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 Толошного Олександра Валерійовича
(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 ТОВ "Агротек-Інвест" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі "
(назва за наказом ректора)

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

Дніпро
2023

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

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавр

студента Толошного О.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 ТОВ "Агротек-Інвест" з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"

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

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

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

Дата видачі 19.12.2022

Дата подання до екзаменаційної комісії 08.06.2023

Прийнято до виконання _____ Толошний О.В.

РЕФЕРАТ

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

Пояснювальна записка: 74с., 28рис., 11табл., 1 додаток, 10 джерел.

Об'єкт розробки: комп'ютерна система для компанії "Агротек-Інвест" та налаштування корпоративної мережі.

Мета проекту: створення комп'ютерної системи для компанії "Агротек-Інвест".

Комп’ютерна мережа яка була розроблена в кваліфікаційній роботі має змогу гнучко змінювати кількість та набір функцій в залежності від вимог. Мережа орієнтовна на побудову систем контролю та редагування для компанії "Агротек-Інвест" яка знаходиться у місті Дніпро. Використовується для збору та підготовки статистичної інформації.

Розробка комп'ютерної мережі виконана в рамках бакалаврської дипломної роботи.

Розроблена схема мережі була втілена у моделі на симуляторі Cisco Packet Tracer, і була перевірена її функціональність.

Технологія проектування мережі передбачає захист всього обладнання внутрішньої мережі від несанкціонованого доступу.

Результати перевірки представлені у вигляді таблиць, графіків та детально описані в пояснювальній записці або додатках.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЬ І ТЕРМІНІВ

КМ – комп’ютерна мережа.

ПК – персональний комп’ютер.

КС – комп’ютерна система.

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

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

VLAN – (Virtual Local Area Network) –логічна група пристроїв в мережі, які фізично можуть знаходитись на різних мережевих сегментах, але з логічною точки зору вони сприймаються як одна і та ж мережа.

VPN – (Virtual Private Network) – технологія, яка дозволяє створювати віртуальні мережі поверх мереж, які мають нижчий ступінь довіри.

LAN – (Local Area Network) – локальна область мережі, яка об'єднує комп'ютери, пристрої зв'язку та ресурси в невеликій географічній області.

DHCP – (Dynamic Host Configuration Protocol) — протокол мережевого рівня, який автоматично надає IP-адреси, мережеві параметри та конфігураційні дані пристроям в комп'ютерній мережі.

ВСТУП

Сучасні організації все більше розуміють важливість ефективного та безперебійного функціонування мережевої інфраструктури для своєї діяльності. Однією з ключових складових успішної мережі є розробка та впровадження корпоративних мереж, які забезпечують надійну та безпечну комунікацію між всіма підрозділами компанії. У цьому контексті, дипломна робота націлена на розробку корпоративної мережі для компанії Агротек-Інвест, що спеціалізується на сільськогосподарському виробництві та інвестиціях.

Об'єктом дослідження є мережева інфраструктура компанії Агротек-Інвест, яка на сьогоднішній день вимагає модернізації та розширення для задоволення зростаючих потреб організації. Розробка корпоративної мережі передбачає створення оптимальної архітектури, вибір необхідного обладнання та налаштування відповідних протоколів і сервісів для забезпечення безперебійного функціонування та високої ефективності мережевого середовища.

Метою дипломної роботи є розробка та впровадження оптимального рішення корпоративної мережі для компанії Агротек-Інвест, з орієнтацією на її конкретні потреби та вимоги.

Правильно налаштована мережа дозволяє покращити комунікацію між підрозділами компанії, забезпечити безпеку та надійність інформаційного обміну, а також підвищити продуктивність працівників та ефективність бізнес-процесів.

Отже, розробка корпоративної мережі для компанії Агротек-Інвест є актуальною і важливою задачею, яка сприятиме поліпшенню роботи організації та забезпеченню її конкурентних переваг на ринку. Дана дипломна робота має на меті розробити оптимальне рішення для мережевої інфраструктури компанії, враховуючи її потреби та вимоги, а також сучасні технологічні тенденції.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАДАЧІ

1.1 Огляд сфери та умов застосування системи

В 21 столітті неможливо уявити аграрну промисловість України без сучасної техніки. В цій техніці використовується багато технологій, однією з яких є Комп’ютерні мережі.

Комп'ютерні мережі в аграрній сфері використовуються для забезпечення ефективності та продуктивності сільського господарства, зменшення витрат та підвищення якості продукції. Одним з основних застосувань комп'ютерних мереж в аграрній сфері є моніторинг та управління сільськогосподарської техніки. Завдяки вбудованим датчикам, GPS-навігації та телеметрії, комп'ютерні мережі дозволяють проводити моніторинг роботи техніки, її розташування та ефективність, а також віддалено керувати її роботою.

Ще одним важливим застосуванням є використання комп'ютерних мереж для моніторингу погодних умов та прогнозування врожаю. Завдяки датчикам, сенсорам та спеціальним програмним забезпеченням, можна проводити моніторинг показників, такі як температура повітря, вологість ґрунту, кількість опадів та інші, що дозволяє точніше прогнозувати врожайність та вживати необхідні заходи для її підвищення. Крім того, комп'ютерні мережі використовуються для моніторингу та керування станом рослин, що дозволяє підтримувати необхідний рівень зростання, вживати необхідні заходи для захисту рослин від хвороб та шкідників, а також підвищувати якість продукції.

Комп'ютерні мережі також використовуються для взаємодії зі споживачами та оптимізації ланцюгів постачання. Завдяки спеціальним програмним забезпеченням, можна керувати та оптимізувати процес доставки та зберігання продукції, відстежувати її рух від постачальника до споживача, а також забезпечити точність та надійність інформації про продукцію, її якість та властивості. Крім того, комп'ютерні мережі використовуються для розвитку ринків та підвищення конкурентоспроможності аграрних підприємств.

Завдяки інтернету та електронним торговим платформам, можна швидко та ефективно знаходити покупців для своєї продукції, залучати інвесторів, знаходити нові ринки збуту та розвивати свій бізнес.

Не менш важливим застосуванням комп'ютерних мереж в аграрній сфері є моніторинг та управління екологічною безпекою сільськогосподарського виробництва. Завдяки спеціальним датчикам та програмному забезпеченню, можна контролювати рівень забруднення ґрунту, водойм та повітря, а також вживати необхідні заходи для зменшення впливу сільськогосподарського виробництва на навколишнє середовище. Узагалі, комп'ютерні мережі в аграрній сфері дозволяють підвищити ефективність виробництва, зменшити витрати та покращити якість продукції, а також забезпечити більш точне та ефективне управління виробництвом та розподілом продукції на ринку.

Тому, мета даної кваліфікаційної роботи – впровадити та покращити комп’ютерну систему підприємства з продажу нової та бувшої у використанні сільськогосподарської техніки «Агротек-Інвест».

1.2 Огляд підприємства та його організація

Агротек-Інвест - українська компанія, яка спеціалізується на продажу і сервісі сільськогосподарської техніки та запасних частин до неї. Компанія була заснована в 2003 році і протягом багатьох років успішно працює на ринку агропромислового комплексу України.

Приватне підприємство «Агротек-Інвест» розташовано у м. Дніпро Дніпропетровської області.

Рисунок 1.1 – «Агротек-Інвест» у м. Дніпро

Підприємство займається такими видами діяльності:

- компанія спеціалізується на реалізації та обслуговуванні сільськогосподарської техніки від виробника John Deere.
- забезпечує постачання оригінальних запасних частин для сільськогосподарської техніки.
- продаж техніки з напрацюванням, яка має певний ресурс роботи.
- надаються послуги трейд-ін, які дозволяють клієнтам обміняти свою стару техніку на нову зі значною знижкою.
- у асортименті також є продаж та обслуговування техніки від інших виробників, таких як Vaderstad, Hagie, Kramer, Mazzotti, Monosem, Sulky.
- постачання сільськогосподарських і вантажних шин від виробників Firestone, Michelin, NeoTerra.

Надаємо продаж та обслуговування зрошувальних систем від компанії OTECH.

Крім продажу сільськогосподарської техніки, компанія надає послуги з проектування та будівництва агротехнічних комплексів, проводить впровадження сучасних технологій в аграрному виробництві, а також

забезпечує комплексне після продажне обслуговування техніки. Агротек-Інвест активно впроваджує сучасні інформаційні технології в свою діяльність, зокрема, забезпечує онлайн-замовлення та консультації клієнтів, а також використовує системи моніторингу і діагностики техніки для підвищення її ефективності.

Компанія має стратегію, спрямовану на надання максимально швидкого і якісного обслуговування клієнтів. Для досягнення цієї мети, компанія побудувала розгалужену сервісну мережу і складську інфраструктуру з центральним офісом у місті Дніпро. За роки активного розвитку, компанія зуміла забезпечити обслуговування більш ніж 12 000 одиниць техніки на полях України за допомогою своїх фахівців, які доступні 24/7.

Компанія зосереджується на оптимізації виробничих процесів клієнтів. Для досягнення цієї мети, вона надає устаткування техніки системами точного землеробства, а також послуги з аналізу ґрунтів через напрям Агротек Farmsight. Крім того, компанія забезпечує навчання клієнтів роботі з технікою шляхом залучення фахівців з Агротек Academy.

Одним з ключових напрямків, що активно розвивається компанією в останні роки, є продаж і сервісне обслуговування техніки з напрацюванням, відоме як Агротек Restart.

1.2.1 Розміщення підприємства

Два офіси компанії знаходяться на правому березі Дніпра, поблизу міста Новомосковськ, поряд пролягає транспортний шлях «Е50», що дає зручний доступ всім видам техніки. Основний офіс розміщується в двоповерховій будівлі з виїздом одразу на дорогу, другий офіс розташований за п’ять кілометрів на північ в одноповерховій орендованій будівлі.

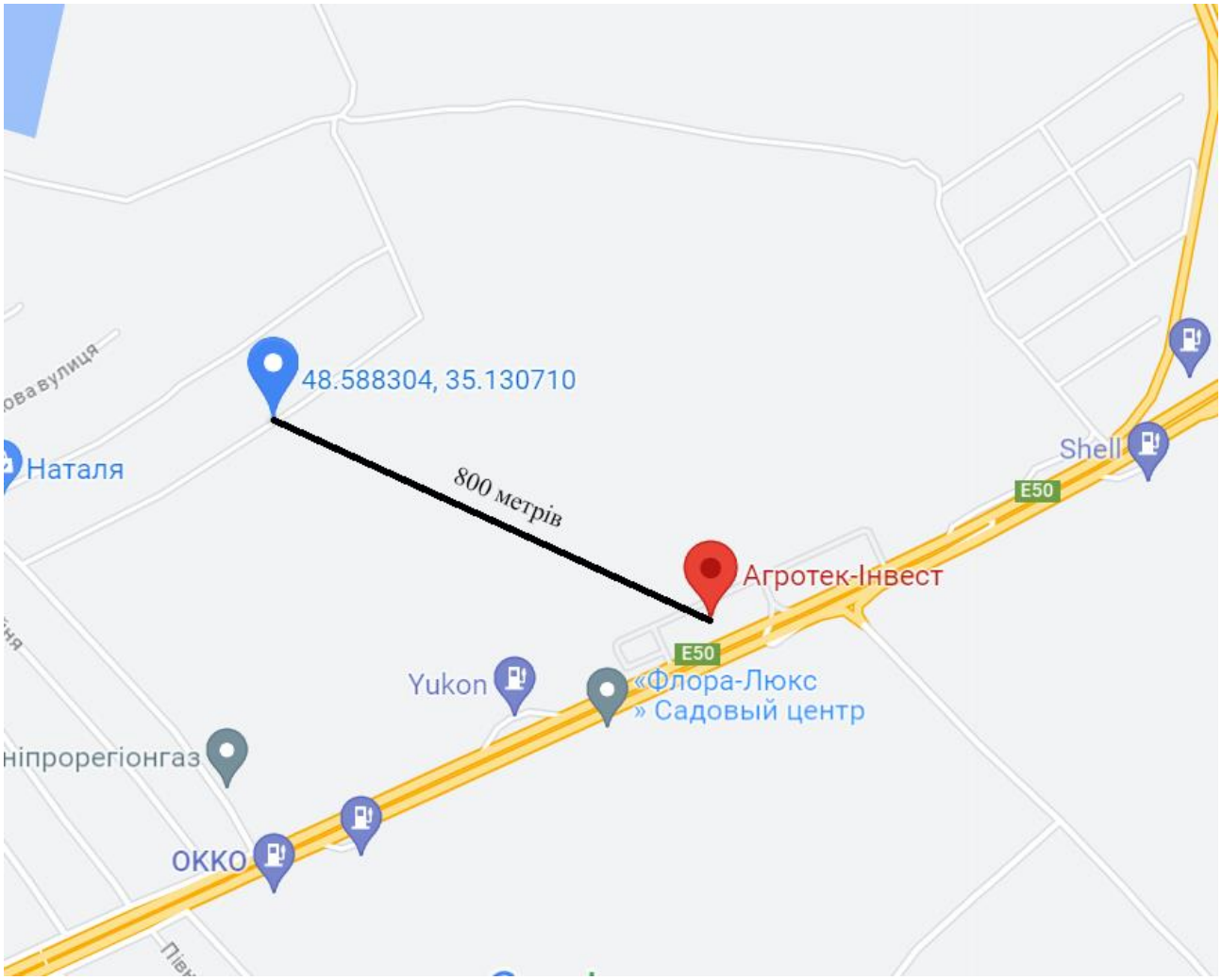


Рисунок 1.2 – Гео-розміщення основного та другого офісу підприємства «Агротек-Інвест»

1.2.2 Організаційна структура підприємства

Організаційна структура підприємства складається з таких посад:

- президент;
- фінансовий відділ;
- юридичний відділ;
- маркетинговий відділ;

Президенту напряму підпорядковуються управляючі трьома цехами, які виконують такі функції

- ремонт техніки;
- підготовка до продажу;

- прийом нової техніки;

Структура компанії по виду належить до дивізіональної. Дивізіональна структура компанії - це організаційна форма, яка базується на розділенні компанії на окремі підрозділи (дивізії) з відповідальністю за окремі функції або групи товарів/послуг. Дивізіональна структура є популярною серед великих компаній, особливо тих, що мають декілька продуктових ліній або займаються діяльністю в різних регіонах світу.

Основні переваги дивізіональної структури:

- Кожна дивізія може бути управляється самостійно, що дозволяє більш ефективно керувати процесами і приймати швидкі рішення.
- Дивізії можуть бути орієнтовані на свої власні ринки та потреби, що дозволяє компанії реагувати на зміни в ринкових умовах більш швидко і ефективно.
- Дивізії можуть бути спеціалізованими на певних продуктах або послугах, що дозволяє компанії більш точно працювати зі своїми клієнтами та ринками.

Основні недоліки дивізіональної структури:

- Дублювання функцій та процесів між дивізіями може призвести до збільшення витрат на управління та складність управління всією компанією.
- Конфлікти між дивізіями можуть виникати, особливо при розподілі ресурсів та управлінні більш складними проектами.
- Менеджмент дивізії може перефокусувати свою увагу на короткострокових цілях дивізії, замість загальних довгострокових цілей компанії.

Схему організаційної структури підприємства зображено на рисунку 1.4.

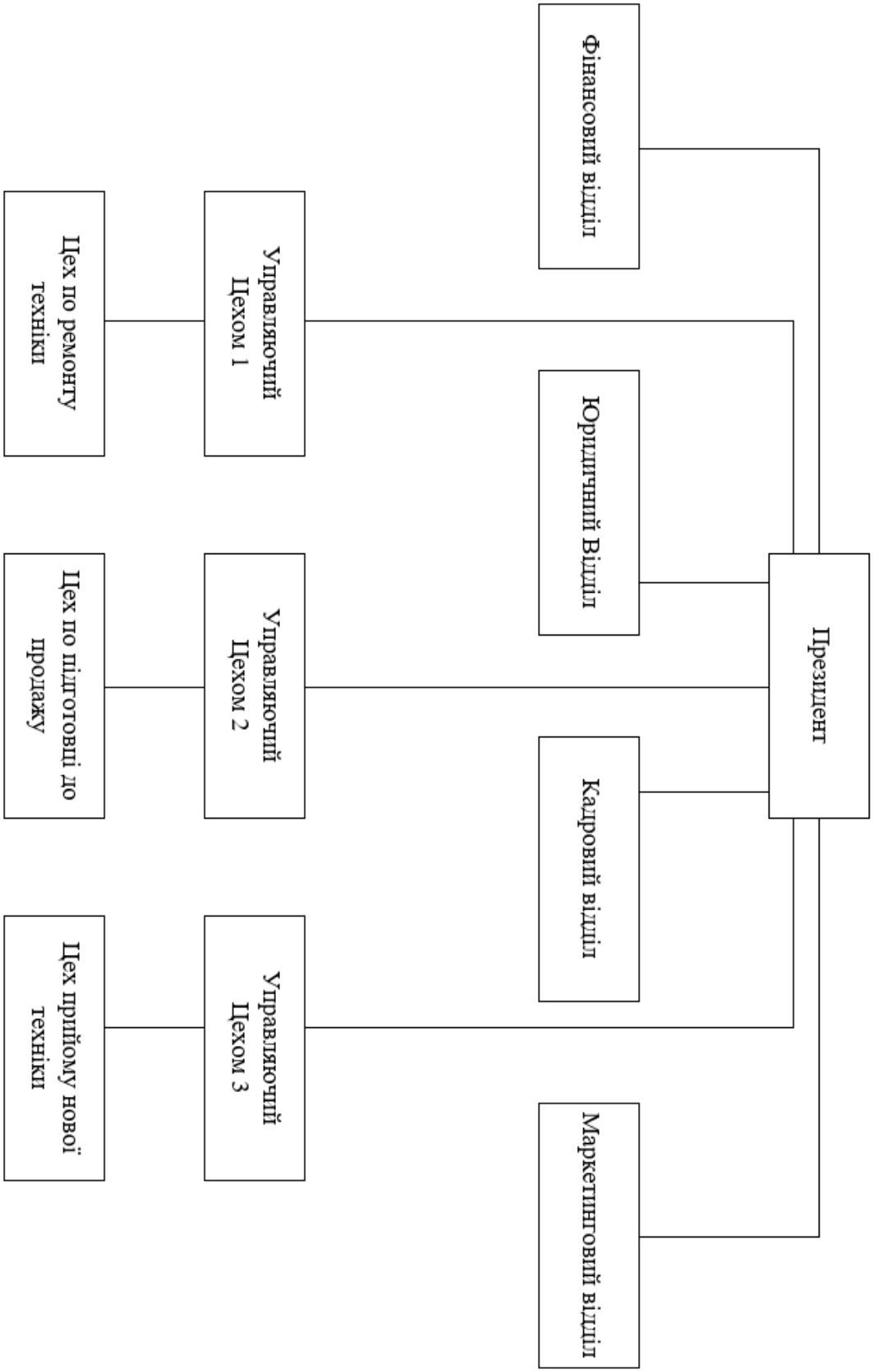


Рисунок 1.3 - Організаційна структура підприємства

1.2.3 Аналіз топологічної схеми розміщення підприємства

Нище наведені структурні схеми відділів підприємства.

Рисунок 1.5 – Фінансовий та кадровий відділи.

Рисунок 1.6 – Маркетинговий та юридичний відділи, які знаходиться в віддаленій мережі.

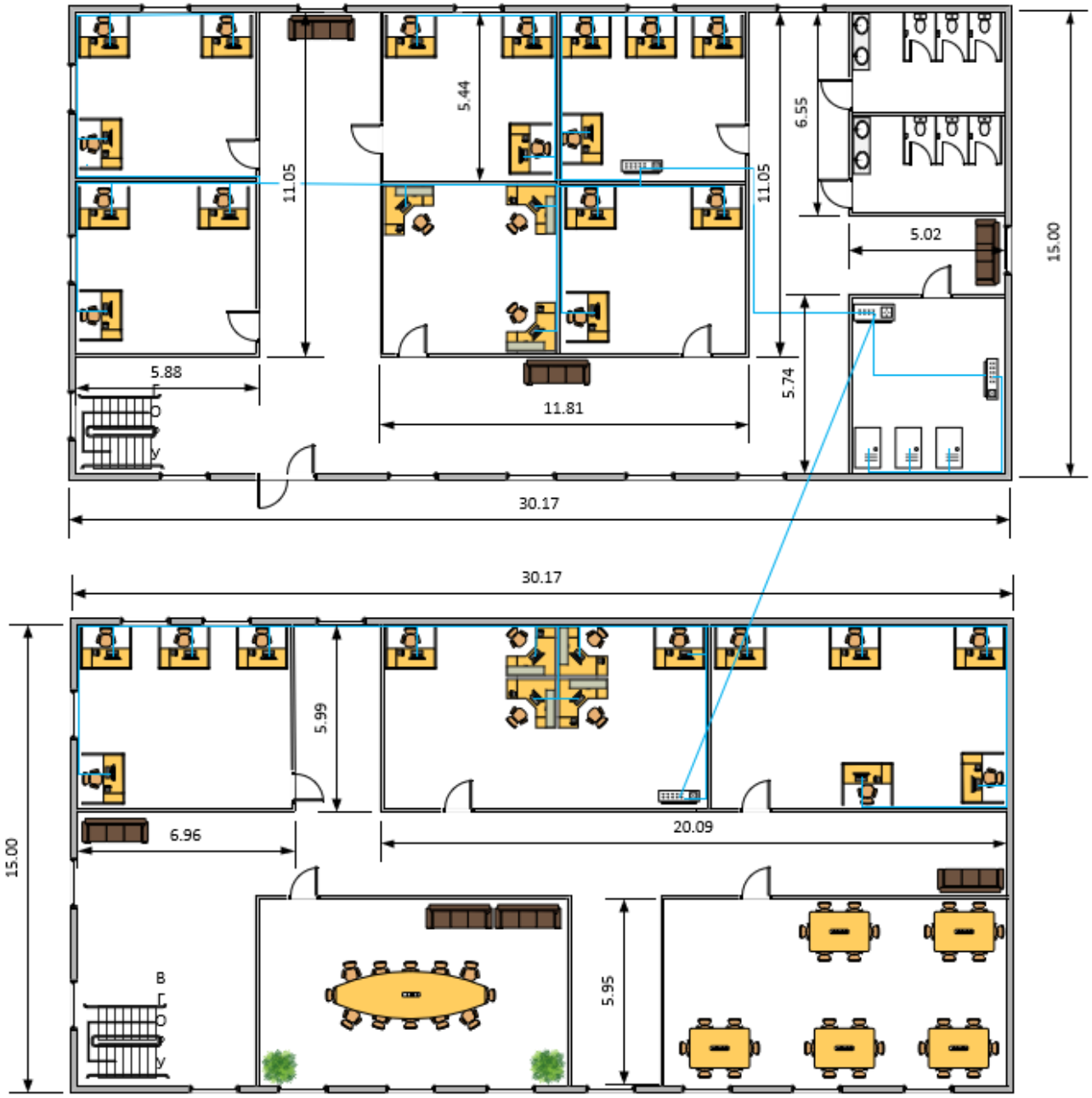


Рисунок 1.4 – Фінансовий та кадровий відділи.

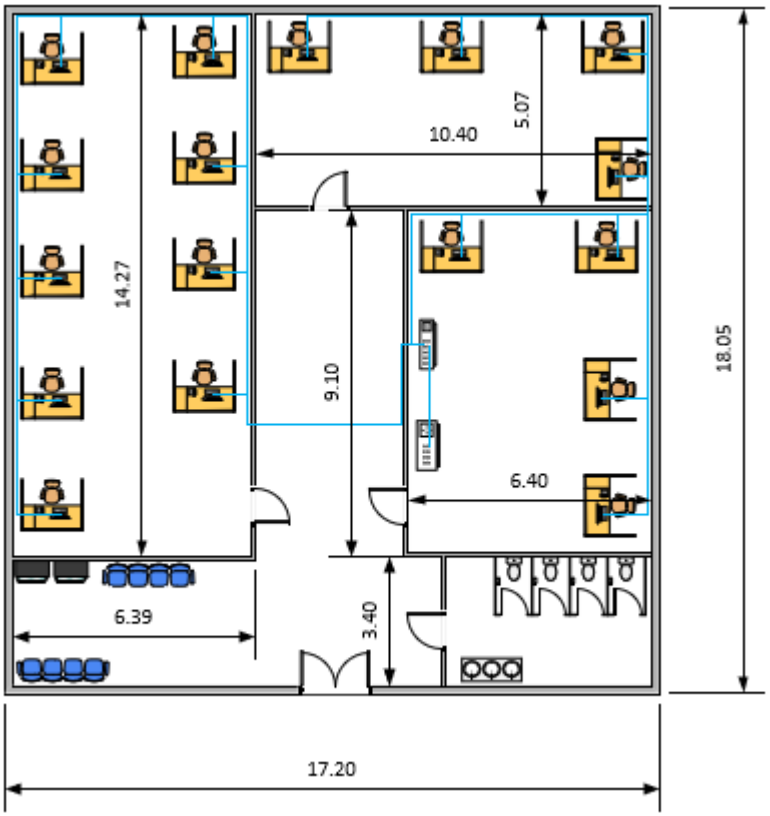


Рисунок 1.5 – Маркетинговий та юридичний відділи

Розміри приміщень, поверхів, перекриттів, стін та інших елементів.

Головний офіс – маркетинговий та юридичний відділи:

- Поверх: Один поверх з загальною площею приблизно 310 квадратних метрів.
- Перекриття: Одношарове перекриття, що охоплює всю площу головного офісу.

Віддалений офіс - фінансовий та кадровий відділи:

- Поверхи: Два поверхи з однаковою площею, кожний поверх має 452.55 квадратних метрів.
- Перекриття: Двошарове перекриття, яке охоплює всю площу віддаленого офісу.

Стіни:

Матеріал стін: Цегляні стіни.

Висота стін: Стандартна висота стін близько 3 метрів.

1.3 Принципи, технічні способи та математичні методи інформаційного забезпечення

ТОВ "Агротек-Інвест" використовує різноманітні технічні та математичні методи для забезпечення ефективності виробництва та керування підприємством.

Одним з ключових принципів інформаційного забезпечення є використання комп'ютерних систем, що дозволяють збирати, обробляти та аналізувати великі обсяги даних. Наприклад, компанія використовує систему моніторингу врожаю, яка дозволяє збирати дані про врожайність на різних ділянках землі та проводити аналіз цих даних для оптимізації виробництва та планування наступних сівозмін. Також в компанії використовуються системи автоматизації бухгалтерського та фінансового обліку, що дозволяє зменшити кількість ручної роботи та зберегти час. Щодо технічних способів, компанія використовує спеціалізовані програмні продукти, що дозволяють проводити аналіз та моделювання різних процесів у виробництві та оптимізувати роботу підприємства. Наприклад, для обробки геоданих використовуються програмні продукти типу GIS (Geographic Information System).

Математичні методи використовуються для розрахунку показників ефективності виробництва, планування ресурсів та керування ризиками. Наприклад, для прогнозування врожаю використовуються математичні моделі на основі статистичних даних та аналізу кліматичних умов.

Таким чином, ТОВ "Агротек-Інвест" використовує різні технічні, математичні та програмні засоби для підвищення ефективності виробництва.

1.4 Аналітичний огляд існуючих способів обробки та передачі інформації

Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проектування та відомих рішень у галузі продажу сільськогосподарської техніки є важливими складовими успішної діяльності

підприємств, що займаються продажом та обслуговуванням сільськогосподарської техніки.

Одним з найбільш поширених способів обробки та передачі інформації є використання інтернет-технологій та електронних сервісів. Наприклад, інтернет-магазини та електронні платформи з продажу сільськогосподарської техніки дозволяють зручно та швидко здійснювати покупки, отримувати інформацію про техніку та звертатися за консультаціями. Для забезпечення ефективної роботи підприємств, що займаються продажом сільськогосподарської техніки, важливо враховувати принципи побудови об'єкта проектування. Один з найбільш поширених підходів - це використання концепції "Internet of Things" (Інтернет речей), що передбачає взаємодію між різними пристроями та системами за допомогою Інтернету. Наприклад, використання сучасних систем GPS та датчиків дозволяє відстежувати місцезнаходження техніки та збирати дані про її роботу, що дозволяє ефективно планувати обслуговування та ремонт.

У галузі продажу сільськогосподарської техніки відомі рішення, що спрямовані на забезпечення ефективності та підвищення якості продажів. Один з таких рішень - це використання програмних продуктів для автоматизації бізнес-процесів, наприклад, систем управління взаємодією з клієнтами (CRM) та систем управління продажами (SFA). Вони дозволяють підприємствам ефективно керувати клієнтською базою, відстежувати всі етапи продажу, зберігати та аналізувати дані про клієнтів та їх замовлення, а також прогнозувати продажі.

Окрім того, важливим елементом в продажі сільськогосподарської техніки є налагодження співпраці зі спеціалізованими виробниками техніки, що дозволяє забезпечувати клієнтів якісним та надійним обладнанням. Також популярним рішенням є створення власних сервісних центрів, що дозволяє забезпечувати оперативний та якісний сервіс для клієнтів та забезпечувати довготривалий та надійний ремонт обладнання.

1.5 Завдання і мета роботи

Метою роботи є організація корпоративної комп'ютерної мережі з детальним опрацюванням побудови, налаштування та безпеки підприємства ТОВ «Агротек-Інвест». Для вирішення мети в роботі вирішуються наступні завдання:

- здійснити аналіз потреб компанії в мережевому забезпеченні та визначити технічні вимоги до мережі;
- підібрати оптимальну архітектуру мережі відповідно до потреб компанії та належним чином розподілити мережеве обладнання;
- налаштувати мережеве обладнання (маршрутизатори, комутатори, файрволи тощо) та забезпечити його взаємодію зі всіма комп'ютерами та пристроями в мережі;
- запровадити систему захисту мережі та даних від зовнішніх загроз та внутрішніх порушень безпеки;
- забезпечити стійкість мережі до непередбачуваних випадків, таких як збої в електромережі, випадкові пошкодження обладнання тощо;
- провести навчання співробітників компанії з користування та забезпечення безпеки в мережі;
- встановити систему моніторингу мережі для контролю за її станом та проактивного виявлення можливих проблем;
- розробити план регулярного обслуговування та підтримки мережі;
- забезпечити інтеграцію мережі з іншими системами компанії (базами даних, електронною поштою тощо);
- оформити документацію з побудови та налаштування мережі та передати її замовнику;

1.6 Визначення можливих напрямків рішення поставлених задач

При побудові корпоративної комп'ютерної мережі для підприємства ТОВ «Агротек-Інвест», можливі наступні напрямки:

- Вибір технології для локальної мережі: Wi-Fi та Ethernet.

- Переваги бездротової мережі: відсутність кабелів, швидке розширення, низькі витрати.
- Недоліки бездротової мережі: менша швидкість та стабільність порівняно з Ethernet.
- Переваги дротової Ethernet мережі: стійкість до перерв та зовнішніх впливів.
- Раціональний вибір для юридичної компанії: побудова мережі на основі Ethernet.
- Вибір топології мережі: зірка, зручна у керуванні та масштабуванні.
- Забезпечення безпеки: паролі на лініях, використання захищеного протоколу SSH, паролі до привілейованого режиму, впровадження VPN.
- Підмережі в мережі: LAN1-LAN5 для відділів з різними спеціалізаціями.
- Використання технологій: VLAN у LAN5, агрегація каналів (Ethernet Channel) у LAN1.
- Вибір протоколу динамічної маршрутизації: OSPF, сумісний з більшістю обладнання.
- Налаштування технології NAT на прикордонному маршрутизаторі для доступу до Інтернету.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Технічні вимоги до комп'ютерної системи

2.1.1 Вимоги до системи в цілому

2.1.1.1 Вимоги до структури і функціонуванню системи

Структура і функціонування комп'ютерної мережі на підприємстві повинні відповідати певним вимогам для забезпечення ефективності, надійності і безпеки. Основні вимоги до структури і функціонування комп'ютерної мережі на підприємстві включають:

- Мережа повинна бути здатна розширюватися і пристосовуватися до зростання потреб підприємства. Це означає, що мережа повинна бути гнучкою і здатною підтримувати збільшення кількості пристроїв і користувачів без значного погіршення продуктивності.
- Мережа повинна бути стійкою до збоїв і забезпечувати безперебійну роботу. Це може бути досягнуто шляхом використання резервування з'єднань, дублювання мережевого обладнання та реалізації механізмів автоматичного відновлення після збоїв.
- Мережа повинна забезпечувати високу швидкодію передачі даних між пристроями. Це може досягатися за допомогою використання високошвидкісних мережевих технологій, таких як Gigabit Ethernet або 10 Gigabit Ethernet, а також оптимізації мережевої інфраструктури.
- Мережа повинна бути захищеною від несанкціонованого доступу, вірусів і атак зовнішніх загроз. Це можна досягти за допомогою використання мережевих протоколів шифрування, фаєрволів, систем виявлення вторгнень і механізмів аутентифікації користувачів.
- Мережа повинна мати централізовану систему управління, що дозволяє контролювати і керувати всіма пристроями і ресурсами мережі. Це полегшує адміністрування, моніторинг і резервне копіювання мережевої інфраструктури.

- Мережа повинна мати достатню пропускну здатність для задоволення потреб користувачів у передачі даних. Це може бути досягнуто шляхом використання високошвидкісних мережевих пристроїв і оптимізації мережевої інфраструктури.

Загалом, структура і функціонування комп'ютерної мережі на підприємстві повинні бути гнучкими, масштабованими, надійними, швидкодійними, безпечними та забезпечувати ефективне управління всією мережевою інфраструктурою.

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

Для забезпечення взаємодії між підсистемами, необхідно використовувати спільний інформаційний простір та стандартизовані протоколи та формати обміну даними.

Всі програмні компоненти підсистеми повинні працювати в рамках 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.)

Вимоги до характеристик взаємозв'язків створюваної системи з суміжними системами та вимоги до сумісності. Система повинна підтримувати необхідні інтерфейси та протоколи для взаємодії з суміжними системами. Це можуть бути стандартні протоколи передачі даних, веб-сервіси, API або інші специфікації, що забезпечують обмін інформацією.

Система повинна підтримувати спільні формати даних з суміжними системами для ефективного обміну інформацією. Це можуть бути

стандартизовані формати, такі як XML, JSON або CSV, або власні формати, які домовилися використовувати різні системи.

Система повинна мати можливість обмінюватися інформацією з суміжними системами за допомогою різних методів. Це може включати автоматичний обмін даними через веб-сервіси або API, пересилання документів електронною поштою або спілкування за допомогою телефонних дзвінків або інших комунікаційних каналів.

Також забезпечення безпеки системи. Система повинна забезпечувати необхідні заходи безпеки для захисту обміну інформацією з суміжними системами. Це можуть бути механізми шифрування, аутентифікації, авторизації та контролю доступу, щоб гарантувати конфіденційність і цілісність даних.

Загалом, вимоги до взаємозв'язків та сумісності створюваної системи з суміжними системами включають наявність сумісних інтерфейсів, протоколів і форматів даних, різні методи обміну інформацією та забезпечення безпеки.

2.1.1.4 Вимоги до режимів функціонування системи

Компоненти комп’ютерної мережі які потребують безперервного цілодобового режиму експлуатації наведено нижче:

- сервери, які забезпечують централізоване зберігання даних, виконання обчислювальних завдань, надання мережевих послуг. Повинні працювати безперебійно, щоб забезпечити доступність інформації та послуг для користувачів.
- мережеві комутатори та маршрутизатори, пристрої забезпечують пересилання даних в мережі. Вони повинні працювати безперебійно, щоб забезпечити неперервну комунікацію між різними пристроями в мережі.
- системи резервного копіювання, збереження резервних копій даних і налаштувань систем дозволяє відновити мережу у разі випадку втрати даних або аварійного зупинення пристроїв.

Задля цього, використовуються безперебійні джерела живлення, такі як безперебійні джерела живлення (UPS). UPS забезпечують постійне живлення цих компонентів навіть під час відключення основного джерела електроенергії. UPS мають додаткові функції, такі як автоматична стабілізація напруги, фільтрація шуму та захист від перепадів напруги. Вони забезпечують безперебійне живлення пристроїв, що дозволяє уникнути втрати даних, пошкодження обладнання та забезпечити неперервну роботу мережі.

2.1.1.5 Вимоги до діагностування системи

На незадовільну роботу мережі можуть впливати кілька основних причин, такі як пошкодження кабельної системи, несправності активного устаткування, перевантаженість мережевих ресурсів, таких як канали зв'язку і сервери, а також помилки в роботі прикладного програмного забезпечення. Часто ці проблеми можуть приховувати одна одну, тому для точного визначення причини незадовільної роботи необхідно провести комплексну діагностику локальної мережі. Комплексна діагностика включає наступні етапи:

- виявлення дефектів фізичного рівня мережі, таких як проблеми з кабельною системою та електроживленням активного устаткування, а також виявлення шуму від зовнішніх джерел.
- оцінка поточного навантаження мережевого каналу та аналіз його впливу на час реакції прикладного програмного забезпечення.
- аналіз кількості колізій в мережі та ідентифікація факторів, що призводять до їх виникнення.
- оцінка кількості помилок передачі даних на рівні каналу зв'язку та встановлення причин, які призводять до їх виникнення.
- виявлення дефектів архітектури мережі.
- оцінка поточного навантаження сервера та встановлення впливу його завантаження на швидкість відгуку прикладного програмного забезпечення.

- виявлення недоліків у функціональності прикладного програмного забезпечення, що можуть призводити до неефективного використання пропускної здатності сервера та мережі.

Ці пункти описують етапи діагностики системи, які допомагають виявити та вирішити проблеми, що впливають на незадовільну роботу мережі.

2.2.1.6 Перспективи розвитку системи

Перспективи розвитку системи включають наступні аспекти:

- Система може бути розширена шляхом додавання нових модулів, функцій та можливостей. Наприклад, можуть бути впроваджені нові функції зв'язку, підтримка нових протоколів, покращення інтерфейсу користувача та інші додаткові можливості, які підвищать продуктивність та зручність використання системи.
- Перспективи розвитку системи також включають можливість масштабування. Це означає здатність системи ефективно працювати в разі збільшення обсягу даних, кількості користувачів або навантаження. Система може бути розроблена таким чином, щоб бути легко розширюваною або горизонтально масштабованою, дозволяючи забезпечити стабільну та швидку роботу при зростанні обсягів.
- Розвиток системи може бути спрямований на підвищення продуктивності та ефективності роботи. Це може включати оптимізацію алгоритмів, вдосконалення архітектури системи, використання новітніх технологій або обладнання для прискорення обробки даних та забезпечення швидкого доступу до ресурсів.
- Система може бути розроблена з можливістю інтеграції з іншими суміжними системами. Це дозволяє обмінюватися даними, спільно використовувати ресурси та забезпечувати злагоджену роботу між різними системами. Наприклад, система може інтегруватися з

системами управління базами даних, системами електронного документообігу або іншими додатками.

- Розвиток системи також повинен враховувати постійні загрози безпеці. Це може включати вдосконалення системи безпеки, впровадження нових методів аутентифікації та авторизації, шифрування даних, моніторингу та виявлення вторгнень, захисту від вірусів та зловмисного програмного забезпечення.

Ці перспективи розвитку системи допомагають забезпечити її актуальність, адаптивність до змінних потреб користувачів та технологічних вимог, а також забезпечити надійну та ефективну роботу системи у майбутньому.

2.2.1.7 Показники призначення

Основна ціль комп'ютерної мережі полягає у забезпеченні зручного, простого та надійного доступу користувачів до загальних ресурсів мережі та спільного використання цих ресурсів з надійним захистом від несанкціонованого доступу. Додатково, мережа повинна забезпечувати зручні та надійні засоби передачі даних між користувачами. Для забезпечення стабільності та надійності роботи комп'ютерної мережі необхідні тривале безвідмовне функціонування апаратного забезпечення, своєчасна заміна частин системи, а також підтримка та оновлення програмного забезпечення. Інші показники призначення визначаються після проведення перед проектного аналізу.

2.1.2 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню

2.1.2.1 Умови і регламент (режим) експлуатації

Система має працювати безперервно протягом усієї доби, з урахуванням часу, необхідного для технічного обслуговування.

Приміщення, де використовується система, повинні бути забезпечені такими умовами:

- відсутність агресивних середовищ.
- рівень масової концентрації пилу в повітрі не повинен перевищувати 0,75 мг/м³.Електрична складова електромагнітного поля не повинна перевищувати 0,3 Н/м у діапазоні частот від 0,15 до 300,00 МГц.
- напруга живлення мережі повинна бути 220 В, 50 Гц.

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

- ДСТУ "ГОСТ 12.1.004-91 ССБТ. Пожежна безпека. Загальні вимоги".
- ДСТУ "ГОСТ Р 50571.22-2000. Електроустановки будівель.

Приміщення для експлуатації системи повинні відповідати вимогам ГОСТ 15150-69

Нормальні кліматичні умови експлуатації системи включають:

- температура навколишнього повітря: від +15°С до +25°С.
- відносна вологість навколишнього повітря: до 75% при атмосферному тиску від 84 кПа до 107 кПа.

Система повинна функціонувати при наступних кліматичних умовах:

- температура навколишнього повітря: від +10°С до +45°С.
- відносна вологість повітря: від 40% до 80% при температурі +10°С.
- атмосферний тиск від 84 кПа до 107 кПа.
-

2.1.2.2 Вимоги до параметрів мереж енергопостачання

Для мережі енергопостачання існують певні вимоги щодо її параметрів. Основні вимоги включають:

- мережа енергопостачання повинна забезпечувати стабільну напругу згідно з встановленими нормами. Зазвичай використовується напруга 220 В.

- частота живлення повинна відповідати стандартним значенням, в Україні 50 Гц.
- мережа енергопостачання повинна забезпечувати стабільну напругу без значних відхилень або флуктуацій, що можуть негативно впливати на роботу підключених пристроїв.
- мережа енергопостачання повинна мінімізувати наявність гармонік, які можуть виникати у зв'язку з неідеальними умовами живлення. Висока концентрація гармонік може призвести до несправностей і пошкоджень електричного обладнання.
- маршрутизатори, комутатори та сервери потребують безперебійного живлення.
- мережа енергопостачання повинна бути правильно заземлена для забезпечення безпеки та запобігання можливості ураження електричним струмом. Заземлення допомагає відвести струми короткого замикання і захищає обладнання та користувачів від небезпечних ситуацій.

Ці вимоги до параметрів мережі енергопостачання спрямовані на забезпечення стабільного та безперебійного живлення систем та обладнання, що працюють у цій мережі.

2.1.2.3 Вимоги до кількості, кваліфікації обслуговуючого персоналу

Вимоги до кількості та кваліфікації обслуговуючого персоналу варіюються в залежності від розміру, складності та особливостей системи. Основні вимоги включають для нашої системи наведено нижче.

Для нашої комп’ютерної мережі потребується:

- адміністратори мережі які відповідають за налаштування управління та підтримку мережевих пристроїв, вирішення проблем мережі, моніторинг мережі та забезпечення безпеки. Один адміністратор для віддаленої мережі, інший для головного офісу.

- системних адміністратори які відповідають за установку, налаштування та підтримку серверів, управління резервними копіями даних, налаштування безпеки та забезпечення відновлення системи в разі аварії.
- спеціалістіи з технічної підтримки які відповідають за вирішення запитів користувачів, надання допомоги з підключення до мережі, вирішення проблем з підключенням, налаштуванням програмного забезпечення.

Обслуговуючий персонал повинен мати достатні знання, навички та досвід для ефективного управління та обслуговування системи. Це можуть бути спеціалісти з мережевої адміністрації, технічної підтримки, безпеки мережі. Нижче наведено перелік обов'язкових пунктів з кваліфікації та досвіду роботи.

Адміністратор мережі:

- Знання мережевих протоколів, включаючи TCP/IP, DNS, DHCP, VLAN, VPN.
- Досвід установки, налаштування та управління мережевими пристроями, такими як комутатори, маршрутизатори, файрволи.
- Розуміння безпекових аспектів мережі та здатність виявляти та вирішувати проблеми безпеки.
- Вміння налагоджувати, моніторити та підтримувати мережеві сервіси, такі як електронна пошта, файлообмін, відеоконференції .
- Навички управління мережевою інфраструктурою, включаючи розподілені системи, резервне копіювання та відновлення даних.

Системний адміністратор:

- Знання операційних систем, таких як Windows Server, Linux/Unix.
- Досвід установки, конфігурації та управління серверами, включаючи апаратне та програмне забезпечення.
- Вміння керувати користувачами, налаштовувати права доступу та забезпечувати безпеку серверів.
- Розуміння технологій віртуалізації.

- Знання базових протоколів мережі, що дозволяють налаштувати мережеві з'єднання на серверах.
- Досвід установки та налаштування служб домену, баз даних, резервного копіювання та відновлення даних.

Технічна підтримка:

- Вміння працювати з користувачами, виявляти та розв'язувати їх проблеми з комп'ютером та мережею.
- Розуміння базових принципів мережевого з'єднання та налаштування мережевих пристроїв.
- Вміння надавати інструкції користувачам та допомагати їм у вирішенні проблем зі з'єднанням, налаштуванням програмного забезпечення тощо.
- Орієнтація на результат, здатність ефективно працювати в умовах термінових запитів та високого навантаження.

Весь обслуговуючий персонал повинен мати одну з трьох сертифікацій, нижче наведено перелік з них:

- cisco Certified Network Associate (CCNA): Це сертифікація від компанії Cisco, яка підтверджує знання основних концепцій мережі, маршрутизації, комутації та налаштування пристроїв Cisco.
- Certified Information Systems Security Professional (CISSP): Ця сертифікація фокусується на аспектах кібербезпеки та інформаційної безпеки, що може бути важливим для обслуговуючого персоналу, особливо при роботі зі збереженням даних і мережевою безпекою.
- compTIA Network+: Ця сертифікація є відкритою і незалежною, вона підтверджує знання про базові мережеві технології, включаючи мережеві протоколи, мережеву безпеку, управління мережею та інші.

Деякі системи можуть вимагати спеціалізованих навичок, наприклад, з використання певного обладнання, програмного забезпечення або мережевих протоколів. Персонал повинен мати необхідні навички для ефективної роботи з такими елементами системи. Обслуговуючий персонал повинен мати хороші комунікаційні навички для ефективного спілкування з іншими членами

команди, користувачами системи та постачальниками послуг. Персонал повинен бути готовим до дій у випадку екстрених ситуацій, таких як випадки відмови системи, кібератаки або природні катастрофи. Знання процедур відновлення та резервування даних, а також навички кризового управління є важливими для таких ситуацій.

2.1.2.4 Вимоги до складу обслуговуючого персоналу

Оскільки наша комп'ютерна мережа поділена на два офіси, нам потребується більша кількість обслуговуючого персоналу ніж зазвичай, а саме:

- чотири адміністратори мережі, по два на кожен відділ.
- чотири системних адміністратори, по два на кожен відділ.
- двадцять співробітників технічної підтримки, які будуть реагувати на проблему в залежності від офісу та відділу.

2.1.2.5 Вимоги до регламенту обслуговування

Вимоги до регламенту обслуговування системи можуть включати наступні аспекти:

- щотижневе, обслуговування залежно від потреб і характеристик системи.
- Встановити графік у перерві роботи системи, задля проведення обслуговування, налаштування та оновлення програмного забезпечення
- Виконувати процедури та вимоги щодо резервування системи
- Дотримуватися процедур відновлення в разі виникнення ситуацій таких як відмова обладнання, збій програмного забезпечення.
- Забезпечити наявність моніторингових інструментів, задля швидкого виявлення та усунення проблем.
- Забезпечити своєчасне оновлення програмного забезпечення, патчів безпеки, драйверів та фімвару обладнання.

- Обов’язкове ведення повної документації про проведені обслуговування, виконані роботи, виявлені проблеми та їх вирішення.

Ці вимоги допоможуть забезпечити ефективне та надійне обслуговування системи, зменшити ризики відмов та забезпечити безперебійну роботу мережі.

2.2.2 Додаткові вимоги

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

Вимоги до активного обладнання мережі включають в себе:

Функціонування:

надійність: максимальний час відмови менше 5 хвилин на рік.

пропускна здатність: маршрутизатора зі швидкістю передачі даних не менше 10 Гбіт/с.

швидкість обробки: комутатор зі швидкістю переключення пакетів не менше 1 млн пакетів в секунду.

Кількість портів та їх запас:

Кількість портів: 24 порти Ethernet для комутатора.

Запас портів: наявність додаткових портів для майбутнього розширення мережі.

Варіанти встановлення:

Монтаж в стійку (rack-mount): можливість встановлення обладнання в стійку стандартного розміру, наприклад, 19 дюймів.

Настінний монтаж: можливість кріплення обладнання на стіну.

Технічні вимоги:

Вхідна напруга: 100-240 В змінного струму при 50Гц.

2.2.2.2 Вимоги до кабель-каналів, інформаційних та електричних розеток

- Кабель-канали повинні бути достатньо просторими для прокладання всіх необхідних кабелів і забезпечувати їх організоване розташування. Вони повинні мати відповідну пропускну здатність, для нашої мережі це 71.21 Мбіт/с що розраховано нижче. Крім того, кабель-канали повинні забезпечувати захист кабелів від пошкоджень та забезпечувати легкий доступ для обслуговування та розширення мережі.
- Інформаційні розетки повинні бути розташовані зручно для підключення комп'ютерів, принтерів, IP-телефонів та інших мережевих пристроїв. Кількість розеток повинна відповідати потребам мережі, а їх розташування - забезпечувати зручний доступ та мінімальну довжину кабелів.
- Електричні розетки повинні бути відповідно заземлені і забезпечувати стабільне живлення для активного обладнання. Кількість розеток повинна відповідати потребам підключення всіх пристроїв, а їх розташування - забезпечувати зручний доступ та легкість обслуговування.
- Вимоги до кабель-каналів, інформаційних та електричних розеток повинні відповідати відповідним стандартам і рекомендаціям, таким як стандарти TIA/EIA або ISO/IEC для кабельної інфраструктури, а також національні норми та правила щодо електричної безпеки та заземлення.
- Кабель-канали, інформаційні та електричні розетки повинні бути розраховані з урахуванням можливості резервування та майбутнього розширення мережі. Це означає, що слід передбачити достатню кількість запасних портів, кабельних трас та розеток для випадку збільшення потреб у мережевих підключеннях.
- Важливо забезпечити безпеку використання інформаційних та електричних розеток. Розетки повинні бути відповідно заземлені, а кабелі повинні бути правильно заізольовані і марковані для запобігання неправильному підключенню.

Загалом, вимоги до кабель-каналів, інформаційних та електричних розеток включають аспекти безпеки, ефективності, розширюваності та відповідності стандартам, забезпечуючи надійне та безперебійне функціонування мережі.

2.2.2.3 Вимоги до комунікаційного обладнання і його розташування

Для забезпечення належного функціонування та безпеки комунікаційного обладнання рекомендується розміщувати його в спеціальних комутаційних шафах. Основні вимоги, які потрібно дотримувати при встановленні таких шаф, включають:

- для забезпечення належного функціонування, комутаційні шафи повинні бути розташовані в місцях, що захищені від вологи та агресивного середовища. Такі місця можуть включати серверні кімнати або технічні приміщення.
- корпус комутаційної шафи має бути заземленим за допомогою окремого провідника. Це необхідно для забезпечення електричної безпеки та захисту обладнання від статичної електрики та інших електричних перешкод.
- в комутаційних шафах також повинно бути встановлено активне обладнання, таке як маршрутизатори, комутатори, сервери та інше. Це дозволяє керувати мережевими процесами, забезпечувати комутацію даних та надавати необхідні сервіси.
- необхідно забезпечити наявність систем вентиляції та охолодження в комутаційних шафах, щоб забезпечити оптимальні температурні умови для надійної роботи обладнання.
-

2.2.2.4 Вимоги до резервування

Вимоги до резервування комп’ютерної мережі на підприємстві «Агротек-Інвет» включають в себе пункти:

- резервна система повинна мати здатність швидко відновити функціонування основної системи після відмови. Це означає, що перехід до резервного обладнання повинен відбутися безперервно і з мінімальними перервами в роботі.
- резервні системи повинні мати власне незалежне живлення у вигляді UPS систем, щоб забезпечити неперервне живлення обладнання в разі відмови основного джерела енергії.
- резервні системи повинні бути обладнані системами моніторингу, які відстежують стан основного обладнання і автоматично вступають в дію при виявленні відмови.
- Резервні системи повинні періодично тестуватися для перевірки їх працездатності та готовності до використання. Обов’язково розробити план резервування, який визначає процедури перемикання, регулярність тестування та резервування, а також роль персоналу у випадку відмови.

Виконання цих вимог допоможе забезпечити надійне резервування системи і зменшити вплив відмови на безперебійну роботу.

2.2.3 Вимоги до функцій, які виконує КС

Основні вимоги до функцій, які виконує комп'ютерна система (КС) підприємства, включають:

- Забезпечення надійного та швидкого доступу до інформації: КС повинна забезпечувати швидкий та безперебійний доступ до всіх необхідних даних та документів, що стосуються роботи підприємства.
- Зберігання, організація та захист даних: КС повинна мати функції зберігання та організації даних, а також забезпечувати їх захист від несанкціонованого доступу, втрати або пошкодження.
- Автоматизація бізнес-процесів: КС повинна підтримувати автоматизацію різних бізнес-процесів підприємства, включаючи облік, фінанси, виробництво, логістику та інші сфери діяльності.

- Керування проектами: КС може мати функції керування проектами, що дозволяють планувати, виконувати та контролювати проекти підприємства, включаючи розподіл ресурсів, ведення графіків та моніторинг виконання завдань.
- Електронна комунікація та спілкування: КС повинна надавати можливості для ефективної електронної комунікації в межах підприємства, включаючи електронну пошту, внутрішні мережеві чати та інші інструменти спілкування.
- Забезпечення безпеки мережі та даних: КС повинна мати заходи для захисту мережі та даних від зовнішніх загроз, таких як хакерські атаки, віруси, шпигунське програмне забезпечення тощо.
- Аналіз та звітність: КС може мати функції аналізу даних та генерації звітів для підтримки процесів прийняття рішень на підприємстві.
- Підтримка резервного копіювання та відновлення даних: КС повинна мати механізми для регулярного резервного копіювання даних та можливості їх відновлення в разі втрати або пошкодження.
- Масштабованість та розширюваність: КС повинна мати гнучкість для масштабування та розширення в разі зростання потреб підприємства.

Ці вимоги спрямовані на забезпечення ефективності, надійності та безпеки комп'ютерної системи підприємства, а також на підтримку його бізнес-процесів та успішного функціонування.

2.2.4 Вимоги до видів забезпечення КС

2.2.4.1 Вимоги до інформаційного забезпечення

Основні вимоги до інформаційного забезпечення комп'ютерної системи включають:

- конфіденційність: інформація повинна бути захищена від несанкціонованого доступу, забезпечуючи конфіденційність даних.
- цілісність: інформація повинна бути збережена в незмінному стані та захищена від несанкціонованої модифікації або втрати даних.

- доступність: інформація повинна бути доступною для авторизованих користувачів у відповідний час, забезпечуючи безперебійний доступ до необхідних даних.
- резервне копіювання: інформація повинна регулярно резервуватися та зберігатися у безпечному місці, щоб уникнути втрати даних у разі непередбачуваних подій або відмов системи.
- масштабованість: інформаційна система повинна бути масштабованою, здатною розширюватися та вміщати зростаючі потреби в обробці даних.
- забезпечення: інформаційна система повинна бути захищена від шкідливих програм, вірусів, хакерських атак та інших загроз безпеки.
- сумісність: інформаційна система повинна бути сумісною з іншими системами, додатками та протоколами, що використовуються в організації.
- зберігання та архівація: інформація повинна бути збережена та архівована згідно з вимогами законодавства та внутрішніми політиками організації.
- швидкодія: інформаційна система повинна працювати швидко та ефективно, забезпечуючи оперативний доступ до інформації та виконання розрахунків.

2.2.4.2 Вимоги до лінгвістичного забезпечення

Основними мовами взаємодії між системою та користувачем є українська, англійська, німецька та французька мови. Нижче наведено перелік вимог до лінгвістичного забезпечення:

- Створення і використання єдиної комунікаційної мови між користувачами та інтерфейсом системи на всіх рівнях її ієрархії.
- Створення єдиної термінологічної системи, включаючи уніфікацію термінів з однаковим смисловим навантаженням.
- Забезпечення єдиних методів формалізації текстів (даних), нормалізації і редагування даних.

- Розробка зрозумілого, простого та відповідного принципам інтерфейсу користувача, з урахуванням наступних аспектів:
- Однорідність в оформленні інтерфейсу для всіх підсистем.
- Використання ресурсів, таких як довідники та шаблони, для полегшення введення даних.
- Надання підказок та повідомлень про помилки користувачеві під час неправильних дій.
- Наявність довідкової інформації для користувачів щодо роботи з системою.
-

2.3 Розробка апаратної частини комп’ютерної системи

2.3.1 Розробка загальної архітектури мережі підприємства

У компанії "Агротек-Інвест" є дві будівлі з трьома поверхами. Головний офіс розташований на одному поверсі, тоді як віддалений офіс знаходиться на двох поверхах. В таблиці 2.1 наведено загальну кількість та характеристики пристроїв, що використовуються компанією Cisco. На рисунку 2.1 наведено структурна схему комплексу технічних засобів комп’ютерної системи.

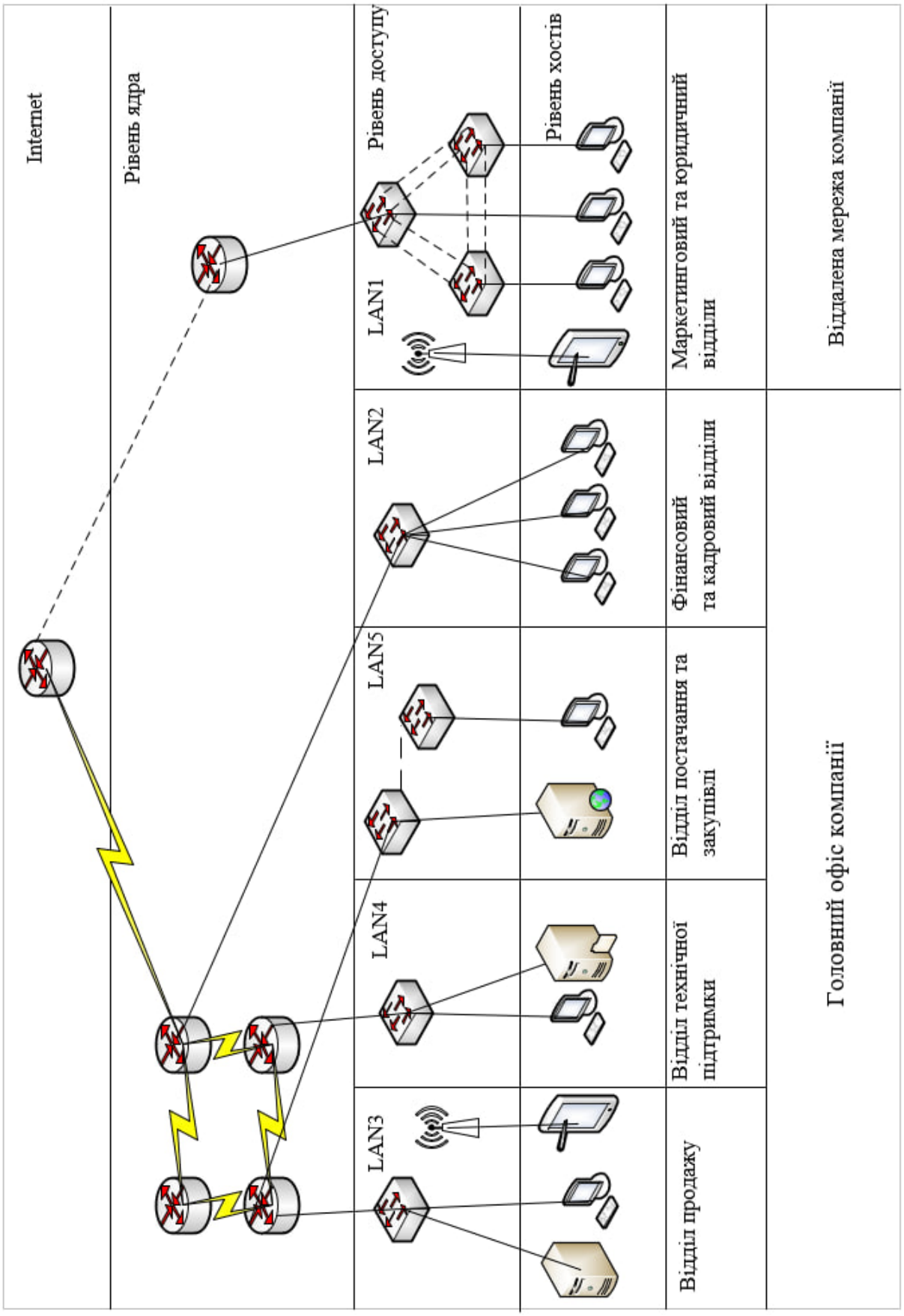


Рисунок 2.1 – Структурна схема комплексу технічних засобів комп’ютерної системи

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

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Маршрутизатор Cisco 2911/K93: 3 порти Gigabit Ethernet 4 слоти EHWIC WAN 2 слоти DSP, 1 слот для плати PVDM Підтримка протоколів: Ethernet, Fast Ethernet, Gigabit Ethernet Підтримка стандартів: IEEE 802.3, IEEE 802.1Q VLAN, IEEE 802.1p QoS, IPv4, IPv6, IPsec, VPN Пам'ять: 512 Мбайт оперативної пам'яті (може бути розширена до 2 Гбайт) Внутрішня флеш-пам'ять: 256 Мбайт	Cisco 2911/K9	од	5	За структурною схемою: Router0-5 Детальні характеристики: https://www.cisco.com/c/en/us/support/routers/2911-integrated-services-router-isr/model.html
2	Комутатор Cisco WS-C2960-24TT-L: 24 порти Ethernet 10/100Base-TX Підтримка стандартів: IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.1Q VLAN, IEEE 802.1p QoS Буферна пам'ять: 64 Мбайт	Cisco WS-C2960-24TT-L	од	15	Детальні характеристики: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html
3	Сервер Cisco UCS C240 M4 12 LFF 2U: До 2-х процесорів Intel Xeon E5-2600 v4 або E5-2600 v3, 3 слоти PCIe 3.0 Контролери мережі: 2 x 1 Гбіт/10 Гбіт Ethernet LOM 4 x USB 3.0, 1 x VGA, 1 x Serial, 2 x RJ-45 Пам'ять: Підтримка до 1.5 ТБ оперативної пам'яті	Cisco UCS C240 M4	од	3	Детальні характеристики: https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c240-m4-rack-server/model.html

Для інтеграції всіх цих пристроїв в єдину мережу і підтримки сайту агентства, необхідні потужні сервери. Один з цих серверів виконує функцію DNS для забезпечення зв'язку. Додатково, наявні ще два сервери: HTTP-сервер, TFTP-сервер і RADIUS-сервер. Для з'єднання між маршрутизаторами використовуються порти типу Serial, тоді як між маршрутизаторами та комп'ютерами використовуються лише порти Fastethernet. Крім того, на комутаторах використовується система VLAN.

Далі ми перейдемо до аналізу системи кабельно-монтажних робіт на прикладі офісу. У цьому випадку компанія займає перший поверх будівлі, структурна схема якої наведена на рисунку 1.6. Ми розробимо план розміщення вузлів комп'ютерної системи та спроектуємо схему розкладки кабельних мереж згідно з рисунком 2.2.

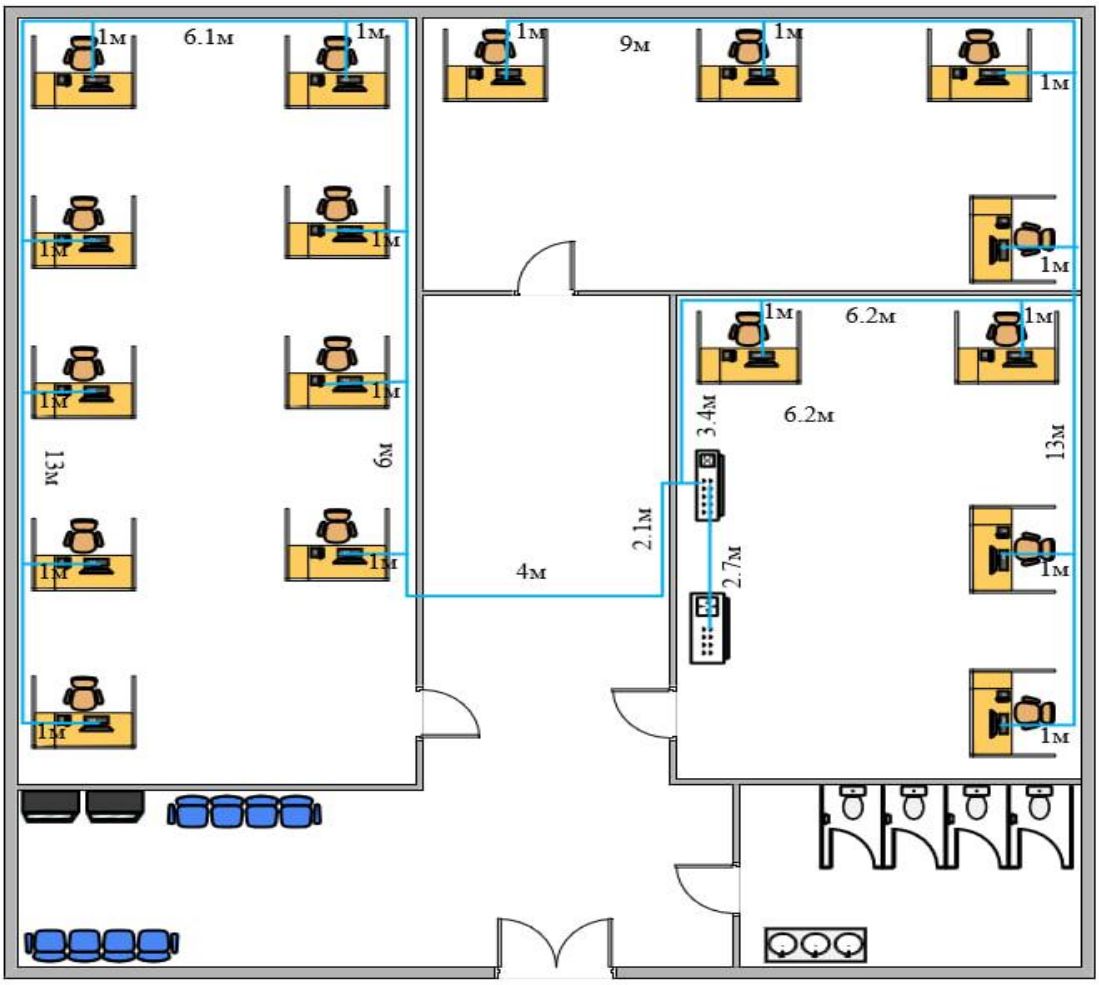


Рисунок 2.2 – Розміщення кабельних мереж віддаленого офісу підприємства «Агротек-Інвест»

Для одноповерхового офісу розроблено схему розміщення кабельних мереж, з обов’язковим використанням кабель-каналів у підлозі. Також використовуються комп’ютерні розетки з виходом RJ-45. Складена специфікація знаходиться в таблиці 2.2.

Таблиця 2.2 – Специфікація структурованої кабельної мережі

Позиція	Найменування і технічна характеристика	Тим, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	**2**	**3**	**4**	**5**	**6**
1	Підлоговий кабельний канал 77х19 Ultra	Schneider Electric	м	90	Відповідно проекту
2	Розетка комп'ютерна подвійна RJ45 UTP KAT.6	Schneider Electric	од	17	Відповідно проекту
3	Розетка із заземленням	Lezard Rain	од	100	Відповідно проекту
4	LAN- кабель U/UTP категорія 6	LSZH	м	105	Відповідно проекту
5	Провід мідний ПВС 3х2,5в	GAL-KAT	м	105	Відповідно проекту
6	Короб пластиковий перфорований 30х50	E.NEXT	м	120	Відповідно проекту

2.4 Специфікація апаратних засобів КС

В офісній мережі було обрано і використано маршрутизатор серії 2911, оскільки він має безліч переваг:

- cisco є одним з провідних виробників мережевого обладнання, а модель 2911/K93 відома своєю надійністю та довговічністю.
- маршрутизатор має достатню пропускну здатність, а саме 180-290 Мбіт/с для обробки трафіку віддаленого офісу.

- маршрутизатор Cisco 2911/K93 підтримує різноманітні функції, такі як маршрутизація, безпека мережі та VPN-з'єднання, що робить його відповідним для потреб офісу.

Також було обрано комутатор Cisco WS-C2960-24TT-L, нижче наведено його переваги:

- модель WS-C2960-24TT-L має 24 порти Ethernet, що дозволяє підключити необхідну кількість пристроїв у віддаленому офісі.
- комутатор підтримує швидкість передачі даних до 1 Гбіт/с на порт, що дозволяє забезпечити ефективну комунікацію у мережі.

Був обраний сервер Cisco UCS C240 M4 12 LFF 2U, який є надійним, захищений та універсальний, декілька його переваг:

- Cisco UCS C240 M4 12 LFF 2U є розширюваним сервером, що дозволяє додавати додаткові жорсткі диски та розширювати обсяг зберігання даних.
- Cisco UCS сервери відомі своєю високою надійністю та захищеністю даних.

Було обрано персональні комп’ютери моделі COBRA Advanced (I11F.8.H1S2.15T.13356), в його комплектуючі входить процесор Intel Core i3-10100F, 8 Гігабайт оперативної пам’яті з можливістю апгрейду, SSD формату M.2 обсягом 480 Гігабайт, відеокарта Nvidia GeForce 1650. Встановлена Windows 11 Home та пакет програм Office.

2.5 Розрахунок інтенсивності трафіку

Найбільша підмережа це LAN1, кількість персональних комп’ютерів в ній – 86.

Пропускна здатність лінії, в яку маршрутизується трафік – 1000 Мбіт/с.

Щоб маршрутизатор працював стабільно повинна виконуватись така вимога, швидкість відправки пакетів більша, за швидкість надходження, розрахуємо це за формулою:

$$\mu_{\text{вих}} = \frac{1000000000}{1500 \times 8} = 83\,000 \frac{\text{пакетів}}{\text{с}}, \quad (2.1)$$

Кожне джерело в середньому виробляє близько 69 кадрів на секунду.

Визначимо максимальну кількість пристроїв, котрі можуть бути під'єднані до мережі:

$$N = \frac{83000}{69} = 1202 \text{ пристрої}, \quad (2.2)$$

Значення 1202 підходить для нашої підмережі на 86 персональних комп'ютерів та залишає можливість масштабування та розвитку мережі.

Кожен персональний комп'ютер надсилає потік 69 кадрів/с.

За допомогою формули визначаємо інтенсивність вихідного трафіку:

$$\lambda = 86 * 69 = 5934 \frac{\text{пакетів}}{\text{с}}, \quad (2.3)$$

Розрахунок затримки відбувається таким чином:

$$\rho = \frac{\lambda}{\mu_{\text{вих}}} = \frac{5934}{83000} = 0.07, \quad (2.4)$$

Розрахунок зайнятості маршрутизатора: 68380

$$\frac{\rho}{1-\rho} = \frac{0.07}{1-0.07} = 0.075, \quad (2.5)$$

Розрахунок середньої затримки кадру:

$$T = \frac{1}{\mu - \lambda} = \frac{1}{83000 - 14620} = 12.9 \text{ мкс}, \quad (2.6)$$

Розрахунок середньої довжини черги:

$$L_{\text{чер}} = \frac{\rho^2}{1-\rho} = \frac{0.07^2}{1-0.07} = 0.05, \quad (2.7)$$

Розрахунок середнього часу перебування пакета в черзі:

$$T_{\text{очікування}} = \frac{L_{\text{чер}}}{\lambda} = \frac{0.05}{5934} = 8.4 \text{ мкс}, \quad (2.8)$$

Розрахуємо пропускну здатність каналу за допомогою формули:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l}, \quad (2.9)$$

Отримаємо такий результат:

$$b = \lambda \times l = 5934 \times 1500 \times 8 = 71\,208\,000 \text{ біт/с } = 71.21 \text{ Мбіт/с}$$

71.21 Мбіт/с повністю задовольняє пропускну здатність каналу в 1000 Мбіт/с.

Висновки: Результати показують, що структура комп'ютерної системи (КС) та вибрана мережева архітектура корпоративної мережі повністю відповідають вимогам поставленого завдання. Аналіз трафіку мережі свідчить про те, що пропускна здатність каналу на рівні 1000Мбіт/с задовольняє встановлені вимоги.

3 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА РОЗРАХУНОК ЇЇ НАЛАШТУВАНЬ

3.1 Розрахунок адресації мережі

У таблиці 3.1 вказано простір адрес, який буде використовуватися для розрахунку адресації та кількість вузлів у підмережах компанії.

Таблиця 3.1 – Простір адрес компанії

№	Блок адрес	LAN1	LAN2	LAN3	LAN4	LAN5
14	10.23.68.0/22	86	46	79	20	81

LAN1 відповідають маркетинговий та юридичний відділи.

LAN2 відповідають фінансовий та кадровий відділи.

LAN3 відповідає відділ продажу.

LAN4 відповідає відділ технічної підтримки.

LAN5 відповідає відділ постачання та закупівлі.

Для розрахунку адресації в мережі буде використовуватися метод VLSM. VLSM є методом розбиття IP-мережі на підмережі з різною довжиною префіксу (маски підмережі), що дозволяє ефективно використовувати IP-адреси та забезпечує більш гнучку конфігурацію мереж. Розмір підмереж, розрахованих методом VLSM, обмежується ступенем двійки, але варто враховувати, що кількість адрес, які доступні для привласнення пристроям, завжди на 2 менша через наявність адреси мережі та широкомовної адреси.

Розрахунок підмереж потрібно проводити у порядку зменшення кількості вузлів. Тому розрахунок почнемо з найбільшої підмережі підприємства – LAN1.

Для зручності розрахунку переведемо частину вихідної адреси у двійковий вигляд. Для першої підмережі виділимо блок у 128-2 адрес, для цього відрахуємо 7 біт з правого боку адреси.

10.23.01000100.0 0000000

Переведемо адресу до звичного вигляду та отримаємо адресу мережі – 10.23.68.0/25. Далі заповнимо біти з правого боку від лінії одиницями та

отримаємо широкомовну адресу – 10.23.68.127/25. Виходячи з розрахунку маємо простір адрес, доступних для вузлів: 10.23.68.1 – 10.23.68.126.

Далі проведемо розрахунок для підмережі LAN5, перед цим додавши один біт до мережевої частини адреси. Для даної підмережі виділимо блок у 128-2 адреси та відрахуємо 7 біт з правого боку.

10.23.01000100.1 0000000

Переведемо адресу до звичного вигляду та отримаємо адресу мережі – 10.23.68.128/25. Далі заповнимо біти з правого боку від лінії одиницями та отримаємо широкомовну адресу – 10.23.68.255/25. Виходячи з розрахунку маємо простір адрес, доступних для вузлів: 10.23.68.129 – 10.23.68.254.

Далі проведемо розрахунок для підмережі LAN3, перед цим додавши один біт до мережевої частини адреси. Для даної підмережі виділимо блок у 128-2 адреси та відрахуємо 7 біт з правого боку.

10.23.01000101.0 0000000

Переведемо адресу до звичного вигляду та отримаємо адресу мережі – 10.23.69.0/25. Далі заповнимо біти з правого боку від лінії одиницями та отримаємо широкомовну адресу – 10.23.69.127/25. Виходячи з розрахунку маємо простір адрес, доступних для вузлів: 10.23.69.1 – 10.23.69.126.

Далі проведемо розрахунок для підмережі LAN2, перед цим додавши один біт до мережевої частини адреси. Для даної підмережі виділимо блок у 64-2 адреси та відрахуємо 6 біт з правого боку.

10.23.01000101.10 000000

Переведемо адресу до звичного вигляду та отримаємо адресу мережі – 10.23.69.128/26. Далі заповнимо біти з правого боку від лінії одиницями та отримаємо широкомовну адресу – 10.23.69.191/26. Виходячи з розрахунку маємо простір адрес, доступних для вузлів: 10.23.69.129 – 10.23.69.190.

Далі проведемо розрахунок для підмережі LAN4, перед цим додавши один біт до мережевої частини адреси. Для даної підмережі виділимо блок у 32-2 адреси та відрахуємо 5 біт з правого боку.

10.23.01000101.110 00000

Переведемо адресу до звичного вигляду та отримаємо адресу мережі – 10.23.69.192/27. Далі заповнимо біти з правого боку від лінії одиницями та отримаємо широкомовну адресу – 10.23.69.223/27. Виходячи з розрахунку маємо простір адрес, доступних для вузлів: 10.23.69.193 – 10.23.69.222.

Розрахована адресація мережі наведена у таблиці 3.2.

Таблиця 3.2 – Схема адресації мережі

Назва мережі	Кількість вузлів	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
LAN1	86	128	10.23.68.0	/25	10.23.68.1 - 10.23.68.126	10.23.68.127
LAN2	46	64	10.23.69.128	/26	10.23.69.129 - 10.23.69.190	10.23.69.191
LAN3	79	128	10.23.69.0	/25	10.23.69.1 - 10.23.69.126	10.23.69.127
LAN4	20	32	10.23.69.192	/27	10.23.69.193 - 10.23.69.222	10.23.69.223
LAN5	81	128	10.23.68.128	/25	10.23.68.129 - 10.23.68.254	10.23.68.255

Щоб розрахувати простір адрес для каналів, які використовуються для зв’язку між маршрутизаторами використаємо блок адрес 10.1.14.0/24. Проведемо розрахунок за методом VLSM. Результати розрахунку наведено у таблиці 3.3.

Таблиця 3.3 – Схема адресації каналів між маршрутизаторами

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN1	2	2	10.1.14.0	/30	10.1.14.1 - 10.1.14.2	10.1.14.3
WAN2	2	2	10.1.14.4	/30	10.1.14.5 - 10.1.14.6	10.1.14.7

Продовження таблиці 3.3

Підмережа	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
WAN3	2	2	10.1.14.8	/30	10.1.14.9 - 10.1.14.10	10.1.14.11
WAN4	2	2	10.1.14.12	/30	10.1.14.13 - 10.1.14.14	10.1.14.15

3.2 Розрахунок адресації пристроїв

Згідно розрахованої адресації привласнимо адреси інтерфейсам маршрутизаторів. Адреси інтерфейсів наведено у таблиці 3.4.

Таблиця 3.4 – Схема адресації маршрутизаторів

Пристрій	Інтерфейс	IP-адреса	Маска
Toloshnyi_Router_0	Gig0/0	64.100.13.2	255.255.255.252
	Gig0/1	10.23.68.1	255.255.255.128
Toloshnyi_Router_1	Gig0/0	10.23.69.193	255.255.255.224
	Se0/3/0	10.1.14.2	255.255.255.252
	Se0/3/1	10.1.14.13	255.255.255.252
Toloshnyi_Router_2	Gig0/1	10.23.69.1	255.255.255.128
	Se0/3/1	10.1.14.10	255.255.255.252
	Se0/3/0	10.1.14.14	255.255.255.252
	Gig0/0.24	10.23.68.129	255.255.255.224
	Gig0/0.34	10.23.68.161	255.255.255.224
	Gig0/0.44	10.23.68.193	255.255.255.224
	Gig0/0.99	10.23.68.225 255	255.255.255.240

Продовження таблиці 3.4

Пристрій	Інтерфейс	IP-адреса	Маска
Toloshnyi_Router_3	Gig0/0	10.23.69.129	255.255.255.192
	Se0/3/0	209.165.202.2	255.255.255.252
	Se0/3/1	10.1.14.1	255.255.255.252
	Se0/2/0	10.1.14.5	255.255.255.252
Toloshnyi_Router_4	Se0/3/0	10.1.14.9	255.255.255.252
	Se0/3/1	10.1.14.6	255.255.255.252
Toloshnyi_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

Привласнимо адреси SVI-інтерфейсам комутаторів в підмережах. Адреси інтерфейсів наведено у таблиці 3.5.

Таблиця 3.5 – IP-адреси комутаторів у підмережах.

Підмережа	Пристрій	IP-адреса SVI інтерфейсу	Маска підмережі	Адреса шлюзу
LAN1	Toloshnyi_Switch_4	10.23.68.2	255.255.255.128	10.23.648.1
	Toloshnyi_Switch_5	10.23.68.3	255.255.255.128	10.23.68.1
	Toloshnyi_Switch_6	10.23.68.4	255.255.255.128	10.23.68.1
LAN2	Toloshnyi_Switch_7	10.23.69.130	255.255.255.192	10.23.69.129
LAN3	Toloshnyi_Switch_1	10.23.69.2	255.255.255.128	10.23.69.1
LAN4	Toloshnyi_Switch_0	10.23.69.194	255.255.255.224	10.23.69.193
LAN5	Toloshnyi_Switch_2	10.23.68.226	255.255.255.240	10.23.68.225
	Toloshnyi_Switch_3	10.23.68.227	255.255.255.240	10.23.68.225

3.3 Налаштування моделі комп’ютерної системи

Нижче наведено розроблену логічну топологію мережі компанії. На топології наведено адресацію підмереж, з’єднання пристроїв в них та з’єднання між маршрутизаторами.

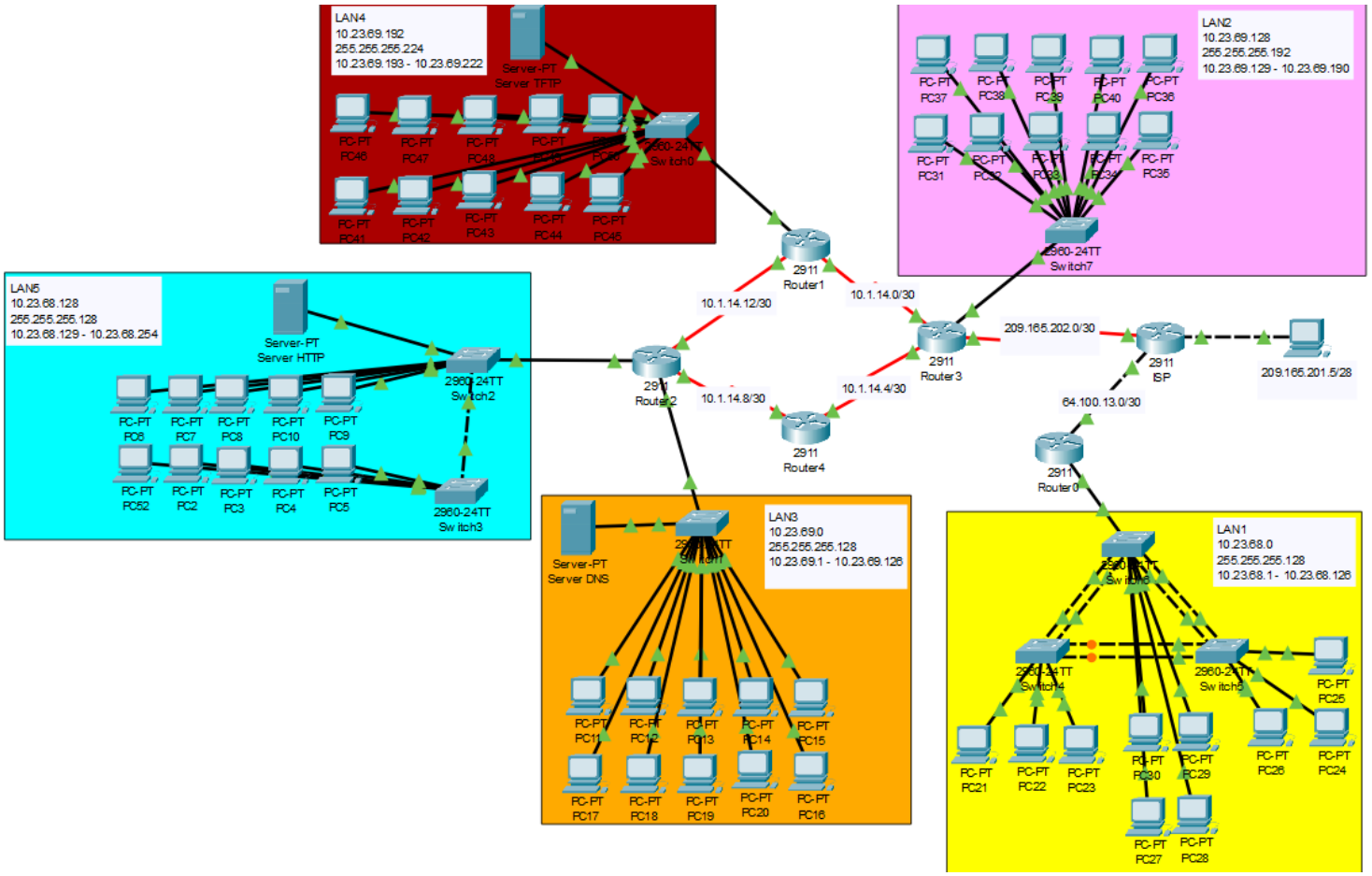


Рисунок 3.1 – Логічна топологія мережі компанії

3.4 Налаштування та перевірка роботи комп’ютерної системи

3.4.1 Базове налаштування конфігурації пристроїв

На комутаторах та маршрутизаторах мережі необхідно виконати базове налаштування конфігурації. Для цього необхідно привласнити ім’я кожному пристрою, встановити усі необхідні паролі, налаштувати банер MOTD, налаштувати роботу ssh та створити користувача з доменним ім’ям.

//Вмикаємо привілейований режим та режим конфігурації

enable

```
Conf t
//Встановлюємо ім’я пристрою
Hostname Toloshnyi_Router_0
//Встановлюємо паролі для ліній vty та console
Line console 0
Password cisco
Login
Line vty 0 15
Password cisco
Login
//Встановлюємо пароль до привілейованого режиму
Enable secret class
//Шифруємо усі паролі
Service password-encryption
//Встановлюємо банер MOTD
Banner motd ‘Toloshnyi_Router_0’
//Створюємо домене ім’я, ключ rsa та користувача з паролем
ip domain-name Toloshnyi_Router_0
Crypto key generate rsa
1024
Username 123191_Toloshnyi password admincisco
//Вмикаємо використання протоколу ssh
Line vty 0 15
Transport input ssh
Login local
```

Під час конфігурування комутаторів у мережі LAN1 необхідно налаштувати агрегацію каналів за технологією EthernetChannel. Приклад команд для налаштування наведено нижче.

```
//Вмикаємо привілейований режим та режим конфігурації\
en
```

```
conf t
//Обираємо діапазон інтерфейсів та виконуємо їх об’єднання
interface range fa0/1-2
channel-group 1 mode active
//Налштовуємо об’єднані порти на режим роботи trunk та дозволяємо проходження трафіку з усіх vlan
interface port-channel 1
switchport mode trunk
switchport trunk allowed vlan all
//Аналогічні налаштування для другого діапазону інтерфейсів
interface range fa0/3-4
channel-group 2 mode active
interface port-channel 2
switchport mode trunk
switchport trunk allowed vlan all
```

3.4.2 Налаштування маршрутизаторів

У якості протоколу динамічної маршрутизації у мережі обрано протокол OSPF. Даний протокол забезпечить маршрутизацію у мережі шляхом поширення власних мереж, вказаних під час налаштування.

Приклад налаштування протоколу наведено нижче.

```
//Вмикаємо роботу протоколу
router ospf 1
//Вимикаємо надсилання пакетів з оновленнями на інтерфейс локальної мережі
passive-interface GigabitEthernet0/0
//Оголошуємо мережі для розповсюдження
network 10.23.69.128 0.0.0.63 area 0
network 10.1.14.0 0.0.0.3 area 0
network 10.1.14.4 0.0.0.3 area 0
```

Після цього на пограничному маршрутизаторі мережі створимо статичні машрути, щоб забезпечити зв’язок з мережою провайдера.

//Оголошуємо статичний маршрут за замовчуванням. Адреса наступного переходу – інтерфейс машрутизатора провайдера.

ip route 0.0.0.0 0.0.0.0 209.165.202.1

//Оголошуємо статичний машрут, щоб забезпечити зв’язок з мережою провайдера з локальної мережі

ip route 209.165.201.0 255.255.255.240 209.165.202.1

Далі на DCE-інтерфейсах необхідно встановити частоту 128000 і встановити пропускну здатність на 128. Приклад налаштування наведено нижче.

//Обираємо інтерфейс

interface Serial0/3/0

//Встановлюємо пропускну здатність на 128

bandwidth 128 //налаштування пропускної спроможності

//Встановлюємо частоту на рівень 128000

clock rate 128000 //налштування частоти

Після цього увімкнемо налаштування служби AAA на маршрутизаторах мережі компанії. Вона повинна реалізовувати аутентифікацію користувачів на основі протоколу Radius. У разі відсутності з’єднання з Radius-сервером необхідно налаштувати використання локальної бази користувачів.

Приклад налаштування наведено нижче.

//Створюємо нову AAA-модель та призначаємо адресу серверу Radius, порт TCP/UDP та ключове слово

aaa new-model

radius-server host 10.23.69.24 auth-port 1645 key radius123

//Налаштовуємо аутентифікацію для доступу до Console

aaa authentication login CONSOLE group radius local

line console 0

```
login authentication CONSOLE
//Налаштовуємо використання локальної бази даних користувачів
aaa authentication login default local
username 123191_Toloshnyi password admin123
line vty 0 15
login authentication default
```

Після цього налаштуємо роботу служби AAA на сервері. Налаштування наведено на рисунку 3.2.

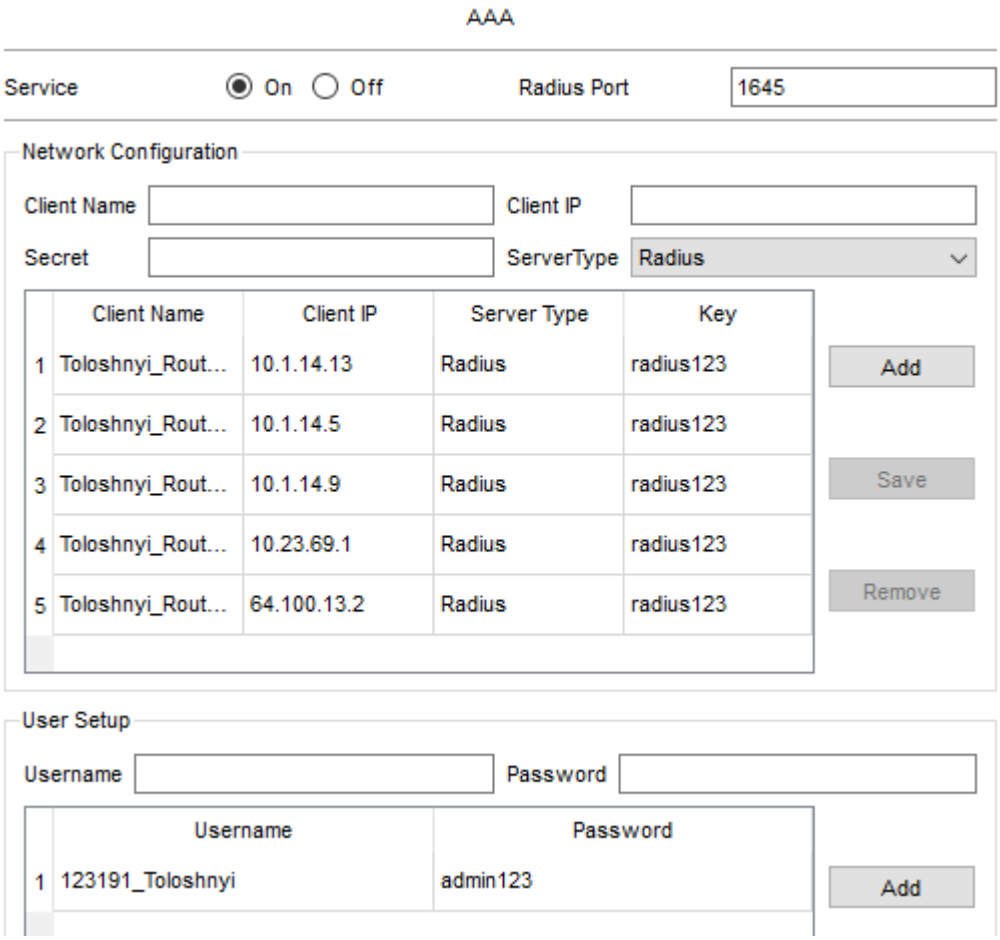


Рисунок 3.2 – Налаштування служби AAA на сервері

3.4.3 Налаштування роботи Інтернет

Щоб забезпечити мережу доступом до інтернету необхідно виконати налаштування технології динамічного NAT на пограничному машрутизаторі мережі. Дана техологія дозволить перетворювати локальні адреси на глобальні, які будуть обиратися з заданого пулу адрес: з 209.165.200.5 по 209.165.200.30.

Налаштування динамічного NAT вимагає створення ACL-списку, в якому буде вказано трафік, якому дозволено брати участь у трансляції.

Створення ACL-списку наведено нижче.

```
//Створюємо новий список з ім’ям NAT14
ip access-list extended NAT14
```

//Блокуємо для транслювання трафік, який проходить з мереж головного офісу до мережі віддаленого, так як для даного трафіку буде виконано налаштування VPN.

deny ip 10.23.69.192 0.0.0.31 10.23.68.0 0.0.0.127

deny ip 10.23.68.128 0.0.0.127 10.23.68.0 0.0.0.127

deny ip 10.23.69.0 0.0.0.127 10.23.68.0 0.0.0.127

deny ip 10.23.69.128 0.0.0.63 10.23.68.0 0.0.0.127

deny ip 10.1.14.0 0.0.0.3 10.23.68.0 0.0.0.127

//Дозволяємо для трансляції увесь інший трафік з підмереж головного офісу

permit ip 10.23.69.192 0.0.0.31 any

permit ip 10.23.68.128 0.0.0.127 any

permit ip 10.23.69.0 0.0.0.127 any

permit ip 10.23.69.128 0.0.0.63 any

permit ip 10.23.14.0 0.0.0.3 any

Після створення ACL-списку налаштуємо NAT-пул глобальних адрес. Приклад налаштування наведено нижче.

//Створюємо пул з ім’ям Internet та привласнюємо йому діапазон адрес

ip nat pool Internet 209.165.200.5 209.165.200.30 netmask 255.255.255.224

//Вмикаємо роботу NAT, вказавши в якості джерела трансляції створений ACL-список

ip nat inside source list NAT14 pool Internet

Після цього необхідно вказати внутрішній та зовнішній інтерфейси трансляції.

interface Serial0/30

ip nat outside

interface Serial0/3/1

ip nat inside

Аналогічні налаштування проведено на маршрутизаторі мережі віддаленого офісу, щоб забезпечити їй доступ в інтернет.

Після цього необхідно виконати налаштування HTTP-сервера таким чином, щоб щоб на вузлах при вводі в рядку браузера http://123.dnipro.ua (http://209.165.200.4) відкривався веб-сайт з відомостями про тему та завдання на кваліфікаційну роботу.

Для того, щоб привласнити HTTP-серверу публічну адресу необхідно створити статичну NAT трансляцію на пограничному маршрутизаторі головного офісу та створити для публічної адреси відповідне доменне ім’я на DNS-сервері.

Налаштування статичної трансляції наведено нижче.

ip nat inside source static 10.23.68.184 209.165.200.4

На рисунку 3.3 наведено налаштування доменного імені на DNS-сервері.

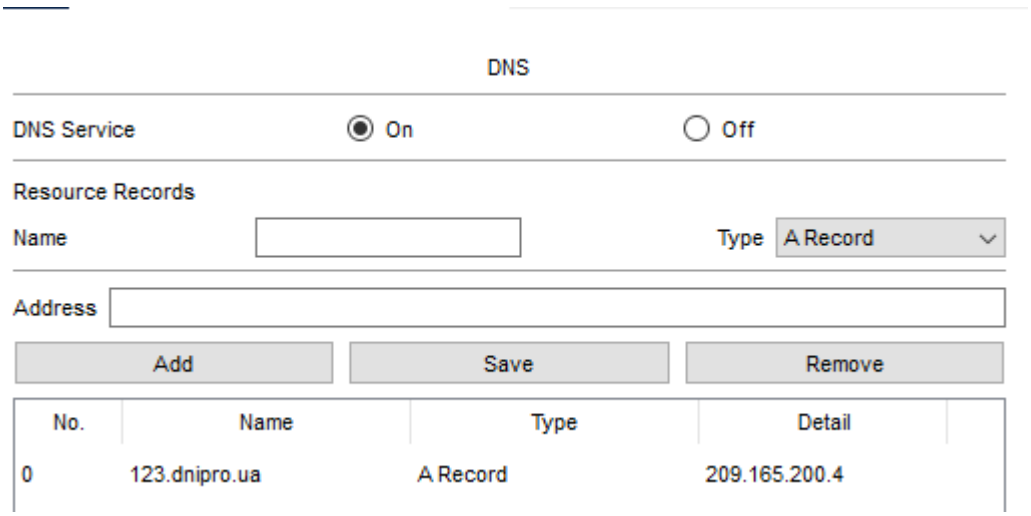


Рисунок 3.3 – Налаштування доменного імені

Для забезпечення зв’язку між мережами головного та віддаленого офісу необхідно налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec. Для роботи VPN необхідно створити ACL-список, в якому буде вказано трафік, який проходитиме через захищений канал. Налаштування ACL-списку наведено нижче.

//Створюємо новий список з ім’ям VPN14

ip access-list extended VPN14

//Вводимо перелік дозволеного трафіку, який буде проходити через захищений канал

permit ip 10.23.69.192 0.0.0.31 10.23.68.0 0.0.0.127

permit ip 10.23.68.128 0.0.0.127 10.23.68.0 0.0.0.127

permit ip 10.23.69.0 0.0.0.127 10.23.68.0 0.0.0.127

permit ip 10.23.69.128 0.0.0.63 10.23.68.0 0.0.0.127

permit ip 10.1.14.0 0.0.0.3 10.23.68.0 0.0.0.127

Після створення ACL-списку потрібно виконати конфігурування VPN на машрутизаторах мережі.

//Вмикаємо модуль безпеки під назвою securityk9

license boot module c2900 technology-package securityk9

//Створюємо нову політику isakmp

crypto isakmp policy 10

//Виконуємо налаштування політики, обравши алгоритм шифрування, хеш та тип аутентифікації, вказуємо групу

encr 3des

hash md5

authentication pre-share

group 2

//Створюємо ключ «cisco», вказавши адресу зовнішнього інтерфейсу машрутизатора віддаленої мережі

crypto isakmp key cisco address 64.100.13.2

//Створюємо набір криптографічних перетворень «TS»

crypto ipsec transform-set TS esp-3des esp-md5-hmac

//Створюємо крипографічне зіставлення «MAP»

crypto map MAP 10 ipsec-isakmp

//Налаштовуємо криптографічне зіставлення, вказавши адресу зовнішнього інтерфейсу машрутизатора віддаленої мережі та набір крипто-перетворень, вказуємо

set peer 64.100.13.2

```
set transform-set TS
match address VPN14
//Вмикаємо роботу криптографічного зіставлення на зовнішньому інтерфейсі машрутизатора
interface Serial0/3/0
crypto map MAP
```

Аналогічно до цього виконується конфігурація пограничного маршрутизатора у мережі віддаленого офісу.

3.5 Захист інформації в комп’ютерній системі від несанкціонованого доступу

3.5.1 Розробка методів для захисту інформації в комп’ютерній системі

Захист інформації в комп'ютерних системах є важливим аспектом забезпечення конфіденційності, цілісності та доступності даних. Існує ряд методів і практик, які можна використовувати для захисту інформації.

Аутентифікація гарантує встановлення ідентичності користувачів перед наданням доступу до системи. Це може включати використання паролів, біометричних даних або двофакторної аутентифікації.

Авторизація контролює доступ до різних ресурсів і функцій системи. Вона визначає рівні привілеї для користувачів, обмежуючи їх дії в системі.

Шифрування перетворює звичайний текст в зашифрований вигляд, непридатний для розуміння без спеціального ключа. Це забезпечує конфіденційність даних.

Фаєрволи контролюють мережевий трафік, що входить і виходить з комп'ютерної системи, блокуючи небажані з'єднання і захищаючи систему від зовнішніх атак.

Встановлення антивірусного програмного забезпечення дозволяє виявляти і нейтралізувати шкідливе програмне забезпечення, забезпечуючи безпеку системи.

Регулярне оновлення програмного забезпечення, включаючи операційну систему і додаткові програми, допомагає виправляти виявлені уразливості і запобігати атакам на систему.

Забезпечення фізичної безпеки включає захист обладнання комп'ютерної системи від несанкціонованого доступу за допомогою контролю доступу, замків, систем відеоспостереження та інших заходів.

Ці методи використовуються в комплексі, і їх комбінація сприяє забезпеченню безпеки інформації в комп'ютерних системах.

3.5.2 Налаштування віртуальних мереж VLAN

За вимогами замовника необхідно виконати розбиття підмережі LAN5 на три віртуальні локальні мережі за допомогою технології VLAN. У таблиці 3.6 наведено номери та імена віртуальних мереж, які необхідно створити.

Таблиця 3.6 – Віртуальні локальні мережі

Номер VLAN	Ім’я VLAN	Примітка
24	VLAN24	Продаж нової техніки
34	VLAN34	Продаж вживаної техніки
44	VLAN44	Продаж запчастин
1	Default	Не використовується
99	Management	Для керування пристроями
100	Native	Власна

Для кожної підмережі VLAN необхідно виконати розрахунок адресації за методом VLSM. Результати розрахунку наведені у таблиці 3.7.

Таблиця 3.7 – Схема адресації VLAN

Назва підмережі	Розмір	Виділений розмір	Адреса	Маска	Діапазон доступних адрес	Широкомовна адреса
VLAN24	30+2	32	10.23.68.128	/27	10.23.68.129 – 10.23.68.158	10.23.68.159
VLAN34	30+2	32	10.23.68.160	/27	10.23.68.161 – 10.23.68.190	10.23.68.191
VLAN44	30+2	32	10.23.68.192	/27	10.23.68.193 – 10.23.68.222	10.23.68.223
Management	14+2	16	10.23.68.224	/28	10.23.68.225 - 10.23.68.238	10.23.68.239
Native	6+2	8	10.23.68.240	/29	10.23.68.241 - 10.23.68.246	10.23.68.247

На кожному комутаторі необхідно розподілити порти для відповідних VLAN. Результат розподілу наведено у таблиці 3.8.

Таблиця 3.8 – Розподіл портів комутатора для під відповідні VLAN

Назва підмережі	VLAN	Розподіл портів
VLAN23	23	Fa0/4-Fa0/8
VLAN33	33	Fa0/10-Fa0/14
VLAN43	43	Fa0/15-Fa0/20

Після цього потрібно створити sub-інтерфейси на маршрутизаторі підмережі, призначити їм адреси та встановити адреси на SVI-інтерфейси комутаторів.

Таблиця 3.9 – Адресація портів пристроїв

Пристрій	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN
Toloshnyi_Switch_2	SVI	10.23.68.226	/28	10.23.68.225	99
Toloshnyi_Switch_3	SVI	10.23.68.227	/28	10.23.68.225	99
Toloshnyi_Router_2	G0/0.24	10.23.68.129	/27	-	24
	G0/0.34	10.23.68.161	/27	-	34
	G0/0.44	10.23.68.193	/27	-	44
	G0/0.99	10.23.68.225	/28	-	99

Для призначення адрес sub-інтерфейсам маршрутизаторів необхідно виконати наступні дії.

//Створюємо новий sub-інтерфейс та вмикаємо на ньому інкапсуляцію, призначаємо адресу

interface GigabitEthernet0/0.23

encapsulation dot1Q 23

ip address 10.23.65.129 255.255.255.224

//Проводимо аналогічні налаштування

interface GigabitEthernet0/0.33

encapsulation dot1Q 33

ip address 10.23.65.161 255.255.255.224

//Проводимо аналогічні налаштування

interface GigabitEthernet0/0.43

encapsulation dot1Q 43

ip address 10.23.65.193 255.255.255.224

//Проводимо аналогічні налаштування

interface GigabitEthernet0/0.99

encapsulation dot1Q 99

ip address 10.23.65.225 255.255.255.240

Після призначення адрес усім інтерфейсам необхідно виконати розподілення інтерфейсів комутаторів між VLAN за даними з таблиці 3.8. Приклад налаштування наведено нижче.

```
//Перехід в режим конфігурації та вибір діапазону інтерфейсів
Conf t
int range fa0/4-8
//Налаштування інтерфейсів на режим доступу та вибір VLAN за номером
switchport mode access
switchport access vlan 24
//Аналогічні налаштування
int range fa0/10-14
switchport mode access
switchport access vlan 34
//Аналогічні налаштування
int range fa0/15-20
switchport mode access
switchport access vlan 44
//Налаштування гігабітних інтерфейсів на режим роботи trunk
int range Gig0/1-2
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 46,26,36,99-100
```

3.5.3 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

У кожній віртуальній локальній мережі необхідно реалізувати динамічне призначення IP-адрес за допомогою протоколу DHCP, робота якого налаштовується на маршрутизаторі, до якого під’єднані підмережі.

Повне налаштування DHCP на машрутизаторі наведено нижче.

```
//Виключаємо з роздачі адрес перші 10 адрес кожної підмережі та адресу серверу
ip dhcp excluded-address 10.23.68.129 10.23.68.138
ip dhcp excluded-address 10.23.68.161 10.23.68.170
ip dhcp excluded-address 10.23.68.193 10.23.68.202
ip dhcp excluded-address 10.23.69.24
//Створюємо новий DHCP-пул, призначаємо йому адресу мережі для динамічного розподілення адрес, адресу шлюзу та DNS-серверу.
ip dhcp pool VLAN-34
 network 10.23.68.160 255.255.255.224
 default-router 10.23.68.161
 dns-server 10.23.69.24
//Проводимо аналогічні налаштування
ip dhcp pool VLAN-24
 network 10.23.68.128 255.255.255.224
 default-router 10.23.68.129
 dns-server 10.23.69.24

//Проводимо аналогічні налаштування
ip dhcp pool VLAN-44
 network 10.23.68.192 255.255.255.224
 default-router 10.23.68.193
 dns-server 10.23.69.24
```

На інтерфейсах FastEthernet, до яких під’єднано сервери компанії необхідно виконати налаштування безпеки портів. Умови наступні: тільки двом унікальним пристроям надається доступ до порту, MAC-адреса пристрою розпізнається динамічно і додається в поточну конфігурацію.

```
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
```

switchport port-security violation restrict

3.5 Перевірка роботи налаштувань мережі

Наступним етапом роботи виконаємо перевірку усіх налаштувань комп’ютерної мережі.

Для перевірки роботи маршрутизації за протоколом OSPF переглянемо таблицю маршрутизації одного з маршрутизаторів. Літерою O відмічені мережі, про які маршрутизатор отримав інформацію за допомогою OSPF (рисунок 3.4).

```
Toloshnyi_Router_2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 18 subnets, 6 masks
O       10.1.14.0/30 [110/1562] via 10.1.14.13, 00:14:34, Serial0/3/0
O       10.1.14.4/30 [110/1562] via 10.1.14.9, 00:14:34, Serial0/3/1
C       10.1.14.8/30 is directly connected, Serial0/3/1
L       10.1.14.10/32 is directly connected, Serial0/3/1
C       10.1.14.12/30 is directly connected, Serial0/3/0
L       10.1.14.14/32 is directly connected, Serial0/3/0
C       10.23.68.128/27 is directly connected, GigabitEthernet0/0.24
L       10.23.68.129/32 is directly connected, GigabitEthernet0/0.24
C       10.23.68.160/27 is directly connected, GigabitEthernet0/0.34
L       10.23.68.161/32 is directly connected, GigabitEthernet0/0.34
C       10.23.68.192/27 is directly connected, GigabitEthernet0/0.44
L       10.23.68.193/32 is directly connected, GigabitEthernet0/0.44
C       10.23.68.224/28 is directly connected, GigabitEthernet0/0.99
L       10.23.68.225/32 is directly connected, GigabitEthernet0/0.99
C       10.23.69.0/25 is directly connected, GigabitEthernet0/1
L       10.23.69.1/32 is directly connected, GigabitEthernet0/1
O       10.23.69.128/26 [110/1563] via 10.1.14.9, 00:14:24, Serial0/3/1
                        [110/1563] via 10.1.14.13, 00:14:24, Serial0/3/0
O       10.23.69.192/27 [110/782] via 10.1.14.13, 00:14:34, Serial0/3/0
     209.165.201.0/28 is subnetted, 1 subnets
O E2    209.165.201.0/28 [110/20] via 10.1.14.9, 00:14:24, Serial0/3/1
                         [110/20] via 10.1.14.13, 00:14:24, Serial0/3/0
S*   0.0.0.0/0 is directly connected, Serial0/3/1

Toloshnyi_Router_2#
```

Рисунок 3.4 – Таблиця маршрутизації

Для перевірки роботи серверу AAA з протоколом Radius необхідно здійснити вхід до консолі будь-якого маршрутизатора. На рисунку 3.5 наведено приклад авторизації на маршрутизаторі Toloshnyi_Router_1.

```
Toloshnyi_Router_1

User Access Verification

Username: 123191_Toloshnyi
Password:
Toloshnyi_Router_1>
```

Рисунок 3.5 – Перевірка роботи AAA-серверу

Щоб перевірити роботу динамічного NAT, необхідно здійснити надсилання трафіку до вузла в мережі Internet (ПК ISP маршрутизатора). Виконання пінг-запиту наведено на рисунку 3.6.

```
C:\>ping 209.165.201.5

Pinging 209.165.201.5 with 32 bytes of data:

Reply from 209.165.201.5: bytes=32 time=2ms TTL=125
Reply from 209.165.201.5: bytes=32 time=3ms TTL=125
Reply from 209.165.201.5: bytes=32 time=2ms TTL=125
Reply from 209.165.201.5: bytes=32 time=3ms TTL=125

Ping statistics for 209.165.201.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\>
```

Рисунок 3.6 – Пінг-запит на публічну адресу ПК провайдера

Виконаємо ще кілька запитів і відобразимо таблицю NAT-трансляції на пограничному маршрутизаторі (рисунок 3.7).

```
Toloshnyi_Router_3#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 209.165.200.5:3   10.23.69.12:3      209.165.201.5:3    209.165.201.5:3
icmp 209.165.200.6:1   10.23.68.203:1     209.165.201.5:1    209.165.201.5:1
---  209.165.200.4     10.23.68.184       ---                ---
```

Рисунок 3.7 – Таблиця NAT-трансляції

Для перевірки роботи HTTP-сервера та DNS-сервера необхідно ввести в пошуковий рядок браузера 123.dnipro.ua (рисунок 3.8).

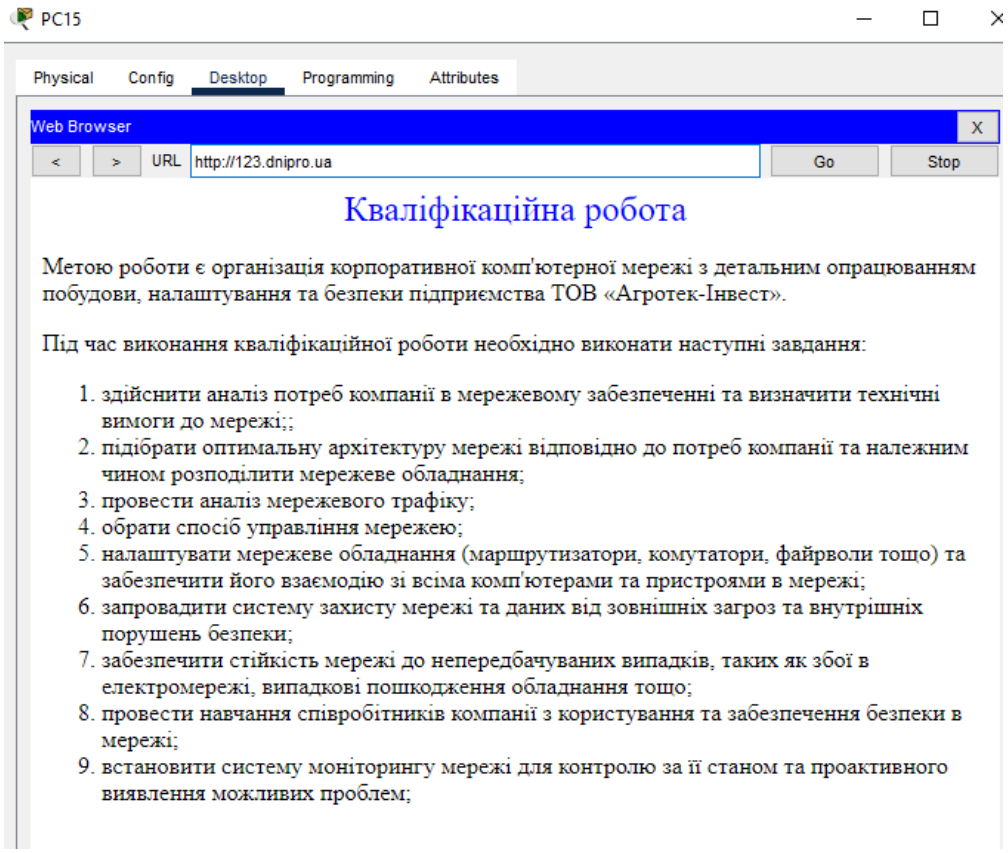
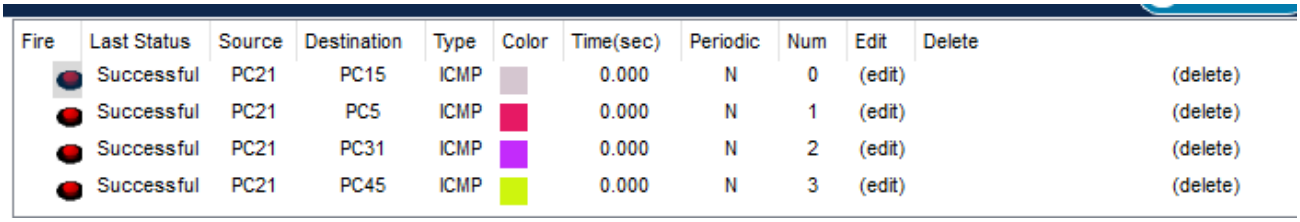


Рисунок 3.8 – Робота сайту

Для перевірки роботи VPN надішлемо по ICMP пакету в кожну підмережу головного офісу з віддаленого офісу (рисунок 3.9).



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC21	PC15	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC21	PC5	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC21	PC31	ICMP		0.000	N	2	(edit)	(delete)
	Successful	PC21	PC45	ICMP		0.000	N	3	(edit)	(delete)

Рисунок 3.9 – Надсилання трафіку через VPN тунель

Також на рисунку 3.10 зображено заголовок зашифрованого пакету.

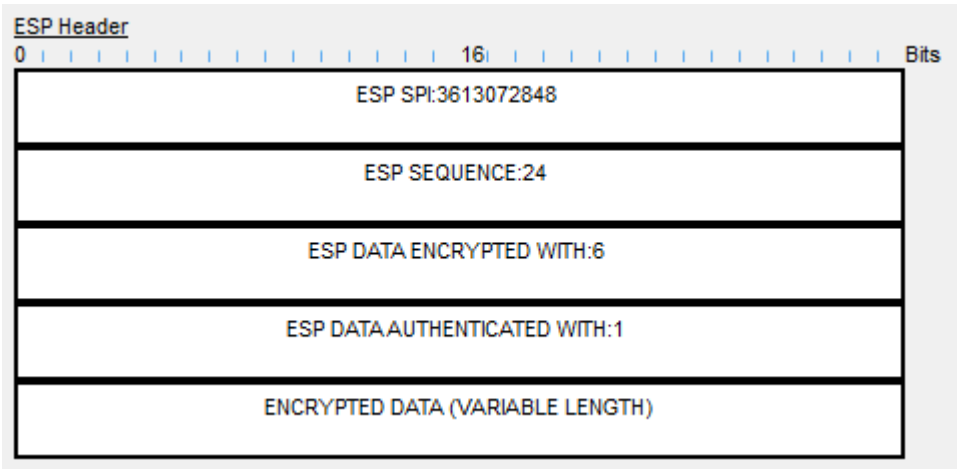


Рисунок 3.10 – Заголовок пакету з доданим шифруванням

На рисунку 3.11 продемонстровано динамічне отримання адреси на ПК за протоколом DHCP.

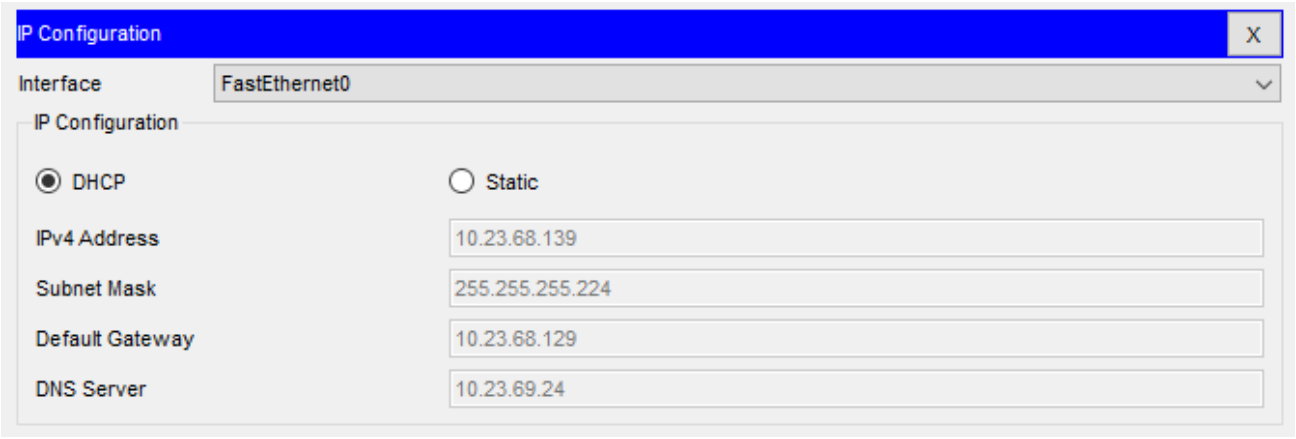


Рисунок 3.11 – Робота DHCP

4 РОЗРОБКА КОМПОНЕНТА СИСТЕМИ

4.1 Інженерне рішення по розробці компонента системи

Інтернет Речей (IoT) - це концепція, за допомогою якої фізичні пристрої, обладнані спеціальними сенсорами, програмним забезпеченням та мережевими з'єднаннями, можуть збирати і обмінюватися даними через Інтернет. Ідея полягає в тому, що ці "речі" можуть бути будь-якими фізичними об'єктами - від простих побутових пристроїв, до складних систем, таких як автомобілі або індустріальне обладнання.

Основна ідея за IoT полягає в тому, що ці речі можуть бути підключені до Інтернету і взаємодіяти одна з одною та з людьми, створюючи "розумні" системи і оточення. Вони можуть збирати дані з оточуючого середовища за допомогою різних сенсорів (таких як датчики температури, вологості, руху тощо), передавати ці дані по мережі і реагувати на них.

Одне з головних застосувань IoT - це управління та моніторинг різних систем. Наприклад, ви можете віддалено керувати системами опалення, освітлення чи безпеки у своєму будинку через мобільний додаток.

Замовник замовив впровадження IoT- систему, за допомогою якої буде відбуватися контроль та спостереження за офісними приміщеннями підприємства.

Система складається з:

- Датчики вогню;
- Сирени;
- Датчики руху;
- RFID-зчитувачі з картками для дверей.

Вимоги до виконання системою:

- При спрацюванні датчику руху, вмикається сирена та закривають вікна і двері.
- Відчинення дверей за допомогою RFID-карток
- Вимикання сирени коли всі показники у нормі

- При спрацюванні датчику вогню, вмикається сирена та відкриваються двері

Зв’язок між пристроями повинно бути реалізовано за допомогою HomeGateway. Він же буде виступати у ролі IoT-сервера. Зв’язок пристроїв з шлюзом реалізовується за допомогою стандарту IEEE 802.11 (Wi-Fi), датчики вогню та RFID-зчитувачі під’єднуються за допомогою Ethernet кабелів.

4.2 Налаштування обладнання та сервісів системи IoT

У першу чергу, ми розмістимо обладнання у середовищі Cisco Packet Tracer і забезпечимо його підключення до HomeGateway. Для з'єднання ми використовуємо протокол безпеки WPA2-PSK з паролем "cisco123". Схема, що відображає результат, можна знайти на рисунку 4.1.

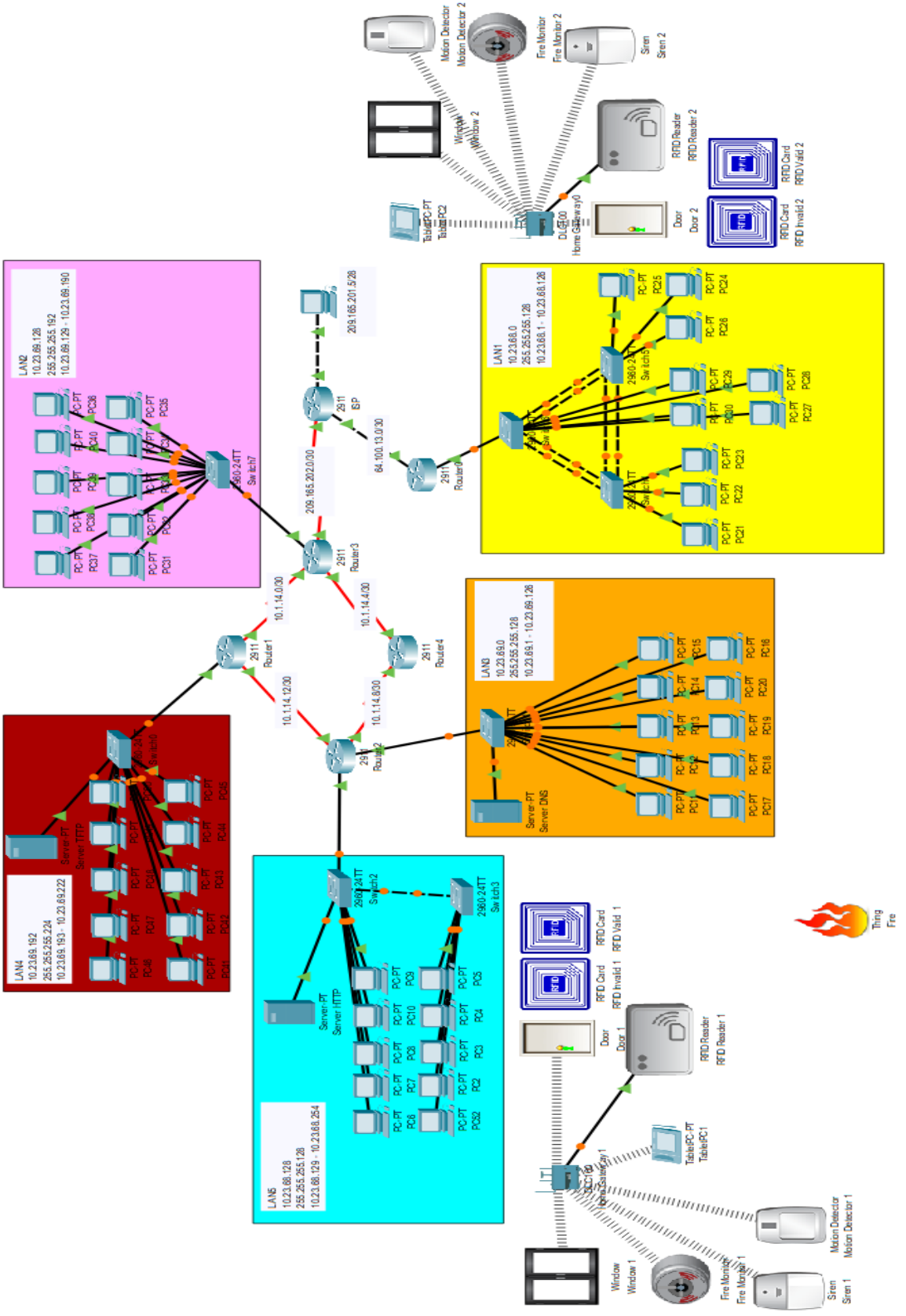


Рисунок 4.1- Схема підключення IoT-пристроїв

Після цього ми приступимо до налаштування роботи системи. Першим кроком буде налаштування всіх пристроїв на автоматичне отримання IP-адрес, а також вказання HomeGateway як сервера IoT (див. рисунок 4.2).

Рисунок 4.2 – Конфігурація пристроїв

Після того, як всі пристрої успішно підключилися до шлюзу, ми можемо переглянути список цих пристроїв на головній сторінці IoT-Monitor (див. рисунок 4.3). Для доступу до сервера використовується Tablet PC.

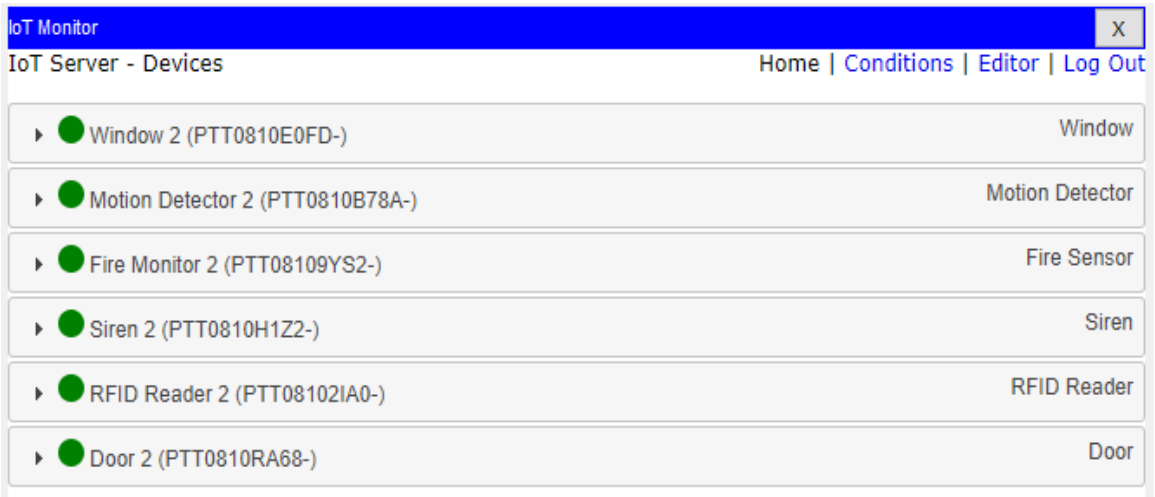


Рисунок 4.3 – Перелік під’єднаних пристроїв

Далі ми приступимо до налаштування роботи сирени, вікна та дверей при спрацюванні датчика руху. Для цього ми створимо відповідний сценарій на сервері (див. рисунок 4.4).

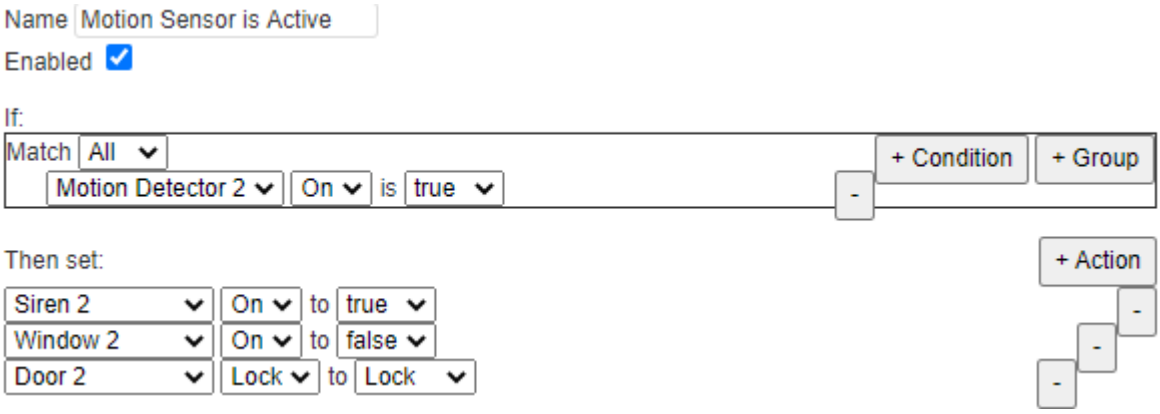


Рисунок 4.4 – Сценарій для спрацювння датчика руху

Після цього ми перейдемо до налаштування активації сирени та відкриття дверей при спрацюванні датчика вогню. Ми створимо відповідний сценарій на сервері (див. рисунок 4.5).

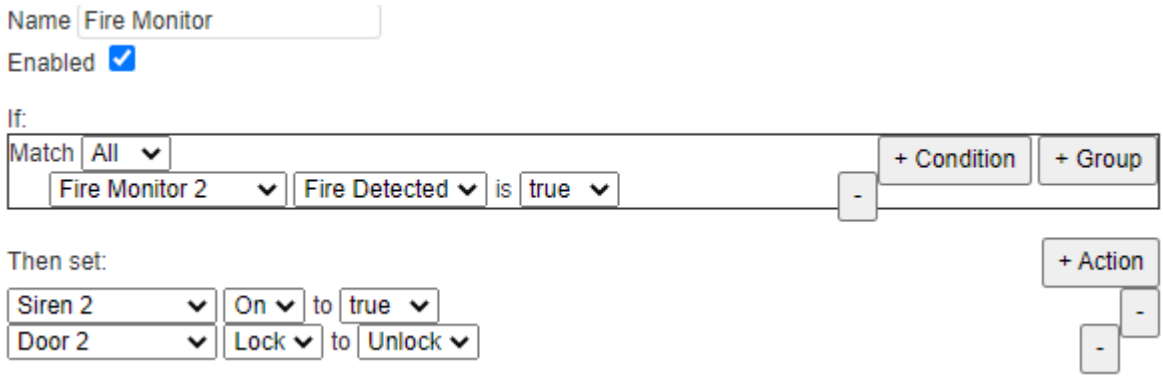


Рисунок 4.5 – Сценарій для спрацювання датчика вогню

Далі ми налаштуємо роботу RFID-зчитувача для відкриття та закриття дверей та вікна. Ми створимо відповідні сценарії на сервері (рисунок 4.5 - рисунок 4.6).

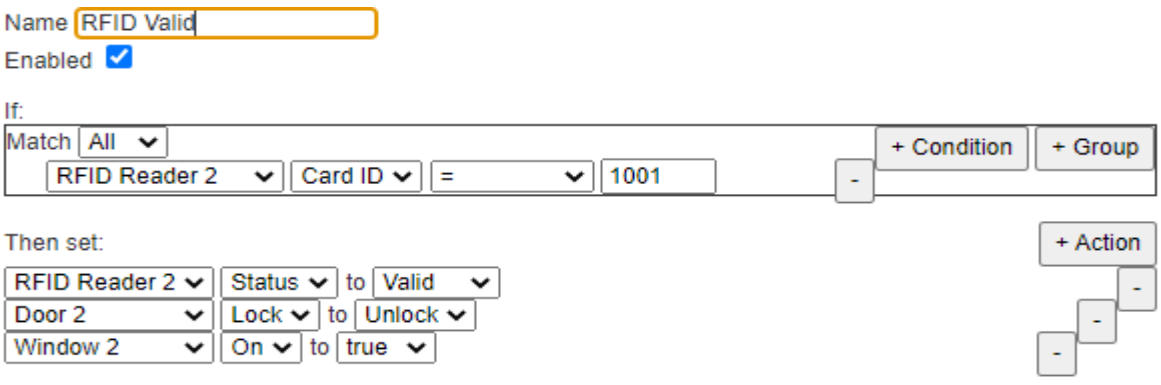


Рисунок 4.5 – Сценарій для відмикання дверей та відчинення вікна

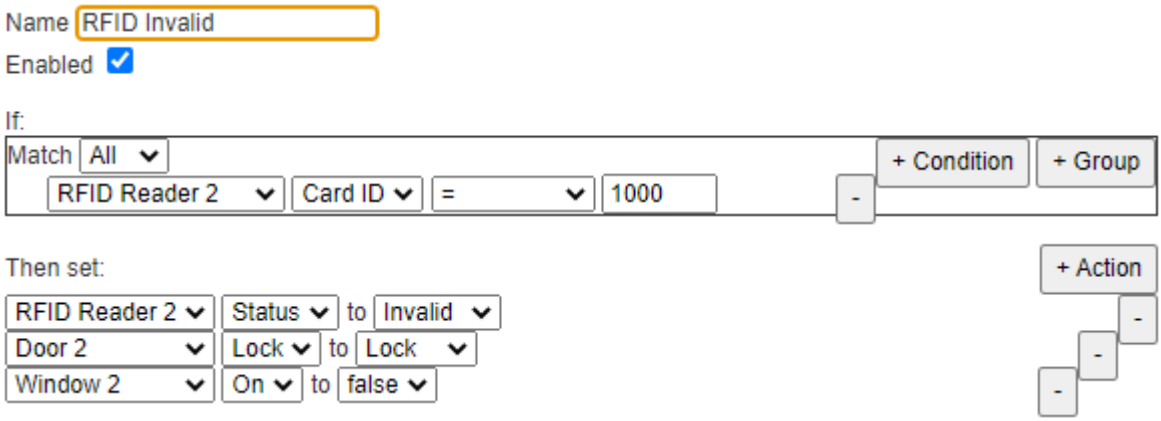


Рисунок 4.6 – Сценарій для замикання дверей та закриття вікна

Останнім налаштуємо сценарій для вимикання сирени за умови, що датчики руху та вогню неактивні (рисунок 4.7).

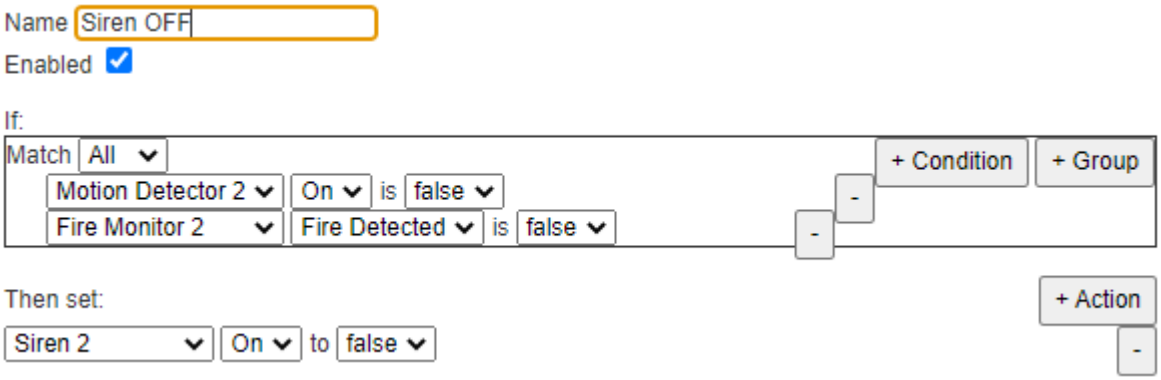


Рисунок 4.7 – Сценарій для вимикання сирени

Перелік створених сценаріїв зображено на рисунку 4.8

Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	RFID Valid	RFID Reader 2 Card ID = 1001	Set RFID Reader 2 Status to Valid Set Door 2 Lock to Unlock Set Window 2 On to true
Edit Remove	Yes	RFID Invalid	RFID Reader 2 Card ID = 1000	Set RFID Reader 2 Status to Invalid Set Door 2 Lock to Lock Set Window 2 On to false
Edit Remove	Yes	Motion Sensor is Active	Motion Detector 2 On is true	Set Siren 2 On to true Set Window 2 On to false Set Door 2 Lock to Lock
Edit Remove	Yes	Fire Monitor	Fire Monitor 2 Fire Detected is true	Set Siren 2 On to true Set Door 2 Lock to Unlock
Edit Remove	Yes	Siren OFF	Match all: • Motion Detector 2 On is false • Fire Monitor 2 Fire Detected is false	Set Siren 2 On to false

Рисунок 4.8 – Перелік сценаріїв

Крім того, для перевірки функціональності датчика вогню був створений компонент під назвою "Fire". Код роботи цього компонента можна знайти на рисунку 4.9.

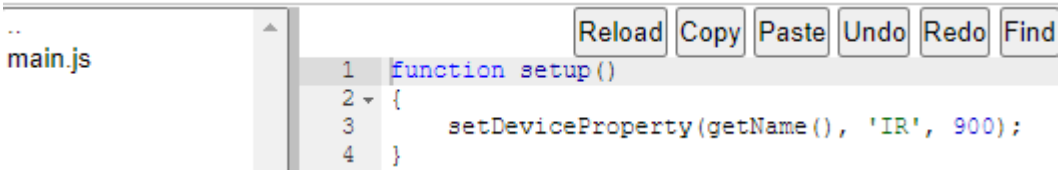


Рисунок 4.9 – Налаштування компоненту «Fire»

Такі ж налаштування застосовуються й для IoT-системи віддаленого офісу.

ВИСНОВКИ

В кваліфікаційній роботі проведено детальне дослідження базових аспектів проетування мережі для підприємства, таких як архітектура, безпека, пропускна здатність та масштабованість. Було обрано компанію «Агротек-Інвест» в якості об’єкта проектування мережі. Згідно до вимог замовника було обрано мережеве обладнання для системи, саме ж моделювання проекту було здійснено за допомогою середовища Cisco Packer Tracer.

Під час проектування були виконані налаштування всіх основних параметрів мережевого обладнання. Використовувалася технологія VLAN для створення віртуальних локальних мереж. Була настроєна динамічна маршрутизація за допомогою протоколу OSPF. Для забезпечення доступу до Інтернету використовувалася динамічна мережева адресація (NAT).

Також були налаштовані ACL-списки для контролю доступу. Для забезпечення безпеки та зв'язку між головним та віддаленим офісом використовувалася технологія VPN. Для автоматичного призначення IP-адрес вузлам мережі використовувався протокол DHCP.

Додатково, було здійснено об'єднання фізичних ліній комутаторів за допомогою технології EtherChannel. У рамках проекту також була реалізована система Інтернету речей (IoT) для забезпечення безпеки офісів компанії.

ПЕРЕЛІК ПОСИЛАНЬ

1. Агротек-Інвест – [Електронний ресурс] – https://agrotek.in.ua/ (дата звернення 11.05.2023)
2. Мережеве обладнання Cisco – [Електронний ресурс] – https://www.cisco.com/c/en/us/products/index.html (дата звернення 12.05.2023)
3. Вимоги до серверних кімнат – [Електронний ресурс] – https://shop.hypernet.com.ua/trebovaniya-k-servernoy-komnate/ (дата звернення 21.05.2023)
4. Дослідження та проектування комп'ютерних систем – [Електронний ресурс] – https://dut.edu.ua/ua/lib/1/category/1214/view/1432 (дата звернення 22.05.2023)
5. Системи технічного захисту інформації – [Електронний ресурс] – https://tzi.com.ua/downloads/1.1-002-99.pdf (дата звернення 25.05.2023)
6. Вимоги до забезпечення – [Електронний ресурс] – https://studfile.net/preview/5647074/page:4/ (дата звернення 27.05.2023)
7. ДСТУ "ГОСТ 12.1.004-91
8. ДСТУ "ГОСТ Р 50571.22-2000
9. ДСТУ "ГОСТ 15150-69 (зі змінами 2004)
10. Атестація здобувачів вищої освіти. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «ДП», 2022. – 62 с.

ДОДАТОК А

Текст програми налаштування обладнання корпоративної мережі

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.23014-01 12 01

Листів 10

2023

АНОТАЦІЯ

У даному додатку приведено програмне забезпечення для налаштування мережевого обладнання Cisco у середовищі моделювання "Cisco Packet Tracer".

Тексти програм складено з використанням мови конфігураційних скриптів для мережевого обладнання Cisco.

Програма має на меті забезпечити налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній, а також створення віртуальних приватних мереж (VPN) та домену комп'ютерної системи.

ЗМІСТ

1. Скрипт налаштування Router3

```
license udi pid CISCO2911/K9 sn FTX1524D70T-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 64.100.13.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 64.100.13.2
set transform-set TS
match address VPN14
!
!
!
!
ip domain-name Toloshnyi_Router_3
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 10.23.69.129 255.255.255.192
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
```

```
speed auto
!
interface Serial0/2/0
bandwidth 128
ip address 10.1.14.5 255.255.255.252
ip nat inside
!
interface Serial0/2/1
no ip address
clock rate 2000000
!
interface Serial0/3/0
bandwidth 128
ip address 209.165.202.2 255.255.255.252
ip nat outside
crypto map MAP
!
interface Serial0/3/1
bandwidth 128
ip address 10.1.14.1 255.255.255.252
ip nat inside
clock rate 128000
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
redistribute static subnets
passive-interface GigabitEthernet0/0
passive-interface GigabitEthernet0/1
network 10.23.69.128 0.0.0.63 area 0
network 10.1.14.0 0.0.0.3 area 0
network 10.1.14.4 0.0.0.3 area 0
!
ip nat pool Internet 209.165.200.5 209.165.200.30 netmask
255.255.255.224
ip nat inside source list NAT14 pool Internet
ip nat inside source static 10.23.68.184 209.165.200.4
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 209.165.201.0 255.255.255.240 209.165.202.1
ip route 209.165.202.0 255.255.255.252 Serial0/3/0
!
ip flow-export version 9
!
!
ip access-list extended VPN14
permit ip 10.23.69.192 0.0.0.31 10.23.68.0 0.0.0.127
permit ip 10.23.68.128 0.0.0.127 10.23.68.0 0.0.0.127
```

```
permit ip 10.23.69.0 0.0.0.127 10.23.68.0 0.0.0.127
permit ip 10.23.69.128 0.0.0.63 10.23.68.0 0.0.0.127
permit ip 10.1.14.0 0.0.0.3 10.23.68.0 0.0.0.127
ip access-list extended NAT14
deny ip 10.23.69.192 0.0.0.31 10.23.68.0 0.0.0.127
deny ip 10.23.68.128 0.0.0.127 10.23.68.0 0.0.0.127
deny ip 10.23.69.0 0.0.0.127 10.23.68.0 0.0.0.127
deny ip 10.23.69.128 0.0.0.63 10.23.68.0 0.0.0.127
deny ip 10.1.14.0 0.0.0.3 10.23.68.0 0.0.0.127
permit ip 10.23.69.192 0.0.0.31 any
permit ip 10.23.68.128 0.0.0.127 any
permit ip 10.23.69.0 0.0.0.127 any
permit ip 10.23.69.128 0.0.0.63 any
permit ip 10.23.14.0 0.0.0.3 any
!
banner motd ^CToloshnyi_Router_3^C
!
radius server 10.23.69.24
address ipv4 10.23.69.24 auth-port 1645
key radius123
!
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```

2. Скрипт налаштування Router0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Toloshnyi_Router_0
!
!
!
```

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
ip dhcp excluded-address 10.23.68.1 10.23.68.10
!
ip dhcp pool LAN-1
network 10.23.68.0 255.255.255.128
default-router 10.23.68.1
dns-server 10.23.69.24
!
!
aaa new-model
!
aaa authentication login CONSOLE group radius local
aaa authentication login default local
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username 123191_Toloshnyi password 7 082048430017544541
!
!
license udi pid CISCO2911/K9 sn FTX1524Z2IB-
license boot module c2900 technology-package securityk9
!
!
!
crypto isakmp policy 10
encr 3des
hash md5
authentication pre-share
group 2
!
crypto isakmp key cisco address 209.165.202.2
!
!
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
!
crypto map MAP 10 ipsec-isakmp
set peer 209.165.202.2
set transform-set TS
match address VPN14
```

```
!
!
!
!
ip domain-name Toloshnyi_Router_0
!
!
spanning-tree mode pvst
!
!
!
!
!
!
interface GigabitEthernet0/0
ip address 64.100.13.2 255.255.255.252
ip nat outside
duplex auto
speed auto
crypto map MAP
!
interface GigabitEthernet0/1
ip address 10.23.68.1 255.255.255.128
ip nat inside
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip nat pool Internet 209.165.205.5 209.165.205.30 netmask
255.255.255.224
ip nat inside source list NAT14 pool Internet
ip classless
ip route 0.0.0.0 0.0.0.0 64.100.13.1
ip route 64.100.13.0 255.255.255.252 64.100.13.1
ip route 209.165.201.0 255.255.255.240 64.100.13.1
!
ip flow-export version 9
!
!
ip access-list extended VPN14
permit ip 10.23.68.0 0.0.0.127 10.23.69.192 0.0.0.31
permit ip 10.23.68.0 0.0.0.127 10.23.68.128 0.0.0.127
permit ip 10.23.68.0 0.0.0.127 10.23.69.0 0.0.0.127
```

```
permit ip 10.23.68.0 0.0.0.127 10.23.69.128 0.0.0.63
permit ip 10.23.68.0 0.0.0.127 10.1.14.0 0.0.0.3
ip access-list extended NAT14
deny ip 10.23.68.0 0.0.0.127 10.23.69.192 0.0.0.31
deny ip 10.23.68.0 0.0.0.127 10.23.68.128 0.0.0.127
deny ip 10.23.68.0 0.0.0.127 10.23.69.0 0.0.0.127
deny ip 10.23.68.0 0.0.0.127 10.23.69.128 0.0.0.63
deny ip 10.23.68.0 0.0.0.127 10.1.14.0 0.0.0.3
permit ip 10.23.68.0 0.0.0.127 any
!
banner motd ^CToloshnyi_Router_0^C
!
radius server 10.23.69.24
address ipv4 10.23.69.24 auth-port 1645
key radius123
!
!
!
line con 0
password 7 0822455D0A16
login authentication CONSOLE
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login authentication default
transport input ssh
line vty 5 15
password 7 0822455D0A16
login authentication default
transport input ssh
!
!
!
end
```