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 Шаравари Сергія Володимировича
(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 фірми "Legalitas" з реалізацією побудови, налаштування та безпеки корпоративної мережі."
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	доц. Бешта Д.О.			
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
(повна назва)
Гнатушенко В.В.
(підпис) (прізвище, ініціали)
" " 2023 року

ЗАВДАННЯ
на кваліфікаційну
роботу ступеня
бакалавр

студента Шаравара С.В. **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 фірми "Legalitas" з реалізацією побудови, налаштування та безпеки корпоративної мережі."

затверджену наказом ректора НТУ «Дніпровська політехніка» від 11.04.2023 № 256-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 доц. Бешта Д.О..

Дата видачі 10.02.2023

Дата подання до екзаменаційної комісії .06.2023

Прийнято до виконання Шаравара С.В,

РЕФЕРАТ

Пояснювальна записка: 76с., 23рис., 12табл., 2додатки, 6 джерел.

VLAN, ACL, DHCP, VPN, NAT, МАРШРУТИЗАТОР, КОМУТАТОР, CISCO, CISCO PACKET TRACER

Об’єкт розробки: комп’ютерна система для компанії — «Legalitas» та налаштуванням корпоративної мережі.

Мета: створення комп’ютерної системи для компанії — «Legalitas»

Розроблена комп’ютерна мережа з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову систем контролю та редагування для компанії — «Legalitas» в м.Дніпро, а також для збору і підготовки статистичної інформації. Система побудована на основі принципів відкритості її архітектури, що дозволяє здійснювати технічну і програмну її модернізацію.

Розробка комп’ютерної мережі виконана відповідно до завдання на дипломну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Також технологія проектування мережі включає захист всього обладнання внутрішньої мережі від несанкціонованого доступу.

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

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПК – Персональний комп’ютер .

ПЗ – Програмне забезпечення.

КС – Комп’ютерна система.

VLAN – Virtual Local Area Network – віртуальна локальна комп'ютерна мережа.

ACL – Access Control List – список контролю доступу.

VPN – Virtual Private Network – віртуальна приватна мережа.

DHCP – Dynamic Host Configuration Protocol – протокол динамічної конфігурації вузла

NAT – Network Address Translation – перетворення мережевих адрес.

СКМ – Структурована кабельна мережа.

VLSM – Variable Length Subnet Mask – маска підмережі змінної довжини.

ВСТУП

В сучасному світі інформаційні технології займають важливе місце у функціонуванні різних сфер діяльності, включаючи правову сферу. Юридичні фірми використовують комп'ютерні мережі для поліпшення ефективності своєї роботи, забезпечення надійного зберігання та обміну конфіденційною інформацією, а також забезпечення безпеки даних клієнтів.

Метою даної кваліфікаційної роботи є дослідження та розробка впровадження комп’ютерної системи в Юридичній Фірмі «Legalitas» з метою підвищення ефективності роботи, забезпечення безпеки даних та поліпшення зв'язку в межах організації.

У процесі виконання кваліфікаційної роботи будуть вирішені такі завдання:

1. Аналіз потреб юридичної фірми Legalitas у впровадженні комп'ютерних мереж.
2. Вивчення сучасних стандартів та технологій у галузі комп'ютерних мереж.
3. Розробка оптимальної архітектури комп'ютерної мережі для Юридичної Фірми «Legalitas».
4. Вибір необхідного обладнання та програмного забезпечення для впровадження комп'ютерних мереж.
5. Розробка плану впровадження та виконання проекту зі створення комп'ютерної мережі в організації.
6. Впровадження комп'ютерної мережі та оцінка результатів.

Для досягнення цілей кваліфікаційної роботи буде використано методи дослідження, включаючи аналіз літературних джерел, вивчення нормативно-правових актів.

Результати кваліфікаційної роботи дозволять Юридичній Фірмі Legalitas покращити свою ефективність, забезпечити безпеку даних та підвищити якість зв'язку в організації.

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика галузі та умови застосування КС

Юридична галузь - це сукупність правових відносин та норм, які регулюють поведінку людей та юридичних осіб в суспільстві. Ця галузь має на меті забезпечення правової охорони прав та свобод громадян та юридичних осіб, забезпечення порядку та стабільності в суспільстві, вирішення конфліктних ситуацій та захист від незаконних дій. Юридичні послуги надаються як юридичними особами (адвокатами, нотаріусами, юристами), так і державними органами (судами, прокуратурою, міліцією, іншими правоохоронними органами).

У сучасному світі юридична галузь постійно розвивається та адаптується до змін у суспільстві та технологій. Комп'ютерні системи та програмне забезпечення дозволяють автоматизувати та оптимізувати багато процесів, пов'язаних з юридичною діяльністю, що підвищує її ефективність та точність. Наприклад, електронні системи обліку та збереження документів, юридичні бази даних, електронний цифровий підпис та інші інструменти дозволяють зберігати, переглядати та обробляти великі обсяги юридичної інформації.

Застосування комп'ютерних систем у юридичній галузі також дозволяє забезпечити безпеку та конфіденційність обробки даних, а також забезпечує швидкий та зручний доступ до потрібної інформації. Багато юридичних компаній та державні органи використовують спеціалізовані програмні засоби для підтримки своєї діяльності. Наприклад, електронні системи управління справами дозволяють зберігати та контролювати всю необхідну юридичну документацію та інформацію про справи, адвокатські програми дозволяють вести облік клієнтів, проводити підрахунок юридичних витрат та інше.

Однак, використання комп'ютерних систем у юридичній галузі також має свої виклики та обмеження. Наприклад, проблеми з безпекою даних, недостатня якість програмного забезпечення, юридичні та етичні проблеми, пов'язані з використанням штучного інтелекту та автоматизації деяких процесів.

1.2 Характеристика і структура об’єкта впровадження

1.2.1 Характеристика об’єкта впровадження

Об’єкт впровадження – офіс юридичної компанії «Legalitas».

Юридична компанія «Legalitas» працює на українському ринку з 2013 року. Сферою спеціалізації компанії є захист прав та інтересів клієнтів у загальних, господарських та адміністративних судах. Важливим напрямком практики Юридичної компанії “Legalitas” є податкове та митне право. Зокрема, вона надає допомогу підприємцям під час податкових перевірок, при оскарженні податкових повідомлень-рішень, а також в спорах з митними органами при здійсненні експортно-імпортних операцій. Компанія надає послуги в області корпоративного права (займається реєстрацією підприємств, заміною учасників, внесенням змін до статуту, ліквідацією підприємств і т. д.).

Компанія має в своєму складі досвідчених адвокатів, які забезпечують надання правової допомоги в справах кримінального права. Цей напрямок є одним з основних видів діяльності компанії.

Одним із головних напрямків діяльності компанії "Legalitas" є надання абонентського юридичного обслуговування для фізичних осіб-підприємців та юридичних осіб. Компанія об'єднує фахівців з різних галузей права, що дозволяє надавати кваліфіковану юридичну допомогу без перерви, забезпечуючи взаємозамінність юристів.[1]

1.2.2 Організаційна структура підприємства

Організаційна структура компанії «Legalitas» складається з наступник відділів:

– керуючий партнер;

– керівники відділів;

– відділ корпоративного права;

– відділ цивільного та господарського права;

– відділ податкового права;

– відділ кримінального права;

– відділ сімейного та спадкового права;

– відділ судової практики;

– відділ юридичного обслуговування бізнесу;

– відділ реєстрації та обслуговування офшорних компаній;

– відділ супроводу зовнішньоекономічної діяльності.

Компанія має організаційну структуру управління типу лінійно-функціональної. Ця структура є одним із варіантів організаційної структури, де всі підрозділи підпорядковані головному керівнику або керівництву ланки.

Керівники кожного підрозділу звітують про свою діяльність безпосередньо керівництву та мають повноваження видачі доручень своїм підлеглим.

Відділи корпоративного, цивільного та господарського, податкового, кримінального, сімейного, та спадкового права, а також відділ судової практики та відділ юридичного обслуговування бізнесу знаходяться у головному офісі. Відділ реєстрації та обслуговування офшорних компаній та відділ супроводу зовнішньоекономічної діяльності знаходяться у віддаленому офісі.

Схему організаційної структури підприємства наведено на рисунку 1.4.

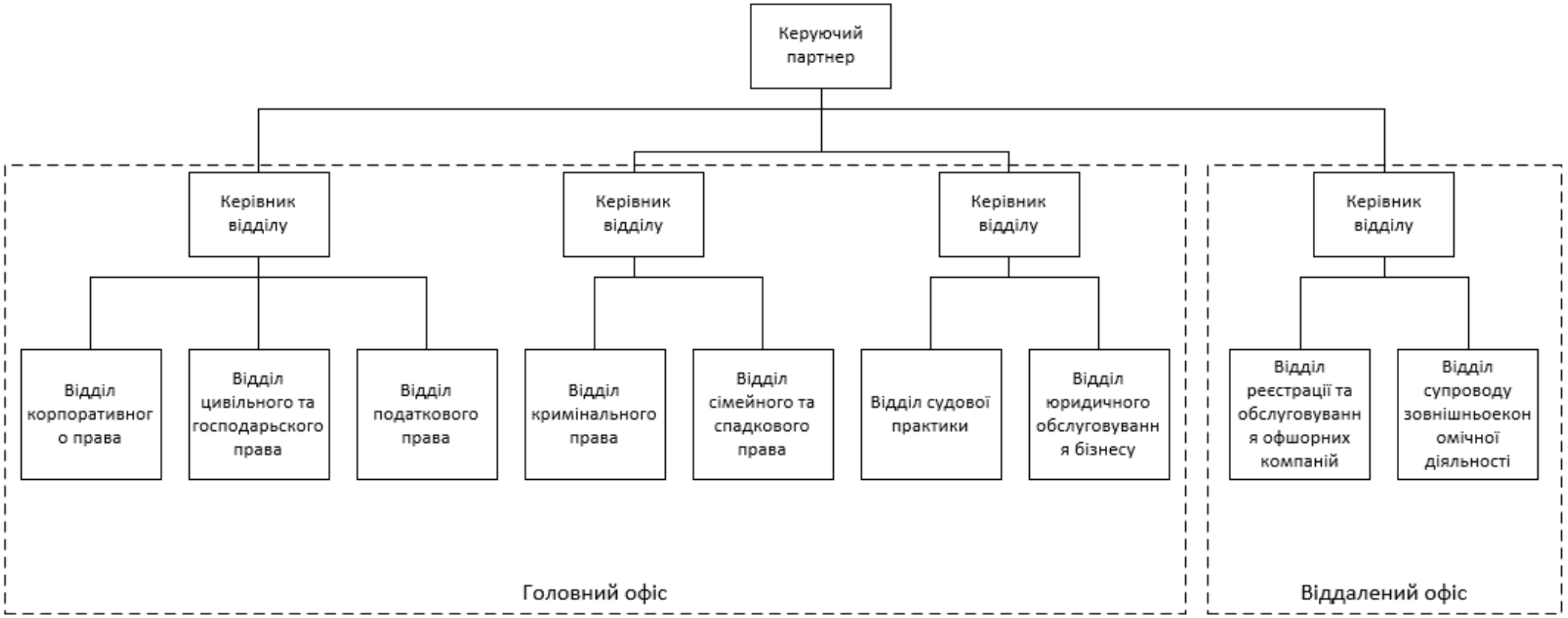

Рисунок 1.1 – Організаційна структура підприємства.

1.2.3 Розміщення структурних підрозділів підприємства

Топографічне розміщення офісу юридичної компанії «Legalitas» складається з двох будівель у м. Дніпро.

Головний офіс складається з трьох поверхів багатоповерхової будівлі, що знаходиться за адресою Україна, 49000, Дніпропетровська область, м. Дніпро, проспект Дмитра Яворницького, 5. Віддалений офіс знаходяться за адресою 49000, Дніпропетровська область, м. Дніпро, вул Січових стрільців, 67-А, компанія орендує перший поверх будівлі. Відстань між офісами 2340м по прямій. Схему гео-розміщення офісів зображено на рисунку 1.1.

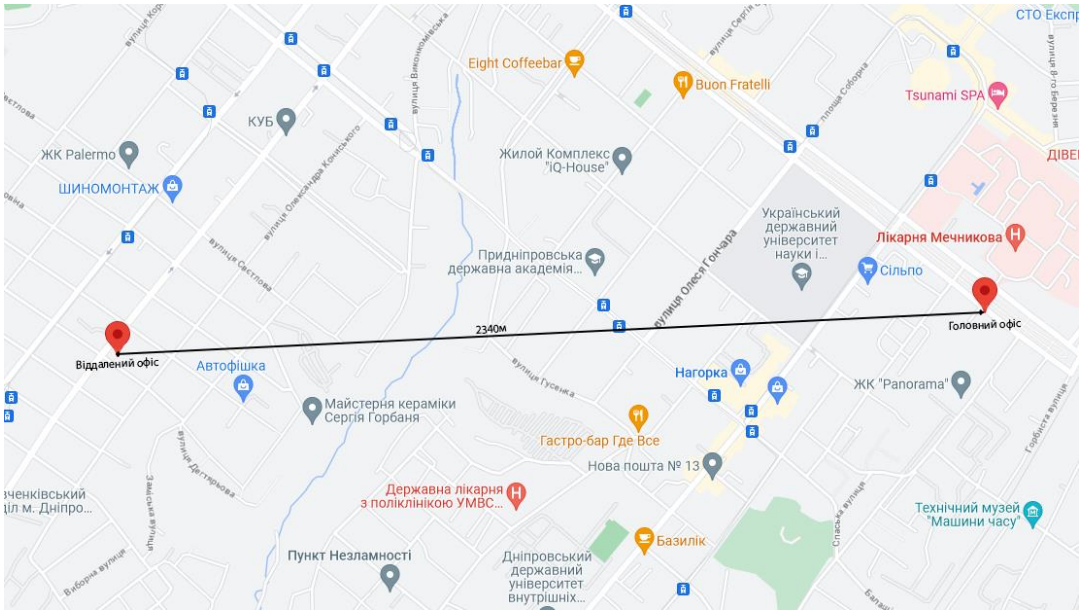

Рисунок 1.2 – Схема гео-розміщення офісів юридичної компанії «Legalitas».

Структурну схему розміщення відділів підприємства розглянемо на відділах корпоративного, цивільного, господарського та податкового права, що знаходяться у головному офісі (рисунок 1.3), та на відділах судової практики та юридичного обслуговування бізнесу, що знаходяться у віддаленому офісі (рисунок 1.4).

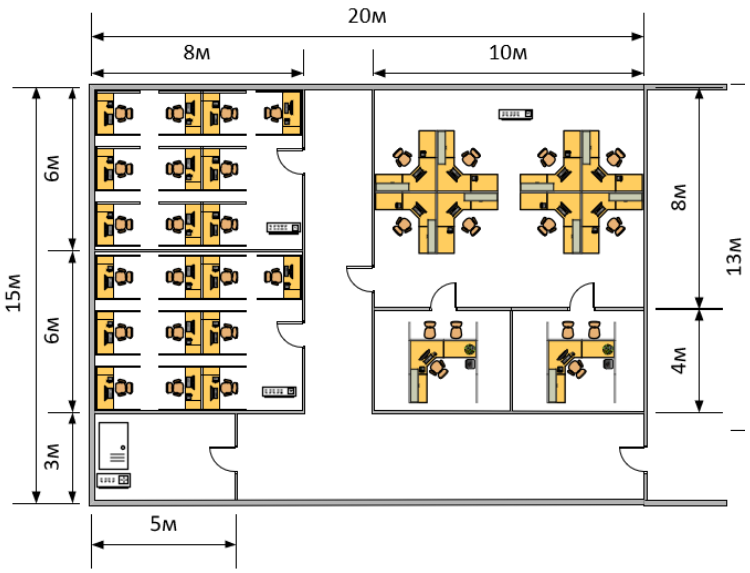

Рисунок 1.3 – Структурна схема відділів корпоративного, цивільного, господарського та податкового права

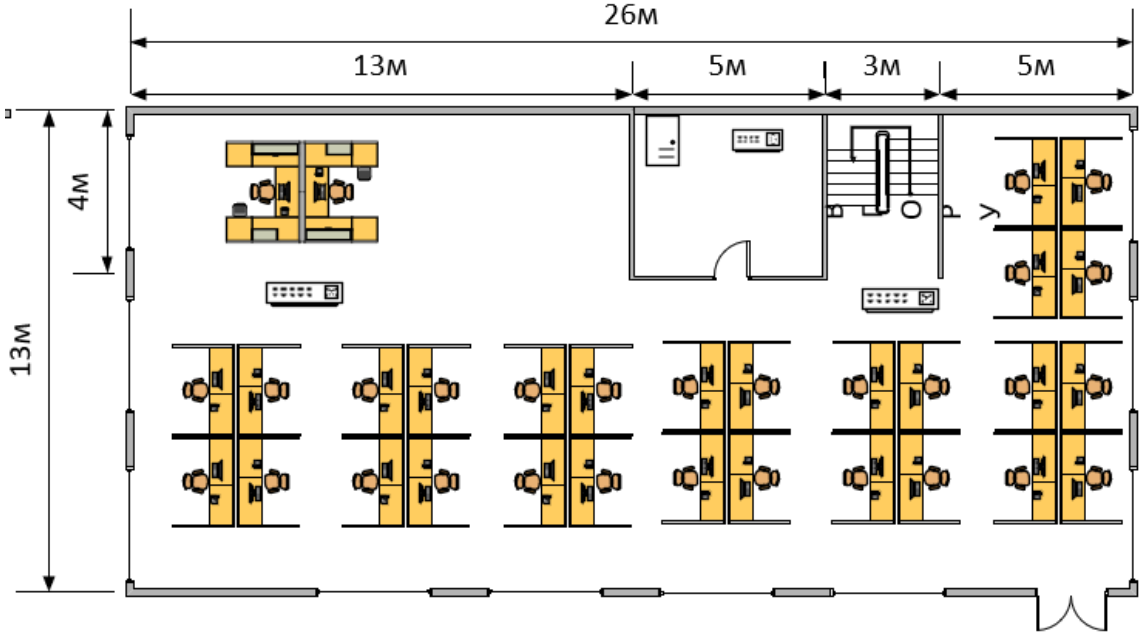

Рисунок 1.4 – Структурна схема віддаленого офісу

1.3 Принципи та технічні способи інформаційного забезпечення об’єкта впровадження

Юридичні організації активно використовують інформаційні технології для забезпечення швидкої та ефективної діяльності. Нижче описано ряд принципів, технічних методів, які використовуються для забезпечення інформаційного супроводу юридичних фірм:

1. Аутентифікація та авторизація:

– Використання паролів, пін-кодів, біометричних даних та інших методів аутентифікації для перевірки ідентифікації користувачів та їхнього доступу до системи.

– Встановлення різних рівнів доступу та прав, залежно від ролі користувача, для забезпечення авторизованого доступу до важливої інформації.

2. Шифрування даних:

– Використання алгоритмів шифрування для захисту конфіденційності даних при їх передачі та збереженні.

– Використання SSL / TLS протоколів для шифрування комунікації між клієнтами і серверами.

3. Бекап та відновлення даних:

– Регулярне створення резервних копій важливої інформації і збереження їх в безпечних місцях, які забезпечують відновлення даних у разі їх втрати, пошкодження

4. Конфіденційність:

– Використання шифрування для захисту конфіденційності даних під час їх передачі та збереження.

– Встановлення політик доступу і контролю прав, щоб забезпечити, що лише авторизовані користувачі мають доступ до конфіденційної інформації.

5. Цілісність:

– Використання методів контролю цілісності даних, таких як хеш-функції, щоб переконатися, що дані не були змінені без дозволу або усвідомлення.

– Встановлення механізмів виявлення вторгнень та інтегрітету даних для виявлення та запобігання несанкціонованим змінам.

6. Доступність:

– Забезпечення належної фізичної і кібернетичної інфраструктури для забезпечення доступності систем та послуг.

– Встановлення механізмів резервування та відновлення для швидкого відновлення роботи у разі відмови або інциденту.

7. Автентифікація та авторизація:

– Використання сильних методів аутентифікації, таких як двофакторна аутентифікація або біометричні дані, для перевірки ідентичності користувачів.

– Встановлення політик авторизації, що дозволяють контролювати рівень доступу користувачів до систем та даних.

8. Моніторинг та аудит:

– Використання систем моніторингу та аудиту для виявлення та відслідковування несанкціонованої діяльності, аномалій та інших потенційних загроз.

– Аналіз журналів подій та реагування на виявлені проблеми для забезпечення безпеки та забезпечення належного функціонування системи.

1.4 Аналітичний огляд існуючих способів обробки та передачі інформації

У юридичних фірмах зазвичай існує велика кількість документів та інформації, які потрібно обробляти та передавати між співробітниками та клієнтами. Отже, важливо забезпечити високий рівень безпеки та конфіденційності цієї інформації. Для досягнення цієї мети можна використовувати різні способи обробки та передачі інформації, зокрема:

– Електронна пошта. Електронна пошта є одним з найпоширеніших способів обміну інформацією у юридичних фірмах. Для забезпечення безпеки інформації можна використовувати шифрування електронної пошти та електронного підпису. Ці засоби забезпечують автентифікацію

відправника та захист від перехоплення та зміни інформації в процесі передачі.

– Хмарні сховища. Хмарні сховища є зручним способом зберігання та обміну документами та іншою інформацією. Для забезпечення безпеки можна використовувати шифрування даних на рівні сервера та на рівні клієнта, а також контроль доступу до даних.

– VPN. Використання віртуальної приватної мережі (VPN) дозволяє забезпечити безпечний доступ до інформації з будь-якого місця з Інтернет-підключенням. За допомогою VPN можна шифрувати трафік та забезпечувати автентифікацію користувача перед доступом до інформації

– Файлові сервери. Використання файлових серверів дозволяє зберігати та обмінюватися документами та іншою інформацією в межах внутрішньої мережі. Для забезпечення безпеки можна використовувати системи контролю доступу, шифрування даних та резервне копіювання даних.

– Електронні підписи. Використання електронних підписів дозволяє забезпечити автентифікацію користувача та підтвердження автентичності документів. Електронні підписи можуть бути використані для підписування документів, відправки електронної пошти та інших дій, що потребують підпису.

– Конференції та відеозв'язок. Використання конференцій та відеозв'язку дозволяє забезпечити взаємодію між співробітниками та клієнтами без необхідності фізичного присутності в одному місці. Для забезпечення безпеки можна використовувати шифрування трафіку та контроль доступу до конференцій.

У кожного зі способів обробки та передачі інформації є свої переваги та недоліки, тому важливо обрати той, що найкраще відповідає потребам конкретної юридичної фірми. Наприклад, якщо важливо забезпечити максимальний рівень безпеки та конфіденційності, то можна

використовувати VPN та електронний підпис. Якщо ж важливо забезпечити зручний доступ до інформації, то можна використовувати хмарні сховища та файлові сервери.

1.5 Постановка завдання та мета роботи

Завданням кваліфікаційної роботи є розробка комп'ютерної система юридичної фірми "Legalitas" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі з реалізацією IoT системи безпеки.

Для вирішення поставленої мети в роботі слід виконати наступні завдання:

– аналіз об’єкту;

– розробка структури КС;

– вибір мережевої архітектури для корпоративної мережі юридичної фірми «Legalitas»;

– вибір комплексу технічних засобів та структурованої кабельної системи

– аналіз трафіку;

– розробка фізичної та логічної топології мережі підприємства;

– налаштування конфігурації мережного обладнання;

– розробка IoT системи безпеки офісу, яка буде обладнана розумними пристроями, датчиками, сенсорами;

– Результуюча мережа має бути надійною, масштабованою, гнучкою, безпечною та швидкою.

1.6 Визначення можливих напрямків рішення поставлених завдань

Для вирішення поставлених завдань щодо розробки комп'ютерної системи юридичної фірми "Legalitas" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі з реалізацією IoT системи безпеки, можливі наступні напрямки рішення:

1. Вибір мережевої архітектури для корпоративної мережі "Legalitas":

– Централізована мережева архітектура, де всі ресурси та обчислювальні потужності зосереджені в центральному вузлі мережі.

– Розподілена мережева архітектура, де ресурси та обчислювальні потужності розподілені між декількома вузлами мережі.

– Вибір кабельної системи корпоративної мережі:

– Кручена пара, що забезпечує добру якість сигналу та підтримку пропускної спроможності на середній дистанції, а саме до 100-1000Мбіт/с на відстані до 100м для кабелю категорії 5е, який є найрозповсюдженішим.

– Оптоволоконний кабель, що забезпечує добру якість сигналу та підтримку дуже високої пропускної спроможності на великій дистанції, а саме 10Гбіт/с на відстані до 550м, або 100Мбіт/с на відстані до 2000м.

2. Аналіз трафіку:

– Використання програмного забезпечення для моніторингу трафіку та аналізу мережевої активності.

– Визначення та призначення пріоритетів для різних типів трафіку.

3. Розробка фізичної та логічної топології мережі підприємства:

– Застосування стандартних топологій, таких як зірка, дерево або магістраль-розгалуження.

– Розробка індивідуальної топології, що відповідає конкретним потребам підприємства.

4. Конфігурація мережного обладнання:

– Встановлення мережевих пристроїв, таких як маршрутизатори, комутатори та файрволи, з урахуванням потреб підприємства та вибраних мережевих архітектур та топологій.

– Налаштування мережевої безпеки та захисту даних, включаючи захист від зовнішніх загроз та внутрішнього зловживання.

5. Реалізація IoT системи безпеки:

– Встановлення різноманітних датчиків, які здійснюватимуть моніторинг та контроль різних параметрів безпеки, таких як температура, вологість, дим, рух тощо.

– Забезпечення інтеграції IoT системи з мережевим обладнанням та програмним забезпеченням, що використовується в підприємстві.

– Розробка системи аналізу даних та прийняття рішень на основі зібраних даних з IoT системи безпеки.

Враховуючи ці напрямки рішення, можна створити надійну, масштабовану, гнучку, безпечну та швидку корпоративну мережу з реалізацією IoT системи безпеки для підприємства "Legalitas". Проте слід мати на увазі, що конкретні рішення залежатимуть від потреб підприємства, його бюджету та доступних ресурсів.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи юридичної фірми

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи підрозділів підприємства

Система юридичної фірми «Legalitas» має складатись з 3 підсистем

– підсистема керівничого відділу

– підсистема віддаленого офісу

– підсистема відділу юридичних послуг

Система повинна забезпечувати безперервну, цілодобову роботу з урахуванням необхідного часу на технічне обслуговування, щоб уникнути втрати даних або проблем з відновленням її працездатності.

Заборонено підключення сторонніх осіб до корпоративної мережі.

Розроблена система має бути логічно-послідовною, зрозумілою та простою, щоб новачок міг без зусиль оволодіти її налаштуванням і розуміти принципи її функціонування.

Усе використовуване програмне забезпечення та обладнання, які використовуються під час розробки та експлуатації системи, має бути ліцензійними і отриманим відповідно до встановлених стандартів і нормативів.

Обладнання системи повинно регулярно піддаватися ревізії та аудиту кожен рік з метою виявлення можливих дефектів або пошкоджень. Під час процесу монтажу необхідно дотримуватися всіх встановлених норм і правил техніки безпеки, щоб гарантувати безпеку для фахівців. Кабелі, використовувані для з'єднання вузлів, повинні мати зручну довжину з невеликим запасом до 0,5 метра, бути логічно-структурованими, чітко позначеними та розгорнутими. На підприємстві завжди має бути наявна

достатня кількість запасного обладнання, кабелів та інструментів для вирішення можливих несправностей.

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

Взаємодія між підсистемами повинна здійснюватися шляхом використання спільного інформаційного простору та стандартизованих протоколів та форматів обміну даними.

Усі програмні компоненти підсистем мають працювати в межах єдиного логічного простору, який забезпечується інтегрованими засобами серверів даних та серверів додатків.

2.1.1.3 Вимоги до характеристик взаємозв'язків створюваної системи із суміжними системами, вимоги до її сумісності, у тому числі вказівки про способи обміну інформацією (автоматично, пересиланням документів, телефоном і т. п.)

Програмне забезпечення системи повинно забезпечувати інтеграцію та сумісність на інформаційному рівні з іншими системами. Інформаційна сумісність досягається шляхом експорту та імпорту XML-документів.

Вимоги щодо структури даних та режимів обміну інформацією між підсистемами та системами визначаються загальним регламентом взаємодії.

Архітектура взаємодії повинна відповідати наступним умовам:

1. Відповідність розробленим регламентам використання системи.
2. Використання відкритих форматів обміну даними під час організації взаємодії між підсистемами та системами, які використовуються на об’єкті.

2.1.1.4 Вимоги до режимів функціонування системи

Компоненти системи, що забезпечують реалізацію рівнів ядра та доступу, а також HTTP-сервер компанії повинні забезпечувати безперервний цілодобовий режим експлуатації та забезпечувати потреби користувачів.

2.1.1.4 Вимоги до діагностування системи

Діагностика системи включає в себе наступні пункти:

1. Виявлення фізичних дефектів мережі:

– перевірка кабельної системи та системи електроживлення активного обладнання;

– виявлення шумів від зовнішніх джерел.

2. Вимірювання поточної завантаженості каналу зв'язку мережі та вивчення впливу завантаження на час реакції прикладного програмного забезпечення.
3. Вимірювання кількості колізій в мережі та виявлення причин їх виникнення.
4. Вимірювання кількості помилок передачі даних на рівні каналу зв'язку та вивчення причин їх виникнення.
5. Виявлення дефектів архітектури мережі.
6. Вимірювання поточної завантаженості сервера та вивчення впливу ступеня його завантаження на час реакції прикладного програмного забезпечення.
7. Виявлення дефектів прикладного програмного забезпечення, які можуть призводити до неефективного використання пропускної здатності сервера та мережі.

2.1.1.5 Перспективи розвитку системи

1. Комп’ютерна система повинна мати довгий термін служби.
2. Комп'ютерна система має бути побудована з використанням стандартизованих і ефективно підтримуваних рішень.
3. Комп'ютерна система має бути реалізована як відкрита система, що допускає розширення функціональних можливостей.
4. Комп'ютерна система має забезпечувати можливість модернізації як шляхом заміни технічного та загального програмного забезпечення (ПЗ), так і шляхом поліпшення інформаційного забезпечення.
5. Комп'ютерна система повинна мати перспективи для подальшого розвитку та удосконалення.
6. Комп'ютерна система має бути гнучкою і адаптивною, щоб враховувати майбутні потреби та зміни в технологічному середовищі.
7. Комп'ютерна система повинна бути розроблена з урахуванням довгострокових вимог і стандартів.

2.1.1.6 Показники призначення

Головним призначенням комп'ютерної мережі є забезпечення простого, зручного і надійного доступу користувачів до розподілених загальних ресурсів мережі та організація їх спільного використання з надійним захистом від несанкціонованого доступу. Крім того, мережа повинна забезпечувати зручні та надійні засоби передачі даних між користувачами.

Призначення системи повинне залишатись незмінним протягом усього періоду функціонування. Тривалість функціонування ПК визначається терміном надійної роботи апаратного забезпечення обчислювальних комплексів, своєчасною заміною (оновленням) апаратних компонентів, забезпеченням супроводу програмного забезпечення системи

і його модернізації. Інші показники призначення формуються після проведення передпроєктного аналізу

2.1.1.7 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

2.1.1.7.1 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, припустимість роботи без обслуговування

Мережеві компоненти системи повинні функціонувати безперервно цілодобово, враховуючи час, необхідний для технічного обслуговування.

У приміщеннях, де використовується Система, необхідно забезпечити відсутність агресивних середовищ. Рівень масової концентрації пилу в повітрі не повинен перевищувати 0,75 мг/м³, а електрична складова електромагнітного поля не повинна перевищувати 0,3 Н/м у діапазоні частот від 0,15 до 300,00 МГц.

Необхідно дотримуватися вимог щодо пожежної безпеки та електробезпеки (заземлення) у приміщеннях згідно з наступними нормативними документами:

– ДСТУ “ГОСТ 12.1.004-91 "ССБТ. Пожежна безпека. Загальні вимоги"”; [2]

– ДСТУ “ГОСТ Р 50571.22-2000. "Електроустановки будівель. Частина 7. Вимоги до спеціальних електроустановок. Розділ 707. Заземлення устаткування обробки інформації"”; [3]

– Правила улаштування електроустановок;

– Правила техніки безпеки при експлуатації електроустановок споживачів.

Приміщення для експлуатації виробів повинні відповідати вимогам ДСТУ “ГОСТ 15150-69 (зі змінами 2004) "Машини, прилади та інші технічні вироби. Виконання для різних кліматичних районів. Категорії, умови експлуатації, зберігання і транспортування в частині впливу кліматичних факторів зовнішнього середовища" для виду кліматичного виконання УХЛ категорії 4.2.” [4]

Нормальні кліматичні умови експлуатації системи включають:

– Температура навколишнього повітря: +15°C до +25°C.

– Відносна вологість навколишнього повітря: до 75% при атмосферному тиску від 84 кПа до 107 кПа.

Система повинна забезпечувати свою працездатність при впливі наступних кліматичних факторів:

– Температура навколишнього повітря: від 10°C до 45°C.

– Відносна вологість повітря: від 40% до 80% при температурі +10°C.

– Атмосферний тиск від 84 кПа до 107 кПа.

2.1.1.7.2 Вимоги до параметрів мереж енергопостачання (живлення та заземлення)

Кожне працююче місце повинно мати електричні розетки з напругою 220 В і частотою 50 Гц, які мають заземлюючий контакт.

Згідно з НАПБ А 01.001-2004, забороняється:

– експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

– користування пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів. [5]

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

При визначенні вимог до персоналу, який обслуговує систему, і режиму його роботи, необхідно враховувати кілька важливих факторів. По-перше, треба розрахувати оптимальну кількість працівників, відповідно до обсягу та складності робіт, пов'язаних з підтримкою системи. Крім того, персонал повинен мати відповідну кваліфікацію, зокрема знання технічних аспектів системи та вміння ефективно виконувати свої обов'язки.

Окрім цього, важливим аспектом є режим роботи персоналу. Визначають графік роботи, включаючи робочі години, дні тижня та можливість працювати у неробочий час при потребі. Також можуть бути встановлені правила щодо взаємозамінності та готовності до виклику у непередбачуваних ситуаціях.

Забезпечення надійності роботи системи вимагає дотримання режиму роботи, включаючи часи обслуговування, планові перерви та виконання завдань у встановлені терміни. Персонал повинен бути дисциплінованим та готовим діяти відповідно до встановлених процедур і стандартів.

Для забезпечення експлуатації системи необхідний певний персонал. До його складу повинні входити:

– Адміністратори системи - спеціалісти, відповідальні за виконання спеціальних технологічних завдань та управління компанією в цілому. Повинні мати доступ до Інтернету, серверів і можливість взаємодіяти між підсистемами.

– Команда експлуатації - фахівці, що забезпечують нормальне функціонування технічних і програмних засобів.

– Відділ кадрів - спеціалісти, які відповідають за пошук нових кваліфікованих працівників. Також повинні мати доступ до Інтернету, серверів і можливість взаємодіяти між підсистемами.

– Бухгалтерія - має отримувати доступ до Інтернету, серверів і мати можливість взаємодіяти між підсистемами.

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

1. Склад запасних виробів і приладів:

– Резервні компоненти комп'ютерної мережі, включаючи мережеві комутатори, маршрутизатори, бездротові точки доступу, кабелі, роз'єми і конектори.

– Запасні блоки живлення для комп'ютерів, серверів та мережевих пристроїв.

– Резервні кабелі Ethernet і бездротові антени.

– Запасні диски для зберігання даних і резервного копіювання.

– Додаткові комп'ютери та ноутбуки.

2. Розміщення:

– Запасні вироби і прилади мають зберігатись в безпечному і захищеному приміщенні, щоб уникнути пошкоджень і крадіжок.

– Наявність замків, системи безпеки і контролю доступу до приміщення, де зберігаються запасні вироби.

– При необхідності, використовувати спеціальні стелажі, шафи або контейнери для організації та захисту запасних виробів.

3. Умови збереження:

– Зберігання повинно здійснюватися в приміщенні з контрольованою температурою і вологістю, щоб уникнути пошкоджень від екстремальних умов. Температура та вологість повинні відповідати умовам у пункті 2.1.1.7.1.

– Запасні вироби і прилади повинні бути захищені від прямих сонячних променів, пилу, вологи і корозії.

– Запасні вироби повинні бути зберігані у спеціальній антистатичній упаковці для захисту від електростатичного розряду.

4. Документування:

– Записи про всі запасні вироби та прилади повинні бути точними і актуальними.

– Ведення інвентаризації та оновлення списку запасних виробів регулярно.

– Документування дати придбання, гарантійного терміну та інших важливих відомостей про запасні вироби.

2.1.1.7.5 Вимоги до регламенту обслуговування

1. Регулярність обслуговування:

– Визначення чіткого графіку обслуговування, який включає періодичні технічні огляди і профілактичні роботи кожні півроку.

– Регулярне проведення оновлення програмного забезпечення, включаючи операційну систему, антивірусне програмне забезпечення, драйвери та інші необхідні програми. Для антивірусного програмного забезпечення оновлення треба проводити не менше ніж раз на день. Операційну систему та інше програмне забезпечення має оновлятися раз на тиждень, за наявності оновлень.

– Моніторинг та діагностика:

– Встановлення системи моніторингу, яка дозволяє виявляти можливі проблеми в мережі та комп'ютерах.

– Регулярне проведення діагностики мережевого обладнання для виявлення можливих несправностей та забезпечення швидкого виявлення проблем.

2. Запобігання відмовам:

– Проведення регулярної перевірки і тестування запасних виробів та компонентів для попередження можливих відмов раз на півроку.

– Встановлення процедур забезпечення резервного живлення, щоб уникнути відключення обладнання через перебої в електропостачанні.

3. Безпека та захист:

– Регулярне, щоденне, оновлення і налаштування системи безпеки для захисту від вірусів, шкідливих програм і несанкціонованого доступу.

– Проведення аудиту безпеки мережі для виявлення можливих проблем та вразливостей і прийняття відповідних заходів для їх усунення.

2.1.1.8 Вимоги до патентної чистоти

Використовуване обладнання та програмне забезпечення повинні мати необхідні патентні документи та сертифікати (якщо це вимагається) для роботи в умовах, в яких вони використовуються.

2.1.2 Додаткові вимоги

2.1.2.1 Вимоги до активного обладнання (функціонування, кількість портів та їх запас, варіанти встановлення, технічні вимоги)

Для забезпечення належного функціонування і безпеки активного обладнання, рекомендується розміщувати його в спеціальних комутаційних шафах.

Активне обладнання повинно відповідати наступним умовам:

1. Пропускна здатність: обладнання повинно мати достатню пропускну здатність для задоволення потреб передачі даних в мережі. Це включає швидкість передачі даних (наприклад, 1 Гбіт/с, 10 Гбіт/с) і пропускну здатність портів.
2. Сумісність і стандарти: обладнання повинно відповідати сучасним стандартам і протоколам мережі, таким як Ethernet, TCP/IP, IPv6

тощо. Воно повинно бути сумісним з іншими пристроями в мережі і забезпечувати взаємодію з ними.

3. Обладнання повинно мати достатню кількість портів, для забезпечення усіх потреб системи.
4. Обладнання повинно бути від відомих виробників, які надають підтримку і сервісне обслуговування. Воно повинно мати гарантію і доступність технічної підтримки, а також оновлення програмного забезпечення і фірмового забезпечення.

2.1.2.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

1. Вимоги до кабель-каналів:

– Кабель-канали повинні бути достатньо великими, щоб помістити всі необхідні кабелі для передачі даних, включаючи мережеві кабелі, кабелі живлення та інші комунікаційні кабелі.

– Кабель-канали повинні бути легкодоступними для обслуговування та зміни кабелів в разі потреби.

– Вони повинні бути відповідно захищені та безпечні, забезпечуючи захист від потенційних небезпек, таких як пожежа або електричний удар.

2. Вимоги до інформаційні розеток:

– Офіс повинен мати достатню кількість інформаційних розеток для підключення комп'ютерів, принтерів, маршрутизаторів та іншого обладнання.

– Розташування розеток повинно бути зручним для співробітників та враховувати розміщення робочих місць.

– Розетки повинні відповідати стандартам безпеки та бути заземленими для запобігання пошкодженню обладнання та захисту від електричних ударів.

3. Вимоги до електричних розеток:

– Офіс повинен мати достатню кількість електричних розеток для живлення комп'ютерів, освітлення, кулерів, зарядних пристроїв та іншого електричного обладнання.

– Розташування розеток повинно бути зручним для співробітників та відповідати вимогам пожежної безпеки.

– Розетки повинні бути відповідно заземлені та мати захисні кришки для запобігання нещасним випадкам.

2.1.2.3 Вимоги до комунікаційного обладнання і його розташування

Так, для забезпечення належного функціонування і безпеки комунікаційного обладнання, рекомендується розміщувати його в спеціальних комутаційних шафах. Основні вимоги до таких шаф включають:

1. Розташування: Комутаційна шафа повинна бути розміщена в захищеному від вологи та агресивного середовища місці. Вона може бути розташована в спеціальних приміщеннях, таких як серверні кімнати або технічні приміщення.
2. Заземлення: Корпус комутаційної шафи повинен бути заземлений окремим провідником. Це необхідно для забезпечення електричної безпеки та захисту обладнання від статичної електрики та інших електричних перешкод.
3. Активне обладнання: У комутаційних шафах також має бути встановлено активне обладнання, таке як маршрутизатори, комутатори, сервери тощо. Це дозволяє керувати мережевими процесами, забезпечувати комутацію даних та надавати необхідні сервіси.

4. Вентиляція та охолодження: Комутаційні шафи також можуть бути обладнані системами вентиляції та охолодження для забезпечення оптимальних температурних умов для працюючого обладнання.

Виконання цих вимог допоможе забезпечити належну працездатність, безпеку та тривалу експлуатацію комунікаційного обладнання.

2.1.2.4 Вимоги до резервування

Для забезпечення резервування даних і можливості їх відновлення рекомендується виконувати наступні кроки:

1. Автоматичне резервне копіювання: Налаштувати систему таким чином, щоб резервне копіювання даних здійснювалося автоматично щодня. Це може включати резервне копіювання на зовнішні носії, такі як жорсткі диски, магнітні стрічки або хмарні сховища.
2. Інкрементальне копіювання: Використовуйте інкрементальну процедуру копіювання, яка копіює тільки змінені дані з попереднього резервного копіювання. Це дозволяє скоротити обсяг копіюваних даних і економити простір для зберігання.
3. Повне копіювання: Враховуйте, що повне копіювання повинно проводитися не рідше одного разу на тиждень. Це дасть можливість створити повну копію всіх даних і забезпечити повну відновлюваність інформації у випадку відновлення.
4. Можливість відновлення даних: Передбачте процедуру відновлення даних у разі виникнення збоїв. Це може включати повторне введення або імпорт даних з резервних копій. Крім того, важливо перевірити, що резервні копії є доступними, а процедура відновлення даних є зрозумілою та ефективною.

5. Тестування відновлення даних: Регулярно проводьте тестування процедури відновлення даних, щоб переконатися, що всі необхідні дані можуть бути успішно відновлені з резервних копій.

Ці заходи забезпечать регулярне резервне копіювання даних і гарантують можливість відновлення даних у разі необхідності. Резервне копіювання і відновлення даних є критичними аспектами для забезпечення безпеки та роботи бізнесу.

2.1.3 Вимоги до налаштувань та функцій, які виконує КС

З метою полегшення користування мережа повинна поділятись на підмережі, які взаємодіють між собою за допомогою кабелів, таких як FastEthernet та GigabitEthernet. Ці кабелі повинні забезпечувати з'єднання між різними комутаторами, які в свою чергу підключені до маршрутизаторів.

Розроблена система повинна відповідати вимогам загальної архітектури мережі (додаток А) .

З метою забезпечення найвищого рівня надійності всі маршрутизатори мережі мають бути взаємопов'язані між собою.

В системі має бути впроваджена IoT-система безпеки офісу.

Основні вимоги до IoT-системи компінї:

– увімкнення сирени при спрацюванні датчика вогню та відмикання дверей;

– доступ до офісних приміщень за допомогою RFID карток та зчитувача.

Основні вимоги до функцій, які виконує комп'ютерна система юридичної фірми включають:

– Забезпечення безперебійного та швидкого доступу до інформації.

– Зберігання, організація та захист даних.

– Реєстрація, аналіз та контроль використання ресурсів комп'ютерної системи.

– Забезпечення безпеки мережі, включаючи захист від вірусів, шпигунського ПЗ та інших загроз.

– Підтримка комунікаційних сервісів, включаючи електронну пошту, відеоконференції, обмін файлами та ін.

– Забезпечення автоматизованого контролю за безпекою та ризиками відповідно до внутрішніх та зовнішніх вимог.

– Підтримка резервного копіювання та відновлення даних у випадку аварії.

– Забезпечення можливості моніторингу та аналізу стану системи для попередження можливих проблем та забезпечення їх своєчасного вирішення.

Основні вимоги до підсистем компанії:

– на кожному мережевому пристрої необхідно призначити ім’я, встановити паролі до режиму EXEC та ліній console та vty. Зазначити використання протоколу SSH замість Telnet при віддаленому з’єднанні з пристроями. На кожному пристрої створити користувача та доменне ім’я;

– налаштувати адресацію усіх пристроїв мережі;

– у відділ корпоративного, цивільного, господарського та податкового права необхідно впровадити технологію агрегації фізичних каналів для забезпечення більшої стабільності та пропускної здатності;

– у відділі корпоративного права та судової практики необхідно виконати розбиття підмережі на VLAN за таким принципом: VLAN26 – керівництво відділів, VLAN36 – судова практика, VLAN46 – керуючий партнер;

– виконати налаштування конфігурації DHCP для забезпечення динамічного призначення адрес вузлам;

– реалізувати аутентифікацію на маршрутизаторах за допомогою служби AAA з використанням протоколу Radius;

– зв’язок між усіма підсистемами необхідно забезпечити налаштуванням динамічної маршрутизації. На кожному маршрутизаторі налаштувати статичні маршрути за замовчуванням;

– на пограничних маршрутизаторах офісів виконати налаштування списків доступу ACL, динамічного NAT та VPN на базі IPsec;

– на DCE-інтерфейсах маршрутизаторів встановити частоту 128000 та пропускну здатність 128;

– виконати налаштування HTTP та DNS серверів таким чином, щоб забезпечити роботу сайту компанії за доменним ім’ям 123.dnipro.ua;

– виконати налаштування безпеки портів комутаторів, до яких під’єднано сервери, за допомогою switchport security.

2.1.4 Вимоги до видів забезпечення КС

2.1.4.1 Вимоги до програмного забезпечення

Основні вимоги до програмного забезпечення комп'ютерної системи юридичної фірми включають:

– Надійність: програмне забезпечення має бути надійним та стабільним для запобігання можливих помилок та аварій.

– Ефективність: програмне забезпечення має бути ефективним та продуктивним для забезпечення швидкого доступу до інформації та операцій з нею.

– Безпека: програмне забезпечення має бути захищеним від можливих загроз, таких як віруси, хакерські атаки та інші.

– Сумісність: програмне забезпечення має бути сумісним з іншими системами та додатками, що використовуються в компанії.

– Розширюваність: програмне забезпечення має бути розширюваним, щоб дозволити додавання нових функцій та можливостей у майбутньому.

– Зручність використання: програмне забезпечення має бути зручним та простим у використанні для користувачів з різним рівнем досвіду.

– Легкість супроводу: програмне забезпечення має бути легким у супроводі та підтримці, щоб зменшити витрати на технічне обслуговування та ремонт.

– Масштабованість: програмне забезпечення має бути масштабованим для забезпечення розвитку та зростання бізнесу.

2.1.4.2 Вимоги до лінгвістичного забезпечення

Головним засобом взаємодії між користувачами та системою є українська мова та англійська мова:

– Користувачі повинні мати можливість взаємодіяти з ПК за допомогою обраних мов.

– Графічний інтерфейс користувача підсистеми повинен бути створений з урахуванням мови, обраної користувачем. Інтерфейс користувача має бути зрозумілим, простим і розробленим з урахуванням таких принципів:

– Використання довідників і шаблонів для введення даних.

– Використання підказок для неправильних дій користувача.

– Наявність довідкової інформації про роботу в системі.

2.1.4.3 Вимоги до технічного забезпечення системи

Для роботи до складу технічних засобів повинні входити комп'ютери з такою конфігурацією:

– Процесор за тактовою частотою не менше 1 ГГц.

– Не менше 4 Гб оперативної пам’яті.

– Обсяг накопичувача не менше 20 Гб.

– Мережеві пристрої рівню ядра та доступу, використані при побудові корпоративної мережі організації, мають бути від фірми Cisco.

– Все технічне забезпечення повинно бути придбано у офіційних дистриб’юторів, повинно мати всю необхідну документацію та гарантійний талон.

– Кожне робоче місце повинне бути забезпечене монітором та пристроями вводу.

– В офісі повинна бути достатня кількість оргтехники, щоб задовольнити потреби працівників.

– Обладнання системи СКМ повинне задовольняти високі стандарти якості та надійності.

– Серверне обладнання повинно мати наступні мінімальні характеристики: процесор з не менше ніж двома ядрами і тактовою частотою 2.8 ГГц, 4 ГБ оперативної пам'яті, жорсткий диск об'ємом не менше 30 ГБ і мережевий контролер з підтримкою 1GbE.

2.1.4.4 Вимоги до організаційного забезпечення системи

Організаційне забезпечення комп'ютерної мережі в офісі юридичної компанії передбачає встановлення чітких та документованих процедур для коректної роботи з мережею.

Доступ до мережевого обладнання повинене мати тільки кваліфікований персонал, описаний у пункті 2.1.1.7.3. А саме адміністратори системи та команда експлуатації.

Інший персонал юридичної фірми, при виникненні несправностей повинен звернутись до персоналу, обслуговуючого мережу.

2.1.4.5 Вимоги до методичного забезпечення системи

Вимоги до методичного забезпечення повинні передбачати наявність чітких інструкцій та рекомендацій щодо використання інформаційної

системи, програмного забезпечення, баз даних та інших технічних засобів. Це включає в себе детальний опис функціональності та можливостей системи, посібники з установки та налаштування ПЗ, правила використання інструментів та функцій системи, а також інструкції щодо роботи з базами даних. Методичне забезпечення повинно бути доступним для всіх користувачів та забезпечувати їхню ефективну роботу з інформаційною системою, зменшуючи можливість помилок та недорозумінь. Крім того, воно повинно бути оновлюваним та відповідати актуальній версії системи та ПЗ, забезпечуючи користувачам доступ до актуальної та правильної інформації.

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

З урахуванням розробленої організаційної структури підприємства (рисунок 1.1), технічних вимог до системи і топологічної схеми розміщення структурних відділів підприємства (рисунки 1.2 та 1.3), потрібно розробити структурну схему комплексу технічних засобів комп'ютерної системи.

Мережа повинна бути поділена на підмережі, враховуючи структурну схему підприємства та технічне завдання.

Пересилання трафіку між маршрутизаторами повинно здійснюватися за рахунок протоколу маршрутизації OSPF. Структурна схема показана на рисунку 2.1.

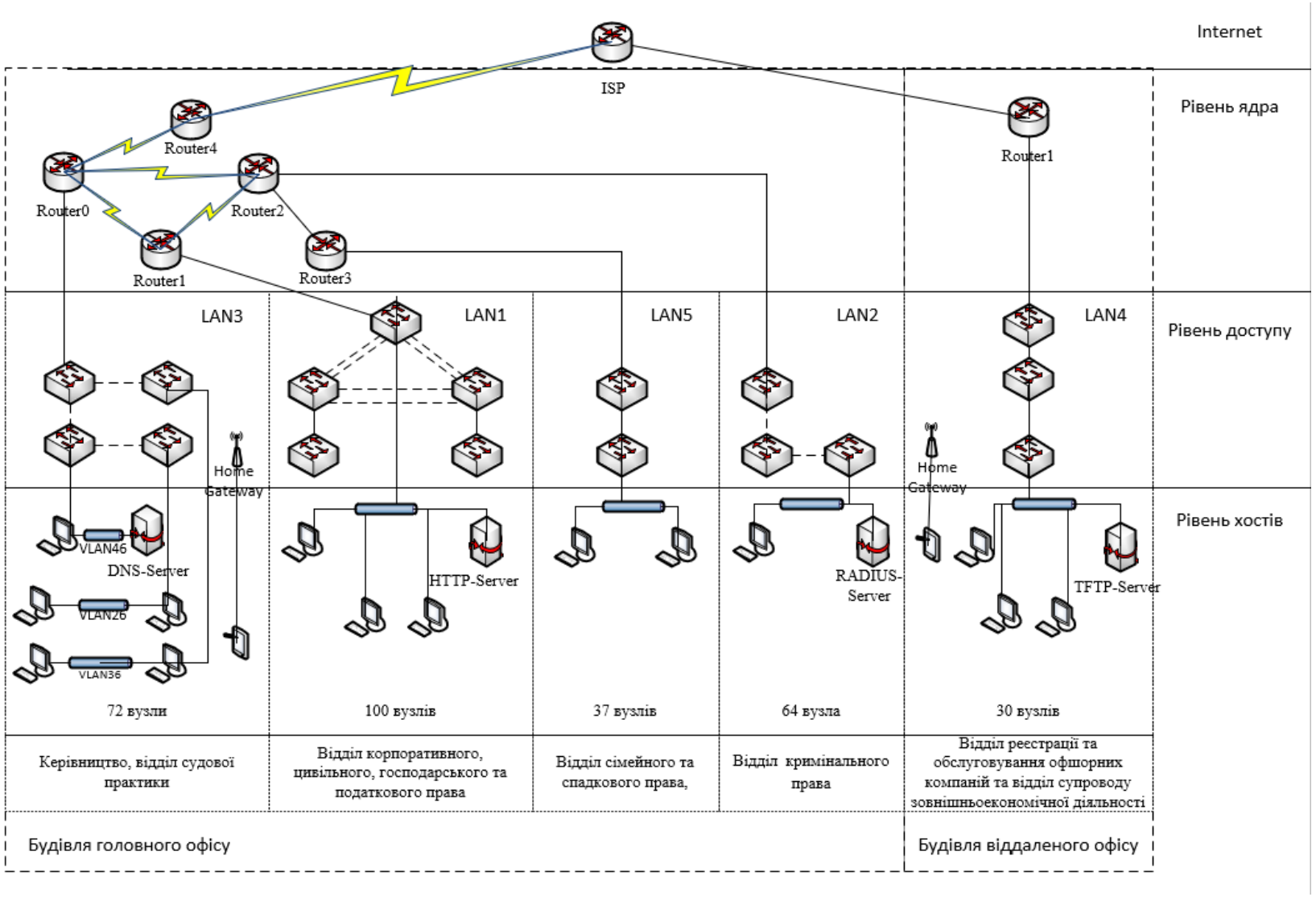

Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи

2.2.1 Розробка специфікації апаратних засобів комп’ютерної системи

Юридична фірма «Legalitas» орендує чотири поверхи у двох різних будівлях. Головний офіс налічує три поверхи у той час, як віддалений – один.

Спираючись на це та на розроблену структурну схему комплексу технічних засобів комп’ютерної системи потрібно розробити специфікацію апаратних засобів системи.

LAN4 та LAN5 мають 30 та 37 вузлів відповідно, враховуючи 10% запасу портів, потрібно обрати 2 комутатора по 24 порти. Загальна кількість портів у підмережах – 48 штук.

LAN2 містить в собі 64 вузли, враховуючи 10% запасу портів, потрібно обрати 3 комутатора по 24 порти. Загальна кількість портів у підмережі – 72 штуки.

LAN3 містить в собі 72 вузла, враховуючи 10% запасу портів, потрібно обрати 4 комутатора по 24 порти. Загальна кількість портів у підмережі – 96 штуки.

LAN1 містить в собі 100 вузлів враховуючи 10% запасу портів, потрібно обрати 5 комутаторів по 24 порти. Загальна кількість портів у підмережі – 220 штук.

Загальна кількість та специфікація використаних пристроїв компанії Cisco представлена у таблиці 2.1.

Таблиця 2.1 – Специфікація обладнання, використаного при побудові корпоративної мережі юридичної фірми «Legalitas»

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Маршрутизатор серії Cisco 2911: 3 integrated GigabitEthernet 4x EHWIC slots 2x onboard DSP slots 1x ISM slot 512 - 2048 MB DRAM 256 MB Compact Flash	Cisco 2900	од	6	За структурною схемою: Router0-5 Детальні характеристики: https://www.cisco.com/c/en/us/support/routers/2911-integrated-services-router-isr/model.html#~tab-specs
2	Комутатор серії Catalyst 2960: 24x 10/100 Ethernet Ports 2x 1GSFP amd RJ-45 combo uplinks	Cisco 2960-24PS	од	16	Детальні характеристики: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-s-series-switches/data_sheet_c78-726680.html
3	Маршрутизатор серії VDSL2: 4x 10/100/1000 LAN ports 1x 10/100/1000 Gigabit Ethernet WAN port 1x VDSL2 IEEE 802.11ac wireless access-point	Cisco RV134W VDSL2	од	2	Детальні характеристики: https://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/datasheet-c78-736465.html

Щоб об’єднати усі ці пристрої в одну мережу і підтримання сайту агентства – потрібні потужні сервери. Один з них забезпечує DNS зв’язок. Інші три – HTTP-сервер, TFTP-сервер та RADIUS-сервер. Порти між маршрутизаторами використовуються Serial, а між маршрутизаторами та комп’ютерами використовується лише порти FastEthernet.

Система VLAN на комутаторах також використовується.

Наступним кроком розглянемо вибір СКМ на прикладі будівлі віддаленого офісу. Фірма займає перший з двох поверхів будівлі, структурна схема якої розглянута на рисунку 1.3. Складемо план розміщення вузлів КС та спроектуємо схему розміщення кабельних мереж, як вказано на рисунку 2.2.

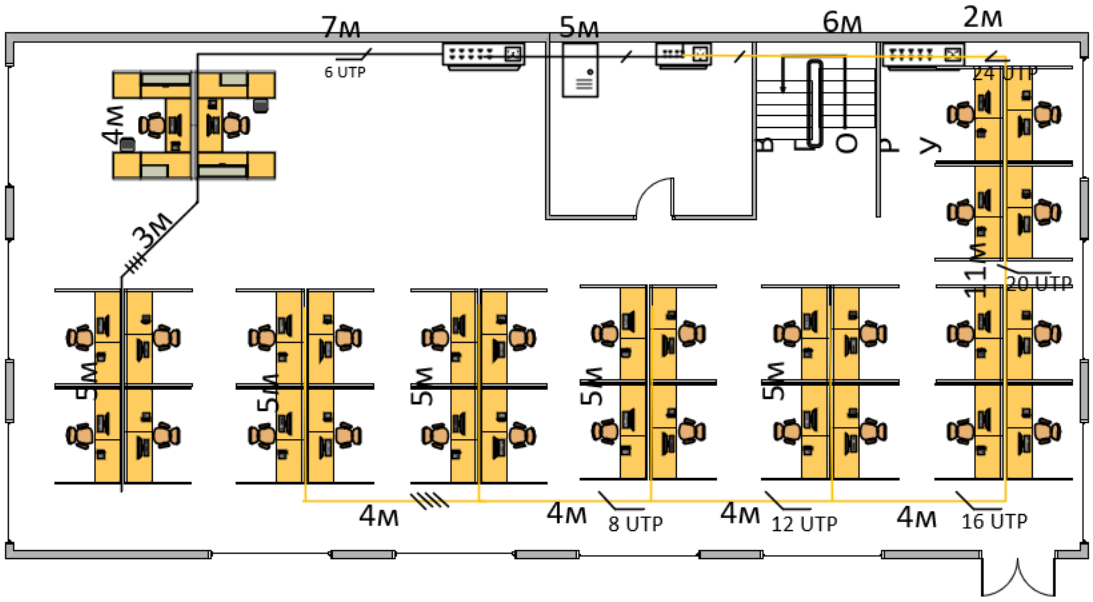

Рисунок 2.2 – Схема розміщення кабельних мереж віддаленого офісу юридичної фірми «Legalitas»

Для віддаленого офісу була розроблена схема розміщення кабельних мереж з використанням кабель-каналів у підлозі та комп’ютерних розеток з виходом RJ-45.

Враховуючи розташування вузлів та фізичні розміри приміщення складаємо специфікацію СКМ (таблиця 2.2).

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Підлоговий кабельний канал алюмінієвий 18х15мм	Simon	м	79	За проєктом LAN4 для крученої пари
2	Розетка комп'ютерна RJ45 UTP кат. 5E подвійна	Asfora	од	30	За проєктом LAN4
3	Розетка із заземленням подвійна	Mono	од	96	За проєктом LAN4
4	LAN-кабель U/UTP кат 5E	OK-Net	м	100	За проєктом LAN4
5	Кабель живлення ПВС 3х1	Одес-Кабель	м	100	За проєктом LAN4
6	Кабельний канал пластиковий 20х40	Simon	м	110	За проєктом LAN4

Для забезпечення зв'язку між комп'ютерами в офісній мережі, згідно таблиці 2.1, були використані маршрутизатор серії 2911 та комутатори 2960-24TT зі стандартними портами (Fast та Gigabitethernet). В цьому випадку не було необхідності використовувати будь-які технології для покращення зв'язку в мережі.

Специфікація комп’ютерів та серверів в офісній мережі написана у таблиці 2.3.

Таблиця 2.3 – Специфікація комп’ютерів та серверів в офісній мережі

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Комп’ютер моделі B38v07Win: Процесор: AMD RYZEN 5 5600G ОЗУ: 8 Гб DDR4 Накопичувач: SSD 240 Гб	ARTLINE Business	Од	303	Детальні характеристики: https://artline.ua/uk/product/nettop-artline-business-b38v07win
2	Сервер C220 M3: Процесор: 2 шт x Intel Xeon E5-2650L v2. ОЗУ: 16 GB DDR3. RAID-контролер: Cisco UCS RAID SAS 2008M-8i Mezzanine Card UCSC-RAID-11-C220 74-10149-01. Мережеві порти: 2x 10/100/1000 Ethernet	Cisco UCS	Од	4	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m3-lff-specsheet.pdf
3	БФП L3256: Роздільна здатність друку: 5.760 x 1.440 DPI. Роздільна здатність сканування 1.200 DPI x 2.400 DPI. Технологія і палітра друку: Струменева кольорова.	Epson EcoTank	Од	100	https://www.epson.com.sg/For-Home/Printers/Ink-Tank/Ink-Tank-System-Printers/Epson-EcoTank-L3256-A4-Wi-Fi-All-in-One-Ink-Tank-Printer/p/C11CJ67504

Комп’ютери підібрано таким чином, щоб підтримувати останні версії Microsoft Windows та Office та їхні майбутні оновлення.

Усе мережеве обладнання підібрано фірми Cisco, тому проблем з сумісністю компонентів системи бути не повинно.

2.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Вихідний трафік маршрутизується в лінію з пропускною здатністю у 1000 Мбіт на секунду.

Для того, щоб уникнути перенавантаження маршрутизатора, швидкість находження пакетів до нього повинна буде менше швидкості їх відправлення.

Для розрахунків візьмемо максимальний розмір навантаження пакетів у канальному рівні моделі OSI:

$$\mu_{вих} = 1000000000/(1500*8) = 83333,33 \text{ пакетів/с} \quad (2.1)$$

Оскільки в середньому, кожне джерело виробляє 142 пакетів/с, то маршрутизатор обмежено кількістю приєднань з наступної формули:

$$N = 83333,33/142 = 586 \text{ джерел.} \quad (2.2)$$

Що задовольняє нашу найбільшу локальну мережу, яка складається з 100 ПК.

Кожен з 100 ПК посилає потік заявок з інтенсивністю у 142 кадрів/с. Інтенсивність вихідного трафіку:

$$\lambda = 100*142 = 14200 \text{ пакетів/с.} \quad (2.3)$$

Коефіцієнт затримки:

$$\rho = \frac{\lambda}{\mu вих} = \frac{14200}{83333,33} = 0,17 \quad (2.4)$$

Коефіцієнт зайнятості маршрутизатора:

$$\frac{\rho}{1-\rho} = \frac{0,17}{1-0,17} = 0,20 \quad (2.5)$$

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

$$T = \frac{1}{(\mu - \lambda)} = \frac{1}{(83333{,}33 - 14200)} = 14{,}46\text{мкс} \quad (2.6)$$

Це значення задовольняє нашим вимогам.

Середня довжина черги:

$$L_{чер} = \frac{\rho^2}{1-\rho} = \frac{0.17^2}{1-0.17} = 0.03 \quad (2.7)$$

Середній час перебування пакета у черзі:

$$T_{оч} = \frac{Lчер}{\lambda} = \frac{0{,}03}{14200} = 2{,}11\text{мкс} \quad (2.8)$$

Пропускна здатність каналу:

$$b = \lambda * \text{довжина кадру} = 14200*1500*8 = 170400000\text{біт/с} = 170{,}4\text{ВМбіт/с} \quad (2.9)$$

Це задовольняє пропускній здатності каналу в 1000Мбіт/с.

Висновки до розділу 2:

Розроблені вимоги до комп'ютерної системи юридичної фірми «Lagilatas», розроблена структура КС, обрана мережева архітектура корпоративної мережі повністю задовольняють поставлене завдання, а аналіз трафіку мережі показує, що пропускна здатність каналу у 1000Мбіт/с задовольняє вимоги.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок адресації корпоративної мережі

В кваліфікаційній роботі необхідно змоделювати КС згідно заданої структури (рисунок 2.1).

Кожній підмережі має бути надана мережна адреса за принципом 10.23.76.0/22 відповідно до таблиці 3.1.

Таблиця 3.1 – Виділений блок адрес для компанії

№	Адреса мережі	LAN_1	LAN_2	LAN_3	LAN_4	LAN_5
16	10.23.76.0	100	64	72	30	37

Необхідно організувати 5 підмереж с загальною кількістю користувачів у 303 штуки.

Для цього ми будемо використовувати метод VLSM, який дозволяє виділити мережу розміру у ступінь двійки. Також слід ураховувати те, що перша та остання адреси мережі зайняті, а тому у мережі з 128 адрес, тільки 126 є корисними.

Враховуючи необхідну кількість пристроїв у кожній підмережі, поділимо діапазон таким чином: 3x128, 1x64. 1x32.

Для виділення переведемо адресу мережі в двійковий вид і відокремимо незадіяну в операції частину.

10.23.01001100.|00000000

Перша та найбільша за розміром підмережа це LAN_1, яка налічує 100 користувачів. Мінімальний блок адрес для такої кількості користувачів містить 2^7 або 128 адрес, дві з яких виділені.

Для розрахунку виділяємо блок в 128 адрес:

10.23.01001100.0|1111111

Отримуємо адресу 10.23.01001100.01111111 - 10.23.76.127 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.76.127 та діапазоном доступних адрес 10.23.76.1 – 10.23.76.126.

Наступна за розміром підмережа, LAN_3, містить в собі 72 користувача. Найменший розмір мережі при цьому також складає 2^7 або 128 адрес.

Для розрахунку заповнимо частину справа та отримаємо кінець діапазону.

10.23.01001100.|11111111

Отримуємо адресу 10.23.01001100.11111111 – 10.23.76.255 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.76.255 та діапазоном доступних адрес 10.23.76.129-10.23.76.254.

Наступна підмережа, LAN_2, містить 64 користувача. Найменший розмір мережі також складає 2^7 або 128 адрес.

Для розрахунку додамо 1 біт до мережевої частини, отримавши

10.23.01001101.|00000000

Після цього до мережі додамо блок в 128 адрес:

10.23.01001101.0|1111111

Отримуємо адресу 10.23.01001100.01111111 – 10.23.77.127 з маскою підмережі 255.255.255.128, широкомовною адресою 10.23.77.127 та діапазоном доступних адрес 10.23.77.0 – 10.23.77.126.

Наступна за розміром мережа, LAN_5, містить у собі 37 користувачів. Мінімальна кількість адрес у цьому випадку становить 2^6 або 64 користувача.

Для розрахунку додамо блок в 64 адреси:

10.23.01001101.|10111111

Отримуємо адресу 10.23.01001101.10111111 – 10.23.77.191 з маскою підмережі 255.255.255.192, широкомовною адресою 10.23.77.191 та діапазоном доступних адрес 10.23.77.129-10.23.77.190.

Остання за розміром підмережа, LAN_4, містить у собі 30 користувачів. Мінімальна кількість адрес у цьому випадку становить 2^5 або 32 користувача.

Для розрахунку додамо блок в 32 адреси:

10.23.01001101.11011111

Отримуємо адресу 10.23.01001101.11011111 – 10.23.77.223 з маскою підмережі 255.255.255.224, широкомовною адресою 10.23.77.223 та діапазоном доступних адрес 10.23.77.193 – 10.23.77.222.

Адресація з врахуванням вимог до мережі і представлена у вигляді таблиці 3.2.

Таблиця 3.2 – Схема адресації мережі

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
LAN1	100	126	10.23.76.0	/25	10.23.76.1 - 10.23.76.126	10.23.76.127
LAN2	64	126	10.23.76.128	/25	10.23.76.129 - 10.23.76.254	10.23.76.255
LAN3	72	126	10.23.77.0	/25	10.23.77.1 - 10.23.77.126	10.23.77.127
LAN4	30	32	10.23.77.192	/27	10.23.77.193 - 10.23.77.222	10.23.77.223
LAN5	37	60	10.23.77.128	/26	10.23.77.129 - 10.23.77.190	10.23.77.191

Схема адресації каналів між маршрутизаторами з діапазону 10.1.16.0/24 представлена у таблиці 3.3.

Таблиця 3.3 – Підмережі каналів WAN між маршрутизаторами

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN1	2	2	10.1.16.0	/30	10.1.16.1 - 10.1.16.2	10.1.16.3
WAN2	2	2	10.1.16.4	/30	10.1.16.5 - 10.1.16.6	10.1.16.7
WAN3	2	2	10.1.16.8	/30	10.1.16.9 - 10.1.16.10	10.1.16.11
WAN4	2	2	10.1.16.12	/30	10.1.16.13 - 10.1.16.14	10.1.16.15
WAN5	2	2	10.1.16.16	/30	10.1.16.17 - 10.1.16.18	10.1.16.19

3.2 Розрахунок адресації пристроїв

У таблиці 3.4 наведена адресація всіх маршрутизаторів мережі з дотриманням всіх необхідних вимог.

Таблиця 3.4 – Схема адресації пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска
Sharavara_Router_0	Gig0/0.46	10.23.76.129	255.255.255.224
	Gig0/0.26	10.23.76.161	255.255.255.224
	Gig0/0.36	10.23.76.193	255.255.255.224
	Gig0/0.99	10.23.76.141	255.255.255.248
	Gig0/1	10.1.16.13	255.255.255.252
	Se0/3/0	10.1.16.6	255.255.255.252
	Se0/3/1	10.1.16.9	255.255.255.252
Sharavara_Router_1	Gig0/0	10.23.76.1	255.255.255.128
	Se0/2/0	10.1.16.1	255.255.255.252
	Se0/3/0	10.1.16.5	255.255.255.252
Sharavara_Router_2	Gig0/0	10.23.77.1	255.255.255.128
	Se0/2/0	10.1.16.2	255.255.255.252
	Se0/3/0	10.1.16.17	255.255.255.252
	Se0/3/2	10.1.16.10	255.255.255.252
Sharavara_Router_3	Gig0/0	10.23.77.129	255.255.255.192
	Gig0/1	10.1.16.14	255.255.255.252

Продовження таблиці 3.4

Пристрій	Інтерфейс	IP-адреса	Маска
Sharavara_Router_4	Se0/3/0	10.1.16.18	255.255.255.252
	Se0/3/1	209.165.202.2	255.255.255.252
Sharavara_Router_6	Gig0/0	64.100.13.1	255.255.255.252
	Gig0/1	10.23.77.193	255.255.255.224
Sharavara_Router_ISP	Gig0/0	64.100.13.1	255.255.255.252
	Gig0/1	209.165.201.1	255.255.255.240
	Se0/3/0	209.165.202.1	255.255.255.252

Адреси в підмережах, що привласнюються інтерфейсам комутаторів, написані у таблиці 3.5.

Таблиця 3.5 – IP-адреси комутаторів в підмережах відділів

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
LAN1	Sharavara_Switch_4	10.23.76.2	255.255.255.128	10.23.76.1
	Sharavara_Switch_5	10.23.76.3		
	Sharavara_Switch_6	10.23.76.4		
	Sharavara_Switch_7	10.23.76.5		
	Sharavara_Switch_8	10.23.76.6		
LAN2	Sharavara_Switch_9	10.23.77.2	255.255.255.128	10.23.77.1
	Sharavara_Switch_10	10.23.77.3		
	Sharavara_Switch_11	10.23.77.4		
LAN3	Sharavara_Switch_0	10.23.76.242	255.255.255.248	10.23.76.241
	Sharavara_Switch_1	10.23.76.243		
	Sharavara_Switch_2	10.23.76.244		
	Sharavara_Switch_3	10.23.76.245		
LAN4	Sharavara_Switch_14	10.23.77.194	255.255.255.224	10.23.77.193
	Sharavara_Switch_15	10.23.77.195		
LAN5	Sharavara_Switch_12	10.23.77.130	255.255.255.192	10.23.77.129
	Sharavara_Switch_13	10.23.77.131		

3.3 Налаштування моделі комп’ютерної системи корпоративної мережі

На рисунку 3.1 зображена топологічна схема корпоративної мережі. Топологічна схема включає в себе головний та віддалений офіс, мережу провайдера. Мережа зв’язана між собою за допомогою кабелів SerialEthernet та GigabitEthernet.

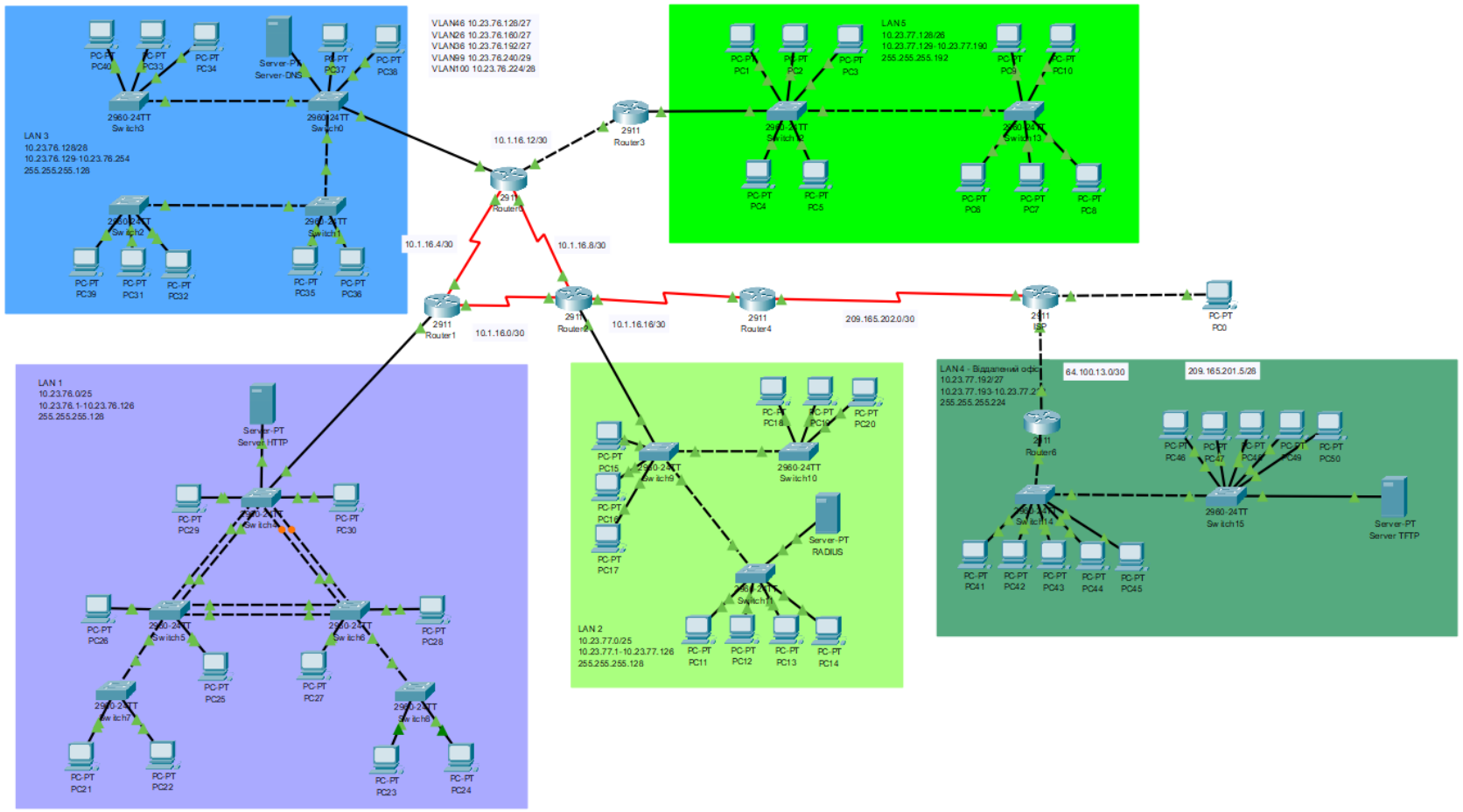

Рисунок 3.1 – Топологічна схема корпоративної мережі юридичної фірми «Legalitas»

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

Для захисту обладнання від несанкціонованого доступу виконаємо базове налаштування пристроїв на прикладі Sharavara_Router_4:

```
en //перехід до привілейованого режиму
conf t // перехід до режиму глобальної конфігурації
hostname Sharavara_Router_4 // зміна назви маршрутизатора
line console 0
password cisco // встановлення паролю до консолі
login
line vty 0 15
password cisco // встановлення паролю для ліній vty
login
enable secret class // встановлення паролю до привілейованого режиму
service password-encryption // увімкнення шифрування паролів
banner motd ‘Sharavara_Router_4’ // встановлення банеру MOTD
ip domain-name Sharavara_Router_4 // встановлення доменного ім’я
crypto key generate rsa // генерація пари ключів для встановлення зв’язку по протоколу SSH
1024 // встановлення кількості бітів ключа
username 123191_Sharavara password admincisco
line vty 0 15
transport input ssh // увімкнення доступу до консолі через SSH
login local
```

3.4.2 Налаштування маршрутизаторів корпоративної мережі

Для того, щоб користувачі із різних підмереж могли взаємодіяти один з одним, необхідна настройка маршрутизації на маршрутизаторах комп’ютерної мережі.

Маршрутизацію можна виконати, як статично, додав маршрути, або динамічно, тобто, за допомогою протоколу динамічної маршрутизації.

Для комп'ютерної мережі юридичної фірми «Legalitas» був обран протокол маршрутизації OSPF, так як це відкритий протокол маршрутизації, який працює на обладнанні будь-якого виробника, на відмінну від протоколу EIGRP, який працює тільки на обладнані Cisco.

Налаштування OSPF включає в себе оголошення безпосередньо підключених локальних мереж та відключення поширення оновлень маршрутизації на інтерфейси локальних мереж.

Налаштування протоколу OSPF на Sharavara_Router_2:

```
router ospf 1 // увімкнення протоколу та надання номеру процесу
passive-interface default // відключення поширення оновлень за замовчуванням на всіх портах
no passive-interface Serial0/2/0 // увімкнення поширення оновлень на портах, через які будуть передаватись дані щодо підключених мереж
no passive-interface Serial0/3/0
no passive-interface Serial0/3/1
network 10.23.77.0 0.0.0.127 area 0 // анонсування всіх необхідних для маршрутизації мереж
network 10.1.16.16 0.0.0.3 area 0
network 10.1.16.0 0.0.0.3 area 0
network 10.1.16.8 0.0.0.3 area 0
```

На граничному маршрутизаторі Sharavara_Router_4 налаштовуємо маршрут за замовчуванням на маршрутизаторі з прямим підключенням до ISP (інтернет-провайдер) і виконуємо його розповсюдження:

```
ip route 0.0.0.0 0.0.0.0 209.165.202.1 // налаштовуємо маршрут за замовчуванням
redistribute static subnets // увімкнення розповсюдження статичних маршрутів через протокол OSPF
```

Додаємо статичний маршрут до мережі провайдера ISP:

```
ip route 209.165.201.0 255.255.255.240 209.165.202.1
```

Налаштовуємо пропускну спроможність та тактову частоту на Serial-інтерфейсаї на прикладі Sharavara_Router_4:

```
int se0/3/1 // вибір інтерфейсу
bandwidth 128 // налаштування пропускної спроможності на рівні 128 Кб/с
clock rate 128000 // встановлення тактової частоти у 128000 на DCE-інтерфейсах мрушрутизаторів
```

Налаштовуємо всі маршрутизаторів на підтримку служби AAA на прикладі Sharavara_Router_0:

```
aaa new-model // увімкнення служби AAA
radius-server host 10.23.77.26 auth-port 1645 key radius123 // налаштування адресу RADIUS-серверу та порт підключення
aaa authentication login CONSOLE group radius local
line console 0
login authentication CONSOLE
aaa authentication login default local // створення локальної бази даних користувачів
username Sharavara_Router_0 password admin123 // налаштування логіну та паролю у локальній базі
line vty 0 15
login authentication default
```

3.4.3 Налаштування роботи Інтернет

Для доступу до мережі Інтернет використовується технологія NAT.

Технологія NAT – це механізм у мережах TCP/IP, який дозволяє змінювати IP-адресу пакунку, який проходить через маршрутизатор. У нашому випадку, він змінює внутрішню IP-адресу пакунку, на IP-адресу з мережі провайдера. Для цього використовується пул адрес адрес 209.165.202.5 – 209.165.202.30.

Переглянемо налаштування NAT на прикладі прикордонного маршрутизатора Sharavara_Router_4:

```
ip access-list extended NAT16 // створення списку NAT16
deny ip 10.23.76.128 0.0.0.127 10.23.77.192 0.0.0.31 // заборона находження пакетів з віддаленої мережі до основної мережі
deny ip 10.23.76.0 0.0.0.127 10.23.77.192 0.0.0.31
deny ip 10.23.77.0 0.0.0.127 10.23.77.192 0.0.0.31
deny ip 10.23.77.128 0.0.0.63 10.23.77.192 0.0.0.31
deny ip 10.1.16.0 0.0.0.255 10.23.77.192 0.0.0.31
permit ip 10.23.76.128 0.0.0.127 any // дозвіл на надходження будь-яких пакетів з основної мережі
permit ip 10.23.76.0 0.0.0.127 any
permit ip 10.23.77.0 0.0.0.127 any
permit ip 10.23.77.128 0.0.0.63 any
permit ip 10.1.16.0 0.0.0.255 any
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 // створення пулу адрес
ip nat inside source list NAT16 pool Internet // прив’язка списку NAT16 до пулу Internet
ip nat inside source static 10.23.76.26 209.165.200.4 // налаштування доступу до веб-сайту з відомостями про тему та завдання кваліфікаційної роботи
```

Для зв’язку між віддаленої та основною мережами, на граничних маршрутизаторах налаштуємо віртуальну приватну мережу VPN з використанням протоколу захисту даних IPsec. Налаштування розглянемо на прикладі Sharavara_Router_4:

Першим кроком потрібно активувати модуль securityk9

```
icense boot module c2900 technology-package securityk9
```

Далі створюємо ACL-список VPN16 таким чином, щоб визначити трафік з основної мережі до віддаленої:

```
ip access-list extended VPN16
```

```
permit ip 10.23.76.128 0.0.0.127 10.23.77.192 0.0.0.31 // надання доступу на проходження пакетів з основної на віддалену мережу
permit ip 10.23.76.0 0.0.0.127 10.23.77.192 0.0.0.31
permit ip 10.23.77.0 0.0.0.127 10.23.77.192 0.0.0.31
permit ip 10.23.77.128 0.0.0.63 10.23.77.192 0.0.0.31
permit ip 10.1.16.0 0.0.0.255 10.23.77.192 0.0.0.31
```

Далі додамо властивості криптографічної політики ISAKMP 10 та загальний ключ шифрування cisco:

```
crypto isakmp policy 10 // створення криптографічної політики
encr 3des // вибір алгоритму шифрування
hash md5 // вибір алгоритму створення геш-суми
authentication pre-share // вибір методу автентифікації пірів
group 2
crypto isakmp key cisco address 64.100.13.2 // створення ключа для взаємодії з обраним партнером
```

Далі створимо набір перетворень (TS) та криптографічне зіставлення MAP:

```
crypto ipsec transform-set TS esp-3des esp-md5-hmac // створення набору перетворень
crypto map MAP 10 ipsec-isakmp // створення криптографічного зіставлення
set peer 64.100.13.2 // створення піра
set transform-set TS // вибір набору перетворень
match address VPN16 // прив’язка до списку VPN16
```

Далі прив’яжемо криптографічне зіставлення MAP до вихідного інтерфейсу s0/3/1:

```
int s0/3/1
crypto map MAP
```

3.5 Перевірка роботи комп'ютерної системи підприємства

Перевірка системи є одним з ключових моментів її розробки.

Першим кроком перевіримо справність DHCP-серверів на прикладі маршрутизатора Sharavara_Router_0. Для цього включимо отримання адрес через DHCP на комп'ютерах підмережі цього маршрутизатора (рисунок 3.2).

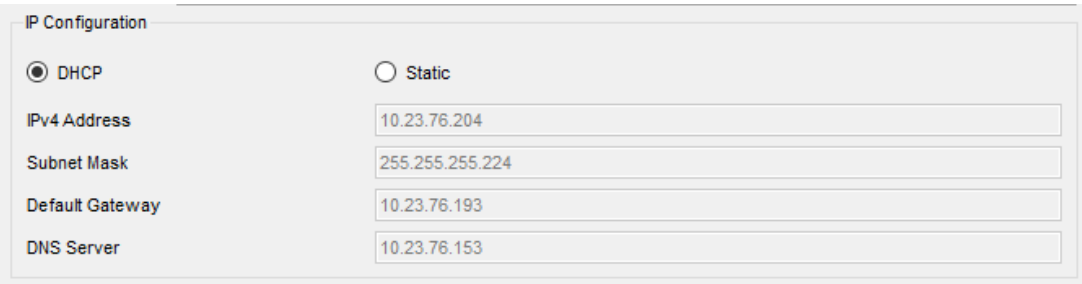

Рисунок 3.2 – Перевірка роботи DHCP-серверу

Комп'ютер успішно отримав адресу та інформацію про DNS-сервер та мережу.

Далі перевіримо протокол динамічної маршрутизації OSPF. Для цього надішлемо PING пакет від комп'ютера з підмережі LAN1 на комп'ютер у підмережі LAN3 (рисунок 3.3).

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC30	PC35	ICMP		0.000	N	0	(edit)	
	Successful	PC29	PC32	ICMP		0.000	N	1	(edit)	
	Successful	PC26	PC39	ICMP		0.000	N	2	(edit)	

Рисунок 3.3 – Перевірка роботи маршрутизації

Наступним кроком перевіримо роботу NAT. Для цього надішлемо пакет від комп'ютеру з мережі організації на комп'ютер у мережі провайдера та подивимось статистику перетворень NAT до та після (рисунки 3.4-6)

```
Sharavara_Router_4#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
---  209.165.200.4     10.23.76.26        ---                ---
```

Рисунок 3.4 – Статистика перетворень до надсилання пакетів

Successful	PC36	PC0	ICMP	0.000	N	0	(edit)
Successful	PC30	PC0	ICMP	0.000	N	1	(edit)
Successful	PC14	PC0	ICMP	0.000	N	2	(edit)

Рисунок 3.5 – Успішна пересилка пакетів

```
Sharavara_Router_4#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.5:3   10.23.76.207:3     209.165.201.5:3    209.165.201.5:3
icmp 209.165.200.5:4   10.23.76.207:4     209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.5:5   10.23.76.207:5     209.165.201.5:5    209.165.201.5:5
icmp 209.165.200.5:6   10.23.76.207:6     209.165.201.5:6    209.165.201.5:6
icmp 209.165.200.5:7   10.23.76.207:7     209.165.201.5:7    209.165.201.5:7
icmp 209.165.200.6:4   10.23.76.13:4      209.165.201.5:4    209.165.201.5:4
icmp 209.165.200.6:5   10.23.76.13:5      209.165.201.5:5    209.165.201.5:5
icmp 209.165.200.6:6   10.23.76.13:6      209.165.201.5:6    209.165.201.5:6
icmp 209.165.200.6:7   10.23.76.13:7      209.165.201.5:7    209.165.201.5:7
icmp 209.165.200.6:8   10.23.76.13:8      209.165.201.5:8    209.165.201.5:8
icmp 209.165.200.7:1   10.23.77.21:1      209.165.201.5:1    209.165.201.5:1
---  209.165.200.4     10.23.76.26        ---                ---
```

Рисунок 3.6 – Статистика перетворень після надсилання пакетів

Далі перевіримо роботу сайту. Для цього на будь-якому з комп’ютерів мережі відкриємо сайт 123.dnipro.ua (рисунок 3.7).

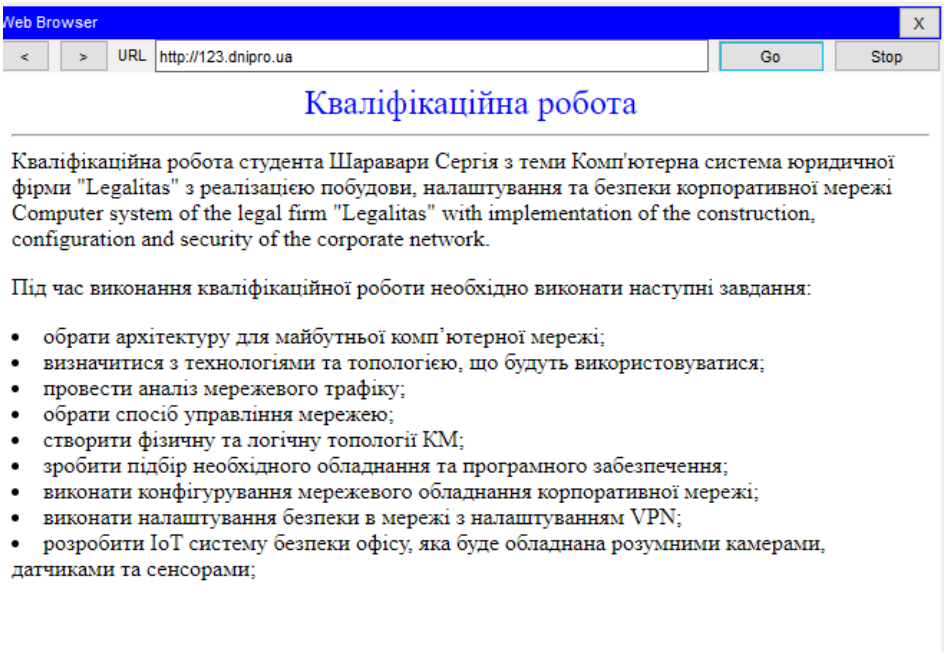

Рисунок 3.7 – Перевірка роботи сайту

Останнім кроком перевіримо роботу VPN. Для цього надішлимо пакет з віддаленої мережі до основної та порівняємо зміст статистики перетворень (Рисунки 3.8-10).

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #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 3.8 – Статистика перетворень до надсилання пакетів

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC20	PC41	ICMP		0.000	N	0	(edit)	
	Successful	PC43	PC19	ICMP		0.000	N	1	(edit)	

Рисунок 3.9 – Успішна робота VPN

```
#pkts encaps: 617, #pkts encrypt: 617, #pkts digest: 0
#pkts decaps: 618, #pkts decrypt: 618, #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 3.10 – Статистика перетворень після надсилання пакетів

3.6 Захист інформації в комп’ютерній системі від несанкціонованого доступу

При доступі до мережі, зловмисник може легко проводити розвідку сусідніх вузлів та збирати передану інформацію. Однак, якщо мережа налаштована належним чином, своєчасне виявлення потенційної загрози допоможе захистити систему від несанкціонованого доступу та знизити витрати.

У даній мережі використовуються наступні типи захисту інформації, які можна розділити на три основні категорії:

1. Засоби фізичного захисту, що охоплюють заходи забезпечення безпеки кабельної системи, електроживлення та засоби архівації.
2. Програмні засоби захисту, включаючи антивірусні програми, системи розмежування повноважень та програми контролю доступу.
3. Адміністративні заходи захисту, що включають контроль доступу до приміщень, розробку стратегії безпеки компанії та планів дій у надзвичайних ситуаціях.

Ці заходи взаємодіють між собою для створення комплексної системи захисту, яка має на меті запобігання несанкціонованому доступу та збереження конфіденційності переданої інформації.

3.6 Налаштування мереж VLAN

Підмережа LAN_3 була розділена на три підмережі VLAN. Номери використаних VLAN мереж внесено до таблиці 3.6

Таблиця 3.6 – Мережі VLAN

Номер VLAN	Ім’я VLAN	Примітка
VLAN46		
VLAN26		
VLAN36		
VLAN1	Default	Не використовується
VLAN100	Native	Власна
VLAN99	Management	Для керування пристроями

Таблиця схеми адресації підмереж VLAN представлена в таблиці 3.7.

Назва	Розмір	Адреса	Маска	Діапазон адрес	Широкомовна адреса
VLAN46	30	10.23.76.128	255.255.255.224	10.23.76.129-10.23.76.158	10.23.76.159
VLAN26	30	10.23.76.160	255.255.255.224	10.23.76.161-10.23.76.188	10.23.76.189
VLAN36	30	10.23.76.190	255.255.255.224	10.23.76.191-10.23.76.222	10.23.76.223
VLAN99	6	10.23.76.240	255.255.255.248	10.23.76.241-10.23.76.247	10.23.76.248
VLAN100	14	10.23.76.224	255.255.255.240	10.23.76.225-10.23.76.238	10.23.76.239

Таблиця призначення портів представлена в таблиці 3.8.

Таблиця 3.8 – Розподіл портів для окремих мереж VLAN

Назва	VLAN	Розподіл портів
VLAN46	46	F0/5-10
VLAN26	26	F0/12-14
VLAN36	36	F0/15-24

Таблиця адресації представлена в таблиці 3.9.

Таблиця 3.9 – Адресація пристроїв в LAN_3.

Пристрій	Інтерфейс	Адреса	Маска	Шлюз	VLAN
Switch0	SVI	10.23.76.242	255.255.255.248	10.23.76.241	99
Switch1	SVI	10.23.76.243	255.255.255.248	10.23.76.241	99
Switch2	SVI	10.23.76.244	255.255.255.248	10.23.76.241	99
Switch3	SVI	10.23.76.245	255.255.255.248	10.23.76.241	99
Router0	G0/0.46	10.23.76.129	255.255.255.224	-	46
	G0/0.26	10.23.76.161	255.255.255.224	-	26
	G0/0.36	10.23.76.191	255.255.255.224	-	36
	G0/0.99	10.23.76.241	255.255.255.248	-	99

Налаштування технології VLAN на прикладі комутатора Sharvara_Switch_0:

```
int range fa0/5-10 // вибір портів
switchport mode access // налаштування портів
switchport access vlan 46 // присвоювання портам влану
int range fa0/12-14
switchport mode access
switchport access vlan 26
int range fa0/15-24
switchport mode access
switchport access vlan 36
int range fa0/1-4
switchport mode trunk
switchport trunk native vlan 100
```

```
switchport trunk allowed vlan 46,26,36,99-100
```

Налаштування портів на комутаторах, привласнивши їм адреси з мережі Management VLAN:

```
int vlan 99
ip address 10.23.76.242 255.255.255.248
ip default-gateway 10.23.76.241
```

3.7 Налаштування параметрів безпеки комутаторів та адресації пк в мережах VLAN

В кожній з підмереж VLAN компанії користувачі можуть отримати мережні налаштування по протоколу динамічної адресації DHCP. Для цього треба виконати налаштування маршрутизатора, який виконує функції маршрутизації між мережами VLAN, як DHCP-сервер:

```
ip dhcp excluded-address 10.23.76.128 10.23.76.138 // виключення адрес з пулу DHCP
ip dhcp excluded-address 10.23.76.153
ip dhcp excluded-address 10.23.76.161 10.23.76.171
ip dhcp excluded-address 10.23.76.129 10.23.76.139
ip dhcp excluded-address 10.23.76.193 10.23.76.203
ip dhcp pool LAN3-VLAN46 // створення пулу адрес для VLAN46
 network 10.23.76.128 255.255.255.224 // налаштування мережі
 default-router 10.23.76.129 // налаштування шлюзу за замовчуванням
 dns-server 10.23.76.153 // налаштування ДНС-серверу
ip dhcp pool LAN3-VLAN26
 network 10.23.76.160 255.255.255.224
 default-router 10.23.76.161
 dns-server 10.23.76.153
ip dhcp pool LAN3-VLAN36
 network 10.23.76.192 255.255.255.224
 default-router 10.23.76.193
 dns-server 10.23.76.153
```

На портах комутаторів, підключених до серверів, налаштовуємо функцію безпеки портів:

```
int f0/7 // вибір необхідного порту
switchport mode acces // налаштування режиму порту
switchport port-security // увімкнення захисту порту
switchport port-security maximum 2 // налаштування кількості унікальних пристроїв, яким дозволений доступ
switchport port-security mac-address sticky // налаштування автоматичного розпізнавання MAC-адресу та додавання його до конфігурації
switchport port-security violation restrict // налаштування дії комутатора під час порушення безпеки
```

Висновки до розділу 3:

Розроблена мережа повністю задовольняє поставлене завдання.

Також мережа повністю перевірена, відповідає всім нормам та функціонує чинним образом.

4. РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента системи

Інтернет речей, відомий також як IoT, є майже невід'ємною складовою сучасних комп'ютерних систем. Згідно з вимогами замовника у комп'ютерній мережі юридичної компанії "Legalitas" було впроваджено IoT-систему безпеки офісу.

Система складається з таких пристроїв, як IoT-двері та вікна, датчики вогню, сирени, RFID-зчитувачі з картками.

IoT-система працює наступним чином:

1. RFID-зчитувач перевіряє ID-картки.

– Якщо ID співпадає з дозволеним, він посилає сигнал на IoT сервер, який відмикає двері та відчиняє вікна.

– Якщо ID не співпадає з дозволеним, вмикається сирена та зачиняються вікна, якщо вони були відімкнуті.

2. Якщо датчик вогню виявляє вогонь, він надсилає сигнал до IoT-серверу, який вмикає сирени.

Зв'язок між пристроями був впроваджений за допомогою HomeGateway, що виконує роль сервера Інтернету речей (IoT). Пристрої підключаються до HomeGateway за допомогою бездротового зв'язку, який базується на стандарті IEEE 802.11 (Wi-Fi).

4.2 Налаштування обладнання та сервісів системи IoT

Для створення IoT-системи безпеки, спочатку розміщуємо необхідне обладнання у мережі та під’єднаємо його до HomeGateway.

Для цього на HomeGateway створюємо бездротову точку доступу з назвою Sharavara-123-19-1 на пристрої у головному офісі компанії та Sharavara-123-19-1-2 у віддаленому офісі. Протокол безпеки мережі

обираємо WPA2-PSK з паролем cisco123. Топологічну схему корпоративної мережі з розміщенними у ній пристроями IoT показано на рисунку 4.1.

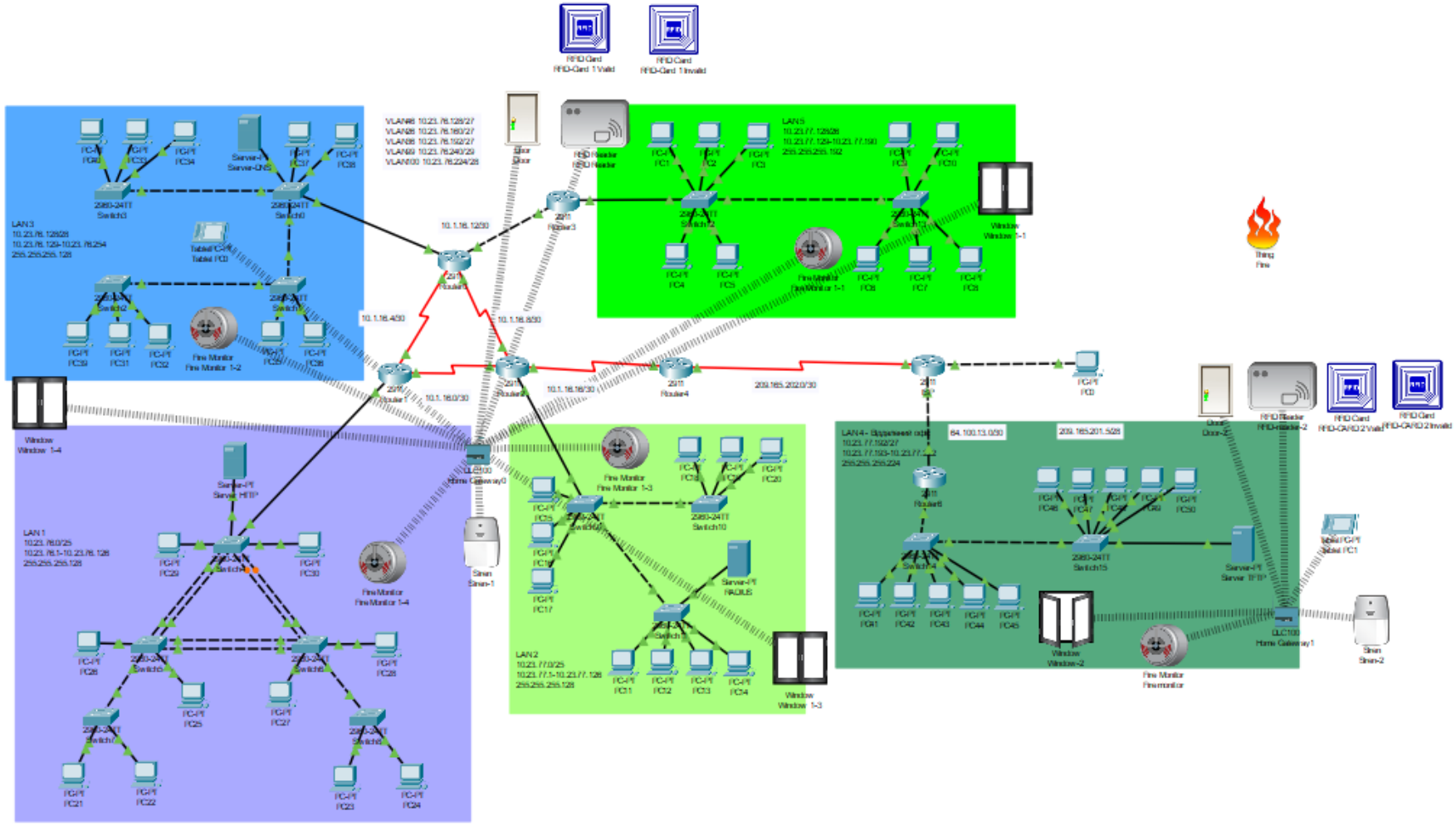

Рисунок 4. 1 – Топологічна схема корпоративної мережі юридичної фірми «Legalitas» з IoT-системою безпеки

Для налаштування IoT-системи були використанні планшети, які підключені до тієї ж мережі, що й IoT-пристрої.

Також для перевірки роботи датчиків вогню був створений пристрій, який симулює вогонь. Код пристрою було написано на мові програмування Python:

```
from physical import *
def setup ():
    setDeviceProperty(getName(), 'IR', 900)
if __name__ == "__main__":
    setup()
```

Щоб налаштувати роботу системи створимо відповідні сценарії роботи на сервері.

Для цього через додані підключений до мережі серверу планшет відкриваємо IoT Monitor, вводимо дані логіну та паролю, після чого потрапляємо на сторінку з усіма підключеними пристроями. Для налаштування сценаріїв переходимо на вкладку «Conditions», яку зображено на рисунку 4.2.

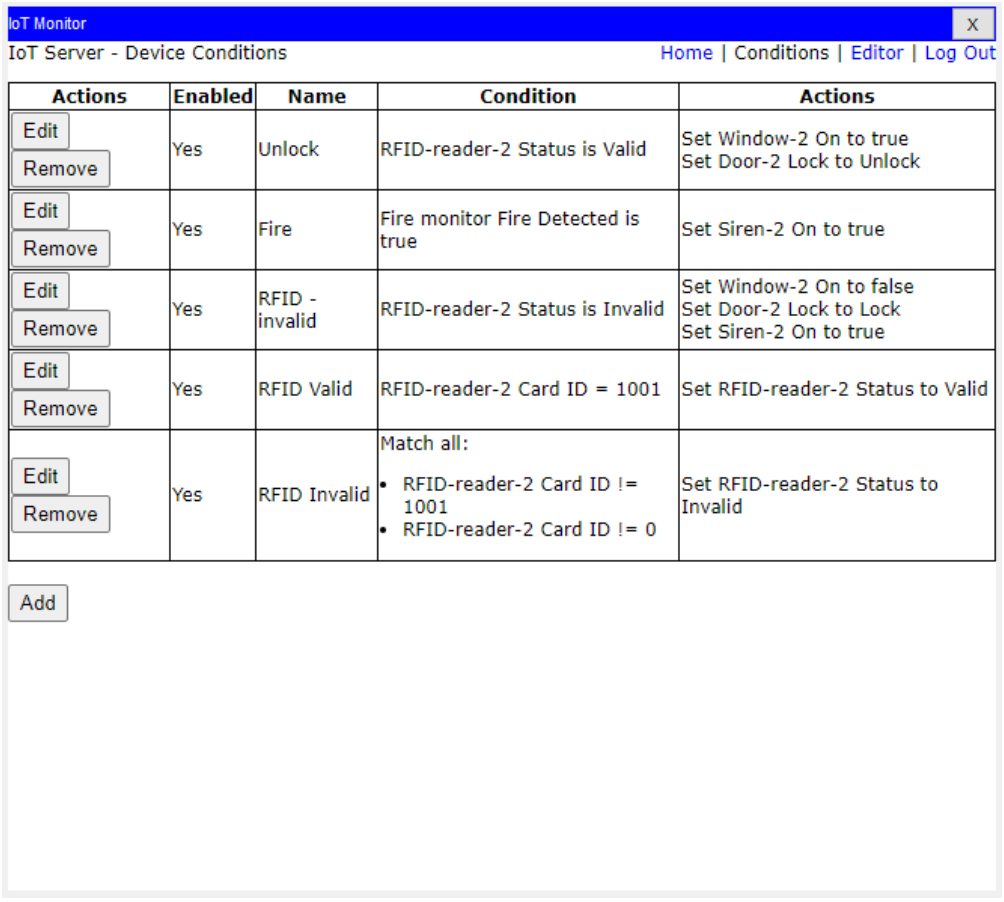

Рисунок 4.2 – Вкладка «Conditions»

Щоб створити новий сценарій натискаємо кнопку «Add».

Для налаштування роботи RFID-зчитувача створимо чотири сценарії.

Спочатку створимо сценарії, які виконують перевірку значення ID у картки. Для цього визначаємо дозволене значення, у нашому випадку це 1001. Далі переходимо до створення сценарію.

Сценарій, що визначає, що картка дозволена показано на рисунку 4.3.

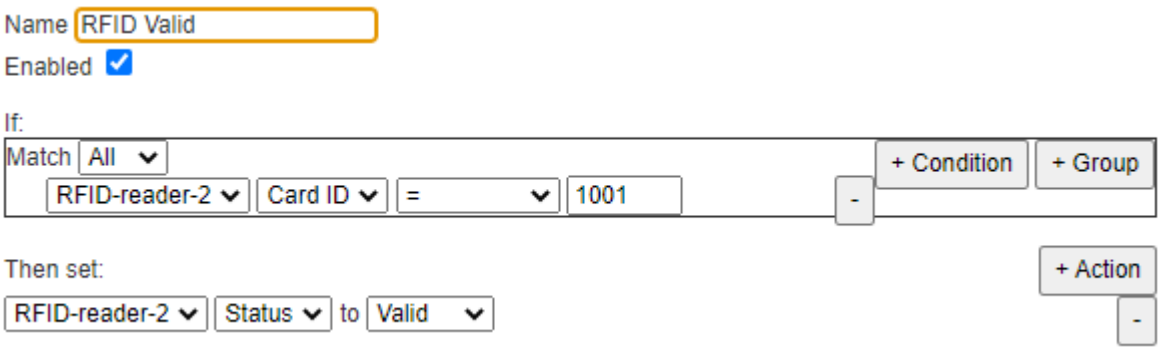

Рисунок 4.3 – Сценарій RFID-зчитувача

Сценарій, що визначає, що картка не дозволена, показано на рисунку 4.4.

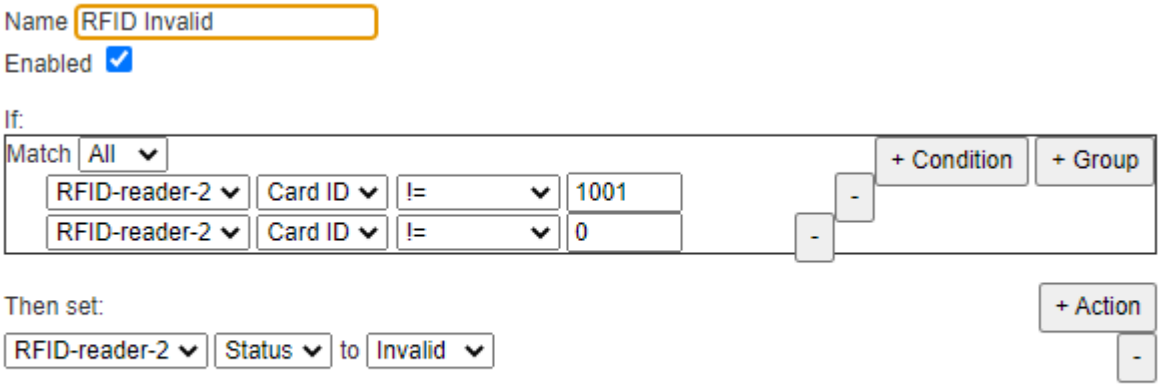

Рисунок 4.4 – Сценарій RFID-зчитувача

Наступним кроком створимо сценарії, що регулюють послідовність дій сервера, після зчитування ID картки.

Першим створимо сценарій, в якому ID картки буде дозволено. В цьому випадку замок дверей буде відімкнуто, та вікна будуть відчинені, а сирена працювати не буде (рисунок 4.5).

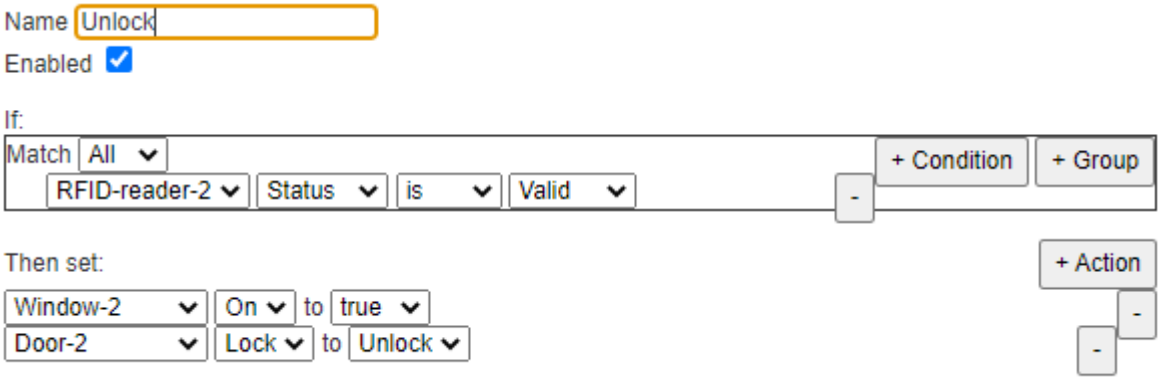

Рисунок 4.5 – Сценарій відімкнення дверей та вікон

Наступним створимо сценарій, в якому ID картки не входить у список дозволених. У цьому сценарії двері замкнуті, а вікна залишаються зачиненими, а сирена вмикається (рисунок 4.6).

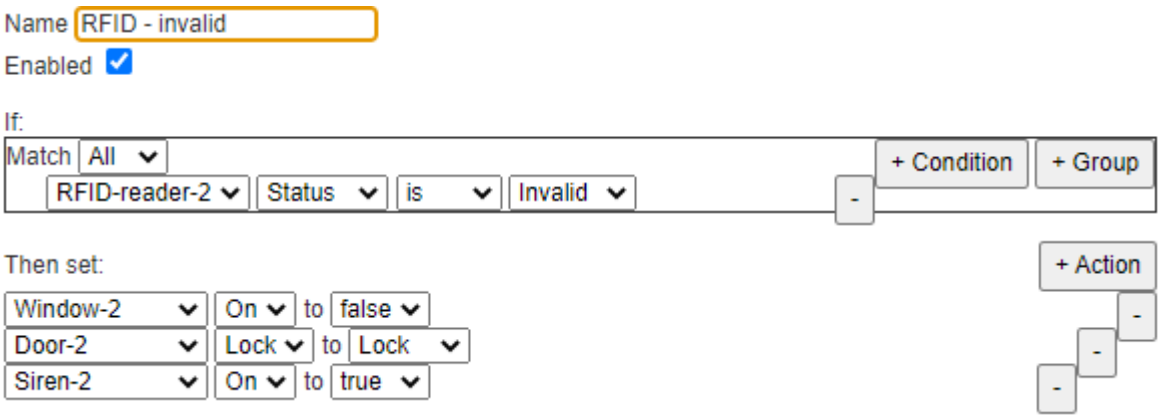

Рисунок 4.6 – Сценарій увімкнення сирени

Також було створено сценарій для роботи датчиків вогню (рисунок 4.7)

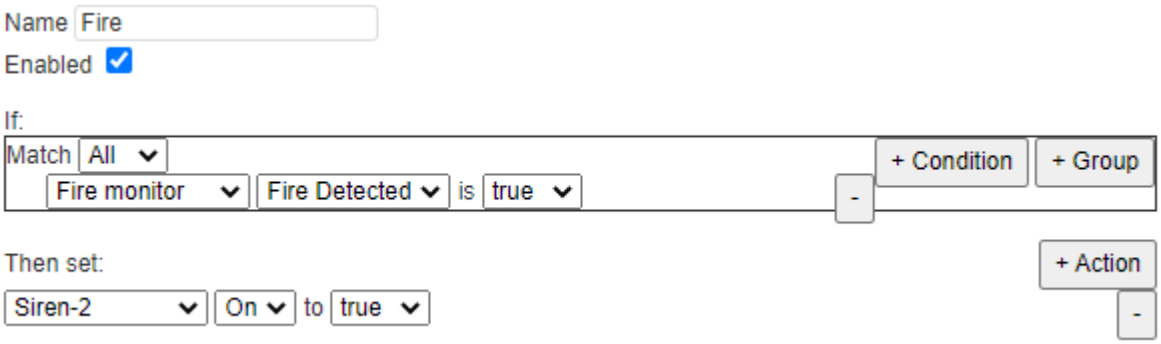

Рисунок 4.7 – Сценарій датчиків вогню

Аналогічні налаштування були виконані для IoT-системи основного офісу.

Висновки до розділу 4:

Розроблена IoT-система охорони відповідає поставленому завданню. Використане обладнання забезпечує безпеку офісу. Показано розміщення та взаємодію розумних пристроїв та датчиків.

Висновки

У даній кваліфікаційній роботі було проведено детальне дослідження основних аспектів проєктування мережі для підприємства, зокрема архітектури, безпеки, пропускної здатності та масштабованості. Обрано юридичну компанію «Legalitas» як об'єкт проєктування мережі. Під час виконання роботи було проведено аналіз потреб компанії та сформульовано вимоги до мережевого проєкту. Відповідно до потреб компанії було здійснено вибір мережевого обладнання для системи. Моделювання проєкту було виконано за допомогою середовища Cisco Packet Tracer.

Під час проєктування було налаштовано всі основні параметри мережевого обладнання, використано технологію VLAN, настроєно динамічну маршрутизацію за протоколом OSPF, забезпечено доступ до Інтернету за допомогою динамічного NAT. Також було налаштовано ACL-списки, використано технологію VPN для забезпечення зв'язку між головним та віддаленим офісом, налаштовано динамічне призначення IP-адрес вузлам за допомогою протоколу DHCP. Додатково, було налаштовано об'єднання фізичних ліній комутаторів за допомогою технології EtherChannel. Також була реалізована система IoT для забезпечення безпеки офісів компанії.

Усі проектні рішення були виконані відповідно до вимог та теми роботи, і були досягнуті поставлені цілі. Робота оформлена згідно з усіма вимогами і стандартами.

Перелік посилань

1. Компанія Legalitas – [Електронний ресурс] – https://legalitas.com.ua/ua/ (дата звернення 10.05.2023)
2. ДСТУ “ГОСТ 12.1.004-91 "ССБТ. Пожежна безпека. Загальні вимоги"”.
3. ДСТУ “ГОСТ Р 50571.22-2000. "Електроустановки будівель. Частина 7. Вимоги до спеціальних електроустановок. Розділ 707. Заземлення устаткування обробки інформації"”.
4. ДСТУ “ГОСТ 15150-69 (зі змінами 2004) "Машини, прилади та інші технічні вироби. Виконання для різних кліматичних районів. Категорії, умови експлуатації, зберігання і транспортування в частині впливу кліматичних факторів зовнішнього середовища" для виду кліматичного виконання УХЛ категорії 4.2”.
5. НАПБ А.01.001-2004 "Про затвердження Правил пожежної безпеки в Україні. Частина 5. Загальні вимоги пожежної безпеки до інженерного обладнання"
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

Схема загальної архітектури мережі підприємства

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

СХЕМА ЗАГАЛЬНОЇ АРХІТЕКТУРИ МЕРЕЖІ ПІДПРИЄМСТВА

Текст програми

804.02070743.23016-01 12 01

Листів 2

2023

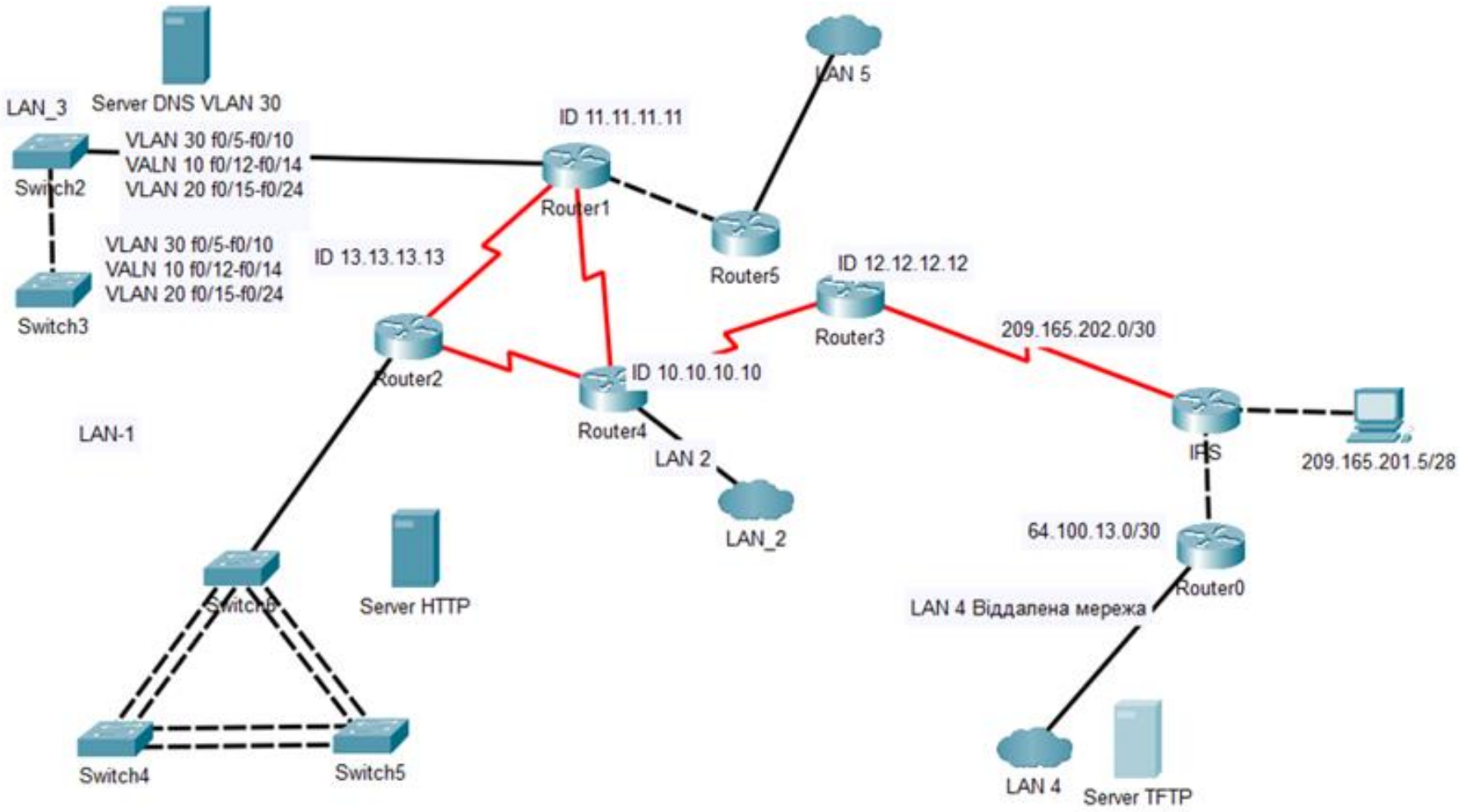

Рисунок А.1 – Схема загальної архітектури мережі підприємства

Додаток Б

Тексти програм налаштування мережі комп’ютерної системи

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23016-01 12 01

Листів 8

2023

АНОТАЦІЯ

Даний документ містить ПЗ налаштувань маршрутизаторів Cisco для структурної схеми моделі комп’ютерної системи.

Тексти програм реалізовані на мові конфігураційних скриптів для мережного обладнання Cisco.

Середовище розробки та налагодження скриптів – пакет моделювання мереж «Cisco Packet Tracer» в середовищі операційної системи Windows 10.

ЗМІСТ

1. Скрипт налаштування Router 4:

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sharavara_Router_4 // Зміна назви маршрутизатора
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1 //зашифрований пароль до привілейованого режмиу
!
!
!
!
!
aaa new-model //увімкнення служби AAA
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
!
no ip cef
no ipv6 cef
!
!
!
username 123191_Sharavara password 7 082048430017061E010803
username Sharavara_Router_4 password 7 082048430017544541 //налаштування логіну та паролю у локальній базі AAA
!
!
license udi pid CISCO2911/K9 sn FTX1524RZ0Q-
license boot module c2900 technology-package securityk9 // Увімкнення модулю безпеки securityk9
!
!
!
crypto isakmp policy 10 // створення криптографічної політики
encr 3des // вибір алгоритму шифрування
hash md5 // вибір алгоритму створення геш-суми
authentication pre-share // вибір методу автентифікації пірів
group 2
!
```

```
crypto isakmp key cisco address 64.100.13.2 // створення ключа для взаємодії з обраним партнером
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac // створення набору перетворень
!
crypto map MAP 10 ipsec-isakmp // створення криптографічного зіставлення
set peer 64.100.13.2 // створення піра
set transform-set TS // вибір набору перетворень
match address VPN16 // прив’язка до списку VPN16
!
!
!
!
ip domain-name Sharavara_Router_4 //визначення доменного ім’я маршрутизатора
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0 //налаштування портів
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 Serial0/3/0
ip address 10.1.16.18 255.255.255.252
ip nat inside //визначення напрямку роботи NAT
!
interface Serial0/3/1
ip address 209.165.202.2 255.255.255.252
ip nat outside
```

```
clock rate 2000000
crypto map MAP //прив’язка крипографічного зіставлення до вихідного інтерфейсу
!
interface Vlan1
no ip address
shutdown
!
router ospf 1 //увімкнення протоколу маршрутизації OSPF
log-adjacency-changes
redistribute static subnets //увімкнення розповсюдження статичних маршрутів по OSPF
network 209.165.202.0 0.0.0.3 area 0 //налаштування мережі та її зони розповсюдження
network 10.1.16.16 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224 //створення
пулу адрес для NAT
ip nat inside source list NAT16 pool Internet //присвоєння пулу адрес до списку доступу
NAT16
ip nat inside source static 10.23.76.26 209.165.200.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1 //створення статичних маршрутів
ip route 209.165.201.0 255.255.255.240 209.165.202.1
ip route 209.165.202.0 255.255.255.252 Serial0/3/1
!
ip flow-export version 9
!
!
ip access-list extended VPN16 //створення списку доступу VPN16
permit ip 10.23.76.128 0.0.0.127 10.23.77.192 0.0.0.31 //дозвіл адреси у списку доступу
permit ip 10.23.76.0 0.0.0.127 10.23.77.192 0.0.0.31
permit ip 10.23.77.0 0.0.0.127 10.23.77.192 0.0.0.31
permit ip 10.23.77.128 0.0.0.63 10.23.77.192 0.0.0.31
permit ip 10.1.16.0 0.0.0.255 10.23.77.192 0.0.0.31
ip access-list extended NAT16
deny ip 10.23.76.128 0.0.0.127 10.23.77.192 0.0.0.31 //заборона адреси у списку доступу
deny ip 10.23.76.0 0.0.0.127 10.23.77.192 0.0.0.31
deny ip 10.23.77.0 0.0.0.127 10.23.77.192 0.0.0.31
deny ip 10.23.77.128 0.0.0.63 10.23.77.192 0.0.0.31
deny ip 10.1.16.0 0.0.0.255 10.23.77.192 0.0.0.31
permit ip 10.23.76.128 0.0.0.127 any
permit ip 10.23.76.0 0.0.0.127 any
permit ip 10.23.77.0 0.0.0.127 any
permit ip 10.23.77.128 0.0.0.63 any
permit ip 10.1.16.0 0.0.0.255 any
!
banner motd ^CSharavara_Router_4^C //створення банеру MOTD
!
radius server 10.23.77.26 //визначення адреси серверу Radius
address ipv4 10.23.77.26 auth-port 1645
key radius123 //визначення паролю доступу
!
```

```
!
!
line con 0
password 7 0822455D0A16 // встановлення паролю для ліній vty
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh //увімкнення доступу до консолі через SSH
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
        end
```

Скрипт налаштування Switch2:

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Sharavara_Switch_2
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
!
ip domain-name Sharavara_Switch_2
!
username 123191_Sharavara privilege 1 password 7 082048430017061E010803
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport trunk native vlan 100 //присвоєння порту номеру VLAN та його режиму
switchport trunk allowed vlan 26,36,46,99-100 //налаштування доступу між VLAN
switchport mode trunk
!
interface FastEthernet0/2
switchport trunk native vlan 100
```

```
switchport trunk allowed vlan 26,36,46,99-100
switchport mode trunk
!
interface FastEthernet0/3
switchport trunk native vlan 100
switchport trunk allowed vlan 26,36,46,99-100
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk native vlan 100
switchport trunk allowed vlan 26,36,46,99-100
switchport mode trunk
!
interface FastEthernet0/5
switchport access vlan 46
switchport mode access
!
interface FastEthernet0/6
switchport access vlan 46
switchport mode access
!
interface FastEthernet0/7
switchport access vlan 46
switchport mode access
!
interface FastEthernet0/8
switchport access vlan 46
switchport mode access
!
interface FastEthernet0/9
switchport access vlan 46
switchport mode access
!
interface FastEthernet0/10
switchport access vlan 46
switchport mode access
!
interface FastEthernet0/11
!
interface FastEthernet0/12
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/13
switchport access vlan 26
switchport mode access
!
interface FastEthernet0/14
switchport access vlan 26
switchport mode access
```

```
!
interface FastEthernet0/15
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/16
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/17
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/18
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/19
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/20
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/21
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 36
switchport mode access
!
interface FastEthernet0/24
switchport access vlan 36
switchport mode access
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
interface Vlan99
```

```
ip address 10.23.76.244 255.255.255.248 //налаштування SVI-адреси комутатора
!
ip default-gateway 10.23.76.241 //налаштування шлюзу за замовчуванням
!
banner motd ^CSharavara_Switch_2^C
!
!
!
line con 0
password 7 0822455D0A16
login
!
line vty 0 4
password 7 0822455D0A16
login local
transport input ssh
line vty 5 15
password 7 0822455D0A16
login local
transport input ssh
!
!
!
!
        end
```