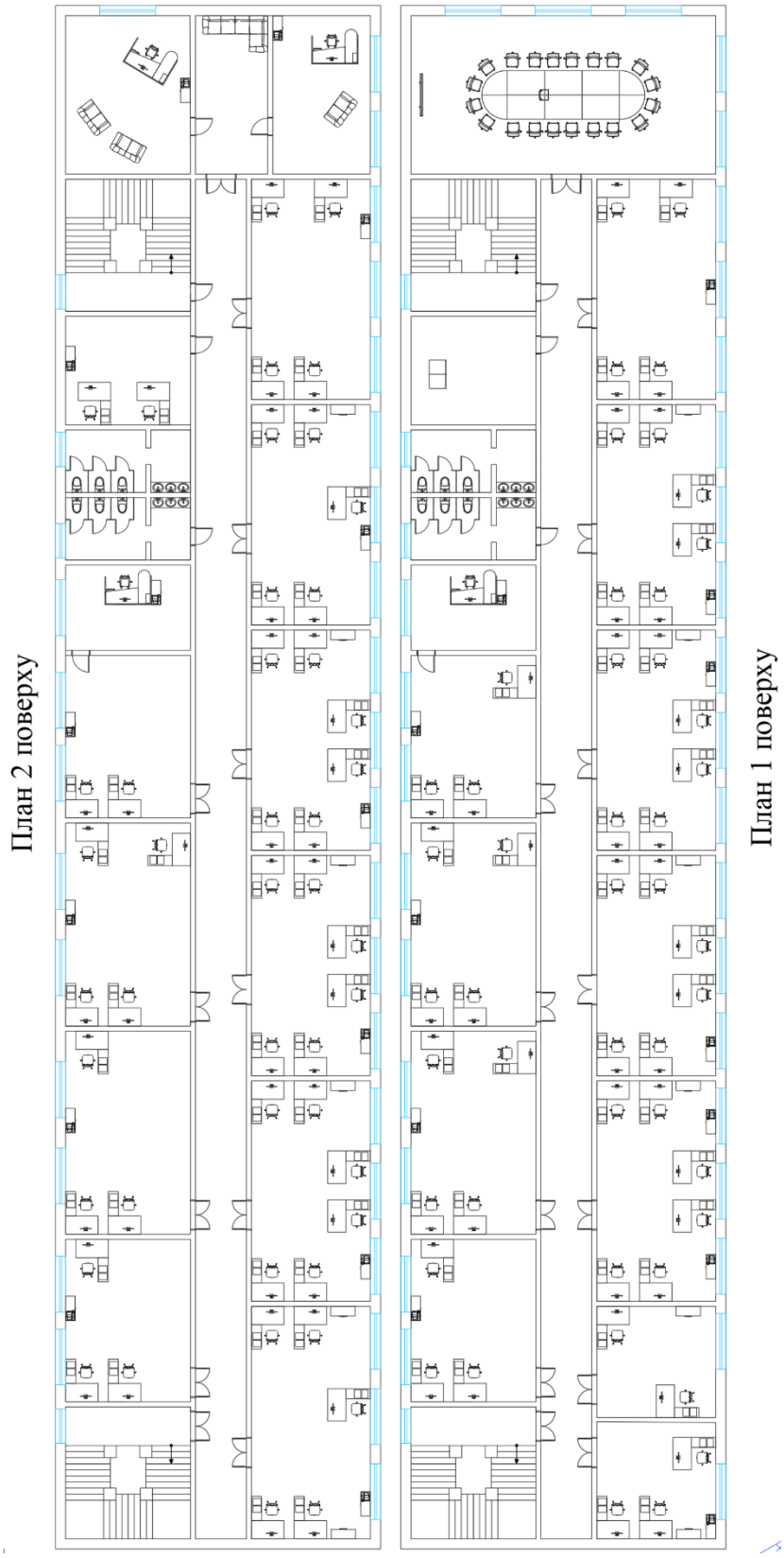
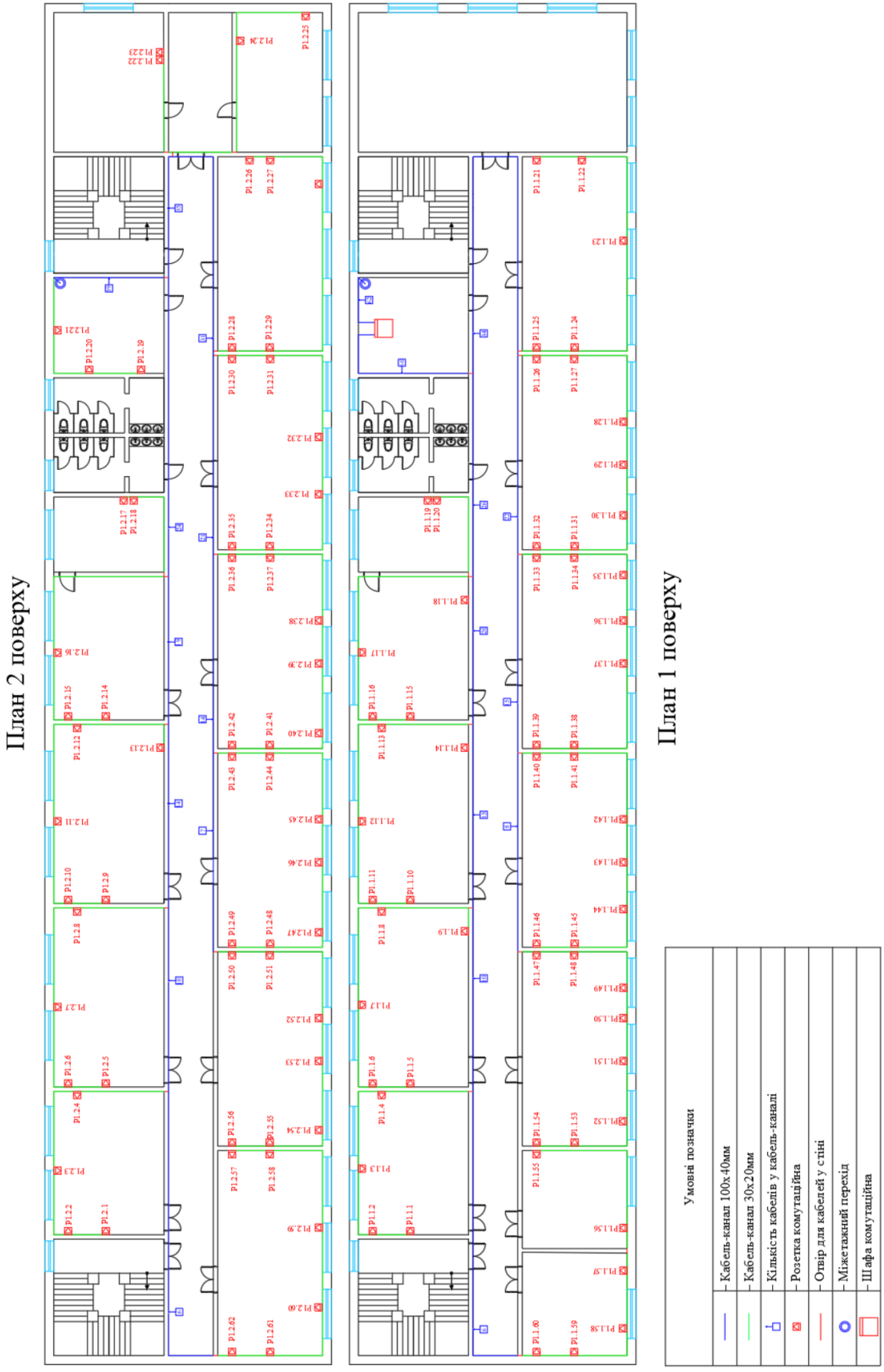


Схема розташування пристроїв в головному офісі

ДОДАТОК Б



Структурована кабельна система головного офісу