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 Фахардінова Владислава Рамільєвича
(ПІБ)
академічної групи 123-19-1
(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 юридичної компанії "Justice" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі "
(назва за наказом ректора)

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

Дніпро
2023

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

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавр

студента Фахардінова В.Р. **академічної групи** 123-19-1
(прізвище та ініціали) (шифр)

спеціальності 123 «Комп'ютерна інженерія»

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

на тему "Комп'ютерна система юридичної компанії "Justice" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі "

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

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постановка завдання	17.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	23.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	26.05.2023
Розробка компонента системи	Виконується детальна розробка компонента системи	27.05.2023

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

Дата видачі 19.12.2022

Дата подання до екзаменаційної комісії 06.06.2023

Прийнято до виконання _____ Фахардінов В.Р.

РЕФЕРАТ

Пояснювальна записка: 71с., 23 рис., 12 табл., 1 дод., 6 джерел.

ВІДДІЛ, СХЕМА, МЕРЕЖА, ОБЛАДНАННЯ, РОЗРОБКА, ПРОТОКОЛ, КОМП’ЮТЕР

Дипломна робота присвячена розробці корпоративної мережі для юридичної компанії Justice. Об'єктом дослідження є створення ефективної та безпечної інфраструктури мережі, що задовольнятиме потреби компанії в обміні даними, спільній роботі та забезпеченні конфіденційності важливої інформації.

Метою даної роботи є розробка та налаштування корпоративної мережі, яка відповідатиме потребам компанії Justice. Для досягнення цієї мети використовувались сучасні технології та найкращі практики в галузі мережевого проектування і впровадження.

У роботі було проведено детальний аналіз вимог компанії до мережі, враховуючи розмір організації, типи послуг та комунікаційні потреби різних відділів. Розроблено оптимальну архітектуру мережі, включаючи сегментацію, використання VLAN та VPN для забезпечення безпеки та ефективного розподілу ресурсів.

Впровадження корпоративної мережі Justice включає установку та налаштування мережевого обладнання, налаштування безпеки та доступу, а також перенесення наявних даних та інтеграцію з існуючими системами компанії.

Результатом даної дипломної роботи є розроблена та впроваджена корпоративна мережа, яка відповідає потребам юридичної компанії Justice. Це сприяє покращенню комунікації, забезпеченню безпеки даних та підвищенню продуктивності праці співробітників.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

IP – Інтернет протокол.

КМ – комп’ютерна мережа.

КС – комп’ютерна система.

ПК – персональний комп’ютер.

VPN – (Virtual Private Network) – є технологією, яка забезпечує безпечне та приватне з'єднання між віддаленими мережами або пристроями через публічну мережу, таку як Інтернет.

DHCP – (Dynamic Host Configuration Protocol) — є протоколом мережевого рівня, що використовується для автоматичного надання мережевих налаштувань пристроям у комп'ютерних мережах.

VLAN – (Virtual Local Area Network) – е логічна група пристроїв в комп'ютерній мережі, яка функціонує незалежно від фізичної інфраструктури мережі.

ACL – (Access Control List) – це механізм контролю доступу, який використовується в комп'ютерних мережах для регулювання доступу до ресурсів і сервісів.

NAT – (Network Address Translation) – є технологією, що використовується в комп'ютерних мережах для перетворення IP-адрес.

ВСТУП

ВСТУП

Сучасні юридичні компанії стикаються з безпрецедентними викликами та змінами в цифровому середовищі. Відчутне зростання обсягу інформації, потреба у безпековому обміні даними, ефективна комунікація та збереження конфіденційності стають життєво важливими для успішного функціонування юридичних практик. У цьому контексті розробка корпоративної мережі для юридичної компанії "Justice" має вирішальне значення.

Світові тенденції розв'язання поставлених задач свідчать про постійний розвиток технологій мережевого забезпечення та безпеки інформації. Розробка корпоративних мереж стає більш інтегрованою та розширеною, використовуючи передові рішення, такі як віртуалізація мереж, розподілені системи зберігання даних та застосування хмарних технологій.

Метою даної кваліфікаційної роботи є розробка та налаштування корпоративної мережі для компанії "Justice", що відповідає її конкретним потребам та вимогам. Цей проект спрямований на створення інфраструктури, яка забезпечить швидкий, безпечний та надійний обмін даними, ефективну співпрацю між співробітниками та покращення управлінських процесів.

Дана дипломна робота використовує накопичений досвід та передові розробки для створення інтегрованої мережевої інфраструктури, яка забезпечить потреби юридичної компанії "Justice" і відповідає сучасним вимогам галузі.

Результати цього дипломного проекту відіграють важливу роль у покращенні роботи юридичної компанії "Justice", підвищенні її конкурентоспроможності та забезпеченні високого рівня захисту даних.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умови застосування КС

Сфера юридичних послуг охоплює широкий спектр діяльності, пов'язаної із правовим регулюванням різних сфер життя, таких як бізнес, фінанси, нерухомість, спадщина, цивільні та кримінальні права, сімейне та трудове право, інтелектуальну власність тощо.

Юридичні послуги можуть включати консультації, підготовку документів, представлення інтересів клієнтів у суді та інших органах, а також вирішення юридичних спорів. До сфери юридичних послуг також можуть входити послуги з супроводу угод, юридичної експертизи, арбітражу та медіації.

Юридичні послуги надаються як юридичними фірмами та адвокатськими конторами, і незалежними юристами. Клієнтами юристів можуть бути як фізичні, так і юридичні особи.

Комп’ютерні мережі мають широке застосування у сфері юридичних послуг. Вони дозволяють здійснювати швидкий та ефективний обмін інформацією між різними сторонами. Це корисно у правових процесах, де швидкий доступ до інформації може бути критичним. Також вони використовуються для збереження та організації юридичних документів. Це дозволяє забезпечувати швидкий та легкий доступ до необхідної інформації, а також захищати документи від втрати або пошкодження.

Узагалі, комп'ютерні мережі покращують ефективність та продуктивність роботи в юридичній сфері, знижують витрати та збільшують доступність до необхідної інформації.

1.2 Характеристика і структура об’єкта впровадження

1.2.1 Характеристика об’єкта впровадження

Об’єкт впровадження – офіс юридичної компанія «Justice».

«Justice» - це українська юридична компанія, заснована у 2005 році, що спеціалізується на наданні юридичних послуг в різних сферах права, зокрема у корпоративному, трудовому, податковому, цивільному, кримінальному, медичному та інших галузях.

Надання юридичних послуг у сфері бізнесу є головною концепцією Юридичної компанії “Justice”. Юридичний супровід діяльності підприємства зведе до мінімуму господарські, податкові, адміністративні, трудові, кримінальні та інші ризики.

Юридичний супровід бізнесу включає в себе:

1. Юридичний аутсорсинг. Юридичний аутсорсинг є комплексом заходів, що забезпечують правове обслуговування підприємців, організацій, інтернет-магазинів та виробництва, за щомісячну плату згідно з договором. Будь-які правові проблеми, які можуть виникнути у процесі діяльності організації, будуть вирішуватись командою юристів вищої кваліфікації.[1]
2. Податкові спори. Однією з найскладніших галузей права є податкова. Компанія «Justice» надає юридичні послуги адвоката з податкових злочинів у вирішенні різних юридичних питань, у тому числі й податкових перевірок та спорів щодо них.[1]
3. Тендерний супровід. Юридична компанія «Justice» надає кваліфіковану юридичну допомогу при тендерному супроводі бізнесу.[1]
4. Судова практика. Юристи компанії «Justice» супроводжують клієнтів на всіх етапах судового розгляду незалежно від того, ким являється клієнт – позивачем чи відповідачем: починаючи від оформлення досудових претензій, складання позовних заяв, поданням інтересів бізнесу в судах першої, апеляційної та

касаційної інстанцій, і закінчуючи примусовим виконанням рішення суду.[1]

5. Господарські спори. Господарські спори – це конфлікти та розбіжності, що виникають у процесі будь-якої підприємницької діяльності. За змістом переважна більшість господарських суперечок виникає у зв'язку з невиконанням чи неналежним виконанням контрагентом умов договору.[1]
6. Адміністративні спори. Компанія «Justice» пропонує своїм клієнтам послуги з врегулювання всіх правових питань, які пов'язані з державними органами будь-якого рівня та спрямованості.[1]
7. Трудові спори. Трудові спори – це конфлікти між роботодавцем та підлеглим, групою підлеглих чи всім колективом. Такі суперечки становлять чималу частку у проблемах бізнесу, їх відносять до категорії найскладніших проблем ведення бізнесу.[1]
8. Складання документації. Компанія надає допомогу у складанні, розробці та аналізі будь-якої документації.[1]
9. Реєстрація бізнесу. Юридична компанія «Justice» пропонує кваліфіковану юридичну допомогу при реєстрації бізнесу.[1]
10. Ліквідація бізнесу. Ліквідація бізнесу процес набагато складніший, ніж його реєстрація. Юридична компанія «Justice» пропонує висококваліфіковану юридичну допомогу для швидкої та безпечної ліквідації бізнесу.[1]
11. Інтелектуальна власність. Юристи компанії «Justice» пропонують кваліфіковану юридичну допомогу для захисту інтелектуальної власності. Інтелектуальна власність включає: авторське право чи право, суміжне з авторським, патентне право, нетрадиційні об'єкти індивідуальної власності, засоби індивідуалізації (торгівельні марки).[1]

1.2.2 Розміщення структурних підрозділів підприємства

Компанія має два офіси - головний офіс та віддалений. Головний офіс розміщено за адресою пр-т. Дмитра Яворницького, 5, м. Дніпро, Україна, 49005. Віддалений офіс розташовано за адресою вул. Святослава Хороброго, 12а. відстань між офісами по прямій – 2650 метрів.

Георозміщення офісів зображено на рисунку 1.1.

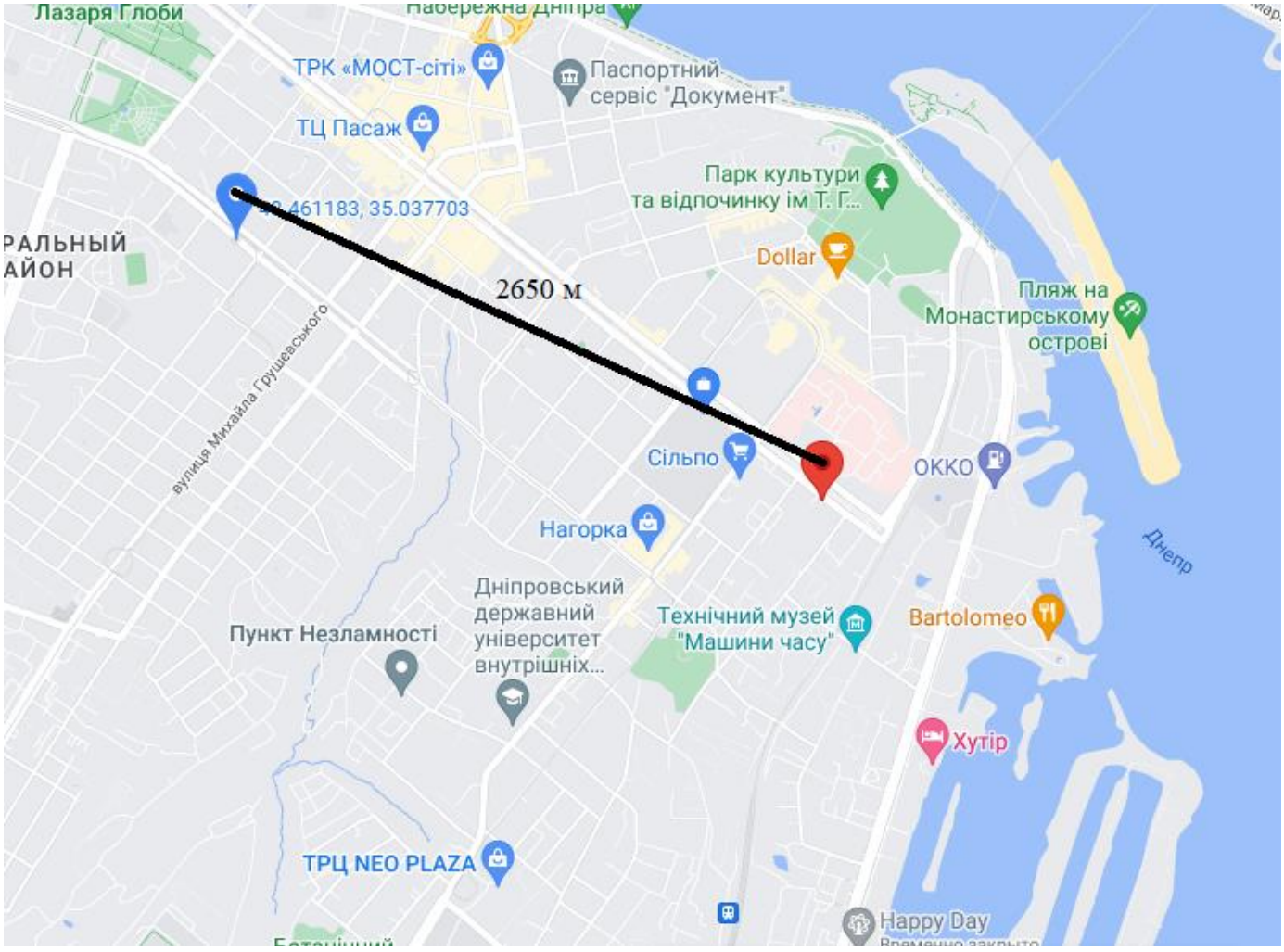

Рисунок 1.1 – Георозміщення офісів компанії

1.2.3 Організаційна структура підприємства

Компанія має ієрархічну організаційну структуру. Ієрархічна організаційна структура має пірамідальну форму, де на вершині знаходиться керівництво компанії, а на нижніх рівнях розташовані юристи та адміністративний персонал.

Керівництво компаніїзазвичай визначає стратегічні цілі компанії, розробляє бізнес-плани та приймає важливі рішення, що стосуються фінансового управління та розвитку компанії.

Юристи є ключовими працівниками компанії, які займаються наданням юридичних послуг. Юристи організовані в департаменти з різних практичних напрямків, таких як корпоративне право, податкове право, нерухомість, судові справи тощо. Кожен департамент має власного керівника.

Ієрархічна структура має наступні переваги:

- Чітке розподілення обов'язків та відповідальності
- Ефективне управління
- Підвищення професійної кваліфікації
- Простота управління та звітування

Однак, ієрархічна структура також має свої недоліки, зокрема:

- Повільний рух інформації
- Обмежена свобода вибору та ініціатива
- Негативний вплив на мотивацію
- Ризик конфліктів

Схему організаційної структури юридичної компанії «Justice» наведено на рисунку 1.2.

Рисунок 1.2 – Організаційна структура компанії «Justice»

1.2.4 Розробка топологічної схеми розміщення структурних підрозділів підприємства

На рисунку 1.3 наведено топологічну схему розміщення структурних підрозділів підприємства. На схемі вказано відділ адвокатів з кримінальних справ, розміщений у головному офісі, та частину відділу судової практики, який розміщено у будівлі віддаленого офісу.

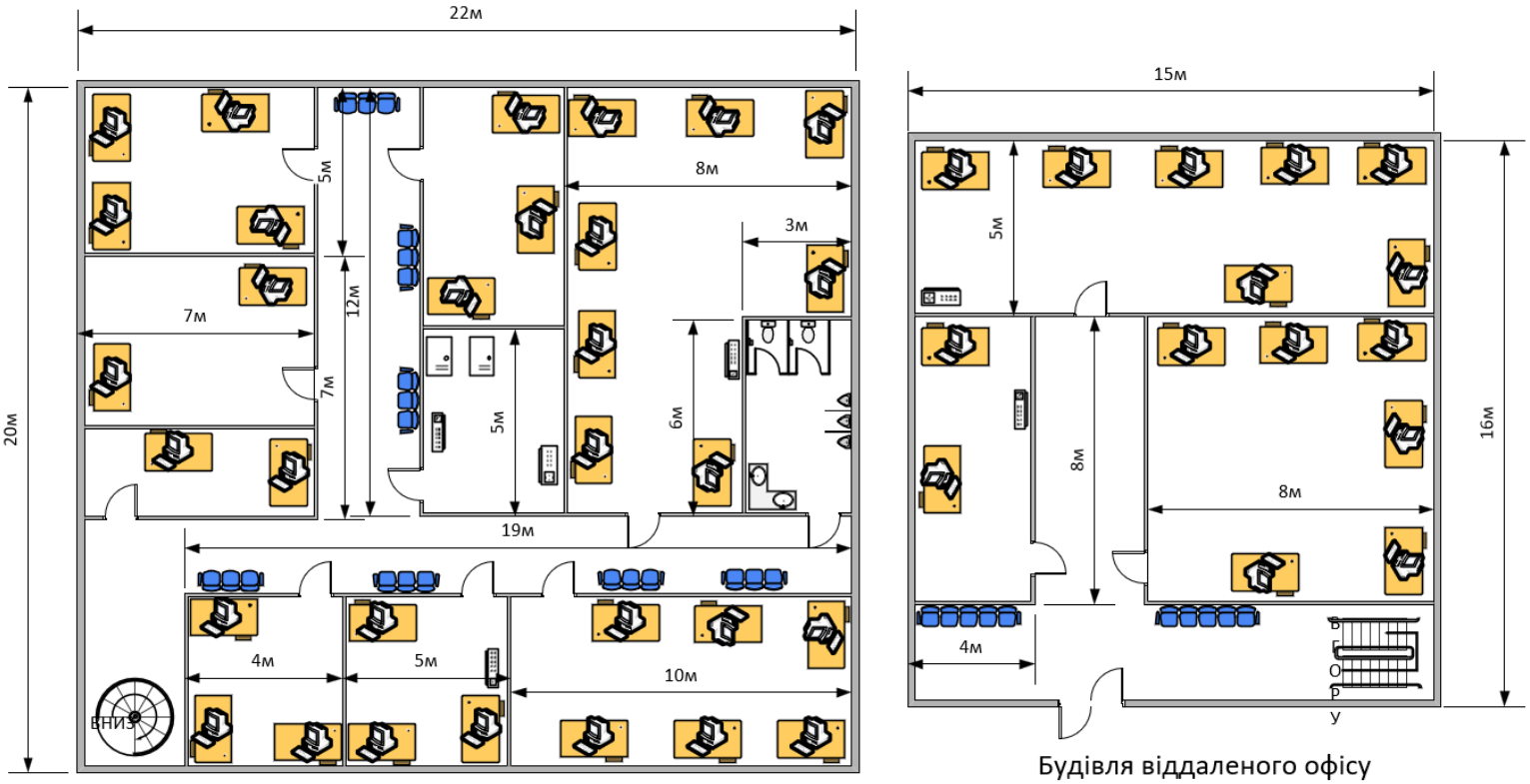

Рисунок 1.3 – Структурна схема підприємства

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

Юридична компанія, як будь-яка інша компанія, потребує інформаційного забезпечення для ефективної роботи. Технології, що використовуються в інформаційному забезпеченні компанії:

1. Інформаційні системи управління. Системи управління є ключовим елементом інформаційного забезпечення юридичної компанії. Вони допомагають керівництву компанії керувати бізнесом, контролювати фінанси, збирати і аналізувати дані про клієнтів та керувати процесом виконання робіт.[2]
2. Електронна пошта та електронний документообіг. Ці технології дозволяють співробітникам компанії обмінюватися інформацією та документами швидко та ефективно, незалежно від географічного розташування.[2]

3. Клієнтські портали та онлайн-сервіси. Онлайн-портал дозволяє клієнтам отримати доступ до своїх документів, звернутися до адвокатів компанії та отримати інші послуги.[2]
4. Математичні методи та аналітика. Використання математичних методів та аналітики допомагає юридичній компанії зрозуміти дані, які вона збирає, та забезпечити їх ефективний аналіз. Аналіз даних може допомогти компанії зрозуміти, які клієнти віддають перевагу, які послуги найбільш популярні, а також виявити нові можливості для бізнесу.[2]

1.4 Аналітичний огляд існуючих способів обробки та передачі інформації

Юридичні компанії мають значну кількість інформації, що потребує обробки, зберігання та передачі. Ця інформація може включати конфіденційні дані клієнтів, фінансові записи та інші чутливі дані, які вимагають високого рівня захисту. У зв'язку з цим, в юридичних компаніях використовуються різні способи обробки та передачі інформації, що варіюються за складністю, швидкістю та вартістю.

Системи аналізу даних дозволяють компанії отримувати більш детальну інформацію про свою діяльність та виконувати аналітичну роботу. Ці системи часто використовують методи машинного навчання та інші математичні методи для аналізу даних та виявлення закономірностей. За допомогою систем аналізу даних юридичні компанії можуть покращити своє прийняття рішень, забезпечити більш ефективне використання ресурсів та покращити якість своїх послуг.

Хмарні технології дозволяють зберігати та обробляти дані на віддалених серверах та надавати доступ до них через Інтернет. Ці технології забезпечують високий рівень доступності та безпеки даних, а також забезпечують більшу мобільність та можливість працювати з даними з будь-якої точки світу. Хоча провайдери надійно захищають хмару, завжди є ризик злому. Через це

використання хмарних технологій може бути ризикованим для юридичної компанії. З іншого боку хмара захищає дані від фізичних небезпек, наприклад пожежі в офісі чи виходу обладнання з ладу.[3]

Система електронного зберігання даних - це спеціальна програма, що використовується для зберігання та організації інформації в електронному вигляді. Реалізація принципів електронного документообігу на базі новітніх інформаційних технологій за допомогою сучасного апаратного та програмного забезпечення дасть можливість створити на підприємстві єдиний інформаційний простір електронного документообігу, інтегруючи в інформаційний вузол усі системи передавання та прийому ЕД. Хоч дані системи значно полегшують роботу, проте варто враховувати їх вразливість до вірусів та хакерів, що може бути критичним для юридичної компанії.[4]

Системи керування взаємодією з клієнтами (CRM) можуть бути корисними для юридичних компаній, оскільки вони дозволяють зберігати та організовувати інформацію про клієнтів та взаємодії з ними. Основна перевага CRM-системи в тому, що вона може принести користь практично будь-якому організаційному підрозділу. Вона дозволяє підвищити якість обслуговування без залучення додаткового персоналу.[5]

1.5 Постановка завдання та мета роботи

Мета роботи – розробка корпоративної мережі для юридичної компанії «Justice», що забезпечує ефективний обмін даними та інформацією між співробітниками компанії, а також забезпечує високий рівень безпеки та захисту конфіденційної інформації.

Для цього необхідно виконати наступні завдання:

- аналіз потреб та вимог юридичної компанії "Justice" до корпоративної мережі;
- формування технічних вимог до комп’ютерної системи на основі проведеного аналізу;

- вибір необхідного обладнання для побудови мережі та складання його специфікації;
- аналіз мережевого трафіку;
- розробка фізичної та логічної топології мережі з урахуванням вимог та потреб компанії;
- конфігурація обраного обладнання;
- налаштування безпеки на обладнанні;
- тестування роботи налаштованої мережі;
- розробка компонента системи з використанням технології IoT.

Корпоративна мережа повинна бути забезпечена високим рівнем надійності та доступності. Вона повинна забезпечувати швидкий та стабільний обмін інформацією між всіма пристроями в мережі, а також забезпечувати захист від зовнішніх загроз.

1.6 Визначення можливих напрямків рішення поставлених завдань

Існує декілька способів створення корпоративної мережі для юридичної компанії, залежно від потреб, вимог та можливостей компанії. Нижче наведено декілька можливих варіантів.

Побудову корпоративної мережі компанії доцільно виконувати на основі технології Ethernet. Ethernet є стандартом для проводових мереж та широко використовується у більшості комп'ютерних мереж. Це забезпечує сумісність між різними пристроями та мережами. Ethernet може передавати дані з високою швидкістю, що робить його ідеальним для швидкісного доступу до Інтернету, обміну файлами та іншими задачами, які потребують великої пропускної здатності. Ethernet є дуже надійним, оскільки він має фізичний кабель для передачі даних. Це знижує ризик втрати даних через перерву у з'єднанні або інші технічні проблеми. Ethernet легко налаштовується та використовується. Більшість комп'ютерів та інших пристроїв мають вбудований роз'єм Ethernet, що дозволяє легко підключати їх до мережі.

У відділі реєстрації та ліквідації бізнесу варто реалізувати технологію VLAN. VLAN – це технологія, яка дозволяє розділити одну фізичну мережу на декілька логічних мереж (віртуальних), які можуть існувати незалежно одна від одної. Кожна віртуальна мережа може мати свій власний набір користувачів та власні параметри мережі, такі як IP-адреси, маски підмереж, шлюзи за замовчуванням, інші налаштування мережі та політики безпеки. Дана технологія допоможе відокремити на різні робочі групи працівників, які займаються реєстрацією та ліквідацією бізнесу відповідно.

Для забезпечення безпеки у мережі необхідно встановити паролі для кожного мережевого пристрою, для віддаленого доступу варто використовувати захищений протокол SSH замість відкритого Telnet. Також потрібно реалізувати технологію VPN. Віртуальна приватна мережа (VPN) – це технологія, яка дозволяє підключати комп'ютери та інші пристрої до мережі Інтернет за допомогою зашифрованого каналу, який забезпечує приватність та безпеку передачі даних. Це допоможе значно підвищити безпеку мережі, що є важливим для юридичної компанії.

При налаштуванні маршрутизації варто використати протокол OSPF замість пропрієтарного EIGRP, так як OSPF працює з будь яким мережевим обладнанням, що значно спрощує масштабування мережі за необхідності.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури та функціонування системи

Замовник, для якого виконується розробка корпоративної мережі, надав для проєктування схему загальної архітектури корпоративної мережі (рисунок 2.1). Вся розробка мережі повинна проводитись згідно цієї схеми.

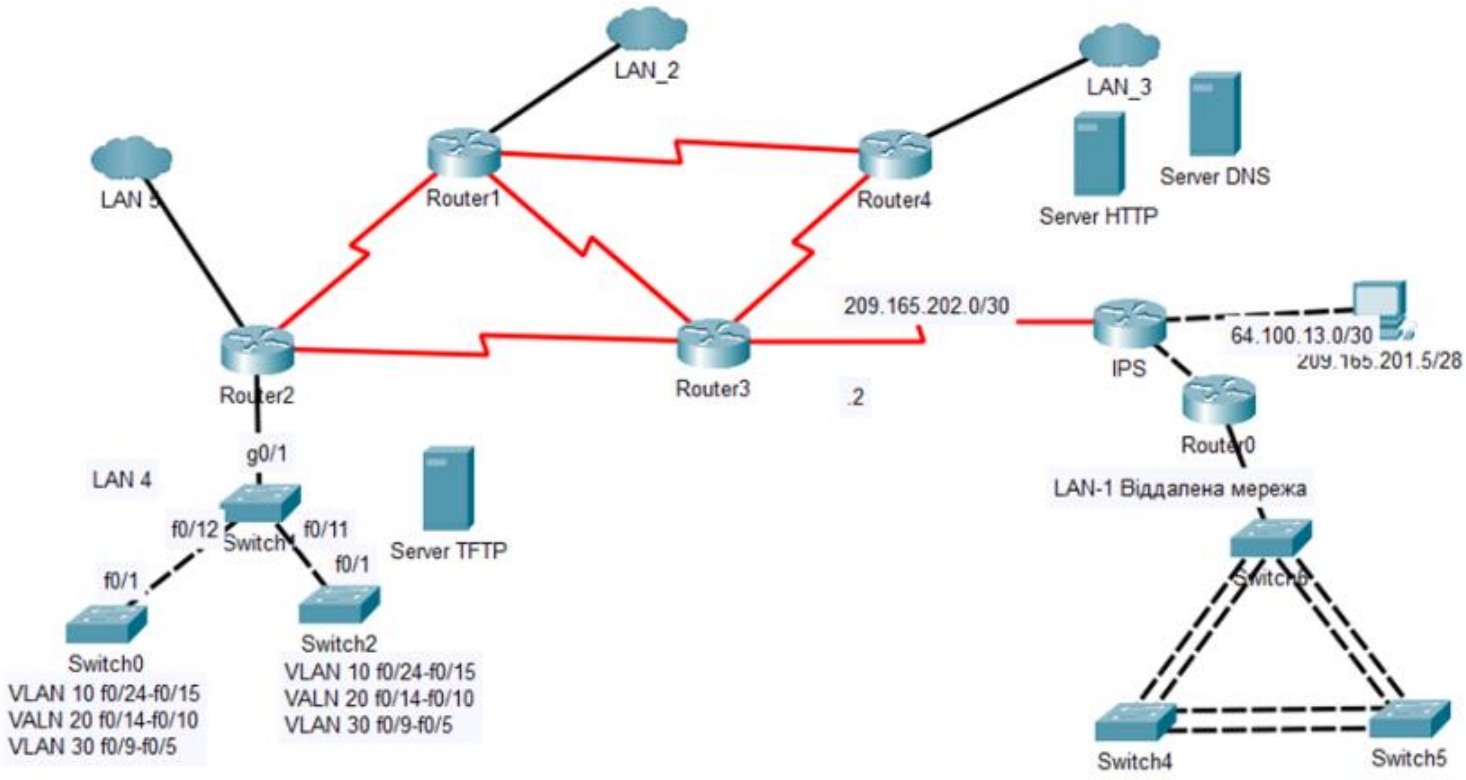

Рисунок 2.1 – Загальна архітектура корпоративної мережі

Також замовник визначив кількість вузлів, які повинні бути розміщені у кожній з підмереж компанії (таблиця 2.1).

Таблиця 2.1 – Кількість вузлів для підмереж компанії

LAN1(Віддалена мережа) Судова практика	LAN2 Супровід бізнесу	LAN3 Земельні спори	LAN4 Адвокати	LAN5 Відділ кадрів
35	44	18	31	15

2.1.1.2 Вимоги до способів і засобів зв’язку між компонентами комп’ютерної системи

Зв’язок усіх пристроїв у мережі потрібно здійснювати за допомогою технології Ethernet з інтерфейсами різної пропускної здатності. Так, для підключення ПК до мережі необхідно використати інтерфейси FastEthernet, для з’єднання комунікаційного обладнання з маршрутизаторами – інтерфейси GigabitEthernet, для з’єднання маршрутизаторів з іншими маршрутизаторами – Serial інтерфейси.

Для забезпечення зв’язку мережі головного офісу з мережею віддаленого офісу необхідно впровадити технологію VPN. Щоб забезпечити вузлам доступ до інтернету потрібно виконати налаштування конфігурації NAT на маршрутизаторах, під’єднаних до ISP.

2.1.1.3 Вимоги до характеристик взаємозв'язків комп’ютерної системи із суміжними системами

Комп'ютерна система повинна забезпечувати можливість обміну даними з іншими суміжними системами. Для цього вона повинна підтримувати стандарти комунікації, такі як REST, SOAP, JDBC, ODBC. Комп'ютерна система повинна бути стабільною та надійною при взаємодії з суміжними системами. Також система повинна забезпечувати захист даних під час їх передачі та обробки між суміжніми системами.

2.1.1.4 Вимоги до режимів функціонування системи

Система повинна працювати безперебійно та надійно, забезпечуючи безперервну доступність та виконання функцій навіть у випадку помилок або збоїв. Для цього вона повинна бути забезпечена резервним апаратим забезпеченням, механізмами відновлення після відмови, моніторингом стану системи та виявлення помилок. Також вона повинна забезпечувати збереження стану після перезавантаження або відновлення.

2.1.1.5 Вимоги до діагностування системи

Система повинна мати засоби для аналізу та діагностики виявлених помилок, такі як автоматичний аналіз помилок, створення звітів про стан системи та відповідні діагностичні інструменти.

Необхідно проводити повне діагностування комп’ютерної системи через кожні півтора місяці експлуатації. Необхідно проводити повний огляд апаратних засобів системи та стану її конфігурації.

Система повинна забезпечувати реєстрацію подій, помилок та діагностичних даних у вигляді логів.

2.1.1.6 Перспективи розвитку системи

Для майбутнього розвитку комп’ютерної системи компанії необхідно вивчати та застосовувати нові технології, які покращать роботу юридичної компанії. Це такі технології, як системи штучного інтелекту, автоматизовані системи управління документами, електронний документообіг та інші інноваційні рішення.

Також, для забезпечення успішної модернізації системи у майбутньому, важливо врахувати вимоги до масштабованості мережі, які дозволять без проблем збільшувати кількість пристроїв та технологій, які у ній використовуються.

Також, Наявність кваліфікованого персоналу, який розуміє систему та може забезпечити її ефективну роботу, є важливим фактором успіху.

2.1.1.7 Показники призначення

Призначення комп'ютерної системи юридичної компанії полягає в автоматизації та підтримці різних аспектів роботи юристів і співробітників компанії для поліпшення ефективності, продуктивності та якості надання юридичних послуг.

Комп'ютерна система дозволяє зберігати, каталогізувати та управляти юридичними документами, включаючи договори, доручення, позовні заяви та внутрішні документи. Завдяки цьому спрощується пошук, спільна робота та контроль версій документів.

Також система дозволяє обмінюватися документами з клієнтами, іншими юридичними організаціями та органами державної влади через електронний шлях, що значно прискорює процеси комунікації, зменшує залежність від паперової документації та полегшує збереження та відстеження документів.

2.1.1.8 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

2.1.1.8.1 умови і регламент (режим) експлуатації, що повинні забезпечувати використання технічних засобів (ТЗ) системи з заданими технічними показниками, у тому числі види і періодичність обслуговування ТЗ чи системи

Найважливіші вимоги до експлуатації комп’ютерної системи – фізичні умови в приміщеннях, в яких встановлено систему.

Температура повітря у приміщеннях, в яких встановлено обладнання, повинна знаходитись у межах від +15 до +25 градусів С. Вологість повітря не повинна перевищувати 75% при атмосферному тиску від 84 кПа до 107 кПа.

Також не менш важливими є вимоги до електроживлення мережі, до якої під’єднуються пристрої. Так, напруга та частота в мережі не повинна

перевищувати значення, зазначені виробником обладнання у його документації.

2.1.1.8.2 Вимоги до параметрів мереж енергопостачання (живлення та заземлення)

В Україні стандартно використовується однофазна система живлення з напругою 220 вольт або трьохфазна система живлення з напругою 380 вольт.

Частота живлення в Україні стандартно становить 50 герц (Гц). Комп'ютерні системи зазвичай працюють з такою частотою без проблем, але необхідно враховувати вимоги до стабільності частоти для деяких видів обладнання.

Заземлення повинно відповідати вимогам нормативних актів та бути належно заземленим для ефективного розподілу струму у разі короткого замикання або перенапруги.

Необхідно забезпечити відповідність параметрів електромережі стандартам, щоб уникнути перебоїв, коливань напруги, шумів або інших проблем, які можуть впливати на роботу комп'ютерних систем.

Для запобігання пошкодженню обладнання внаслідок перенапруги або коливань напруги, повинні бути встановлені пристрої стабілізації напруги.

Усі кабелі та розетки, які використовуються в офісах компанії, повинні бути без ознак пошкоджень та несправностей.

Енергоживлення офісів компанії повинно відповідати даним вимогам.

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

Кількість обслуговуючого персоналу повинна бути достатньою для забезпечення ефективної роботи мережі. Для цього компанія повинна забезпечити не менше 20 системних адміністраторів, які будуть займатися діагностуванням та обслуговуванням мережі. Обслуговуючий персонал повинен мати достатні знання та навички у галузі мережевих технологій. Вони

повинні бути ознайомлені з принципами мережевої архітектури, протоколами, конфігурацією та управлінням мережею. Крім того, вони повинні мати розуміння засобів безпеки мережі та вміти вирішувати технічні проблеми та неполадки.

Персонал повинен працювати відповідно до постійного денного режиму. Важливо мати документований регламент, який визначає вимоги до режиму роботи та взаємодії з іншими відділами або підрозділами компанії. Швидкий розвиток технологій мережі вимагає від персоналу постійного навчання та оновлення знань. Рекомендується проводити тренінги, курси або сертифікаційні програми для підвищення кваліфікації персоналу та ознайомлення з новими технологіями та методиками.

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

Комплект запасних виробів повинен включати необхідне обладнання, компоненти і кабелі, які використовуються для заміни або відновлення елементів мережі. Це включає маршрутизатори, комутатори, кабелі Ethernet, модулі пам'яті, жорсткі диски тощо.

Запасні вироби і прилади повинні зберігатися в безпечній та доступній складській кімнаті, де обладнання зберігається на полицях або в стелажах. Важливо, щоб розміщення забезпечувало захист від пилу, вологи, перепадів температури та інших негативних факторів, які можуть впливати на якість обладнання.

Запасні вироби повинні зберігатися відповідно до рекомендацій виробників та специфікацій обладнання.

Кожен запасний виріб повинен бути чітко ідентифікований і маркований, щоб легко визначити його тип, модель та стан.

2.1.1.8.5 Вимоги до регламенту обслуговування

Регламент обслуговування включає перевірку працездатності обладнання, виявлення та усунення несправностей, поновлення програмного забезпечення, оновлення конфігурації та забезпечення безпеки мережі.

Обслуговуючий персонал повинен вести записи про виконані завдання обслуговування, виявлені проблеми, вжиті заходи та їх результати. Це допомагає відстежувати стан мережі та робити необхідні корективи.

Необхідно впровадити моніторинг мережевих пристроїв і зв'язку, аналіз журналів подій, використання програмних засобів для діагностики мережевих проблем та швидку реакцію на неполадки.

Політика обслуговування мережі повинна включати заходи безпеки, такі як застосування захисних механізмів, оновлення програмного забезпечення з метою усунення вразливостей, забезпечення контролю доступу і резервне копіювання даних.

2.1.1.9 Вимоги до патентної чистоти

Необхідно забезпечити внутрішні процедури та контроль, щоб уникнути навмисних порушень патентної чистоти. Потрібно повідомляти співробітників про важливість дотримання прав інтелектуальної власності та надавати їм відповідну освіту і навчання.

Необхідно підтримувати постійний моніторинг змін в області патентної охорони, щоб вчасно виявляти нові патенти або зміни в правовому статусі існуючих патентів, які можуть впливати на комп'ютерну систему.

Якщо виявлено патентні права або обмеження, необхідно оцінити ризики, пов'язані з їхнім порушенням, та розглянути можливість отримання ліцензій або укладення угод з власниками патентів для легального використання технології або продукту.

2.1.2 Додаткові вимоги

2.1.2.1 Вимоги до активного обладнання

Активне обладнання мережі повинно мати достатню кількість портів для підключення до мережевих пристроїв, комп'ютерів та інших пристроїв. Також важливо враховувати типи портів, які підтримуються (GigabitEthernet, Serial).

Активне обладнання мережі повинно підтримувати необхідні мережеві протоколи, такі як TCP/IP, DHCP, SNMP та інші, для забезпечення взаємодії з іншими пристроями у мережі.

Також важливо, щоб активне обладнання включало захист мережі від потенційних загроз, таких як атаки зовнішніх користувачів, несанкціонований доступ та перехоплення даних.

Вимоги до надійності включають наявність резервування та резервних блоків живлення, можливість швидкого відновлення після відмови, вбудовані механізми контролю стану та моніторингу, високу якість компонентів та відповідність стандартам надійності.

Активне обладнання повинно мати можливість масштабування, тобто додавання нових пристроїв або модулів для забезпечення росту мережі без великих перерв у роботі.

2.1.2.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

Кабель-канали повинні мати достатню витримку навантаження для підтримки всіх кабелів і проводів, які проходять через них. Вони повинні бути стійкими до ваги кабелів та не піддаватися деформації під час експлуатації.

Кабель-канали повинні забезпечувати захист кабелів від зовнішніх факторів, таких як фізичні пошкодження, волога та пил. Вони повинні бути встановлені таким чином, щоб уникнути небажаних згинів, стиснень і перетягування кабелів.

Інформаційні та електричні розетки повинні бути розташовані зручно для доступу та обслуговування. Крім того, вони повинні бути чітко позначені та марковані для легкого ідентифікування кабелів та підключення пристроїв.

Електричні розетки повинні відповідати національним і міжнародним нормам безпеки, включаючи правильне заземлення, захист від короткого замикання, витримку струму тощо. Вони повинні бути встановлені професіоналами з електромонтажу відповідно до вимог електробезпеки.

Кабель-канали, інформаційні та електричні розетки повинні бути доступними для обслуговування і модифікацій. При необхідності їх повинно бути легко переміщати, замінювати або розширювати.

2.1.2.3 Вимоги до комунікаційного обладнання і його розташування

Комунікаційне обладнання повинно відповідати встановленим стандартам і нормам, таким як стандарти IEEE, TIA/EIA та ISO/IEC.

Комунікаційне обладнання повинно мати достатню пропускну здатність для передачі даних у потрібних обсягах.

Комунікаційне обладнання повинно мати вбудовані механізми контролю стану, резервування та відновлення після відмови, а також можливість швидкого виявлення і усунення несправностей.

Обладнання повинно бути сумісним з іншими компонентами мережі і здатним до інтеграції з різними системами. Воно повинно підтримувати стандартні протоколи і інтерфейси для забезпечення взаємодії з іншими пристроями та системами.

Комунікаційне обладнання повинно бути розташоване в спеціально обладнаних приміщеннях та шафах, які забезпечують належні умови для його функціонування, такі як належну вентиляцію, охолодження, захист від пилу, вологи, електромагнітних перешкод та інших негативних впливів.

2.1.2.4 Вимоги до резервування

Система повинна мати механізми для регулярного резервного копіювання даних (автоматичне створення резервних копій даних на віддалених серверах або зовнішніх носіях зберігання). Резервне копіювання повинно бути регулярним (кожен тиждень). Резервні копії і репліковані дані повинні бути захищені від несанкціонованого доступу і втрати (для цього використовуються механізми шифрування, контролю доступу і захисту від вірусів та інших загроз).

Всі процедури і політики щодо резервування даних повинні бути добре задокументовані і доступні для відповідного персоналу.

2.1.3 Вимоги до функцій, які виконує КС

КС повинна забезпечувати можливість обробки та зберігання різних типів даних, таких як текстові документи, числа, зображення, відео та аудіо. Вона повинна мати можливості для створення, редагування, видалення та пошуку даних.

Також КС повинна мати механізми для керування користувачами, реєстрації, аутентифікації та авторизації. Вона повинна забезпечувати різні рівні доступу до функцій та даних залежно від ролі та прав користувачів.

Вона повинна мати можливості для підтримки та обслуговування, включаючи оновлення програмного забезпечення, виправлення помилок, надання технічної підтримки та навчання користувачів.

Також система потребує інтеграції з іншими системами, такими як електронна пошта, бази даних, CRM-системи та фінансові системи. Це забезпечує обмін даними та спільну роботу з іншими системами.

2.1.4 Вимоги до видів забезпечення

2.1.4.1 Вимоги до інформаційного забезпечення

Інформаційне забезпечення мережі повинно забезпечувати швидкий доступ до даних та оптимальну продуктивність мережі. Це реалізовується

через оптимізацію шляху передачі даних, використання швидкодіючих мережевих пристроїв та розробку ефективних алгоритмів обробки даних.

Інформаційне забезпечення мережі повинно бути сумісним з різними пристроями, операційними системами та програмними засобами. Воно повинно підтримувати стандарти комунікації і взаємодії, щоб забезпечити сумісність між різними компонентами мережі.

Інформаційне забезпечення мережі повинно забезпечувати можливості моніторингу та керування мережевими ресурсами (моніторинг пропускної здатності, навантаження, стану мережевих пристроїв), а також можливості керування налаштуваннями та ресурсами мережі.

2.1.4.2 Вимоги до лінгвістичного забезпечення

Вимога до лінгвістичного забезпечення полягає в можливості локалізувати КС для різних країн або регіонів. Це включає переклад і адаптацію інтерфейсу, документації та повідомлень у відповідну мову та контекст.

Лінгвістичне забезпечення КС може враховувати культурні аспекти, такі як культурні норми, етикет, вирази та фразеологізми, що характерні для певної мовної спільноти або регіону.

Лінгвістичне забезпечення КС повинно включати можливості мовної обробки (розпізнавання мовлення, синтаксичний аналіз, семантичний аналіз, машинний переклад).

2.1.4.3 Вимоги до технічного забезпечення

При проєктуванні мережі необхідно використовувати виключно мережеве обладнання від виробника Cisco для забезпечення успішної взаємодії усіх пристроїв у мережі. Також необхідно забезпечити підтримку стандарту IEEE 802.11 для усіх розумних пристроїв, які будуть використовуватися у побудові компонента системи.

Комп’ютери працівників компанії повинні бути забезпечені наступними характеристиками:

1. Процесор: Intel Core i5 або вище, або AMD Ryzen 5 або вище.
2. Оперативна пам'ять (RAM): Мінімум 8 ГБ RAM, що дозволить запускати багатозадачні програми та забезпечувати плавну роботу системи.
3. Жорсткий диск (HDD або SSD): Жорсткий диск обсягом 500 ГБ або більше для зберігання файлів та програм. Додатково, SSD (Solid State Drive) може бути використаний для швидшого завантаження операційної системи та програм.
4. Графічна карта: Інтегрована графічна карта буде достатньою для офісних завдань та перегляду мультимедійного вмісту.
5. Операційна система: Windows 10.
6. Монітор: Монітор з роздільною здатністю Full HD (1920 x 1080 пікселів), розміром 22 дюйми або більше для зручної роботи з документами та програмами.
7. Клавіатура та миша: Стандартна USB-клавіатура та оптична миша для зручного введення даних та навігації по комп'ютеру.
8. Підключення та роз'єми: Наявність USB-портів для підключення периферійних пристроїв, а також Ethernet-порт для підключення до локальної мережі.
9. Безпека: Наявність антивірусного програмного забезпечення та можливість оновлення системи для забезпечення безпеки даних.

2.1.4.4 Вимоги до організаційного забезпечення

Комп'ютерна мережа вимагає наявності кваліфікованого персоналу, який має знання та навички з управління, налаштування та підтримки мережевого обладнання і програмного забезпечення. Усі інженери, які займаються обслуговуванням системи, повинні мати ступінь не нижче бакалавра та досвід роботи не менше року.

Організаційне забезпечення персоналу повинно визначати чіткі завдання та відповідальність кожного спеціаліста. Це включає моніторинг мережі, налагодження з'єднань, вирішення проблем, резервне копіювання даних та інші завдання.

Персонал, що працює з комп'ютерною мережею, повинен мати доступ до необхідного тренінгу та підготовки для підвищення своїх навичок та оновлення знань у сфері мережевих технологій.

2.1.4.5 Вимоги до методичного забезпечення

Вимоги до методичного забезпечення комп'ютерної мережі включають такі аспекти:

1. Документація: документи з описом конфігурації мережевого обладнання, інструкції з налагодження та управління мережею, правила безпеки, процедури резервування даних та інші документи, що стосуються роботи з мережею.
2. Стандарти та норми: стандарти та норми для проектування, розгортання та управління комп'ютерною мережею. Стандарти з кабельної розводки, мережевих протоколів, безпеки мережі та інші.
3. Інструкції та процедури: Методичне забезпечення повинно містити інструкції та процедури з налаштування мережевого обладнання, встановлення програмного забезпечення, управління користувачами, резервне копіювання даних та інші процедури.
4. Навчальні матеріали: навчальні посібники, відеоуроки, онлайн-курси або інші матеріали, що допомагають персоналу ознайомитися з принципами та процедурами роботи з мережею.
5. Підтримка та консультації: контактна інформація технічної підтримки, форуми обміну досвідом та інші способи отримання допомоги та порад.

6. Оновлення та моніторинг: методичне забезпечення повинно враховувати процес оновлення та моніторингу мережі.

2.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп'ютерної системи

Після того, як усі технічні вимоги до комп'ютерної системи було розроблено та структура компанії була проаналізована, необхідно розробити схему комплексу технічних засобів комп'ютерної системи (рисунок 2.2).

На даній схемі наведено з'єднання мережевих пристроїв з комп'ютерами та серверами мережі та вказано інформацію стосовно назви відділів та кількості ПК.

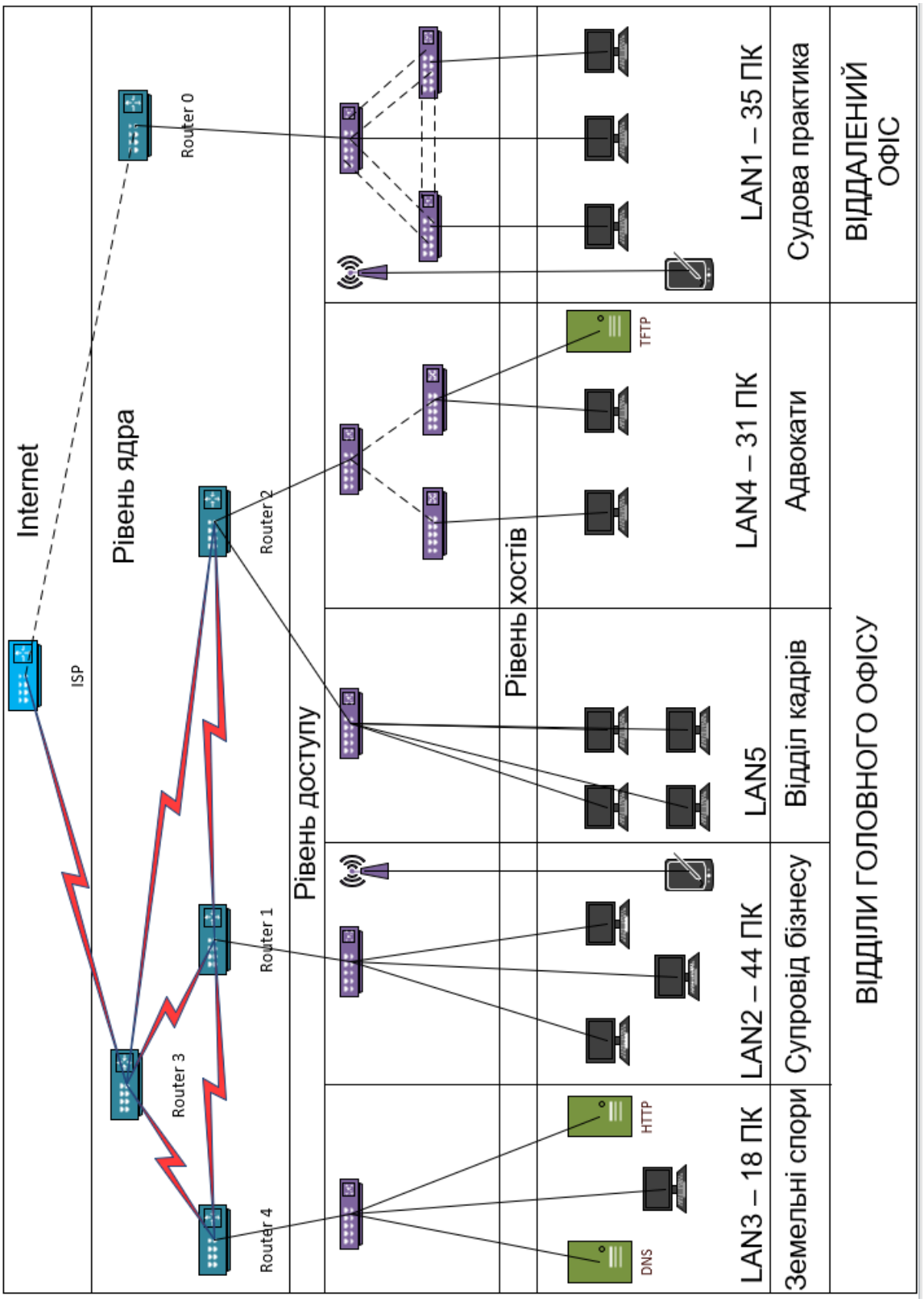

Рисунок 2.2 – Схема комплексу технічних засобів комп’ютерної системи

2.3 Розробка специфікації апаратних засобів комп’ютерної системи

Виконаємо розробку специфікації апаратних засобів КС для мережі віддаленого офісу компанії.

Для мережі віддаленого офісу було обрано маршрутизатор Cisco 2901/K9. Маршрутизатори Cisco ISR серії 2900 спеціально розроблені для невеликих та середніх організацій, які шукають сучасні технологічні рішення, що гарантують надійний та продуктивний доступ до мережі Інтернет з маршрутизаційною швидкістю до 75 Мбіт/с.

Для комутації у підмережі було обрано комутатори Cisco WS-C2960-24LC-S. Дані комутатори мають відносно невелику ціну і відповідають усім потребам компанії. Дана серія є лінійкою комутаторів з фіксованою конфігурацією та портами FastEthernet і GigabitEthernet, комутатори серії мають розширені LAN сервіси для підприємств початкового рівня та мереж віддаленого офісу.

Для впровадження IoT системи у приміщеннях віддаленого офісу було обрано бездротовий маршрутизатор Cisco RV215W-E-K9-G5. Даний маршрутизатор забезпечує просте, доступне та високообчислювальне з'єднання бізнес-класу для малих офісів, домашніх офісів та віддалених розташувань. Cisco RV215W має USB-порт для підключення 3G та 4G WAN, що ідеально підходить для віддалених регіонів або тимчасового з'єднання.

Розроблену специфікацію апаратних засобів комп’ютерної системи для мережі віддаленого офісу компанії наведено у таблиці 2.2.

Таблиця 2.2 – Специфікація апаратних засобів віддаленого офісу компанії

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Маршрутизатор Cisco 2901: 2 onboard GE, 4 EHWIC slots, 2 DSP slots, 1 ISM slot, 256MB CF default ,512MB DRAM default.	Cisco 2901/K9	од	1	Security Features: Cisco Security Manager; Cisco IOS Firewall; Cisco IOS Zone-Based; Firewall; Cisco IOS IPS; Cisco IOS Content Filtering; Flexible Packet Matching (FPM); AAA.
2	Комутатор Cisco WS-C2960: Catalyst 2960 24 10/100 (8 PoE) + 2 T/SFP LAN Lite Image.	Cisco WS-C2960-24LC-S	од	2	24 x Fast Ethernet Network; 2 x Gigabit Ethernet Uplink; 2 x Gigabit Ethernet Expansion Slot.
3	Бездротовий маршрутизатор Cisco RV215W: 1 10/100 Mbps Fast Ethernet WAN port; 4 10/100 Mbps Fast Ethernet LAN ports.	Cisco RV215W-E-K9-G5	од	1	Security Stateful packet inspection (SPI) firewall; Port forwarding and triggering; Firewall access control lists and content filtering; Denial-of-service (DoS) prevention; MAC-based wireless access control; Static URL blocking or keyword blocking

Після розробки специфікації апаратних засобів віддаленого офісу розглянемо його кабельну структуру, зображену на рисунку 2.3.

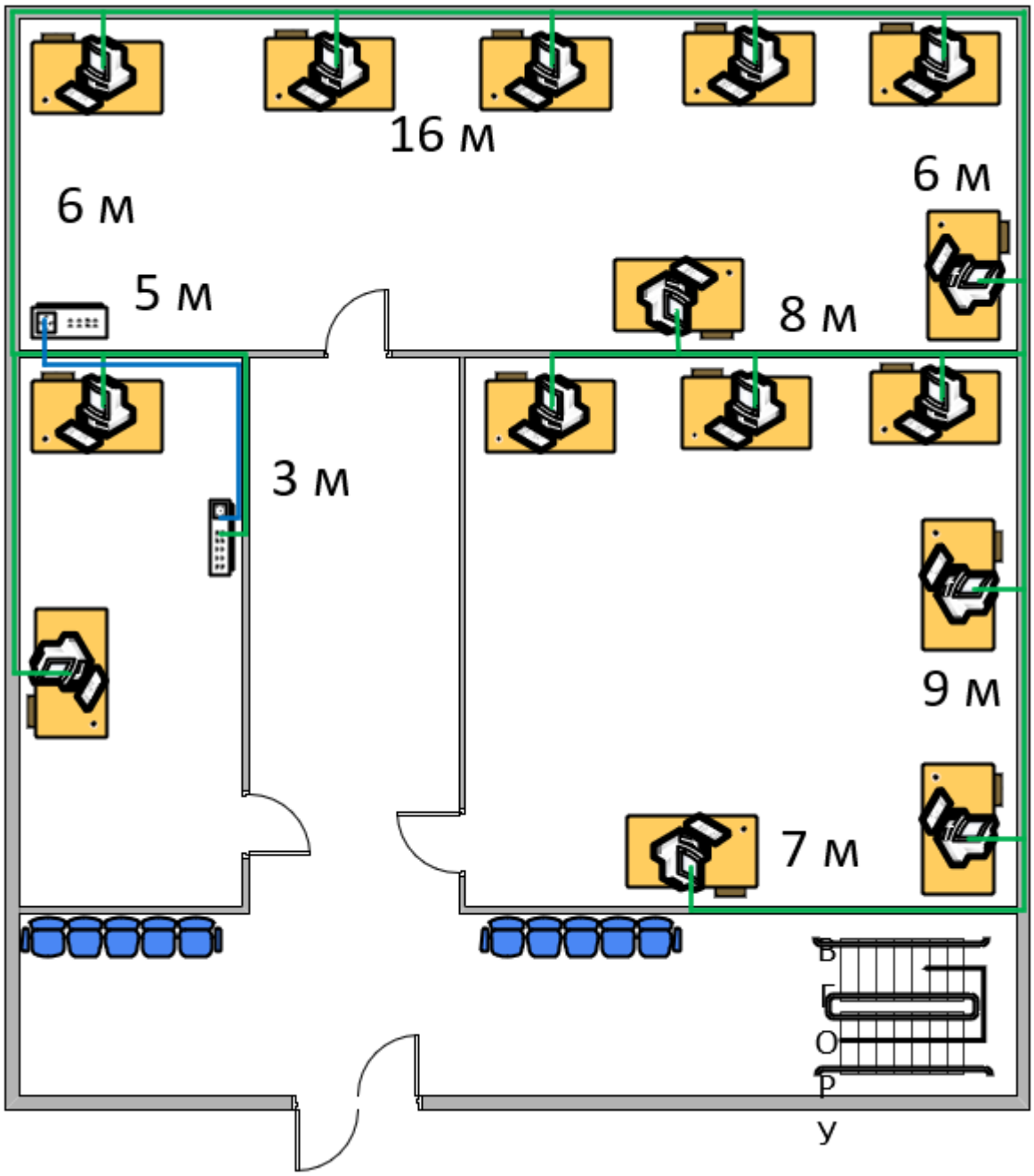

Рисунок 2.3 – Структура кабельних з’єднань віддаленого офісу

Для прокладання кабелів у мережі офісу було обрано настінне розміщення кабальних каналів. Це вбереже кабелі від фізичних пошкоджень та забезпечить зручне обслуговування.

Специфікацію кабельної структури наведено у таблиці 2.3.

Таблиця 2.3 – Специфікація кабельної структури віддаленого офісу

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Канал кабельний Expert 10x20 мм	Expert	м	60	Матеріал: ПВХ. Застосування: для внутрішньої прокладки.
2	Розетка інформаційна однопортова Cablexpert	Cablexpert	од	35	Інтерфейс: Ethernet (RJ45) Категорія: 5e
3	Розетка із заземленням Panasonic Arkedia	Panasonic Arkedia Slim	од	50	Матеріал корпусу: ABS-пластик. Номінальний струм: 16 А. Ступінь захисту: IP20.
4	Кабель комп'ютерний Expert Power UTP мідь	Expert Power	м	65	Матеріал ізоляції: ПВХ. 5E категорія.
5	Кабель ORANGE STAR ВВГ-ПНГ 3Х1,5	ORANGE STAR	м	110	Наявність протипожежної ізоляції і оболонки з полівінілхлоридних сумішей.

2.2.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Необхідно виконати розрахунок інтенсивності трафіку для найбільшої підмережі підприємства. Найбільша підмережа має 44 ПК.

Маршрутизація трафіку виконується в лінію з пропускною здатністю 1000 Мбіт/с.

Тоді, навантаження на маршрутизатор повинно бути не більше, ніж:

$$\mu_{вих}=\frac{1000000000}{650\times8}=192\ 300 \text{ пакетів/с (2.1)}$$

Кожен ПК у підмережі в середньому виробляє 122 пакети. Виходячи з даного значення отримуємо максимальну кількість ПК, які можна під'єднати до мережі.

$$N=\frac{192300}{122}=1576 \text{ пристроїв (2.2)}$$

Помноживши значення кількості ПК у мережі на кількість пакетів, які вони виробляють, отримуємо інтенсивність трафіку у мережі:

$$\lambda=44*122=5368 \text{ пакетів/с (2.3)}$$

Далі визначимо коефіцієнт затримки у мережі:

$$\rho=\frac{\lambda}{\mu_{вих}}=5368/192300=0.03 \text{ (2.4)}$$

Отримавши значення коефіцієнту затримки можна визначити коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho}=\frac{0.03}{1-0.03}=0.03 \text{ (2.5)}$$

Середня затримка кадру, пов'язана з чергою M/M/1, розраховується за формулою:

$$T=\frac{1}{\mu-\lambda}=\frac{1}{192300-5368}=5.3 \text{ мкс (2.6)}$$

Середня довжина черги у мережі визначається за наступною формулою:

$$L_{чер}=\frac{\rho^2}{1-\rho}=\frac{0.03^2}{1-0.03}=0.0009 \text{ (2.7)}$$

Далі визначимо середній час перебування пакета в черзі:

$$T_{оч}=\frac{L_{чер}}{\lambda}=\frac{0.0009}{5368}=167.7 \text{ нс (2.8)}$$

Пропускна здатність каналу можна визначити за наступною формулою:

$$b=\lambda\times l=5368\times 650\times 8=27913600 \text{ біт/с} =27.9 \text{ Мбіт/с} \quad (2.10)$$

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації мережі

Для корпоративної мережі компанії виділено блок адрес 10.23.72.0/22, який буде використано для розрахунку адресації у підмережах головного та віддаленого офісу. У таблиці 3.1 наведено кількість ПК у кожній підмережі.

Таблиця 3.1 – Виділений блок адрес

№	Блок адрес	LAN1(Віддалена мережа) Судова практика	LAN2 Супровід бізнесу	LAN3 Земельні спори	LAN4 Адвокати	LAN5 Відділ кадрів
15	10.23.72.0/22	35	44	18	31	15

Розрахунок підмереж раціонально виконувати за методом маски змінної довжини (VLSM). VLSM (Variable Length Subnet Masking) - це метод поділу мережі на підмережі з масками різної довжини. За допомогою VLSM можна розбити велику мережу на багато менших підмереж з різною кількістю доступних IP-адрес в кожній підмережі, в залежності від потреб мережі. Розміри підмереж обмежені варіаціями степеню двійки. При розбитті мережі на підмережі необхідно починати розрахунок з найбільшої за розміром підмережі. Також варто взяти до уваги, що в кожній розрахованій підмережі кількість корисних адрес на 2 менше, ніж виділена степінь двійки.

Почнемо розрахунок підмереж з мережі LAN4, так як для неї буде виділено 128 адрес через необхідність подальшого розбиття мережі на VLAN.

Розрахунок підмереж виконується за допомогою маніпуляцій з бітами адреси основної мережі, тому для зручності представимо половину адреси у двійковій системі числення. Після переведення необхідно відрахувати з кінця адреси 7 біт ($2^7 = 128$). Після переведення адреси до звичного вигляду отримаємо адресу підмережі. Якщо заповнити праву частину адреси 1 замість

0, то отримаємо широкомовну адресу підмережі. Все, що знаходиться між адресою мережі та широкомовною адресою – діапазон корисних адрес.

10.23.01001000.0 0000000

10.23.01001000.0 1111111

Адреса мережі – 10.23.72.0/25;

Діапазон корисних адрес – 10.23.72.1 - 10.23.72.126;

Широкомовна адреса – 10.23.72.127.

Після цього перейдемо до розрахунку мережі LAN2, так як дана підмережа друга за розміром – 44 вузли. Для даної підмережі достатньо виділити блок з 64 адрес. Перед початком розрахунку необхідно збільшити значення мережевої частини вихідної адреси на 1 біт. Результати розрахунку наведено нижче.

10.23.01001000.10|000000

10.23.01001000.10|111111

Адреса мережі – 10.23.72.128/26;

Діапазон корисних адрес – 10.23.72.129 - 10.23.72.190;

Широкомовна адреса – 10.23.72.191.

Після цього перейдемо до розрахунку мережі LAN1, так як дана підмережа третя за розміром – 35 вузлів. Для даної підмережі достатньо виділити блок з 64 адрес. Результати розрахунку наведено нижче.

10.23.01001000.11 000000

10.23.01001000.11 111111

Адреса мережі – 10.23.72.192/26;

Діапазон корисних адрес – 10.23.72.193 - 10.23.72.254;

Широкомовна адреса – 10.23.72.255.

Після цього перейдемо до розрахунку мережі LAN3, так як дана підмережа четверта за розміром – 18 вузлів. Для даної підмережі достатньо виділити блок з 32 адрес. Результати розрахунку наведено нижче.

10.23.01001001.000 00000

10.23.01001001.000 11111

Адреса мережі – 10.23.73.0/27;

Діапазон корисних адрес – 10.23.73.1 - 10.23.73.30;

Широкомовна адреса – 10.23.73.31.

Остання підмережа до розрахунку – LAN5. Вона має 15 вузлів. Для даної підмережі достатньо виділити блок з 32 адрес. Результати розрахунку наведено нижче.

10.23.01001001.001 00000

10.23.01001001.001 11111

Адреса мережі – 10.23.73.32/27;

Діапазон корисних адрес – 10.23.73.33 – 10.23.73.62;

Широкомовна адреса – 10.23.73.63.

Результати розрахунків наведено у таблиці 3.2.

Таблиця 3.2 – Схема адресації мережі

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
LAN1	35	64	10.23.72.192	/26	10.23.72.193 - 10.23.72.254	10.23.72.255
LAN2	44	64	10.23.72.128	/26	10.23.72.129 - 10.23.72.190	10.23.72.191
LAN3	18	32	10.23.73.0	/27	10.23.73.1 - 10.23.73.30	10.23.73.31
LAN4	31	128	10.23.72.0	/25	10.23.72.1 - 10.23.72.126	10.23.72.127
LAN5	15	32	10.23.73.32	/27	10.23.73.33 – 10.23.73.62	10.23.73.63

Також необхідно виконати розрахунок адрес для каналів, які забезпечують зв’язок між маршрутизаторами мережі. Для цього використаємо

виділений блок адрес 10.1.15.0/24. Розрахуємо за методом VLSM 5 підмереж на 2 корисні адреси в кожній. Результати наведено у таблиці 3.3.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN1	2	4	10.1.15.0	/30	10.1.9.1 – 10.1.9.2	10.1.9.3
WAN2	2	4	10.1.15.4	/30	10.1.9.5 – 10.1.9.6	10.1.9.7
WAN3	2	4	10.1.15.8	/30	10.1.9.9 – 10.1.9.10	10.1.9.11
WAN4	2	4	10.1.15.12	/30	10.1.9.13 – 10.1.9.14	10.1.9.15
WAN5	2	4	10.1.15.16	/30	10.1.9.17 – 10.1.9.18	10.1.9.19

3.2 Розрахунок адресації пристроїв

Далі необхідно визначити, які адреси будуть призначені відповідним інтерфейсам маршрутизаторів у мережі. За правилом перша корисна адреса привласнюється інтерфейсу маршрутизатора (шлюзу). Результати наведено у таблиці 3.4.

Таблиця 3.4 – Схема адресації маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
Fakhardinov_Router_0	Gig0/0	10.23.72.193	255.255.255.192
	Gig0/1	64.100.13.2	255.255.255.252
Fakhardinov_Router_1	Gig0/0	10.23.72.129	255.255.255.192
	Se0/2/1	10.1.15.10	255.255.255.252
	Se0/3/0	10.1.15.18	255.255.255.252
	Se0/3/1	10.1.15.14	255.255.255.252

Продовження таблиці 3.4

Fakhardinov_Router_2	Gig0/0	10.23.73.33	255.255.255.224
	Se0/3/0	10.1.15.17	255.255.255.252
	Se0/3/1	10.1.15.2	255.255.255.252
	Gig0/0.25	10.23.72.1	255.255.255.224
	Gig0/0.35	10.23.72.33	255.255.255.224
	Gig0/0.45	10.23.72.65	255.255.255.224
	Gig0/0.99	10.23.72.97	255.255.255.240
Fakhardinov_Router_3	Se0/2/0	10.1.15.5	255.255.255.252
	Se0/2/1	10.1.15.9	255.255.255.252
	Se0/3/0	209.165.202.2	255.255.255.252
	Se0/3/1	10.1.15.1	255.255.255.252
Fakhardinov_Router_4	Gig0/0	10.23.73.1	255.255.255.224
	Se0/3/0	10.1.15.6	255.255.255.252
	Se0/3/1	10.1.15.13	255.255.255.252
Fakhardinov_Router_ISP	Gig0/0	209.165.201.1	255.255.255.240
	Gig0/1	64.100.13.1	255.255.255.252
	Se0/3/0	209.165.202.1	255.255.255.252

Другі з доступних адрес у підмережі необхідно призначити SVI-інтерфейсам комутаторів мережі. Результати наведено у таблиці 3.5.

Таблиця 3.5 – IP-адреси комутаторів у підмережах

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
LAN1	Fakhardinov_Switch_4	10.23.72.195	255.255.255.192	10.23.72.193
	Fakhardinov_Switch_5	10.23.72.196	255.255.255.192	10.23.72.193
	Fakhardinov_Switch_6	10.23.72.194	255.255.255.192	10.23.72.193
LAN2	Fakhardinov_Switch_7	10.23.72.130	255.255.255.192	10.23.72.129
LAN3	Fakhardinov_Switch_3	10.23.73.2	255.255.255.224	10.23.73.1
LAN4	Fakhardinov_Switch_0	10.23.72.99	255.255.255.240	10.23.72.97
	Fakhardinov_Switch_1	10.23.72.98	255.255.255.240	10.23.72.97
	Fakhardinov_Switch_2	10.23.72.100	255.255.255.240	10.23.72.97
LAN5	Fakhardinov_Switch_8	10.23.73.34	255.255.255.224	10.23.73.33

3.3 Налаштування моделі комп’ютерної системи

Виходячи з отриманих даних змоделюємо мережу компанії у середовищі Cisco Packet Tracer. На логічній топології, наведеній на рисунку 3.1,

зображено адресацію підмереж компанії та схему підключень мережевих пристроїв та вузлів.

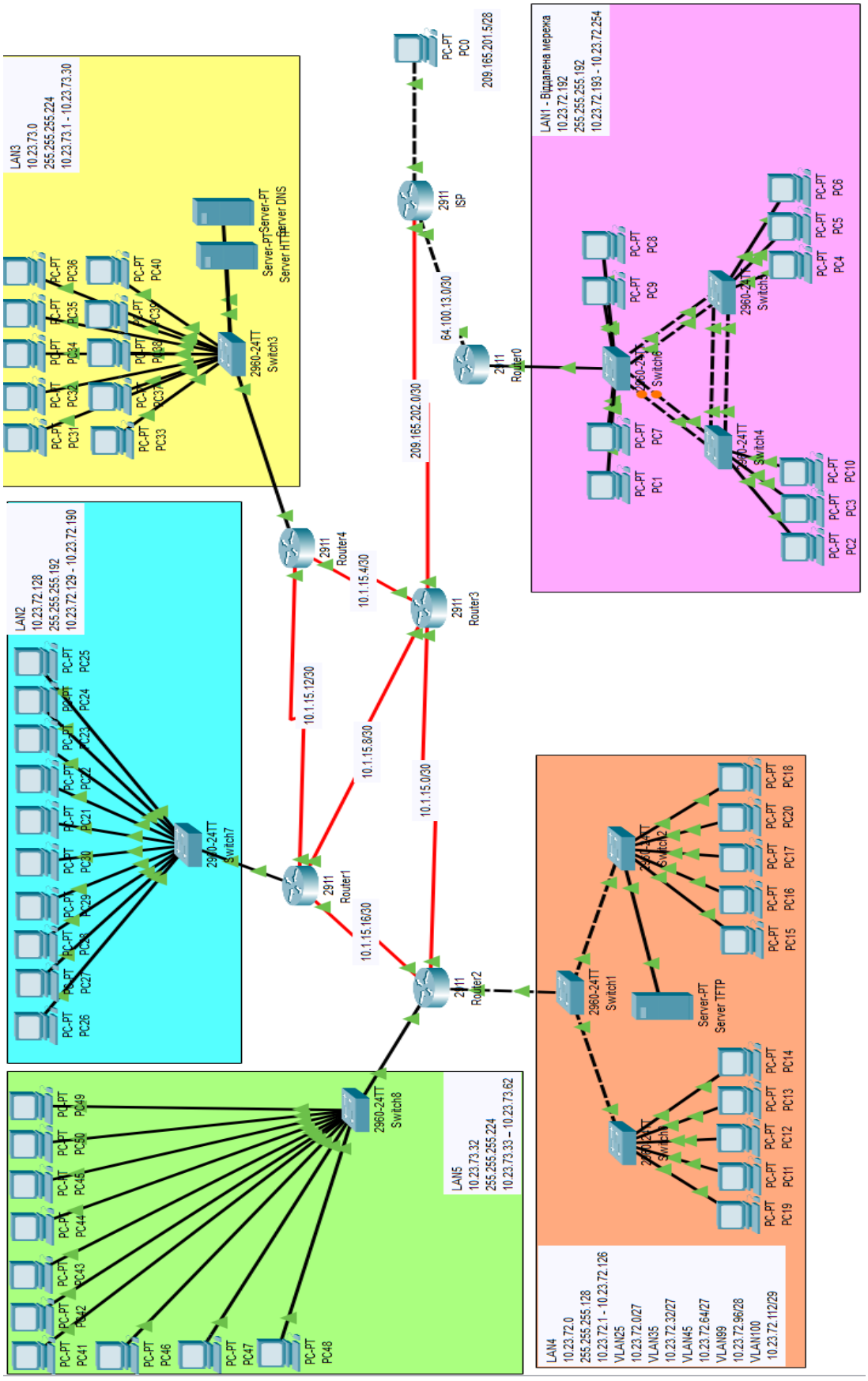

Рисунок 3.1 – Логічна топологія мережі

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

На усіх мережевих пристроях компанії необхідно налаштувати базову конфігурацію, до якої входить призначення імені пристрою, налаштування банеру MOTD, створення користувача та доменного імені, призначення паролів до привілейованого режиму, ліній console та vty, шифрування створених паролів, створення зашифрованого ключа довжиною 1024 біти за допомогою алгоритму RSA та налаштування роботи захищеного протоколу ssh. Розглянемо налаштування базової конфігурації пристроїв на прикладі маршрутизатора Fakhardinov_Router_1.

Enable //Вмикаємо привілейований режим EXEC

Conf t //Переходимо в режим конфігурації

Hostname Fakhardinov_Router_1 //Призначаємо пристрою ім’я

Line console 0 //Обираємо лінію console 0

Password cisco //Встановлюємо пароль cisco

Login //Вмикаємо авторизацію

Line vty 0 15 //Обираємо лінії vty 0 15

Password cisco //Встановлюємо пароль cisco

Login //Вмикаємо авторизацію

Enable secret class //Встановлюємо пароль для привілейованого режиму EXEC

Service password-encryption //Шифруємо усі створені паролі

Banner motd ‘Fakhardinov_Router_1’ //Встановлюємо банер MOTD

ip domain-name Fakhardinov_Router_1 //Створюємо доменне ім’я

Crypto key generate rsa //Генеруємо ключ RSA

1024 //Вказуємо довжину ключа

Username 123191_Fakhardinov password admincisco //Сторюємо користувача з паролем admincisco

Line vty 0 15 //Обираємо лінії vty 0 15

Transport input ssh //Вмикаємо роботу протоколу ssh

Login local

Також необхідно виконати об’єднання фізичних портів комутаторів у мережі LAN1. Це забезпечить більш стабільну роботу мережі та більшу швидкість передачі даних. Розглянемо налаштування на прикладі комутатора Fakhardinov_Switch_4.

en

conf t

interface range fa0/1-2 //Вибір діапазону інтерфейсів

channel-group 1 mode active //Активація групування каналів на обраних інтерфейсах

interface port-channel 1 //Увімкнення об’єднаного інтерфейсу

switchport mode trunk //Вмикання режиму trunk

switchport trunk allowed vlan all //Дозвіл на передачу даних для усіх VLAN

interface range fa0/5-6

channel-group 2 mode active

interface port-channel 2

switchport mode trunk

switchport trunk allowed vlan all

3.4.2 Налаштування маршрутизаторів

Після базового налаштування обладнання першим чином необхідно налаштувати усі маршрутизатори мережі компанії. Для того, щоб підмережі могли обмінюватися даними, необхідно виконати налаштування маршрутизації. У якості протоколу динамічної маршрутизації використаємо протокол OSPF. Після налаштування даного протоколу маршрутизатори будуть встановлювати зв’язки з сусідами та поширювати їм свої оголошені мережі. Варто вимкнути поширення пакетів з оновленнями на внутрішні інтерфейси підмереж. Це дозволить уникнути зайвого навантаження на мережу.

Розглянемо налаштування на прикладі маршрутизатора Fakhardinov_Router_1.

router ospf 1 //Створюємо нову схему маршрутизації

passive-interface GigabitEthernet0/0 //Вказуємо пасивний інтерфейс

network 10.23.72.128 0.0.0.63 area 0

//Оголошуємо усі мережі маршрутизатора, які бажаємо розповсюджувати

network 10.1.15.8 0.0.0.3 area 0

network 10.1.15.16 0.0.0.3 area 0

network 10.1.15.12 0.0.0.3 area 0

Після налаштування динамічної маршрутизації необхідно додати статичні маршрути на маршрутизаторі з прямим під'єднанням до ISP. Необхідно створити маршрут за замовчуванням, який буде надсилати увесь невідомий трафік до провайдера.

ip route 0.0.0.0 0.0.0.0 209.165.202.1 //Створюємо маршрут за замовчуванням

Після нього створимо статичний маршрут безпосередньо до мережі провайдера.

ip route 209.165.201.0 255.255.255.240 209.165.202.1 //Створюємо статичний маршрут до мережі провайдера

Також потрібно виконати налаштування DCE-інтерфейсів машрутизаторів мережі. Для цього необхідно встановити частоту 128000 та пропускну здатність 128.

interface Serial0/3/0 //Обираємо потрібний DCE-інтерфейс

bandwidth 128 //Встановлюємо пропускну здатність

clock rate 128000 //Встановлюємо частоту

Необхідно налаштувати доступ до маршрутизаторів мержі через службу AAA за протоколом Radius. У якості серверу, на якому буде налаштовано роботу служби, оберемо DNS-сервер компанії. Налаштування служби повинно

бути виконане таким чином, щоб аутетнтифікація користувачів до консолі виконувалась через протокол Radius. Також потрібно створити локальну базу користувачів, яка буде використовуватись у тому разі, якщо зв’язок з Radius-сервером відсутній. Розглянемо налаштування нижче.

aaa new-model //Створення нової AAA-моделі

radius-server host 10.23.75.25 auth-port 1645 key radius123 //Вказуємо адресу Radius-сервера

aaa authentication login CONSOLE group radius local //Вмикаємо аутентифікацію користувачів на лінії consol за протоколом Radius

line console 0

login authentication CONSOLE

aaa authentication login default local //Вмикаємо використання локальної бази користувачів

username 123191_Fakhardinov password admin123 //Створюємо нового користувача

line vty 0 15

login authentication default

Після коніфгурації служби на маршрутизаторах необхідно увімкнути та наалштувати її на віддаленому сервері. Налаштування служби AAA на сервері зображено на рисунку 3.2.

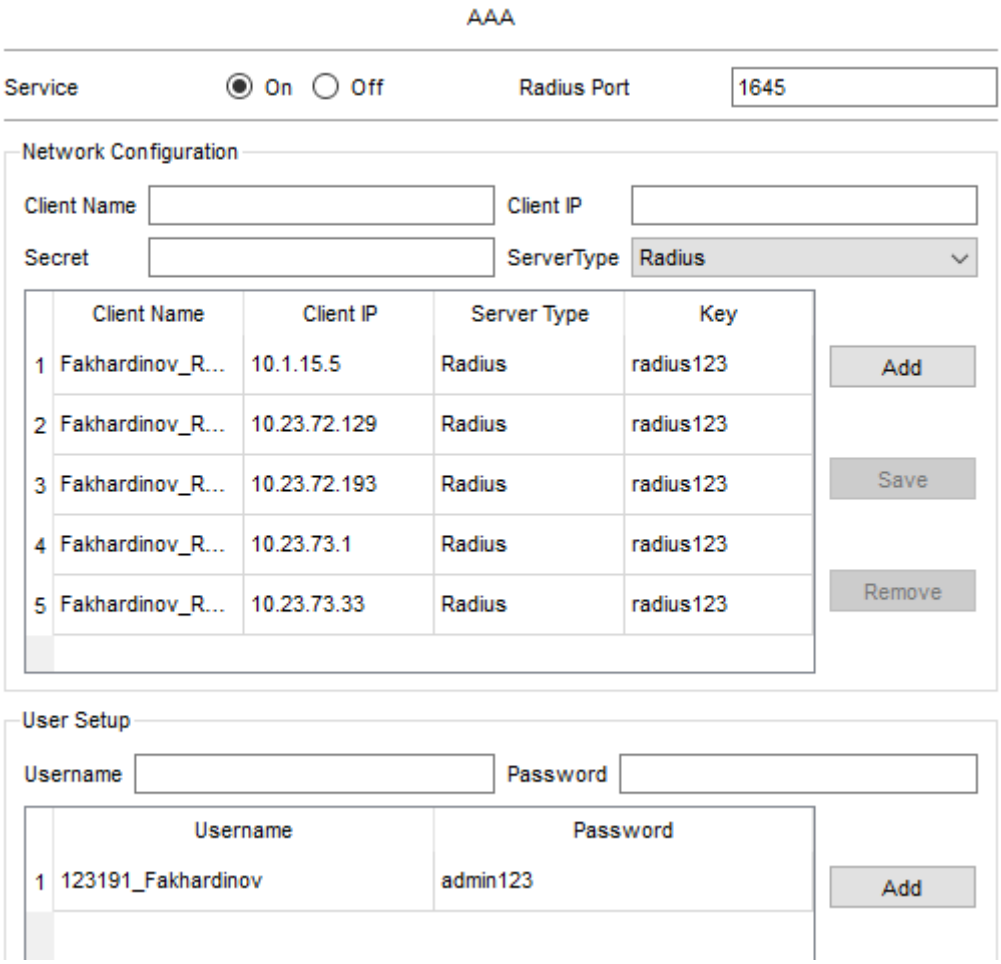

Рисунок 3.2 – Налаштування служби AAA на сервері

3.4.3 Налаштування роботи Інтернет

Після конфігурації маршрутизаторів у мережі необхідно забезпечити доступ до інтернету для вузлів головного та віддаленого офісів компанії. Для цього потрібно виконати налаштування технології NAT, яка буде транслювати локальні адреси у публічні. В нашому випадку використаємо динамічний NAT, який обирає та привласнює публічні адреси з виділеного пулу адрес. Для нашої компанії виділено такий пул адрес: від 209.165.200.5 по 209.165.200.30.

Щоб визначити, який трафік потрібно транслювати, а який ні, потрібно створити ACL-списки на пограничних маршрутизаторах. Необхідно заборонити трянсляцію адрес для трафіку, який надходить з мережі головного офісу до віддаленого, так як далі цей трафік буде проходити по VPN-каналу.

Розглянемо налаштування ACL-списку на прикладі маршрутизатора Fakhardinov_Router_3.

ip access-list extended NAT15 //Створюємо новий розширений ACL-список

//Забороняємо трафік з кожної підмережі головного офісу до віддаленого офісу

deny ip 10.23.73.0 0.0.0.31 10.23.72.192 0.0.0.63

deny ip 10.23.72.128 0.0.0.63 10.23.72.192 0.0.0.63

deny ip 10.23.73.32 0.0.0.31 10.23.72.192 0.0.0.63

deny ip 10.23.72.0 0.0.0.127 10.23.72.192 0.0.0.63

deny ip 10.1.15.0 0.0.0.255 10.23.72.192 0.0.0.63

//Дозволяємо увесь інший трафік

permit ip 10.23.73.0 0.0.0.31 any

permit ip 10.23.72.128 0.0.0.63 any

permit ip 10.23.73.32 0.0.0.31 any

permit ip 10.23.72.0 0.0.0.127 any

permit ip 10.1.15.0 0.0.0.255 any

Після налаштування списку доступу перейдемо безпосередньо до налаштування технології NAT. Необхідно створити пул адрес з ім’ям Internet, увімкнути роботу NAT, вказавши ACL-список та пул адрес, та налаштувати інтерфейси маршрутизатора як внутрішні та зовнішній. Налаштування на маршрутизаторі Fakhardinov_Router_3 наведено нижче.

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 //Створюємо новий NAT-пул та вказуємо наш діапазон адрес

ip nat inside source list NAT15 pool Internet //Вмикаємо NAT, вказавши ACL-список та пул адрес

interface Serial0/3/0

ip nat outside //Налаштовуємо інтерфейс у якості зовнішнього

interface Serial0/2/0

ip nat inside //Налаштовуємо інтерфейс у якості внутрішнього

interface Serial0/2/1

ip nat inside

interface Serial0/3/1

ip nat inside

Аналогічно налаштовуємо NAT на маршрутизаторі віддаленого офісу.

Результат роботи NAT можна переглянути за допомогою відповідної команди на маршрутизаторі (рисунок 3.3).

```
Fakhardinov_Router_3#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.10:2  10.23.73.13:2      209.165.201.5:2    209.165.201.5:2
icmp 209.165.200.11:1  10.23.72.144:1     209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.5:4   10.23.72.146:4     209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.5:5   10.23.72.146:5     209.165.201.5:5    209.165.201.5:5
icmp 209.165.200.5:6   10.23.72.146:6     209.165.201.5:6    209.165.201.5:6
icmp 209.165.200.6:1   10.23.73.18:1      209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.6:2   10.23.73.18:2      209.165.201.5:2    209.165.201.5:2
icmp 209.165.200.7:3   10.23.73.51:3      209.165.201.5:3    209.165.201.5:3
icmp 209.165.200.8:1   10.23.72.43:1      209.165.201.5:1    209.165.201.5:1
icmp 209.165.200.9:7   10.23.72.11:7      209.165.201.5:7    209.165.201.5:7
---  209.165.200.3     10.23.73.25        ---                ---
---  209.165.200.4     10.23.73.26        ---                ---
```

Рисунок 3.3 – Результат роботи NAT

Також потрібно налаштувати роботу HTTP-сервера мережі компанії. За допомогою статичної трансляції NAT необхідно привласнити йому публічну адресу та створити доменне ім’я на DNS-сервері. При введені у рядок браузера http://123.dnipro.ua (http://209.165.200.4) повинен відкриватися сайт з відомостями ро тему та завдання на кваліфікаційну роботу. Налаштування статичної трансляції та DNS-серверу наведено нижче.

ip nat inside source static 10.23.73.26 209.165.200.4 //Створення статичної трансляції NAT

Після цього створимо доменне ім’я та привласнимо йому публічну адресу HTTP-сервера. Налаштуванна показано на рисунку 3.3.

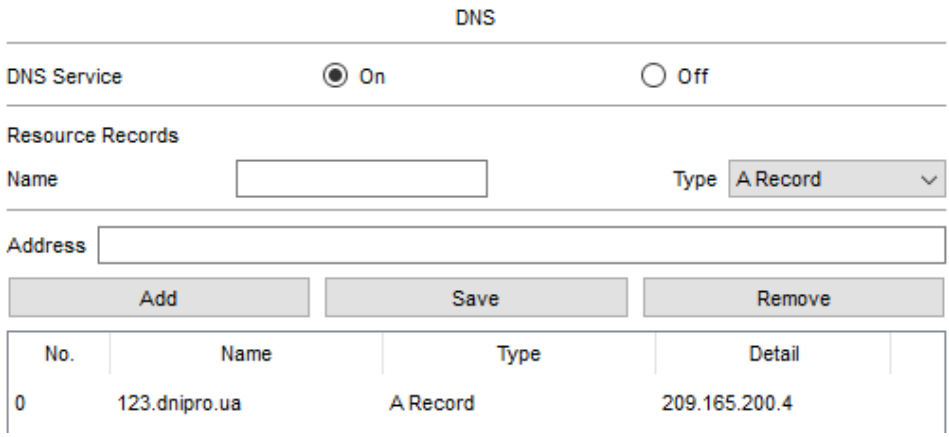

Рисунок 3.4 – Створення доменного імені

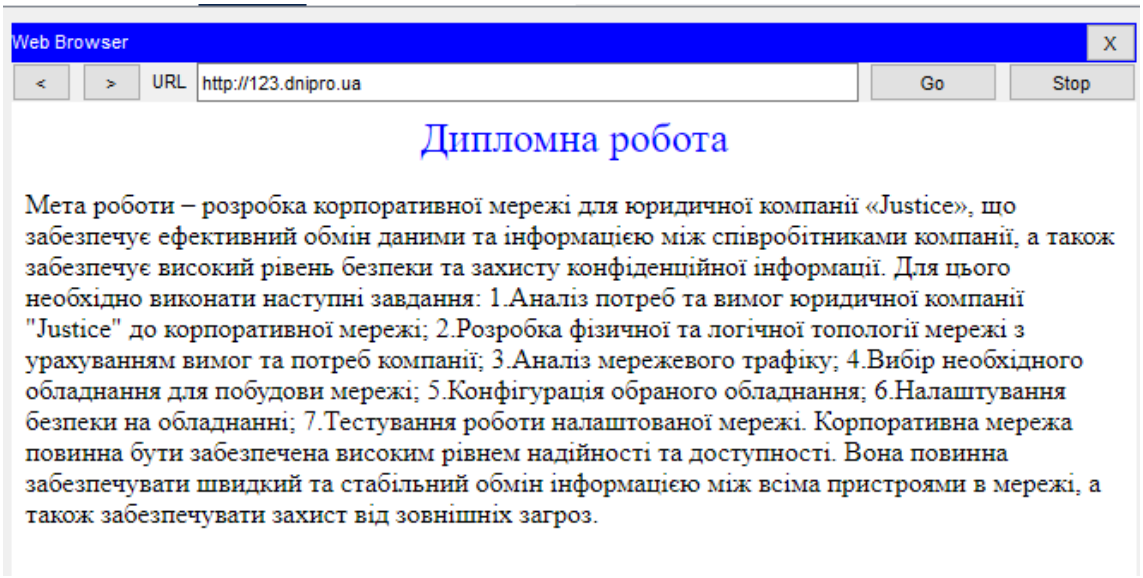

Рисунок 3.5 – Робота DNS-сервера

Наступним постає завдання забезпечити зв’язок між підмережами головного офісу та мережою віддаленого. Для цього потрібно реалізувати на пограничних маршрутизаторах офісів технологію VPN з використанням протоколу IPsec. Для того, щоб маршрутизатори могли визначити, який трафік спрямовувати у захищений VPN-канал, необхідно створити та налаштувати ACL-списки, в яких вкажемо дозвіл на проходження трафіку з мережі головного офісу до мережі віддаленого та навпаки. Розглянемо налаштування ACL-списку на прикладі маршрутизатора Fakhardinov_Router_3.

ip access-list extended VPN15 //Створюємо новий ACL-список

//Дозволяємо проходження трафіку з підмереж головного офісу до мережі віддаленого

permit ip 10.23.73.0 0.0.0.31 10.23.72.192 0.0.0.63

permit ip 10.23.72.128 0.0.0.63 10.23.72.192 0.0.0.63

permit ip 10.23.73.32 0.0.0.31 10.23.72.192 0.0.0.63

permit ip 10.23.72.0 0.0.0.127 10.23.72.192 0.0.0.63

permit ip 10.1.15.0 0.0.0.255 10.23.72.192 0.0.0.63

Після створення ACL-списку необхідно налаштувати конфігурацію VPN на маршрутизаторі. Налаштування з маршрутизатора Fakhardinov_Router_3 наведено нижче.

license boot module c2900 technology-package securityk9 //Вмикаємо модуль безпеки securityk9, який необхідний для технології VPN

crypto isakmp policy 10 //Створюємо нову політику ISAKMP

encr 3des //Обираємо алгоритм 3des для шифрування трафіку, який проодитиме каналом

hash md5 //Обираємо хеш

authentication pre-share //Встановлюємо тип аутентифікації pre-share

group 2 //Обираємо групу

crypto isakmp key cisco address 64.100.13.2 //Створюємо ключ cisco та вказуємо адресу зовнішнього інтерфейсу маршрутизатора віддаленого офісу

crypto ipsec transform-set TS esp-3des esp-md5-hmac //Створюємо новий набір перетворень з назвою TS

crypto map MAP 10 ipsec-isakmp //Створюємо криптографічне зіставлення з номером 10

set peer 64.100.13.2 // Вказуємо адресу зовнішнього інтерфейсу маршрутизатора віддаленого офісу

set transform-set TS //Вказуємо попередньо створений набір перетворень

match address VPN15 //Вказуємо використання створеного ACL-списку

interface Serial0/3/0

crypto map MAP //Вмикаємо роботу зіставлення на зовнішньому інтерфейсі машрутизатора головного офісу

Після конфігурації пограничного маршрутизатора головного офісу, аналогічні налаштування виконуються на маршрутизаторі віддаленого офісу.

Вигляд заголовка пакету після проходження пограничного маршрутизатора показано на рисунку 3.6.

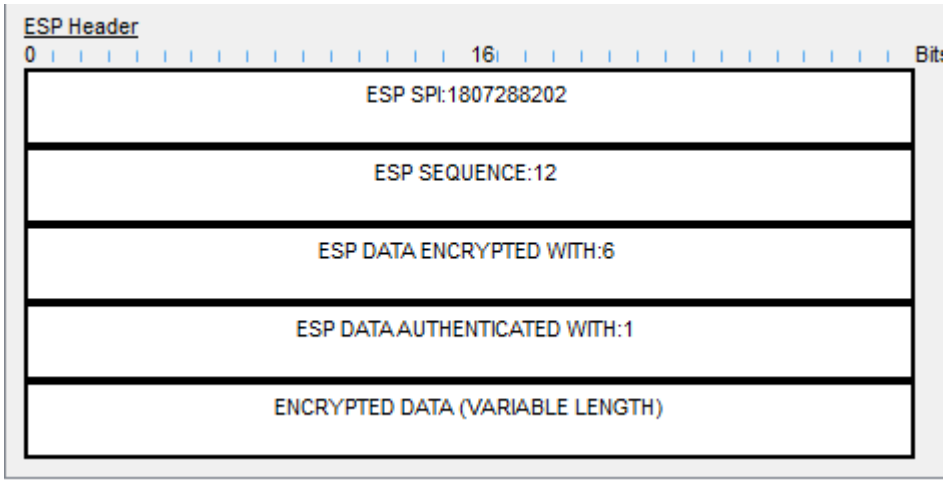

Рисунок 3.6 – Шифрування пакету

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Захист інформації в комп'ютерній системі є важливою задачею з точки зору забезпечення конфіденційності, цілісності та доступності даних. Нижче наведено декілька методів, які можуть бути використані для захисту інформації в комп'ютерній системі.

Аутентифікація і авторизація: Встановлення механізмів перевірки ідентифікації користувачів та контролю доступу до ресурсів системи на основі прав доступу. Це може включати використання паролів, біометричних методів (відбитки пальців, розпізнавання обличчя) або двофакторної аутентифікації.

Шифрування даних: Використання шифрування для захисту конфіденційності даних під час їх передачі або зберігання. Розрізняють симетричне шифрування (один ключ використовується для шифрування та

розшифрування) і асиметричне шифрування (використовується пара ключів: публічний для шифрування і приватний для розшифрування).

Фаєрволи: Використання фаєрволу для контролю мережевого трафіку і фільтрації пакетів даних. Фаєрволи можуть блокувати небажаний доступ до системи, а також допомагати виявляти та запобігати атакам.

Оновлення та патчі: Систематичне оновлення програмного забезпечення та встановлення патчів для усунення відомих вразливостей. Це допомагає запобігати зламу системи через використання вразливостей програм.

Фізичний захист: Забезпечення фізичної безпеки комп'ютерної системи, що включає контроль доступу до приміщення з серверами, використання захисних систем для запобігання крадіжок апаратного забезпечення та забезпечення резервного копіювання даних.

Моніторинг безпеки: Використання систем моніторингу безпеки для виявлення аномалій, наприклад, спроби несанкціонованого доступу або атаки на систему. Це допомагає вчасно реагувати на потенційні загрози та запобігати пошкодженню даних.

3.5.2 Налаштування віртуальних мереж VLAN

При проєктуванні підмережі LAN4 головного офісу виникла потреба розділити працівників компанії на окремі робочі групи без застосування нових маршрутизаторів. Для цього використаємо технологію віртуальних локальних мереж (VLAN). У таблиці 3.6 наведено номери та назви VLAN, які буде впроваджено у LAN4.

Таблиця 3.6 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
25	VLAN25	Відділ кадрів
35	VLAN35	Бухгалтерія
45	VLAN45	Call-центр

Продовження таблиці 3.6

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
99	Management	Для керування пристроями
100	Native	Власна

Для кожної VLAN, яку буде впроваджено, необхідно розрахувати адресу мережі. Для цього використаємо метод VLSM. Результати розрахунку адресації наведено у таблиці 3.7.

Таблиця 3.7 – Схема адресації VLAN

Назва підмережі	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
VLAN25	32	32	10.23.72.0	/27	10.23.72.1 – 10.23.72.30	10.23.72.31
VLAN35	32	32	10.23.72.32	/27	10.23.72.33 – 10.23.72.62	10.23.72.63
VLAN45	32	32	10.23.72.64	/27	10.23.72.65 – 10.23.72.94	10.23.72.95
Management	16	16	10.23.72.96	/28	10.23.72.97 - 10.23.72.110	10.23.72.111
Native	8	8	10.23.72.112	/29	10.23.72.113 - 10.23.72.118	10.23.72.119

Далі необхідно розподілити інтерфейси комутаторів у підмережі між VLAN, призначеними для вузлів. Результати розподілу наведено у таблиці 3.8.

Таблиця 3.8 – Розподіл портів комутаторів

Назва підмережі	VLAN	Розподіл портів
VLAN25	25	Fa0/15-Fa0/24
VLAN35	35	Fa0/10-Fa0/14
VLAN45	45	Fa0/5-Fa0/9

Після розподілу інтерфейсів призначимо адреси усім мережевим пристроям у підмережі. Результати наведено у таблиці 3.9.

Таблиця 3.9 – Адресація портів пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN
Fakhardinov_Switch_0	SVI	10.23.72.99	/28	10.23.48.225	99
Fakhardinov_Switch_1	SVI	10.23.72.98	/28	10.23.48.225	99
Fakhardinov_Switch_2	SVI	10.23.72.100	28		99
Fakhardinov_Router_2	G0/0.25	10.23.72.1	/27	-	23
	G0/0.35	10.23.72.33	/27	-	33
	G0/0.45	10.23.72.65	/27	-	43
	G0/0.99	10.23.72.65	/28	-	99

Наступним кроком необхідно виконати налаштування пристроїв, зазначені у таблицях вище. Спочатку налаштуємо інтерфейси комутаторів. Розглянемо налаштування на прикладі маршрутизатора Fakhardinov_Switch_0.

int range fa0/5-9 //Обираємо діапазон інтерфейсів для відповідного VLAN

switchport mode access //Вмикаємо режим access

switchport access vlan 45 //Призначаємо VLAN

int range fa0/10-14

switchport mode access

switchport access vlan 35

int range fa0/15-24

switchport mode access

switchport access vlan 25

int fa0/1

switchport mode trunk //Вмикаємо режим trunk

switchport trunk native vlan 100 //Призначаємо native VLAN

switchport trunk allowed vlan 19,29,39,99-100 //Вказуємо VLAN, які матимуть дозвіл на пересилання трафіку

Далі необхідно виконати конфігурування маршрутизатора таким чином, щоб забезпечити маршрутизацію для VLAN. Налаштування наведено нижче.

interface GigabitEthernet0/1.25 //Створюємо sub-інтерфейс на основному інтерфейсі маршрутизатора

encapsulation dot1Q 25 //Вмикаємо інкапсуляцію dot1Q

ip address 10.23.72.1 255.255.255.224 //Призначаємо адресу інтерфейсу

interface GigabitEthernet0/1.35

encapsulation dot1Q 35

ip address 10.23.72.33 255.255.255.224

interface GigabitEthernet0/1.45

encapsulation dot1Q 45

ip address 10.23.72.65 255.255.255.224

interface GigabitEthernet0/1.99

encapsulation dot1Q 99

ip address 10.23.72.97 255.255.255.240

3.5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

Для створених VLAN необхідно виконати налаштування DHCP. Налаштування маршрутизатора наведено нижче.

//Виключаємо з роздачі перші 10 адрес кожного VLAN та адресу сервера.

ip dhcp excluded-address 10.23.72.1 10.23.72.10

ip dhcp excluded-address 10.23.72.33 10.23.72.42

ip dhcp excluded-address 10.23.72.65 10.23.72.74

ip dhcp excluded-address 10.23.72.25

ip dhcp pool VLAN25 //Створюємо новий DHCP-пул

network 10.23.72.0 255.255.255.224 //Призначаємо мережу для розподілення адрес

default-router 10.23.72.1 // Вказуємо шлюз за замовчуванням

dns-server 10.23.73.25 //Вказуємо DNS-сервер

ip dhcp pool VLAN35

network 10.23.72.32 255.255.255.224

default-router 10.23.72.33

dns-server 10.23.73.25

ip dhcp pool VLAN45

network 10.23.72.64 255.255.255.224

default-router 10.23.72.65

dns-server 10.23.73.25

Для забезпечення безпеки серверів у мережі необхідно виконати конфігурацію інтерфейсів, до яких вони підєднані. Команди конфігурації наведені нижче.

switchport port-security //Вмикаємо захист на інтерфейсі

switchport port-security maximum 2 //Дозволяємо тільки двом унікальним пристроям доступ до порту

switchport port-security mac-address sticky //Закріплюємо за інтерфейсом адресу, яка в даний момент працює на інтерфейсі

switchport port-security violation restrict //Вмикаємо відкидання пакетів з незареєстрованої MAC-адреси та повідомляє про це у консоль.

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента системи

У якості компоненту системи буде впроваджено IoT-систему в офісах компанії.

IoT означає Інтернет речей. Концепція IoT полягає в тому, щоб цим пристроям дозволити комунікувати та взаємодіяти один з одним. Ця взаємодія дозволяє безперешкодний обмін даними та призводить до покращення ефективності, автоматизації та комфорту у різних сферах життя, таких як домашні господарства, промисловість, охорона здоров'я, транспорт та міста.

Необхідно впровадити систему інтернету речей, яка буде забезпечувати базову безпеку приміщень офісів (за допомогою RFID зчитувача карток, сенсору руху та сирени) та виявляти пожежі (за допогою датчика вогню). Також у приміщенні головного офісу система повинна регулювати температуру повітря за допомогою кондиціонеру та обігрівача (температура повинна знаходитись у межах від 15 до 25 градусів за Цельсієм).

4.2 Налаштування обладнання та сервісів системи IoT

Для того, аби все обладнання могло взаємодіяти одне з одним, необхідно під’єднати його до HomeGateway за допомогою Wi-Fi (в даному випадку необхідно вказати SSID маршрутизатора та пароль) або Ethernet кабелів. Після цього в налаштуваннях необхідно зазначити, що у ролі IoT сервера буде використовуватися безпосередньо HomeGateway. Приклад налаштування пристроїв зображено на рисунку 4.1 та 4.2.

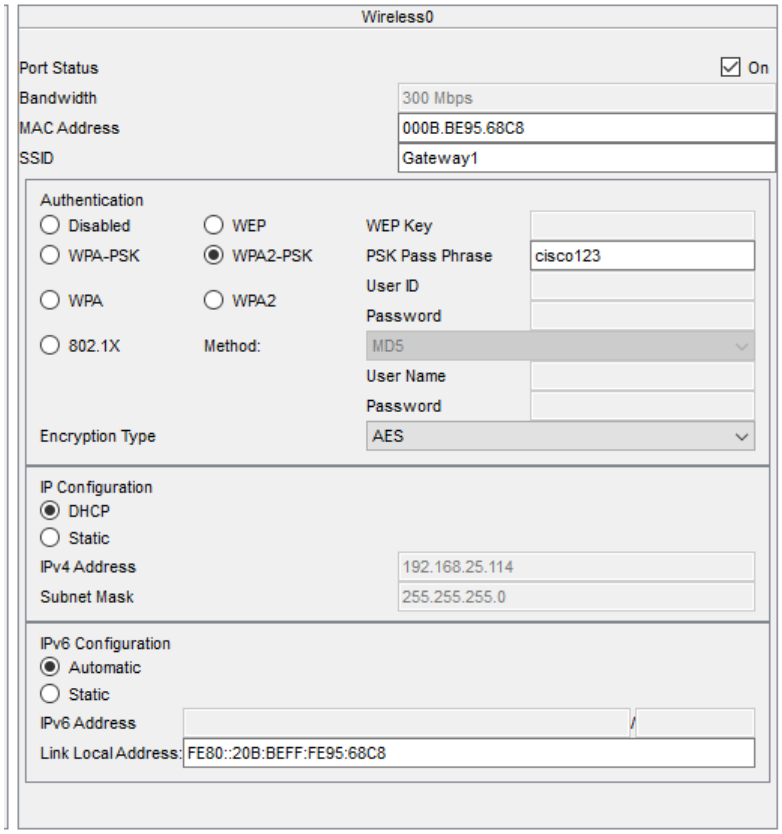

Рисунок 4.1 – Налаштування бездротового з’єднання

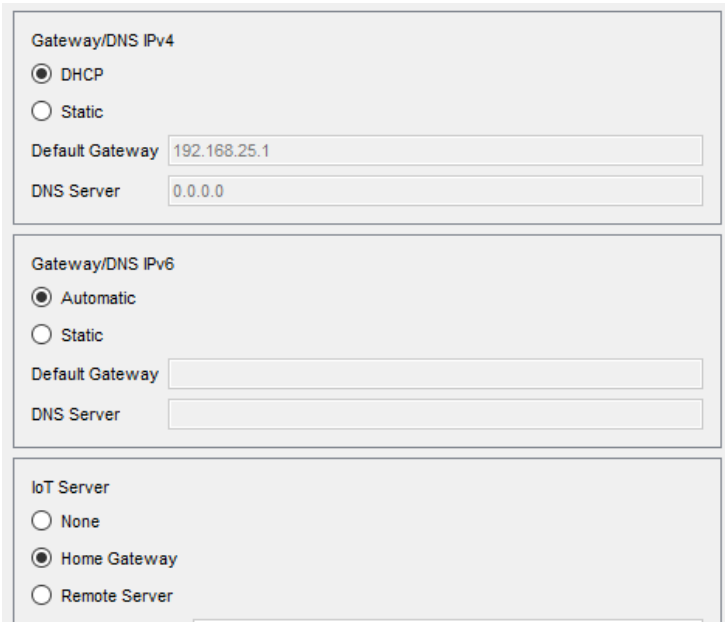

Рисунок 4.2 – Налаштування IoT сервера на пристроях

Після під’єднання усіх пристроїв до шлюзів отримуємо схему мережі з IoT системою (рисунок 4.3).

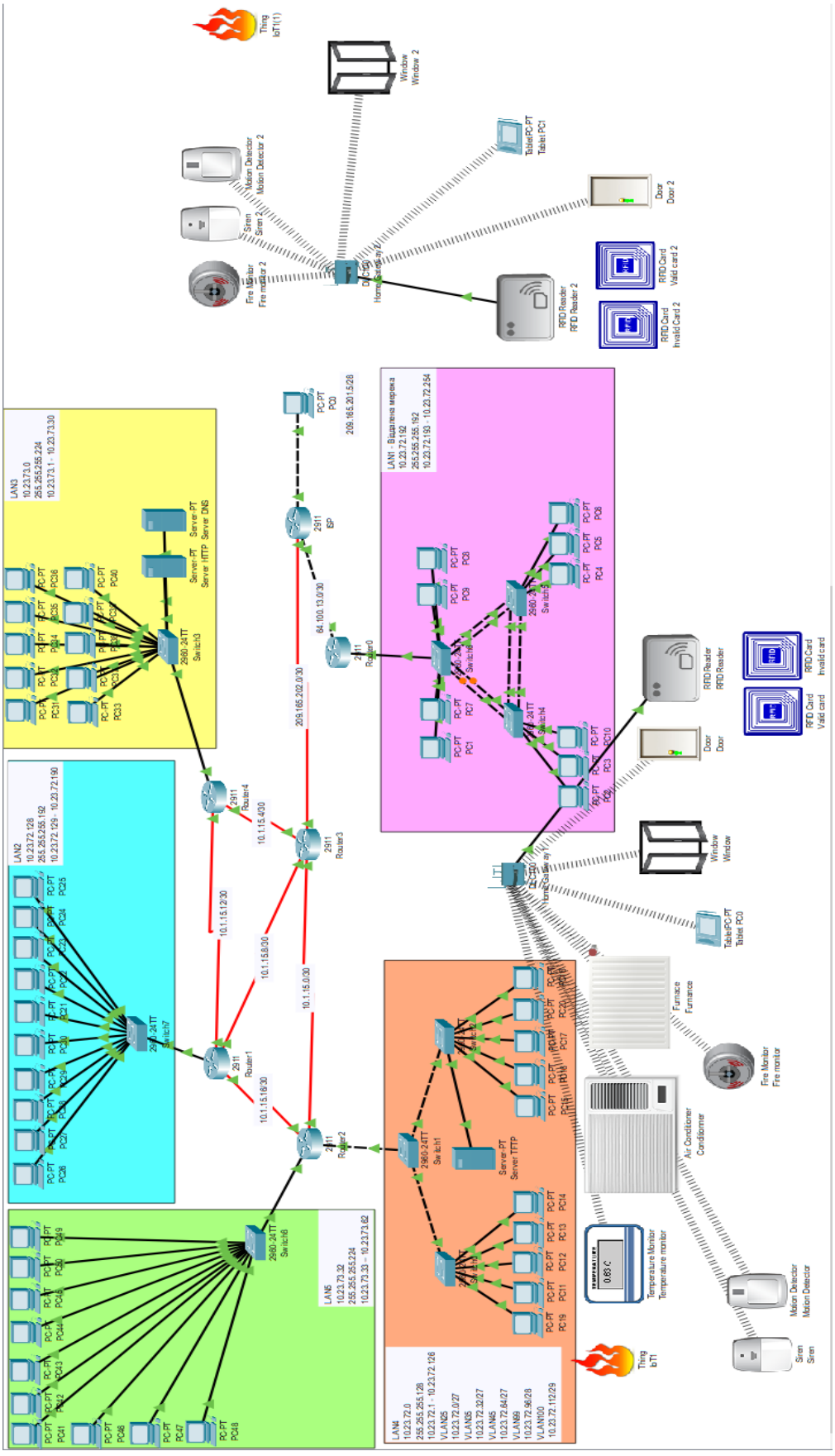

Рисунок 4.3 – Схема мережі з IoT системою

Далі перейдемо до налаштувань розумних пристроїв за допомогою створення сценаріїв. Першим створимо сценарій для відмикання дверей за RFID картокою (рисунок 4.4).

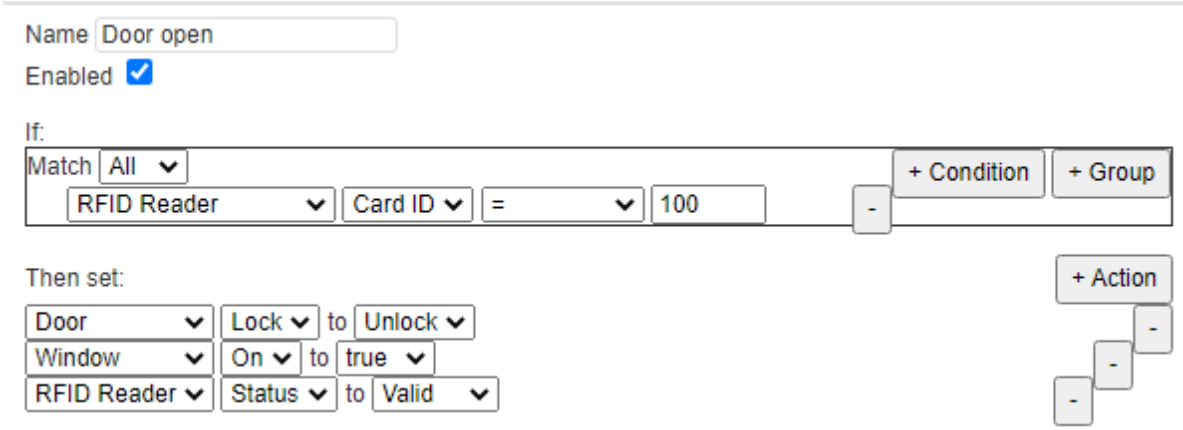

Рисунок 4.4 – Сценарій для відчинення дверей

Аналогічно створимо сценарій для замикання дверей (рисунок 4.5).

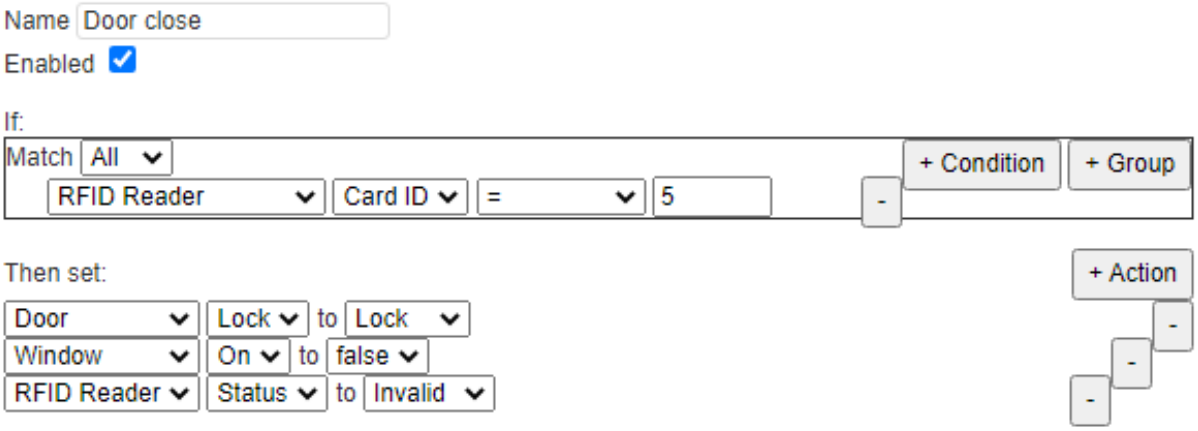

Рисунок 4.5 – Сценарій для відмикання дверей

Далі створимо сценарій, за яким буде вмикатися кондиціонер, якщо температура повітря піднялася вище 25 градусів за Цельсієм (рисунок 4.6).

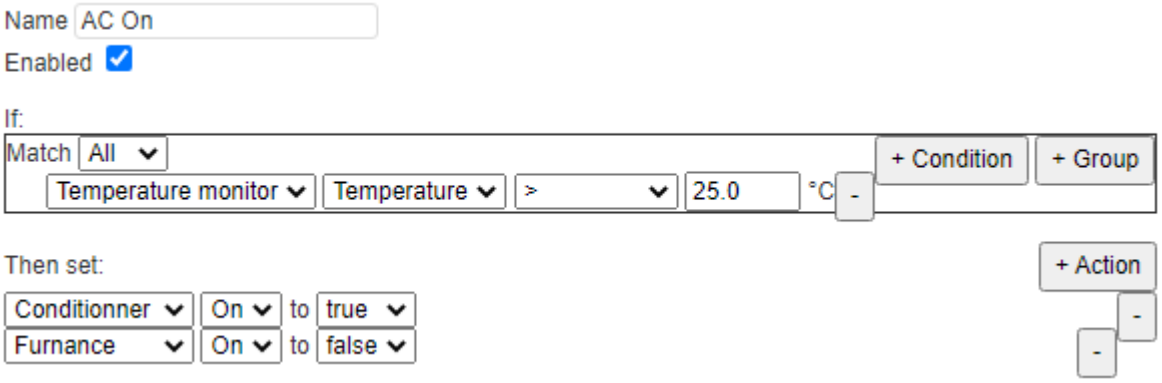

Рисунок 4.6 – Сценарій увімкнення кондиціонеру

Після нього створимо сценарій увімкнення обігрівача, якщо температура опуститься нижче 15 градусів за Цельсієм (рисунок 4.7).

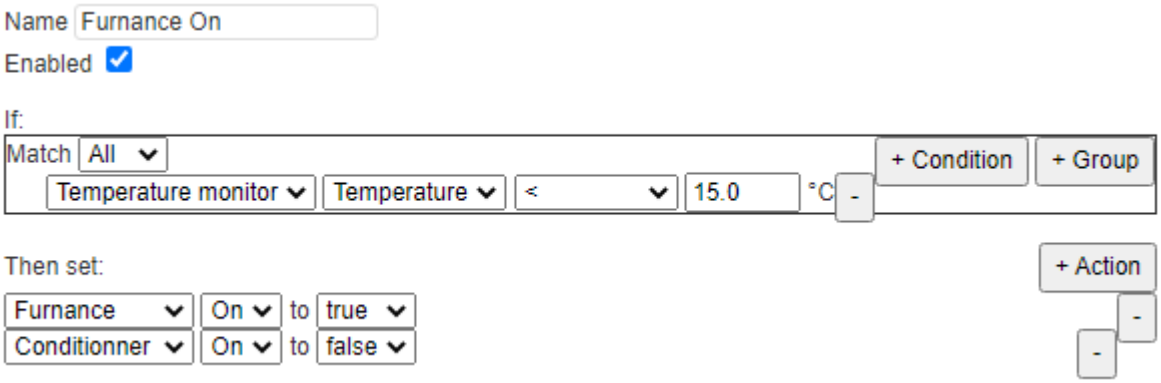

Рисунок 4.7 – Сценарій увімкнення обігрівача

Далі створюємо сценарій, який спрацьовує у випадку активації детектора вогню (рисунок 4.8). За даним сценарієм вмикається сирена, відчиняються вікна та двері, а також вимикаються прилади контролю температури.

Рисунок 4.8 – Сценарій спрацювання детектора вогню

Після цього створимо сценарій для спрацювання сенсора руху, який вмикає сирену та замикає двері та вікна (рисунок 4.9).

Рисунок 4.9 – Сценарій спрацювання сенсора руху

Останнім налаштуємо сценарій, який буде вимикати сирену у разі відсутності загроз (рисунок 4.10).

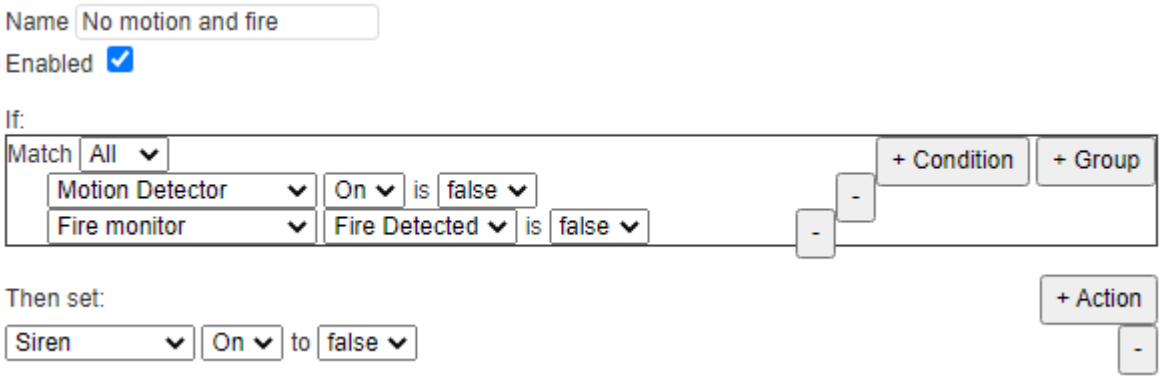

Рисунок 4.10 – Сценарій вимикання сирени

Усі створені на сервері сценарії наведено на рисунку 4.11. Аналогічні до цих налаштування виконуються для офісу віддаленої мережі.

IoT Monitor X

IoT Server - Device Conditions

Home | Conditions | Editor | Log Out

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	Door open	RFID Reader Card ID = 100	Set Door Lock to Unlock Set Window On to true Set RFID Reader Status to Valid
Edit Remove	Yes	Door close	RFID Reader Card ID = 5	Set Door Lock to Lock Set Window On to false Set RFID Reader Status to Invalid
Edit Remove	Yes	AC On	Temperature monitor Temperature > 25.0 °C	Set Conditionner On to true Set Furnance On to false
Edit Remove	Yes	Furnance On	Temperature monitor Temperature < 15.0 °C	Set Furnance On to true Set Conditionner On to false
Edit Remove	Yes	Fire detected	Fire monitor Fire Detected is true	Set Siren On to true Set Window On to true Set Door Lock to Unlock Set Furnance On to false Set Conditionner On to false
Edit Remove	Yes	Motion True	Motion Detector On is true	Set Siren On to true Set Door Lock to Lock Set Window On to false
Edit Remove	Yes	No motion and fire	Match all: • Motion Detector On is false • Fire monitor Fire Detected is false	Set Siren On to false

Рисунок 4.11 – Список сценаріїв на сервері

ВИСНОВКИ

У даному дипломному проекті була проведена розробка та налаштування корпоративної мережі для юридичної компанії "Justice". Метою проекту було створення надійної, безпечної та ефективної мережевої інфраструктури, яка задовольняла потреби компанії в комунікації та обміні даними.

Проект включав кілька основних етапів. Починаючи з аналізу потреб компанії, були визначені вимоги до мережі та її функціональні характеристики. На основі цих вимог було розроблено проект мережевої інфраструктури, включаючи фізичну топологію, вибір обладнання та схему адресації IP.

Після розробки проекту було проведено налаштування та розгортання мережі. Було встановлено необхідне обладнання, налаштовані параметри безпеки та забезпечено взаємозв'язок між мережевими пристроями. Після завершення налаштування були проведені тестування та впровадження мережі.

Результатом проекту є створена корпоративна мережа, яка задовольняє потреби компанії "Justice" у забезпеченні безперебійного обміну даними та комунікації між внутрішніми підрозділами. Мережа виявилася ефективною та надійною, забезпечуючи швидку передачу даних і захищений доступ до ресурсів.

Процес розробки та налаштування корпоративної мережі показав важливість детального аналізу потреб компанії, правильного вибору обладнання та налаштування безпеки мережі. Даний проект може послужити прикладом для інших організацій, які прагнуть покращити свою мережеву інфраструктуру.

ПЕРЕЛІК ПОСИЛАНЬ

1. Юридична компанія «Justice», Бізнесу – [Електронний ресурс] – https://www.justice.dp.ua/zashhita-biznesa/ (дата звернення 13.05.2023)

2. Харківський національний університет внутрішніх справ, «Інформаційне забезпечення професійної діяльності», С. М. Виганяйло, 2021 – [Посібник] – 19 с.

3. Що таке хмарні технології – [Електронний ресурс] – https://business.diia.gov.ua/cases/tehnologii/so-take-hmarni-tehnologii-i-ak-voni-mozut-dopomogti-vasomu-pidpriemstvu (дата звернення 14.05.2023)

4. Основні принципи та переваги впровадження електронного документообігу – [Електронний ресурс] - https://sites.google.com/site/elektrdokumentoobig/osnovni-principi-ta-perevagi-vprovadzenna-elektronnogo-dokumentoobigu (дата звернення 14.05.2023)

5. Що таке CRM-система – [Електронний ресурс] – https://www.creatio.com/page/uk/definition-crm (дата звернення 14.05.2023)

6. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 62 с.

ДОДАТОК А

Текст програми налаштування обладнання корпоративної мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23015-01 12 01

Листів 10

2023

АНОТАЦІЯ

Дана програма включає частину програмного коду, яка служить для програмування налаштування складових елементів корпоративної мережі комп'ютерної системи.

Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і VTY ліній та створення віртуальних приватних мереж (VPN) та домену комп'ютерної системи.

ЗМІСТ

1. Скрипт налаштування Router3

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Fakhardinov_Router_3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username 123191_Fakhardinov password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX15241WO1-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 64.100.13.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
```

```
!
crypto map MAP 10 ipsec-isakmp
set peer 64.100.13.2
set transform-set TS
match address VPN15
!
!
!
!
ip domain-name Fakhardinov_Router_3
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/2/0
ip address 10.1.15.5 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Serial0/2/1
ip address 10.1.15.9 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Serial0/3/0
ip address 209.165.202.2 255.255.255.252
ip nat outside
crypto map MAP
```

```
!
interface Serial0/3/1
ip address 10.1.15.1 255.255.255.252
ip nat inside
clock rate 2000000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
network 10.1.15.4 0.0.0.3 area 0
network 10.1.15.8 0.0.0.3 area 0
network 10.1.15.0 0.0.0.3 area 0
network 209.165.202.0 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
ip nat inside source list NAT15 pool Internet
ip nat inside source static 10.23.73.26 209.165.200.4
ip nat inside source static 10.23.73.25 209.165.200.3
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 209.165.201.0 255.255.255.240 209.165.202.1
ip route 209.165.202.0 255.255.255.252 Serial0/3/0
!
ip flow-export version 9
!
!
ip access-list extended VPN15
permit ip 10.23.73.0 0.0.0.31 10.23.72.192 0.0.0.63
permit ip 10.23.72.128 0.0.0.63 10.23.72.192 0.0.0.63
permit ip 10.23.73.32 0.0.0.31 10.23.72.192 0.0.0.63
permit ip 10.23.72.0 0.0.0.127 10.23.72.192 0.0.0.63
permit ip 10.1.15.0 0.0.0.255 10.23.72.192 0.0.0.63
ip access-list extended NAT15
deny ip 10.23.73.0 0.0.0.31 10.23.72.192 0.0.0.63
deny ip 10.23.72.128 0.0.0.63 10.23.72.192 0.0.0.63
deny ip 10.23.73.32 0.0.0.31 10.23.72.192 0.0.0.63
deny ip 10.23.72.0 0.0.0.127 10.23.72.192 0.0.0.63
deny ip 10.1.15.0 0.0.0.255 10.23.72.192 0.0.0.63
permit ip 10.23.73.0 0.0.0.31 any
permit ip 10.23.72.128 0.0.0.63 any
permit ip 10.23.73.32 0.0.0.31 any
permit ip 10.23.72.0 0.0.0.127 any
permit ip 10.1.15.0 0.0.0.255 any
!
banner motd ^CFakhardinov_Router_3^C
!
```

```
radius server 10.23.73.25
address ipv4 10.23.73.25 auth-port 1645
key radius123
!
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```

2. Скрипт налаштування Router0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Fakhardinov_Router_0
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 10.23.72.193 10.23.72.202
!
ip dhcp pool LAN1
network 10.23.72.192 255.255.255.192
default-router 10.23.72.193
dns-server 209.165.200.3
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
```

```
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username 123191_Fakhardinov password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX15247463-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 209.165.202.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.2
set transform-set TS
match address VPN15
!
!
!
!
ip domain-name Fakhardinov_Router_0
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.23.72.193 255.255.255.192
ip nat inside
```

```
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 64.100.13.2 255.255.255.252
ip nat outside
duplex auto
speed auto
crypto map MAP
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Vlan1
no ip address
shutdown
!
ip nat pool Internet 209.165.205.5 209.165.205.30 netmask
255.255.255.224
ip nat inside source list NAT15 pool Internet
ip classless
ip route 0.0.0.0 0.0.0.0 64.100.13.1
ip route 64.100.13.0 255.255.255.252 64.100.13.1
ip route 209.165.201.0 255.255.255.240 64.100.13.1
!
ip flow-export version 9
!
!
ip access-list extended VPN15
permit ip 10.23.72.192 0.0.0.63 10.23.73.0 0.0.0.31
permit ip 10.23.72.192 0.0.0.63 10.23.72.128 0.0.0.63
permit ip 10.23.72.192 0.0.0.63 10.23.73.32 0.0.0.31
permit ip 10.23.72.192 0.0.0.63 10.23.72.0 0.0.0.127
permit ip 10.23.72.192 0.0.0.63 10.1.15.0 0.0.0.255
ip access-list extended NAT15
deny ip 10.23.72.192 0.0.0.63 10.23.73.0 0.0.0.31
deny ip 10.23.72.192 0.0.0.63 10.23.72.128 0.0.0.63
deny ip 10.23.72.192 0.0.0.63 10.23.73.32 0.0.0.31
deny ip 10.23.72.192 0.0.0.63 10.23.72.0 0.0.0.127
deny ip 10.23.72.192 0.0.0.63 10.1.15.0 0.0.0.255
permit ip 10.23.72.192 0.0.0.63 any
!
banner motd ^CFakhardinov_Router_0^C
!
radius server 10.23.73.25
address ipv4 10.23.73.25 auth-port 1645
key radius123
!
```

```
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```