Національний технічний університет
«Дніпровська політехніка»
Інститут електроенергетики
(інститут)

Факультет інформаційних технологій
(факультет)

Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи бакалавра

студента Шарипова Дмитра Олександровича
(ПІБ)

академічної групи 123-17-1
(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 контроля і керування доступом котеджного містечка «Sun Coast Dnipro» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Проф. Цвіркун Л.І.			
розділів:				
апаратний розділ	Доц. Ткаченко С.М.			
проектування мережі та захист інформації	Ас. Панферова Я.В.			
програмне забезпечення	Ас. Бешта Л.В.			
Рецензент				
Нормоконтролер	Проф. Цвіркун Л.І.			

Дніпро

2021

ЗАТВЕРДЖУЮ
Завідувач кафедри
Інформаційних
технологій та
комп'ютерної інженерії

проф._____ В.В. Гнатушенко
" " _____ 2021 р.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту Шарипов Д.О. (прізвище та ініціали) академічної групи 123-17-1 (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 контроля і керування доступом котеджного містечка «Sun Coast Dnipro» з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"

затвержена наказом ректора НТУ "Дніпровська політехніка" від 07.06.2021 р. № 317

Розділ	**Зміст**	**Термін виконання**
Стан питання та постановка завдання	Застосувати звіт з виробничої практики, інших науково-технічних джерел та розробити технічні вимоги до комп'ютерної системи контроля і керування доступом котеджного містечка «Sun Coast Dnipro»	05.05.2021
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи контроля і керування доступом котеджного містечка «Sun Coast Dnipro»	14.05.2021
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи контроля і керування доступом котеджного містечка «Sun Coast Dnipro»	31.05.2021
Графічна частина	Графічні результати розробки системи подати у вигляді рисунків електричних схем та інших креслень на 18 арк. формату А4	07.06.2021

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

Дата видачі 03.02.2021 р.

Дата подання до екзаменаційної комісії 12.06.2021 р.

Прийнято до виконання _____ Шарипов Д.О.
(підпис студента) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 58 с., 18 рис., 8 табл., 10 джерел, 1 додаток.

Об’єктом розробки являється комп’ютерна система контроля і керування доступом котеджного містечка «Sun Coast Dnipro»

Метою цієї роботи є підбір та налаштування обладнання для створення мережі котеджного містечка «Sun Coast Dnipro»”, а також розробка та підключення системи контроля і керування доступом на території котеджного містечка «Sun Coast Dnipro». Метою системи являється підвищення рівня безпеки у котеджному містечку.

У розділі «Стан питання і постановка задачі» проведено аналіз підприємства, для якого розроблена та буде впроваджуватись система, докладно розглянута специфіка об’єкта впровадження системи з точки зору потреби у посиленні безпеки, а також поставлена задача, та запропоновані можливі путі її вирішення.

У наступному розділі - «Технічні вимоги до комп’ютерної системи», - вказані технічні вимоги для впровадження системи, та запропоновані вимоги до забезпечення.

У розділі «Розробка апаратної частини комп’ютерної системи» наведено структурну схему технічних заходів підприємства, підібрано апаратні засоби комп’ютерної мережі, розроблена архітектура комп’ютерної мережі, та зроблені розрахунки вихідного трафіку.

У розділі «Проектування комп’ютерної мережі та перевірка роботи комп’ютерної системи» здійснено розрахунок підмереж, та проведено налаштування комп’ютерної мережі «Sun Coast Dnipro»

СКУД, ВІДЕОНАГЛЯД, CISCO, КОМПЬЮТЕРНІ МЕРЕЖІ.

ЗМІСТ

ВСТУП

Захист будь-якого об'єкта включає кілька рівнів, число яких залежить від необхідного стандарту безпеки об'єкта. При цьому у всіх випадках важливою складовою безпеки буде система контролю та управління доступом (СКУД).

Добре організована з використанням сучасних технічних засобів СКУД дозволить вирішувати цілий ряд завдань, наприклад:

- захист від розкрадання;
- захист від саботажу з боку конкурентів;
- захист від вандалізму;
- захист конфіденційної інформації;
- обмеження потоку відвідувачів;
- контроль в'їзду та виїзду на об’єкті.

Крім цього, СКУД є бар'єром для «цікавих». При реалізації конкретних СКУД використовують різні способи і реалізують їх пристрої для ідентифікації і аутентифікації особистості. Слід зазначити, що популярність систем СКУД як засоба безпеки постійно збільшується. Число фахівців, що працюють з системами такого типу, за останні роки подвоїлось та становить на даний момент близько 500 тис. чоловік.

В якості найбільш часто використовуваних СКУД можна назвати такі:

- турнікети звичайні і настінні;
- турнікети для проходу в коридорах;
- шлюзові кабіни;
- автоматичні хвіртки;
- роторні турнікети;
- обертові двері;
- дорожні блокіратори;
- шлагбауми;
- паркувальні системи;
- круглі розсувні двері;

- повнозростові турнікети;
- розсувні турнікети.

Дуже важливим є питання про можливість інтеграції СКУД з будь-якою системою безпеки з використанням відкритого протоколу.

Метою даної роботи є проект комп'ютерної системи контроля і керування доступом котеджного містечка Sun Coast Dnipro з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Для досягнення поставленої мети к роботі необхідно виконати низку завдань:

- описати стан питання і здійснити постановку завдання;
- навести технічні вимоги до комп’ютерної системи контролю та керування доступом;
- розробити апаратну частину комп’ютерної системи об’єкта;
- виконати проектування корпоративної мережі та перевірку роботи комп’ютерної системи об’єкта;
- описати захист інформації в комп’ютерній системі від несанкціонованого доступу.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Характеристика галузі та умов застосування системи, що проектується

Котеджне містечко – це, земельна ділянка за містом, викуплена компанією-забудовником для подальшого розбиття на менші за розміром ділянки та подальшого продажу фізичним або юридичним особам у якості житлового фонду. Зазвичай, на території таких ділянок, забудовник зводить типові будинки. Після продажу усіх котеджів, компанія-забудовник за певну платню бере на себе догляд за інфраструктурою прилеглих територій, наприклад: підведення і обслуговування міських комунікацій (вода, газ, електричний струм), вивезення сміття, благоустрій території, охорона території, тощо.

Таким чином, особа, яка викупає ділянку у котеджному містечку отримує право власності на заміське житло у охоронюваному та добре облаштованому районі та звільняється від типових проблем нерозвиненої інфраструктури за містом. В Україні практика котеджних містечок ще недостатньо популярна, проте поступово розвивається через великий попит на заміське житло.

1.2 Характеристика і структура об’єкта впровадження

Об’єктом впровадження системи є Sun Coast Dnipro - це котеджне містечко, що розташоване на березі ріки Мокра Сура у с. Новоалександрівка на відстані 8 км від м. Дніпро. Компанія-забудовник DDC розбила загальну площу містечка 7.5 га на 63 окремі ділянки. Приблизну схему ділянок відображено на рис 1.1.

Рисунок 1.1 – Схема котеджного містечка

На цих ділянках будуються типові будинки. Ділянки виставлені на продаж як об’єкти житлового фонду. Усі ділянки є приватизованими об’єктами з присвоєним кадастровим номером. До кожної ділянки підведено комунікації:

- Водопостачання із індивідуальної свердловини (грунтові води)
- Електричний струм (20 кВт на ділянку)
- Каналізація (септичний танк)
- Природний газ (магістральне постачання)

Крім, цього компанія-забудовник надає послуги забезпечення охорони на всій території містечка. Основними засобами безпеки є:

- Огорожа по всьому периметру містечка
- Цілодобова охорона

На виїздах на приміські дороги розташовані пропускні пункти з залізними воротами, відкриття яких контролюють працівники охорони. Такий пропускний пункт зображено на рис 1.2.

Рисунок 1.2 – Пропускний пункт котеджного містечка

1.3 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проектування

Очевидною проблемою котеджного містечка є невідповідність сучасним стандартам в галузі безпеки. Для захисту від зловмисників створені лише 2 шара безпеки:

- Огорожа, пасивний засіб безпеки, який виконує упереджувальну функцію
- Охорона, активний засіб безпеки, що має реагувати на виникаючі загрози.

Для незначних загроз таких засобів достатньо, проте для підготовленого злочинця сама по собі огорожа не створює значних перешкод. У такому випадку, система безпеки має серйозну ваду: охорона не може реагувати на загрози, якщо вона про них не знає. Навіть при великій кількості

співробітників (що зазвичай є неефективним рішенням з економічної точки зору) ефективно охопити територію містечка у 7.5 га надзвичайно важко.

Системі безпеки бракує засобів моніторингу, які могли б вчасно сповіщати охорону про можливі загрози.

Крім цього, існує проблема контролю доступу до території у денний час. Якщо в нічній час через пропускні пункти зазвичай пересувається незначна кількість людей, яку легко контролювати, то у денний час потік людей збільшується. Охорона не може запам’ятати усіх мешканців містечка і не може активно обмежувати доступ до комплексу. адже це може створити незручності для власників будинків. У той же час, поодинокі люди, які не викликають підозри у охоронців, можуть створювати небезпеку і спричиняти дискомфорт мешканцям містечка.

1.4 Завдання і мета роботи

“Комп'ютерна система контроля і керування доступом котеджного містечка Sun Coast Dnipro з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі” - це комплекс цифрових засобів безпеки, для регулювання переміщення людей чи транспортних об’єктів на території котеджного містечка, а також здійснення моніторингу прилеглих до нього територій.

Виходячи із пункту 1.3, комп’ютерна система, що впроваджується на підприємстві має на меті допомогу охороні у виконанні своїх обов’язків щодо створення безпечного середовища для мешканців котеджного містечка. За рахунок використання сучасних технологій охоронна система зможе вчасно реагувати на виникаючі загрози. Мешканці котеджного містечка отримають необхідну їм приватність і безпеку з мінімальними незручностями. Після розгортання та налаштування системи, на її підтримку буде витрачатися значно менше коштів, ніж на утримання великої кількості охоронців, тож таке рішення є економічно обґрунтованим у довготривалій перспективі. Кажучи про довготривалу перспективу, після розроблення детальної схеми і створення

працюючої реалізації , компанія-замовник, користуючись набутим досвідом інтеграції комп’ютерної системи може впровадити її у інших своїх проектах подібного типу.

Завданням роботи є розробка детальної схеми проектуємої системи. Оскільки використання реального обладнання потребує вкладень коштів, які не доступні на момент розробки, прототип працюючої системи буде створено у додатку Cisco Packet Tracer.

1.5 Визначення можливих напрямків рішення поставлених завдань

Системи контролю і управління доступом (надалі СКУД) є поширеним рішенням на об'єктах, де необхідно обмежити переміщення людей або транспорту в охоронювані зони.

Система контролю і управління доступом складається з технічних пристроїв, програмного забезпечення і обмежуючих заходів, що дозволяє отримувати, обробляти і зберігати інформацію про переміщення людей і транспорту через точки входу на територію об’єкта, а також забезпечити обмеження несанкціонованого доступу до охоронюваної зони.

Кожна система контролю і управління доступом має підключення до мережі, надаючи точкам проходу (турнікети, хвіртки, двері) свою мережеву адресу.

Можна виділити такі основні частини будь-якої СКУД:

1) Ідентифікатори

Використовуються у якості ключа доступу до системи, а також для опізнавання особи, яка отримує доступ до об’єкту. Існує велика кількість можливих пристроїв для ідентифікації, таких як наприклад:

- Безконтакті картки
- Брелоки
- Магнітні або безконтактні картки

Також ідентифікаторами можуть виступати біометричні ознаки людей, такі як, наприклад, малюнок сітківки або відбиток пальця.

2) Зчитувачі

Зчитувачі використовуються у парі з ідентифікаторами та передають отримані від них дані контролеру для подальшого надання доступу. Оскільки вони працюють у парі з ідентифікаторами, можна виділити такі основні типи:

- Магнітні
- Безконтактні (використовують радіохвилі як канал зв'язку із ідентифікатором)
- Біометричні

Окремим типом зчитувачів можна виділити кнопки виходу, які дозволяють будь-кому покинути об'єкт у випадку надзвичайної ситуації.

3) Обмежуючі пристрої

Виконують функції фізичної перешкоди для обмеження доступу. За типом дії поділяються на електромеханічні і електромагнітні. В основному використовується три типи пристроїв:

- Електрозамки - виконують такі ж функції, що і звичайні замки, але можуть бути відчинені при поданні струму.
- Турнікети - обмежують пересування людей до об'єкту до однієї людини за раз, що змушує проходити аутентифікацію всіх, хто отримує доступ.
- Дверні доводчики - дозволяють уникнути ситуацію, при якій двері залишаються відкритими після входу.

4) Контроллери

Контроллери є центральною частиною системи і виконують функції управління всіма пристроями, зберігання бази користувачів та ведення журналу подій надання доступу. Вони бувають:

- Автономні - не можуть взаємодіяти з іншими контроллерами.
- Мережеві - здатні об'єднуватися у мережу та поширювати дані між собою.

Для того, щоб забезпечити кращий контроль активності навколо об’єкту і на пропускних пунктах, СКУД доповнюється системою моніторингу навколишнього середовища. Зазвичай, для цього використовується система відеосростереження.

Система відеоспостереження - це комплект обладнання, який здійснює зоровий контроль за територією. Існує декілька типів систем відеоспостереження, вибір яких залежить від умов використання системи.

За структурною ознакою вони бувають:

- Однорівневі - складається з однієї або кількох камер, блока живлення, а також монітора, куди виводиться отримана інформація. Дані не зберігаються для подальшого відтворення.
- Багаторівневі - мають більш складну будову і додатково включають центральний сервер, на якому зберігається інформація. Можливе отримання віддаленого доступу до системи.
- Розподілена - мають велику кількість варіантів побудови. Складові системи можуть обмінюватися даними через Інтернет.
- За типом передачі даних вони бувають:
- Аналогові - використовують для передачі даних коаксіальний кабель. Потік відео нестиснутий, не дуже високої якості. Найдешевші у впровадженні, проте сильно обмежені у використанні.
- Цифрові мережеві - використовують мережеві технології (ethernet) для передачі даних. Мають вищу якість, ніж аналогові камери. Для цифрових мереж легше налаштувати віддалений доступ та управління пристроями. Дані можно зберігати на віддаленому сервері. Проте камери, що підтримують мережеві технології зазвичай коштують значно більше, ніж аналогові камери.
- Гібридні - підтримують як цифрові, так і аналогові камери. Аналоговий відеосигнал кодується відеокодером, після чого його можна пересилати як цифровий.

Також, для правильного функціонування системи необхідно правильно підібрати тип відеокамер для системи. Камери мають бути пристосовані до умов, у яких вони використовуються. Є багато чинників, що можуть вплинути на вибір камери, таких як:

1 Форм-фактор

- Купольні - мають затемнену оболонку, що робить неможливим розпізнавання, куди направлений об’єктив.
- Циліндричні - встановлюються на кронштейні, направлені на чітко визначену ділянку, займають більше місця, ніж купольні.
- Риб'яче око - плоскі камери з широким кутом зору.
- PTZ - камери з сервоприводом, що дозволяє віддалено змінювати положення об’єктиву.

2 Середа застосування

- Вуличні
- Для приміщень

3 Інфрачервоне підсвічування - камери з інфрачервоним підсвічуванням дозволяють ефективно використовувати відеокамеру вночі.

4 Захист - існують спеціальні види камер, захищені від вандалів та пристосовані до роботи у будь-яку погоду.

5 Тип підключення - аналогові відеокамери підключаються за допомогою коаксіального кабеля. Цифрові можуть буду дротовими або бездротовими.

6 Чіткість зображення - для розпізнавання людей і номерних знаків необхідна краща якість зображення, проте такі камери зазвичай коштують дорожче.

2 ТЕХНІЧНІ ВИМОГИ ДО КОМП'ЮТЕРНОЇ СИСТЕМИ КОНТРОЛЮ ЧИ КЕРУВАННЯ

2.1 Вимоги до системи в цілому

Програмно-апаратний комплекс рішення можна поділити на два напрямки:

- Система моніторингу навколишнього середовища
- Система керування доступом до внутрішньої території об'єкту

2.1.1 Система моніторингу навколишнього середовища

Моніторинг навколишнього середовища може бути реалізований як централізована система камер відеоспостереження. Керувати системою буде оператор, в обов'язки якого входить нагляд за територією через монітор, на який транслюється зображення з камер і координація дій інших охоронців. До системи висуваються наступні вимоги:

- Камери мають охоплювати всю зовнішню територію по периметру містечка
- Охоплена камерами територія мусить не мати так званих "сліпих зон" (ділянок, які знаходяться поза межами поля зору будь-якої із камер)
- Оператор системи (охоронець) мусить мати цілодобовий доступ до зображення всіх камер
- Камери мусять мати можливість реєструвати рух та сповіщати про це оператора системи
- Камери мусять не заважати мешканцям містечка і не порушувати їх приватність
- Зображення з камер мусить зберігатися локально, а також на віддаленому сервері у випадку необхідності подальшого аналізу
- Камери, що знаходяться на пропускних пунктах, мусять мати можливість розпізнавати номерні знаки машин, що проходять через

пропускний пункт

- Система має продовжувати функціонувати при короткочасному відключенні електроенергії, бо воно може бути спричинене діями зловмисників

Таким чином, можна виділити декілька типів пристроїв, необхідних для розгортання системи:

1. Зовнішні камери, встановлені по периметру
2. Камери, встановлені на пропускних пунктах
3. Мережеве обладнання, для об’єднання пристроїв між собою
4. Центральний сервер, який буде об’єднувати зображення камер і транслювати його оператору, а також синхронізувати дані із віддаленим сервером
5. Монітор та засоби управління для оператора
6. NAS (мережева система зберігання даних) для локального зберігання відеозаписів зберігання відеозаписів

2.1.2 Система керування доступом до внутрішньої території об’єкту

Система керування доступом має на меті фізичне обмеження входу/виходу до об’єкта. Зазвичай системи керування доступом складаються з обмежуючих елементів (турнікети, електронні замки, механізми доведення дверей тощо) та ключів доступу (картка з магнітною смужкою; безконтактна картка; спеціальний брелок, цифровий код, що безпосередньо вводиться на клавіатурі; кнопка виходу тощо). При активації ключа доступу, обмежуючий засіб тимчасово дозволяє фізичний доступ до об’єкта.

Беручи до уваги специфіку умов застосування системи, я вважаю доцільним використання у якості обмежуючого засобу - електронних замків, а у якості ключа доступу - спеціальний безпровідний брелок та кнопку виходу. Електронні замки будуть встановлені на пропускних пунктах.

Вимоги до системи:

- Електронні замки за замовчуванням завжди закриті, навіть при

знеструмленні

- Електронні замки можуть бути тимчасово відчинені при натисканні на кнопку виходу чи активації безпровідного брелка
- Відчинити замок з внутрішньої сторони завжди можливо, навіть при знеструмленні (на випадок надзвичайної ситуації)
- Інформація про відкриття за допомогою брелків (час відкриття, власник брелка) зберігається локально та на віддаленому сервері на випадок необхідності подальшого аналізу

Таким чином, можна виділити декілька типів пристроїв, необхідних для розгортання системи:

1. Електронні замки, що встановлюються на воротах пропускних пунктів
2. Контролери електронних замків
3. Безпровідні брелки доступу
4. Мережеве обладнання
5. Центральний сервер з журналом доступу до системи

2.2 Вимоги до надійності

Система має використовувати обладнання, яке можна швидко замінити у випадку його відмови. Система мусить залишатися працездатною під час короткочасного знеструмлення.

2.3 Вимоги до чисельності і кваліфікації персоналу

1) Мережевий інженер – обслуговує існуюче мережеве обладнання та встановлює нове при необхідності розширення системи. Кількість: одна людина. Графік роботи: з 9 до 18 понеділок – п’ятниця.

2) Адміністратор – відповідає за коректність роботи системи контролю доступу та займається моніторингом системи відеоспостереження. . Кількість: три людини. Графік роботи: цілодобово, позмінно.

2.4 Вимоги до захисту інформації від несанкціонованого доступу

Уся конфіденціальна інформація має бути доступна тільки користувачам, що ідентифікувалися у системі. Для передання інформації між елементами системи має використовуватися шифрування. На всіх пристроях у системі мають бути встановлені останні патчі безпеки. Система не має порушувати особистий простір мешканців містечка. Зовнішні не авторизовані підключення до системи мають бути заблоковані мережевою політикою.

2.5 Вимоги до патентної чистоти

Система має використовувати лише сертифіковане ПЗ з дійсною ліцензією.

2.6 Вимоги до видів забезпечення

2.6.1 Вимоги до інформаційного забезпечення системи

Зображення з камер і логи дій користувачів мають зберігатися у деякому сховищі для подальшого аналізу при необхідності.

Алгоритми шифрування, що будуть використані для зберігання і передачі інформації, мають бути визнаними надійними та мають пройти відповідну сертифікацію.

Для покращення стабільності системи, слід використовувати сучасні мережеві технології та обладнання.

2.6.2 Вимоги до технічного забезпечення системи

Мережеві пристрої мають підтримувати пропускну здасть 100 мбіт/с, оскільки їм буде необхідно транслювати відеопотік. Також необіхдна підтримка технології VLAN для забезпечення необхідної безпеки мережі.

Сервер, на якому мають зберігатися відеозаписи, мусить мати дисковий об’єм від 1 тб для довгострокового зберігання даних.

2.6.3 Вимоги до організаційного забезпечення системи

Доступ до системи повинен бути побудований на принципах RBAC (Role based access control). Користувачі мають отримувати доступ до тих елементів системи, які дозволені їх ролі.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1 Обстеження об'єкту розробки з метою аналізу всіх способів внутрішнього і зовнішнього доступу до інфраструктури мережі

Комп'ютерна система, створювана на підприємстві включає в себе:

- Мережа систему нагляду за периметром котеджного містечка
- Мережа фінансового відділу компанії забудовника;
- Мережа відділу продажу компанії забудовника;
- мережа IT відділу котеджного містчека;
- мережа юридичного відділу котеджного містечка;
- сервер для налагодження віддаленого доступу;
- сервер для зберігання даних відеонагляду и користувацьких логів;

Таким чином, систему можна розподілити на такі рівні:

1) Рівень ядра – об'єднує між собою локальні мережі, займається маршрутизацією між ними і забезпечує доступ в інтернет
2) Рівень доступу – відповідає за локальні мережі типу VLAN
3) Кінцеві пристрої – пристрої, що знаходяться на периферії та взаємодіють з користувачами або зовнішнім середовищем.

Загалом, схематично, структуру можна зобразити так (рис 3.1):

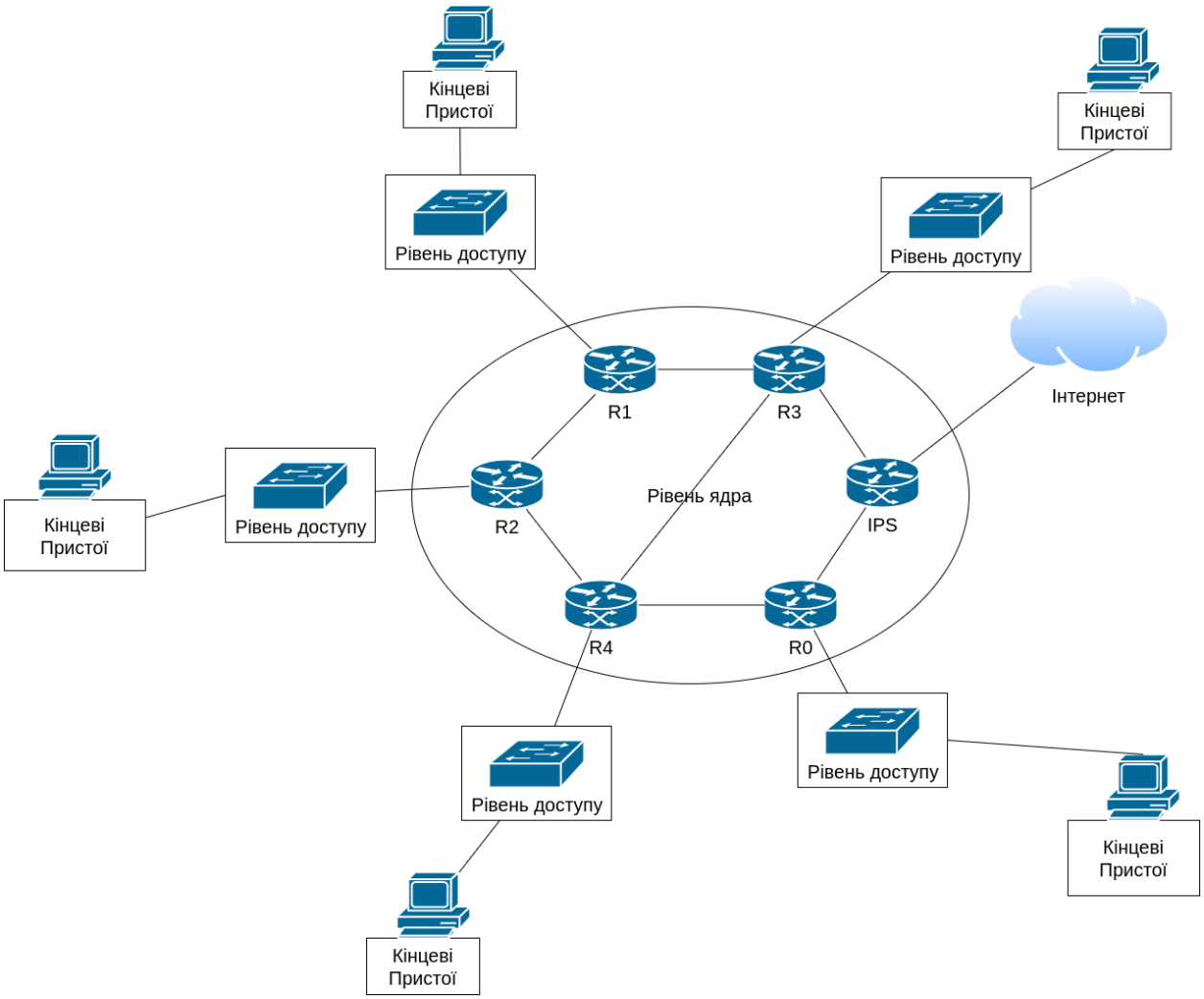

Рисунок 3.1 – Структурна схема комплексу технічних заходів

3.1.1 Розташування камер відеоспостереження і електронних замків

Наразі я вважаю доцільним встановити камери відеоспостереження по периметру котеджного містечка та на контрольно-пропускних пунктах. Таким чином, вони будуть виконувати свої функції та не заважати мешканцям містечка.

Також на контрольно-пропускних пунктах необхідно встановити грати з сервоприводом та електронними замками, які матимуть на меті фізичнообмежувати доступ до об’єкту. Схематично це можна зобразити так (рис 3.2):

Рисунок 3.2 – Охоронний периметр з контрольно-пропускними пунктами

3.1.2 Аналіз входів і виходів

Тип	Назва	Функціональне значення
Вхід	КПП1 Електричний замок	Знаходиться на гратах КПП1 та обмежує доступ неавторизованим користувачам. Передає інформацію про відкриття/закриття у мережу.
Вхід	КПП2 Електричний замок	Знаходиться на гратах КПП2 та обмежує доступ неавторизованим користувачам. Передає інформацію про відкриття/закриття у мережу.
Вхід	КПП3 Електричний замок	Знаходиться на гратах КПП3 та обмежує доступ неавторизованим

		користувачам. Передає інформацію про відкриття/закриття у мережу.
Вхід	Камери периметру (об``єднані)	Знаходяться по периметру та на пропускних пунктах. Транслюють зображення у мережу в реальному часі.
Вихід	Сервер віддаленого доступу	Надає доступ до записів відеокамер ззовні.
Вихід	Сервер зберігання даних	Отримують користувацькі логи і записи камер і зберігають їх для подальшого аналізу.
Вихід	Термінал користувача	Відображає відеопоток з камер та логи відкриття замків на КПП.

Таблиця 3.1 Входи та виходи

3.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи шляхом узгодження структури з топологічними особливостями об’єкту розробки

Протоколи маршрутизації вибираються, виходячи з характеристик, перерахованих нижче.

- оптимальність визначає можливості протоколу та алгоритму щодо вибору найбільш оптимального маршруту на підставі метрик і їх вагових значень, використовуваних при розрахунках. Наприклад, якийсь протокол може використовувати лічильник вузлів і затримки для визначення метрик; затримки мають більш високий вагу при обліку остаточного значення, але зате їх складніше розрахувати.
- Простота і низькі накладні витрати. Ідеальної ефективності роботи алгоритму маршрутизації можна досягти при мінімальному завантаженні процесора і пам'яті маршрутизатора. Ця характеристика важлива для масштабованості мережі, яка в граничному випадку може бути розширена до розмірів мережі Internet.

- Стійкість і надійність. Алгоритм маршрутизації повинен коректно функціонувати навіть при наявності нестандартних і непередбачених обставин, таких, як збій обладнання, високе завантаження і помилки експлуатації.
- Швидка конвергенція. Конвергенцією називається процес встановлення домовленості між усіма маршрутизаторами про наявні маршрути. Коли в мережі відбуваються події, що впливають на доступність маршрутизатора, для встановлення повторного треба зробити перерахунки. Алгоритми маршрутизації, що не володіють швидкою конвергенцією, можуть викликати збій або значну затримку при доставці інформації.
- Гнучкість. Алгоритм і протокол маршрутизації повинні швидко адаптуватися до різноманітних змін в мережі, а саме: змін в стані пристроїв, зокрема, маршрутизаторів, зміна пропускної здатності каналів, зміна розміру черг або мережевої затримки.
- Масштабованість. Деякі протоколи розроблені таким чином, що можуть бути масштабовані краще за інших. У разі, що якщо планується розширення мережі, або така можливість в майбутньому передбачається, перевага віддається протоколу EIGRP, ніж RIP.

Головним завданням алгоритму маршрутизації при оновленні таблиці маршрутизації є у визначення інформації, яка повинна бути внесена в таблицю. Попри використання різних метрик для визначення найкращого маршруту різними алгоритмами, інтерпретація вибору кращого варіанту шляху здійснюється кожним алгоритмом у різний спосіб. Алгоритм маршрутизації розраховує метрику для кожного мережевого маршруту. Складні алгоритми маршрутизації можуть засновувати вибір маршруту на основі декількох параметрів, об'єднуючи їх в одну загальну метрику, як показано на рисунку 3.3. Чим менше метрика, тим краще обраний маршрут.

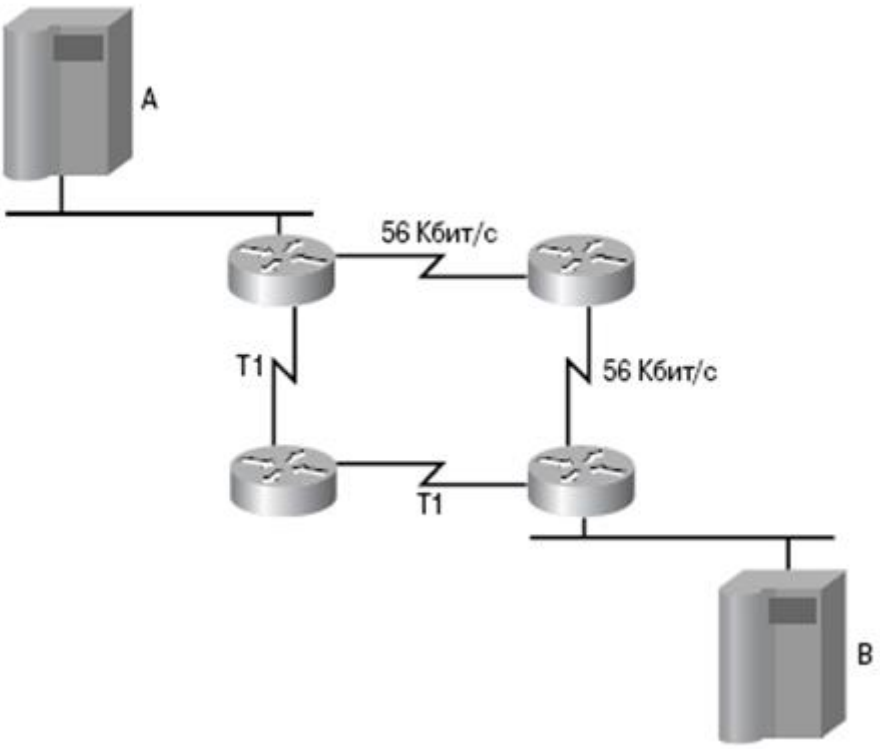

Рисунок3.3 – Метрики маршрутизації

Метрики маршрутизації обчислюються на основі однієї або кількох характеристик. В алгоритмах маршрутизації використовуються найчастіше такі параметри метрики:

- Ширина смуги пропускання - є засобом оцінки обсягу інформації, який може бути переданий по каналу зв'язку (канал Fast Ethernet зі швидкістю 100 Мбіт / с кращий, ніж виділена лінія зі швидкістю 512 Кбіт / с).
- Затримка - проміжок часу, необхідний для проходження пакета по кожному з каналів зв'язку від відправника одержувачу. Затримка залежить від пропускної здатності проміжних каналів, розміру черг в портах маршрутизаторів, завантаження мережі і фізичної відстані, тощо.
- Завантаження - обсяг операцій, які виконуються мережевим пристроєм, таким, як маршрутизатор, або середня завантаженість каналу зв'язку.

- Надійність - відносне значення кількості помилок для кожного з каналів зв'язку.
- Лічильник транзитних вузлів - кількість маршрутизаторів, через які проходить пакет до потрапляння у пункт призначення. При проходженні через маршрутизатор значення лічильника вузлів збільшується на одиницю. Якщо значення лічильника вузлів дорівнює чотирьом, то дані, відправлені по цьому маршруту, пройдуть через чотири маршрутизатора перед тим, як будуть отримані адресатом. За наявності кількох шляхів маршрутизатор вибирає шлях з найменшим значенням лічильника вузлів.
- Вартість - значення, яке визначається на підставі критеріїв виміру, відібраних адміністратором, які враховують грошову вартість рішення з точки зору економічної ефективності.

Маршрутизатори використовують протоколи маршрутизації для обміну маршрутною інформацією. Іншими словами, протоколи маршрутизації визначають, як маршрутизуються протоколи передачі даних (тобто маршрутизовані). Як показано на рисунку 3.4, двома родинами протоколів маршрутизації є протоколи внутрішніх шлюзів (Interior Gateway Protocol - IGP) і протоколи зовнішніх шлюзів (Exterior Gateway Protocols - EGP). Класифікація всіх протоколів за цими двома родинами заснована на принципі їх роботи по відношенню до автономних систем.

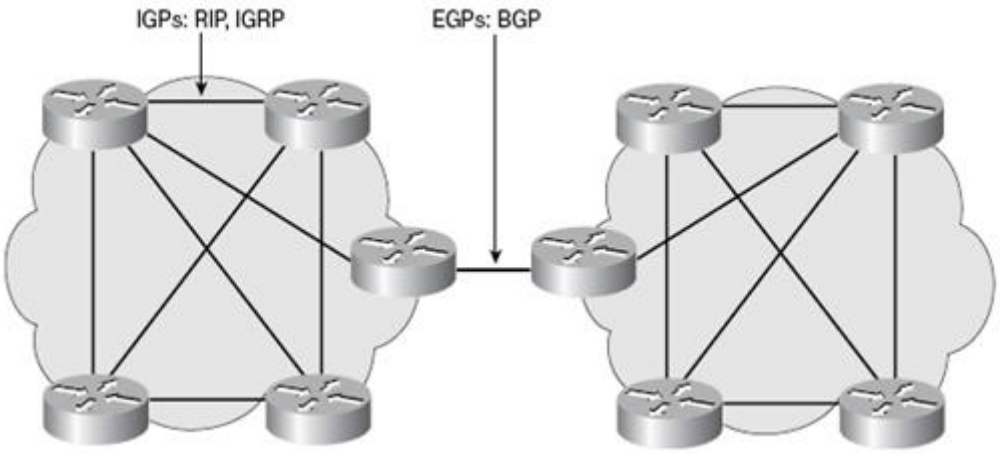

Рисунок 3.4 – Протоколи EGP і IGP

Автономною системою (Autonomous System - AS) називається мережа або група мереж, що знаходяться під єдиним адміністративним контролем, як, наприклад, домен Cisco.com. Автономна система складається з маршрутизаторів, які для зовнішнього світу (тобто для інших мереж) виглядають як єдина мережа.

Протоколи класу IGP маршрутизируют дані всередині автономних систем. До класу IGP відносяться такі протоколи маршрутизації:

- протоколи RIP і RIP V2;
- IGRP;
- EIGRP;
- OSPF;
- протокол обміну даними між проміжними системами (Intermediate system-to-Intermediate System - IS-IS).

Протоколи класу EGP маршрутизують дані між автономними системами. Протокол BGP є найбільш широко відомим представником класу EGP.

Протокол RIP

Протоколом маршрутної інформації (Routing Information Protocol - RIP) передбачено використання лічильника кількості транзитних вузлів для визначення напрямку і відстані для будь-якого з каналів мережі. У разі існування кількох маршрутів, протокол RIP вибирає маршрут з найменшим значенням лічильника транзитних вузлів. Оскільки протокол RIP використовує лічильник як єдину метрику, обраний маршрут не завжди виявляється найкоротшим. Протокол RIP версії 1 дозволяє використовувати тільки класову (classfull) маршрутизацію. Це вимагає, щоб усі мережеві пристрої мали однакову маску мережі, оскільки RIP версії 1 не передбачає поновлення інформації.

Протокол RIP версії 2 використовує так звану префіксну маршрутизацію (prefix routing), і пересилає маску мережі разом з анонсами таблиць маршрутизації. За рахунок цієї функції здійснюється підтримка безкласової

маршрутизації. Протоколи безкласової маршрутизації надають можливість використовувати підмережі з різної довжини масками всередині однієї і тієї ж мережі. Таке використання масок підмережі різної довжини всередині однієї мережі називається технологією масок змінної довжини (Variable-Length Subnet Mask -VLSM).

Протокол IGRP

Протокол маршрутизації внутрішнього шлюзу (Interior Gateway Routing Protocol - IGRP), розроблений корпорацією Cisco, використовує дистанційно-векторний алгоритм, та призначений для вирішення проблем маршрутизації в великих мережах, де неможливо використовувати такі протоколи, як RIP. Протокол IGRP вибирає найшвидший шлях завдяки таким якостям як затримка, пропускна спроможність, завантаження і надійність каналу. Стандартно протокол IGRP використовує в якості 24-бітових метрик тільки пропускну здатність і затримку. Цей протокол має значно більше максимальне значення лічильника вузлів, ніж протокол RIP, що дозволяє використовувати його у великих мережах. Протокол IGRP дозволяє використовувати тільки класову маршрутизацію.

Протокол EIGRP

Так само, як і IGRP, протокол EIGRP (Enhanced Interior Gateway Routing Protocol - розширений протокол маршрутизації внутрішнього шлюзу) був розроблений корпорацією Cisco і є її фірмовим продуктом. Цей протокол – є вдосконаленою версією протоколу IGRP, з використанням 32-бітових метрик. Зокрема, протокол EIGRP відзначається підвищеною ефективністю завдяки пришвидшеній конвергенції і високій пропускної здатності. Він працює на основі дистанційно-векторного алгоритму, та також використовує деякі функції алгоритмів з урахуванням стану каналу. У зв’язку з цим використання терміна гібридний цілком підходить при описі протоколу IGRP.

Протокол OPFS

Відкритий протокол пошуку найкоротшого шляху (Open Shortest Path First - OSPF) використовує алгоритм маршрутизації за станом каналів.

Проблемна група проектування Internet (IETF) розробила протокол OSPF в 1988 році [6]. Остання версія цього протоколу, OSPF версії 2, описана в специфікації RFC 2328. OSPF є протоколом IGP-типу, що передбачає, що цей протокол поширює маршрутну інформацію між маршрутизаторами, що знаходяться в єдиній автономній системі. Протокол OSPF був розроблений для використання в великих мережах, в яких неможливе використання протоколу RIP.

Протокол IS-IS

Протокол обміну маршрутною інформацією між проміжними системами (Intermediate System-to-Intermediate System - IS-IS) використовує алгоритм маршрутизації за станом каналу для стека протоколів моделі OSI. Він поширює маршрутну інформацію для протоколу мережевого обслуговування (Connectionless Network Protocol - CLNP), для відповідних ISO-служб мережевого обслуговування без встановлення з'єднання (Connectionless Network Service - CLNS).

Інтегрований протокол IS-IS є варіантом реалізації протоколу IS-IS для маршрутизації декількох мережевих протоколів, та об'єднує CLNP-маршрути з інформацією про IP-мережі і маски підмереж. Завдяки такому поєднанню ISO CLNS і IP-маршрутизації в одному протоколі інтегрований протокол IS-IS надає альтернативу протоколу OSPF при використанні в IP-мережах.

Протокол BGP

Протокол граничного шлюзу (Border Gateway Protocol - BGP) є прикладом протоколу EGP-типу. Протокол BGP забезпечує обмін маршрутною інформацією між автономними системами і гарантує вибір маршрутів без зациклення. Він є базовим протоколом повідомлень маршрутизації, які використовуються більшістю великих компаній і постачальниками послуг доступу до Internet (ISP). Протокол BGP-4 став першою версією протоколу BGP, в якому вмонтовано безкласову міждоменну маршрутизацію (Classless InterDomain Routing - CIDR), і першим з тих , що використовують механізм агрегації маршрутів. На відміну від поширених

протоколів IGP-типу, таких, як RIP, OSPF і EIGRP, BGP не використовує в якості метрики лічильник вузлів, пропускну здатність або затримку в мережі. Замість цього протокол BGP приймає рішення про вибір маршруту,

Проаналізувавши цю інформацію, приходимо до висновку, що прикордонні PE-маршрутизатори провайдера створюють окрему таблицю маршрутизації для кожного клієнта. Таблиця маршрутизації прикріплюється до того ж інтерфейсу, на якому працює клієнт і використовує клієнтський протокол маршрутизації. З цього можна зробити висновок, що для провайдера не має значення, на якому протоколі побудована мережа клієнта. Отже, я вважаю доцільним використовувати EIGRP.

3.3 Розробка специфікації апаратних засобів комп'ютерної системи

У якості постачальника мережевого та IoT обладнання була обрана компанія "Cisco". "Cisco" - це міжнародна компанія, яка є одним із найбільших у світі виробників обладнання, призначеного для обслуговування мереж віддаленого доступу, сервісів безпеки, мереж зберігання даних, маршрутизації і комутації, а також для потреб комерційного ринку IP-комунікацій і корпоративного ринку. Перевагами компанії "Cisco" є:

- надійність - компанія багато років є лідером ринку і зарекомендувала себе як постачальник якісних апаратних рішень
- ширина модельного ряду - для створення системи знадобиться багато різнопланових пристроїв, і якщо всі вони будуть створені однією компанією, це позитивно позначиться на стабільності та вартості підтримки системи
- гнучкість налаштування системи - внутрішнє програмне забезпечення маршрутизаторів "Cisco" дозволяє налаштовувати обладнання для будь-якої конфігурації і топології мережі
- підтримка - компанія "Cisco" пропонує своїм клієнтам цілодобову підтримку щодо питань пов'язаних з роботою обладнання

- гарантія - компанія “Cisco” пропонує своїм клієнтам гарантію на власне обладнання, яка може бути подовжена. У разі настання гарантійного випадку, клієнт може отримати повну заміну пошкодженого обладнання у строк від 4 до 24 годин.
- безпека - внутрішнє програмне забезпечення компанії відповідає сучасним стандартам безпеки при умові правильного налаштування і конфігурації пристроїв.

Cisco 7200, одні з найпоширеніших в галузі універсальних граничних маршрутизаторів для великих підприємств і операторів зв'язку. Маршрутизатор серії Cisco 7200 відрізняються чудовим співвідношенням ціна / продуктивність, пропонуючи найширший спектр підтримуваних інтерфейсів і неперевершений набір функцій. Компактні за розмірами і побудовані на високопродуктивних модульних процесорах, ці пристрої відрізняються найвищою в галузі експлуатаційною надійністю і зручністю в управлінні. Завдяки модульній архітектурі ці маршрутизатори дозволяють створювати масштабовані рішення, що відповідають самим різним вимогам до щільності, продуктивності і асортименту послуг, одночасно забезпечуючи захист інвестицій з урахуванням майбутнього розвитку мережі.

У числі переваг маршрутизаторів серії Cisco 7200:

- підтримка самого широкого спектру функцій IP / MPLS в програмному забезпеченні Cisco IOS (управління якістю обслуговування, агрегування широкосмугових підключень, безпеку, мультисервісний доступ, мультипротокольну комутацію на основі міток і інші);
- широкий асортимент гнучких, модульних інтерфейсів (від DS0 до OC12);
- підтримка інтерфейсів Fast Ethernet, Gigabit Ethernet, Packet Over Sonet та інших;
- повністю модульна конструкція в форматі 3RU;
- повна підтримка термінації L2TP і PPP;
- підтримка до 16000 широкосмугових абонентських сесій;

- акселератор послуг на базі технології Cisco PXF;
- підтримка різних протоколів;
- низькі початкові капіталовкладення;
- масштабованість і гнучкість;
- ідеально підходять для модернізації мереж.

Рисунок 3.5– Маршрутизатор Cisco серії 7200 в розібраному вигляді

Маршрутизатор серії Cisco 7200 призначені для використання в якості центрального високопродуктивного маршрутизатора великих мереж. Маючи широкий вибір доступних інтерфейсних модулів (порт-адаптерів) він може бути підключений практично до будь-якої мережі, а можливості операційної системи Cisco IOS, дозволяють ефективно маршрутизувати будь-який трафік при практичній відсутності будь-яких обмежень на конфігурацію мережі.

Це дозволяє, зокрема, використовувати маршрутизатори серії 7200 для об'єднання мереж департаментів підприємства (локальних і територіально розподілених), незалежно від застосовуваних у них технологій і їх поточної конфігурації

Модуль обробки (NPE - Network Processing Engine) використовує процесор MIPS RISC і випускається в чотирьох варіантах - 100, 200 і 300 МГц, а також модель NPE-100, яка використовує також процесор 150 Мгц, але не має 1 Мб SRAM, що обмежує його продуктивність. Кожен модуль має 32 Мб оперативної пам'яті, що розширюється до 128 Мб (NPE 300 - до 256) і 8 Мб флеш-пам'яті, що розширюється до 40 Мб.

Набір шасі і модулів NPE серії 7200 надає можливість вибору оптимальної конфігурації і продуктивності при мінімальних витратах і можливості подальшого нарощування потужності пристрою шляхом заміни шасі або модуля NPE. Шасі серії 7200 мають пропускну здатність шини 600 Мбіт / сек. В даний час анонсована серія шасі 7200VXR, яка має шину з пропускною спроможністю 1 Гбіт / сек. Модулі NPE мають наступну продуктивність: NPE-100 - 100 kpps, NPE - 150 kpps, NPE-200 - 200 kpps, NPE-300 - 300 kpps.

Таблиця 3.2 Специфікації

Функція	Опис
Управління	Підтримка всіх функцій ПЗ Cisco IOS. Технологія NetFlow accounting дає можливість зібрати докладну статистику використання мережевих ресурсів для ведення обліку, системи тарифікації та планування майбутнього зростання мережі. Великий спектр функціональності управління смугою пропускання і мережевими перевантаженнями. Агрегування передплатників мереж широкосмугового доступу. Функціональність Service Selection Gateway (SSG) дозволяє реалізувати розмежування доступу до послуг з можливістю динамічного вибору необхідних послуг на основі бажань передплатника. Підтримка технології многопротокольної комутації на основі ознак (MPLS). Можливість інтеграції з шлюзами ОКС-7 для побудови великомасштабних мереж доступу. Гнучкість мультисервісних додатків завдяки вбудованій шині MIX.
Продуктивність	Багатофункціональні платформи Cisco 7200 є ефективну з точки зору вартості систему, яка поєднуватиме в собі можливості підтримки наступних технологій: висока продуктивність завдяки застосуванню технології паралельної швидкісний пересилання PXF (Parallel eXpress Forwarding); гнучка модульна структура, підтримка інтерфейсів Multichannel STM-1, Fast Ethernet, Gigabit Ethernet, Packet Over SONET / SDH і ін .; IP і ATM QoS / CoS; підтримка MPLS VPN і L2TP; різноманіття IP сервісів і термінування PPP; підтримка мультисервісних функцій. Внутрішня шина підтримує MIX (Multiservice Interchange) - комутацію DS0 каналів до будь-якого інтерфейсного модулю.

	Підтримка MIX дозволяє інтегрувати на одному інтерфейсі голос і дані. Cisco 7200 може виступати в ролі гнучкого шлюзу між різними середовищами передачі голосу: ATM, Frame Relay і IP. Cisco 7200 підтримує такі стандарти передачі голосу: VoATM з використанням рівня адаптації ATM Adapter Layer 2 (AAL2); FRF. 11 and FRF. 12; H. 323 v2; Підтримує загальні для серій Cisco 7200, Cisco 7100, Cisco 7400 і Cisco 7500 модулі розширення. Підтримка апаратного прискорення шифрування даних за технологією IPSec (модулі SA-ISA, SA-VAM).
Відмовостійкість	Для забезпечення відмовостійкості системи в пристроях серії Cisco 7200 передбачена можливість підключення двох джерел живлення, а також можливість заміни інтерфейсних модулів без зупинки роботи пристрою. Підтримка маршрутизаторами Cisco 7200 протоколу Cisco IOS Hot Standby Router Protocol (HSRP) забезпечує можливість швидкого переходу на резервне обладнання в разі відмови частини мережевих пристроїв або з'єднань. Резервний внутрішнє джерело живлення забезпечує рівномірне навантаження по харчуванню і подвоює час напрацювання на відмову.
Безпека	Маршрутизатор Cisco серії 7200VXR працюють під управлінням ПО Cisco IOS і дозволяють реалізовувати на практиці сервіси QoS, посилити безпеку і використовувати стиснення і шифрування трафіку. Адаптер ISA (Integrated Services Adapter) реалізує високопродуктивне тунелювання трафіку, а також сервіси шифрування для мереж WAN і VPN. міжмережевий екран, контекстна перевірка трафіку (CBAC) і запобігання мережевих атак (IDS); трансляція мережевих адрес (NAT); фільтри трафіку (ACL); фіксована швидкість доступу (Committed Access Rate, CAR); PPP поверх ATM або Ethernet; Route Bridged Encapsulation; підтримку тунелювання L2TP, PPT і ATMP; підтримку MPLS VPN і Full L2TP; різні додаткові сервіси, в тому числі з апаратними послугами PXF.

Таблиця 3.3 – Технічні характеристики

Характеристики	Опис
Загальна	
Тип пристрою	Тип пристрою
Форм-фактор	Rack-mountable - модульний
Максимальна кількість встановлених модулів	7

Ширина	42.7 cm
Глибина	43.2 cm
Глибина	13.3 cm
пам'ять	
RAM	1 GB DDR SDRAM
Флеш-пам'ять	256 MB
параметри мережі	
Технологія підключення	Wired
Канальний протокол	Ethernet, Fast Ethernet, Gigabit Ethernet
Мережевий / Транспортний протокол	TCP / IP, UDP / IP, PPPoA
Протокол маршрутизації	OSPF, IGRP, RIP, IS-IS, BGP, EIGRP, HSRP
Протокол віддаленого адміністрування	SNMP, Telnet, HTTP
Характеристики	Flow control, modular design, full duplex capability, Layer 2 switching, auto-sensing per device, підтримка DHCP, підтримка VPN, BOOTP support, підтримка ARP, підтримка MPLS, підтримка VLAN, manageable, підтримка IPv6
інтерфейси зв'язку	
Інтерфейси	3 x network - Ethernet 10Base-T / 100Base-TX / 1000Base-T - RJ-45 | 1 x management - console - RJ-45 | 4 x serial - auxiliary - RJ-45 | 1 x management - Ethernet 10Base-T / 100Base-TX - RJ-45 | 2 x USB - 4 PIN USB Тип A

Таблиця 3.4 – Характеристики

Характеристики	Опис
Різне	
Спосіб аутентифікації	Secure Shell (SSH), RADIUS, PAP, CHAP, TACACS
Стандарти	NEBS level 3, FCC Class A certified, CSA, EN 60950, IEC 61000-3-2, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC950, UL 1950 VCCI-II, CSA 22.2 No. 950, EN55022 Class B, AS / NZ 3548 Class A
Живлення	
Пристрій живлення	Блок живлення - redundant
Встановлене кількість / Максимально підтримуваний кількість	2 (встановлено) / 2 (максимально)
необхідну напругу	AC 120/230 V (50/60 Hz)
Попередньо встановлене пристрій харчування	280 Watt
Програмне забезпечення / Системні вимоги	
Попередньо встановлено операційна система	Cisco IOS
Програмне забезпечення Included	Cisco IOS IP Base
Параметри навколишнього середовища	
Мінімальна робоча температура	5 ° C
Максимальна робоча температура	40 ° C

Робочий діапазон вологості	5 - 85%

Одним з ключових пристроїв нашого маршрутизатора є процесорний керуючий модуль NPE-G2 для маршрутизаторів Cisco серії 7200 забезпечує більш високу продуктивність маршрутизації і обробки потоків даних, володіючи найбільш повним набором функцій Cisco IOS.

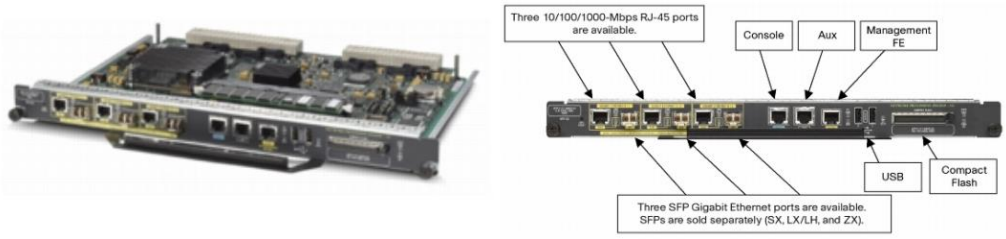

Рисунок 3.6 – Процесорний керуючий модуль NPE-G2

Основні особливості керуючого процесорного модуля NPE-G2:

- подвоєна продуктивність в порівнянні з керуючими модулями попередніх серій (до 2 мільйонів пакетів в секунду при використанні швидкісний пересилання Cisco);
- 3 RJ-45 10/100 / 1000Ethernet порту (з підтримкою динамічного рефлектометра), оптичні порти;
- спеціальний керуючий порт;
- 2 USB порту для підключення резервних носіїв і ключів безпеки;
- 1 Гб ОЗУ;
- Усунення необхідність використання контролерів входу / виходу.

Таблиця 3.5 – Технічні характеристики

Характеристика	Опис
Оперативна пам'ять	ОЗУ: 1 Гб Compact Flash: 256 Мб 2 Мб NVRAM Кеш другого рівня: 1-Мб USB Flash: 64-256 Мб

Процесор	1.67 ГГц Motorola Freescale 7448
Розміри	3,556 x 38, 481 x 28, 245 см

У якості CE-маршрутизаторів були обрані маршрутизатори Cisco серії 2600. Так як модульні маршрутизатори доступу серії CISCO 2600 - це високоефективні мультісервісні пристрої, що забезпечують гнучкість у виборі LAN і WAN конфігурацій, безпеку з'єднання і високу продуктивність. Сукупність цих характеристик робить серію CISCO 2600 ідеальною для створення постійних інтернет-каналів зв'язку між центральним офісом підприємства і його філіями.

Серія Cisco 2600 є економічною серією модульних маршрутизаторів для малих і середніх офісів, що включає в себе можливість передачі голосу і факсу. Пропонований набір модулів дозволяє так само використовувати Cisco 2600 у якості серверів доступу і мережевих екранів. Модульна архітектура цих пристроїв забезпечує гнучке рішення комплексу таких завдань, як:

- Підключення невеликого офісу в загальну корпоративну мережу компанії через комутований або виділений канал, ISDN BRI, мережі загального користування X.25, Frame Relay і Інтернет;
- Забезпечення точки доступу в загальну корпоративну мережу офісу для мобільних користувачів і співробітників, які працюють з дому;
- Побудова віртуальної корпоративної мережі (Virtual Private Network, VPN) через мережу Інтернет;
- Передачу голосу і факсів між офісами поверх мереж комутації пакетів, а так само використання послуг операторів VoIP;
- Маршрутизація даних усередині корпоративної локальної мережі між декількома віртуальними локальними мережами (VLAN);
- Підключення банкоматів і POS-терміналів до центрального процесингового центру.

Для маршрутизаторів Cisco 2600 існує більше 30 мережевих інтерфейсних модулів і карт, що дозволяють використовувати маршрутизатори цієї серії практично в будь-яких існуючих мережах. Є модулі для Ethernet, синхронних і асинхронних послідовних портів, каналів E1 і T1, ATM, аналогових модемів, ISDN BRI, передачі голосу (FXO, FXS, E & M, ISDN BRI-S / T), модуль стиснення даних.

Для передачі критичного до смуги пропускання і затримок трафіку (наприклад, мультимедіа) маршрутизатори Cisco 2600 підтримують гарантовану якість обслуговування (Quality of Service - QoS).

У якості зовнішніх відеокамер було обрано Cisco 7530PD IP Camera (рис 3.6) - відеокамера захищена від впливу навколишнього середовища за стандартом IP67, має достатні кути огляду, режим для роботи вночі та пропонує високу якість отримуваного зображення, що робить її хорошим вибором для встановлення по периметру та на пропускних пунктах.

Рисунок 3.7 – 7530PD IP Camera

Cisco Physical Access Gateway - шлюз контролю фізичного доступу, який можна налаштувати на роботу із більшістю електронних замків із можливістю роботи у автономному режимі при втраті зв’язку з сервером.

Рисунок 3.8 – Cisco Physical Access Gateway

3.4 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства та основних характеристик трафіку з метою підтвердження надійної роботи мережі

У рамках мережі встановлено обладнання Cisco, це маршрутизатори та комутатори.

Вихідний трафік пересилається на маршрутизатор в лінію з пропускною здатністю 1000Мбіт/с. Для того, щоб комутатор не потерпав через надлишковий трафік швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=155 (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахуємо пропускну здатність корпоративної мережі котеджного містечка Sun Coast Dnipro допускаючи, що послугами одночасно користуються 100% користувачів.

Пропускна здатність корпоративної мережі котеджного містечка Sun Coast Dnipro розраховується наступним чином. Загальна кількість

користувачів дорівнює 80. Пропускна здатність мережі на рівні доступу буде дорівнювати:

$$Pр.р = \mu * l * N * 8 = 155 * 650 * 80 * 8 = 59{,}5 \text{ (Мбіт/с)},$$

де N – кількість вузлів в мережі.

Результат дає підстави стверджувати, що перевантажень на обраному обладнанні не буде.

Комутатор рівня доступу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000Мбіт/с. Загальне навантаження на комутатор не повинно перевищувати:

$$\mu вих = 1000\ 000\ 000/(650 * 8) = 20830 \text{ пакетів/с}$$

Максимальне завантаження знаходимо:

$$N = 20830/155 = 134 \text{ джерел}$$

Інтенсивність вихідного трафіку від всіх користувачів дорівнює:

$$\lambda = N * \mu = 80 * 155 = 12400 \text{ (пакетів/с)}$$

Коефіцієнт затримки:

$$\rho = \lambda\, \mu вих = 12400\ 20830 = 0{,}28$$

Коефіцієнт зайнятості комутатора рівня розподілу:

$$r = \rho\, 1 - \rho = 0{,}12\ 1 - 0{,}12 = 0{,}02$$

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

$$T = 1\ (\mu - \lambda) = 1\ 20830 - 12400 = 3{,}2 * 10^{-6} \text{ с}$$

Середня довжина черги:

$$L\text{чер} = \rho\, 2\, 1 - \rho = 0{,}122\, 1 - 0{,}12 = 0{,}001$$

Середній час перебування пакета в черзі:

$$\text{Точ} = L\text{чер}\, \lambda = 0{,}001 \cdot 12400 = 8\text{мкс}$$

Пропускна здатність каналу:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l}$$

$$b = \lambda * l = 12400 * 650 * 8 = 59520000\ \text{біт/с} = 59{,}5\ \text{Мбіт/с}$$

Що є нормою.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

4.1 Розрахунок налаштувань для заданої топології мережі, вибір інтерфейсу каналів зв'язку та протоколу обміну

Сформуємо структурну схему мережі котеджного містечка та виведемо основні показники.

Таблиця 4.1 – Кількість вузлів у підмережах

LAN 1	LAN 2	LAN 3	LAN 4	LAN 5
247	233	39	32	212

Таблиця 4.2 − Схема адресації мережі

Назва мережі	Кількість вузлів	Адреса мережі	Маска мережі	Початкове значення діапазону можливих адрес вузлів у підмережі	Кінцеве значення діапазону можливих адрес вузлів у підмережі
LAN 1	247	192.168.184.0	255.255.255.0	192.168.184.1	192.168.184.254
LAN 2	233	192.168.185.0	255.255.255.0	192.168.185.1	192.168.185.254
LAN 3	39	192.168.187.0	255.255.255.192	192.168.186.1	192.168.186.62
LAN 4	32	192.168.187.64	255.255.255.192	192.168.187.65	192.168.161.126
LAN 5	212	192.168.186.0	255.255.255.0	192.168.186.1	192.168.186.254
WAN 1	2	10.0.23.0	255.255.255.252	10.0.23.1	10.0.23.2
WAN 2	2	10.0.23.4	255.255.255.252	10.0.23.5	10.0.23.6
WAN 3	2	10.0.23.8	255.255.255.252	10.0.23.9	10.0.23.10
WAN 4	2	10.0.23.12	255.255.255.252	10.0.23.13	10.0.23.14
WAN 5	2	10.0.23.16	255.255.255.252	10.0.23.17	10.0.23.18

WAN 6	2	10.0.23.20	255.255.255.252	10.0.23.21	10.0.23.22

В таблиці 4.1 вказані мережі та кількості вузлів. В таблиці 4.2 указана схема адресації мережі. На рисунку 4.1 зображена топологічна схема структури мережі.

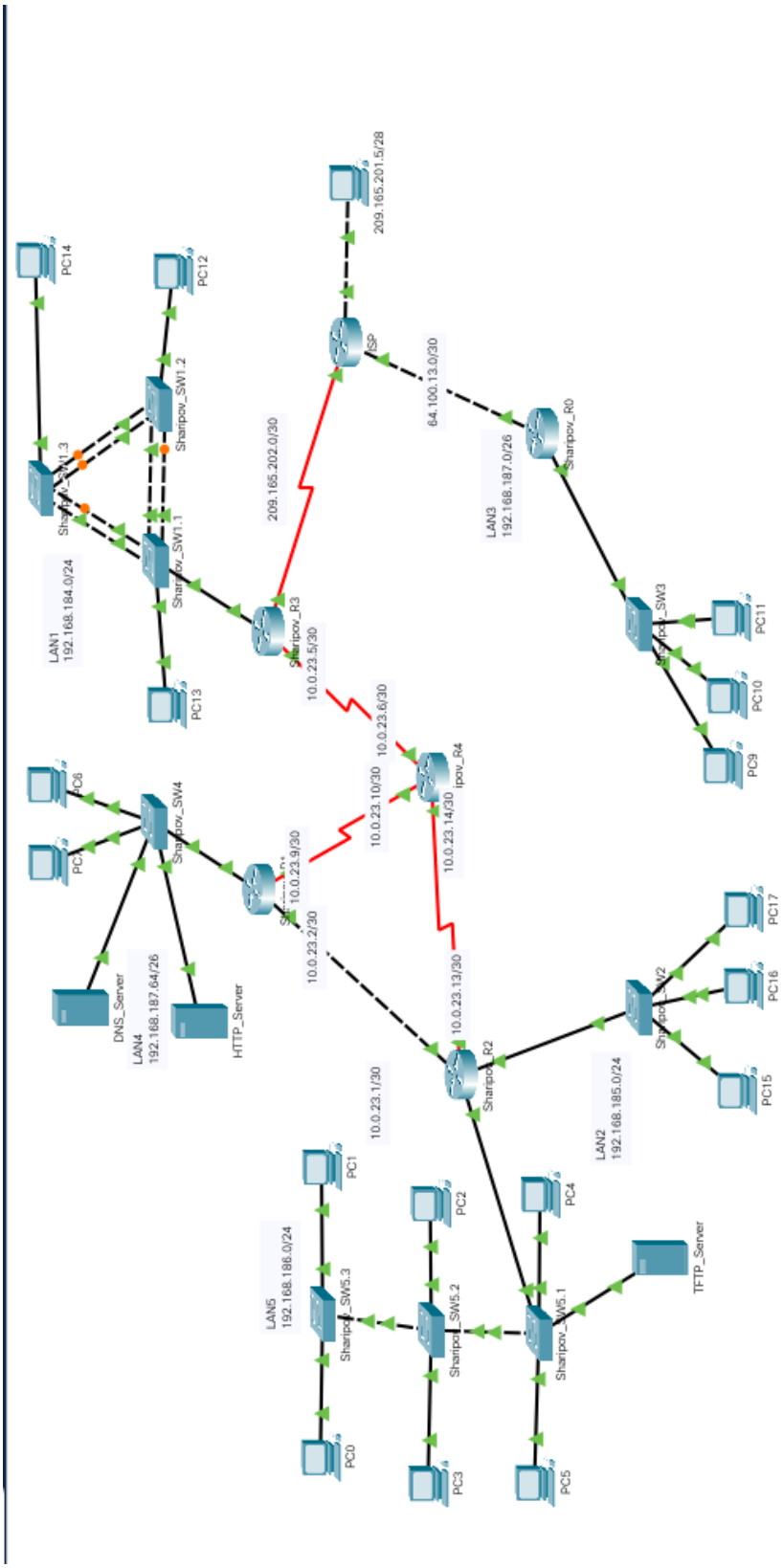

Рисунок 4.1 – Топологічна схема структури мережі

4.2 Налаштування та перевірка роботи комп'ютерної системи

4.2.1 Базове налаштування конфігурації пристроїв

Для налаштування була розроблена базова конфігурація пристроїв:

Приклад налаштування Sharipov_R3:

Router>enable

Router#configure terminal

Router(config)#hostname Sharipov*_R3*

Sharipov*_R3(config)#enable password class*

Sharipov*_R3(config)#username 12317_*Sharipov *password cisco*

Sharipov_R3(config)#ip domain-name Sharipov_R3

Sharipov_R3(config)#banner motd # 123-17-1 Sharipov #

Sharipov_R3(config)#*crypto key generate rsa general-keys modulus 1024*

Sharipov_R3(config)#line con 0

Sharipov_R3(config-line)#password cisco

Sharipov_R3(config-line)#login

Sharipov_R3(config-line)#line vty 0 4

Sharipov_R3(config-line)#password cisco

Sharipov_R3(config-line)#login

Sharipov_R3(config-line)#transport input ssh

Sharipov_R3(config-line)#line vty 5 15

Sharipov_R3(config-line)#password cisco

Sharipov_R3(config-line)#login

Sharipov_R3(config-line)#transport input ssh

Sharipov_R3(config-line)#service password-encryption

Sharipov_R3#copy running-config startup-config

4.2.2 Налаштування маршрутизаторів корпоративної мережі

Для коректної роботи системи потрібно налаштувати маршрутизацію. За вимогами потрібно використовувати протокол динамічної маршрутизації EIGRP.

Приклад налаштування EIGRP:

Sharipov_R3*(config)#router eigrp 23*

Sharipov_R3*(config-router)#network 192.168.184.0 0.0.0.255*

Sharipov_R3*(config-router)#network 10.0.23.1 0.0.0.3*

Sharipov_R3*(config-router)#network 10.0.23.5 0.0.0.3*

Sharipov_R3*(config-router)#network 10.0.23.9 0.0.0.3*

```
    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D      10.0.23.0/30 [90/21026560] via 10.0.23.6, 00:09:32, Serial0/1/0
C      10.0.23.4/30 is directly connected, Serial0/1/0
L      10.0.23.5/32 is directly connected, Serial0/1/0
D      10.0.23.8/30 [90/21024000] via 10.0.23.6, 00:10:09, Serial0/1/0
D      10.0.23.12/30 [90/21024000] via 10.0.23.6, 00:10:03, Serial0/1/0
    192.168.184.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.184.0/24 is directly connected, FastEthernet0/0
L      192.168.184.1/32 is directly connected, FastEthernet0/0
D   192.168.185.0/24 [90/21026560] via 10.0.23.6, 00:09:17, Serial0/1/0
D   192.168.186.0/24 [90/21026560] via 10.0.23.6, 00:09:12, Serial0/1/0
    192.168.187.0/26 is subnetted, 1 subnets
D      192.168.187.64/26 [90/21026560] via 10.0.23.6, 00:08:20, Serial0/1/0
    209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.202.0/30 is directly connected, Serial0/0/0
L      209.165.202.2/32 is directly connected, Serial0/0/0
```

Рисунок 4.2 – Маршрутизація EIGRP

4.2.3 Налаштування роботи Інтернет

Для роботи працівників підприємства та коректної роботи системи взагалі потрібно налаштувати Інтернет провайдера. Як інтернет провайдер було обрано Трайфл, цей інтернет провайдер має покриття в будівлі підприємства.

Щоб пристрої підприємства мали доступ в інтернет потрібно налаштувати NAT. Приклад налаштування NAT:

Sharipov_R3*(config)#access-list 23 permit 192.168.184.0 0.0.7.255*

Sharipov_R3*(config)#ip nat inside source list 23 pool Internet*

Статичний NAT на Sharipov_R3:

Sharipov_R3*(config)#ip nat inside source static 192.168.184.179 209.165.200.4*

4.2.4 Налаштування агрегування каналів PAgP

Протокол PAgP використовується в системі для забезпечення відмовостійкості мережі рівня доступу.

Для інтегрування PAgP потібно налаштувати три коммутатора Sharipov_SW1.1, Sharipov_SW3.2 та Sharipov_SW3.3.

Приклад налаштування Port-channel 1:

Sharipov_SW1.1*(config)#interface range f0/1-2*

Sharipov_SW1.1*(config-if-range)#switchport mode trunk*

Sharipov_SW1.1*(config-if-range)#channel-group 1 mode auto*

Sharipov_SW1.1*(config-if-range)#interface Port-channel 1*

Sharipov_SW1.1*(config-if)#switchport mode trunk*

Приклад налаштування Port-channel 2:

Sharipov_SW1.1*(config)#interface range f0/3-4*

Sharipov_SW1.1*(config-if-range)#switchport mode trunk*

Sharipov_SW1.1*(config-if-range)#channel-group 2 mode auto*

Sharipov_SW1.1*(config-if-range)#interface Port-channel 2*

Sharipov_SW1.1*(config-if)#switchport mode trunk*

Для подальшого налатуваня PAgP потрібно налаштувати інтерфейси на відповідний Port-channel.

4.2.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Для налаштування каналу зв’язку між мережею головної будівлі та віддаленою мережею потрібно налаштувати зв’язок завдяки VPN з'єднанню.

Для встановлення зв’язку VPN було обрано протокол GRE з шифруванням IPSEC. Налаштування gre:

Sharipov_R3*(config)#interface Tunnel0*

Sharipov_R3*(config-if)#ip address 10.0.23.13 255.255.255.252*

Sharipov_R3*(config-if)#tunnel destination 209.165.202.2*

Sharipov_R3*(config-if)#tunnel source FastEthernet 0/0*

Налаштування параметрів 1 фази ISAKMP

Sharipov_R3(config)#crypto isakmp policy 23

Sharipov_R3(config-isakmp)#encryption aes

Sharipov_R3(config-isakmp)#authentication pre-share

Sharipov_R3(config-isakmp)#group 2

Sharipov_R3(config-isakmp)#exit

Sharipov_R3(config)#crypto isakmp key cisco address 64.100.13.2

Налаштування параметрів 2 фази ISAKMP

Sharipov_R3(config)#crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac

Sharipov_R3(config)#crypto map VPN-MAP 23 ipsec-isakmp

Sharipov_R3(config-crypto-map)#description VPN connection to Sivruk _R2

Sharipov_R3(config-crypto-map)#set peer 64.100.13.2

Sharipov_R3(config-crypto-map)#set transform-set VPN-CONF

Sharipov_R3(config-crypto-map)#match address 110

Sharipov_R3(config-crypto-map)#exit

Налаштування криптографічного порівняння

Sharipov_R3(config)#interface Serial 0/0/1

Sharipov_R3(config-if)#crypto map VPN-MAP

4.2.6 Перевірка роботи комп’ютерної системи

Перевірка комп’ютерної системи буде виконуватись завдяки комаді ping та вбудованим методам аналізу трафіку у Packet Tracer. Для виконання

перевірки було надіслано пакети ICPM за допомогою команди ping, зображено на рис 4.3, 4.4.

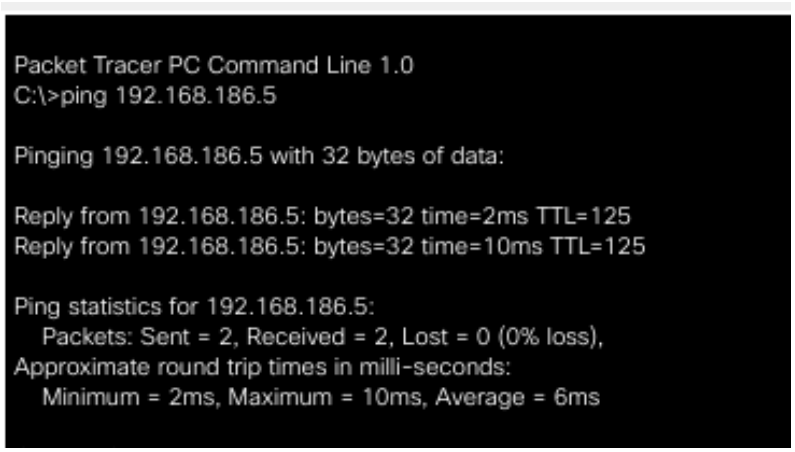

Рисунок 4.3 – Відправка ICMP пакетів у мережу LAN5

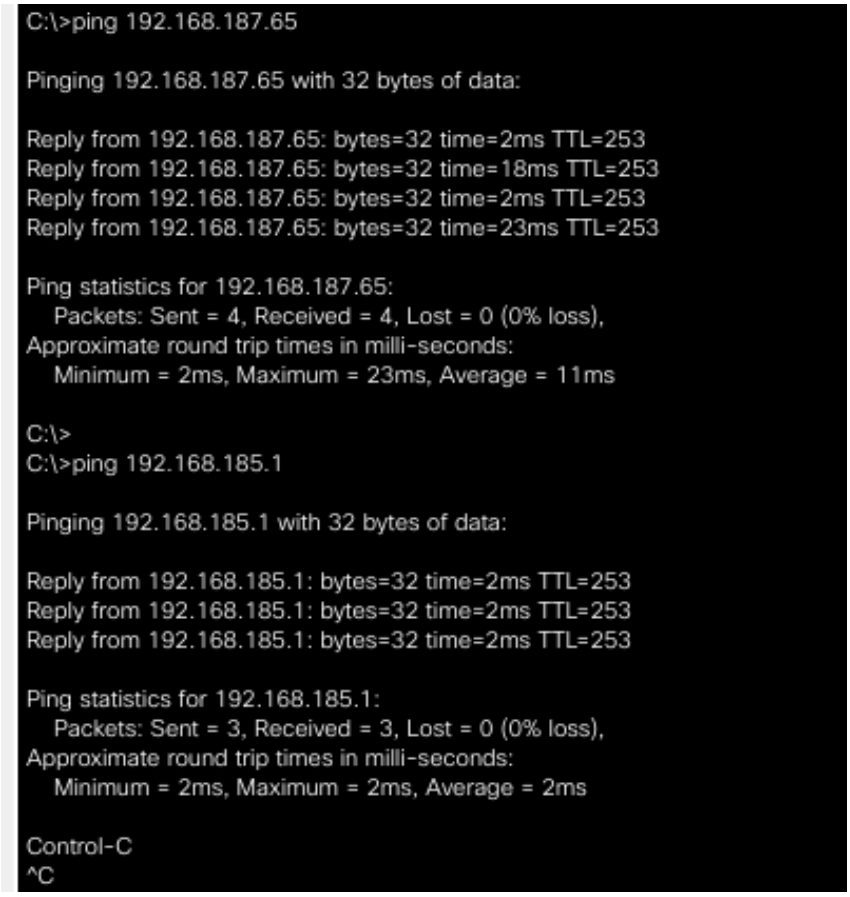

Рисунок 4.4 – Відправка ICMP пакетів у мережу LAN2 та LAN4

Перевірка SSH виконується завдяки команді ssh -l username ipaddress. Результат перевірки зображено на рис. 4.5

Рисунок 4.5 – Перевірка налаштування SSH

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Методи для захисту інформації в комп'ютерній системі

Методи захисту комп'ютерів від несанкціонованого доступу діляться на програмно-апаратні і технічні. Перші відсікають неавторизованих користувачів, другі призначені для виключення фізичного проникнення сторонніх людей в приміщення компанії.

Створюючи систему захисту інформації (СЗІ) в організації, слід враховувати, наскільки велика цінність внутрішніх даних в очах зловмисників.

Для грамотного захисту від несанкціонованого доступу важливо зробити наступне:

- впорядкувати і розбити інформацію на класи, визначити рівні допуску до даних для користувачів;
- оцінити можливості передачі інформації між користувачами (встановити зв'язок співробітників один з одним).

В результаті цих заходів з'являється певна ієрархія інформації в компанії. Це дає можливість розмежування доступу до відомостей для співробітників залежно від роду їх діяльності.

Аудит доступу до даних повинен входити в функціонал засобів інформаційної безпеки. Крім цього, програми, які компанія вирішила використовувати, повинні включати наступні опції:

- аутентифікація та ідентифікація при вході в систему;
- контроль допуску до інформації для користувачів різних рівнів;
- виявлення та реєстрація спроб несанкціонованого доступу;
- контроль працездатності використовуваних систем захисту інформації;
- забезпечення безпеки під час профілактичних або ремонтних робіт.

Ідентифікація та аутентифікація користувачів

Для виконання цих процедур необхідні технічні засоби, за допомогою яких проводиться двоступеневе визначення особистості і справжності повноважень користувача. Необхідно враховувати, що в ході ідентифікації необов'язково встановлюється особа. Можливо прийняття будь-якого іншого ідентифікатора, встановленого службою безпеки.

Після цього слід аутентифікація - користувач вводить пароль або підтверджує доступ до системи за допомогою біометричних показників (сітківка ока, відбиток пальця, форма кисті і т. п.). Крім цього, використовують аутентифікацію за допомогою USB-токенів або смарт-карт. Цей варіант слабкіше, так як немає повної гарантії збереження або справжності таких елементів.

Протоколи секретності для паперової документації

Незважаючи на повсюдну ціфровизацію, традиційні паперові документи, як і раніше використовуються в організаціях. Вони містять велику кількість інформації - бухгалтерські відомості, маркетингову інформацію, фінансові показники та інші критичні дані. Отримавши ці документи, зловмисник може проаналізувати масштаби діяльності організації, дізнатися про напрямки фінансових потоків.

Для захисту документів, які містять відомості критичної важливості, використовуються спеціальні протоколи секретності. Зберігання, переміщення і копіювання таких файлів проводиться за спеціальними правилами, що виключає можливість контакту з сторонніми особами.

Для захисту інформації, що зберігається на жорстких дисках комп'ютерів, використовуються багатоступінчасті засоби шифрування та авторизації. При завантаженні операційної системи використовується складний пароль, який неможливо підібрати звичайними методами. Можливість входу в систему користувача з боку виключається шляхом шифрування даних в BIOS і використання паролів для входу в розділи диска.

Для особливо важливих пристроїв слід використовувати модуль довіреної завантаження. Це апаратний контролер, який встановлюється на

материнську плату комп'ютера. Він працює тільки з довіреними користувачами і блокує пристрій при спробах включення за відсутності власника.

Також застосовуються криптографічні методи шифрування даних, що перетворюють текст «поза системою» в нічого не значущий набір символів.

Ці заходи забезпечують захист відомостей і дозволяють зберегти їх в недоторканності.

З методичної точки зору процес захисту інформації можна розділити на чотири етапи:

- запобігання - профілактичні заходи, щоб обмежити доступ сторонніх осіб;
- виявлення - комплекс дій, що вживаються для виявлення зловживань;
- обмеження - механізм зниження втрат, якщо попередні заходи зловмисникам вдалося обійти;
- відновлення - реконструкція інформаційних масивів, яка проводиться за схваленою і перевіреної методикою.

Кожен етап вимагає використання власних засобів захисту інформації, проведення спеціальних заходів. Необхідно враховувати, що наведене поділ умовно. Одні і ті ж дії можуть бути віднесені до різних рівнів.

Комп'ютери, підключені до Інтернету, постійно піддаються ризику зараження шкідливим програмним забезпеченням. Існує маса ПЗ, призначеного для відстеження паролів, номерів банківських карт і інших даних. Нерідко віруси містяться в розсилках електронної пошти, потрапляють в систему через сумнівні мережеві ресурси або викачані програми.

Для захисту системи від шкідливих програм, необхідно використовувати антивірусні програми, обмежити доступ в Мережу на певні сайти. Якщо в організації паралельно використовуються локальні мережі, слід встановлювати файрволи (міжмережеві екрани).

Більшість користувачів зберігає інформацію в окремих папках, які названі «Паролі», «Мої карти» і т. п. Для зловмисника такі назви є підказками. У назвах таких файлів необхідно використовувати комбінації букв і цифр, нічого не говорять стороннім людям. Також рекомендується шифрувати цінні дані в комп'ютерах і періодично проводити їх резервне копіювання.

Грамотне використання систем захисту інформації дозволяє досягти сприятливих результатів:

- зменшити ризики втрати репутації та втрати грошових коштів;
- виключити втрати наукових розробок, інтелектуальної власності, особистих даних;
- знизити витрати на заходи щодо захисту інформації, виключення стороннього доступу до цінних відомостей.

Несанкціонований доступ до інформації можливий у будь-якій системі - від невеликих організацій до великих державних структур. Уважне ставлення до захисту відомостей, створення підрозділів інформаційної безпеки дозволяють мінімізувати втрати і запобігти спробам розкрадання або копіювання даних. Окрему увагу слід приділяти роботі з авторизованими співробітниками, які мають доступ до критичної інформації. Заходи захисту повинні бути прийняті завчасно, оскільки поступитися ініціативу - значить допустити втрату даних.

5.2 Налаштування маршрутизаторів на підтримку служби AAA

Службу AAA потрібно встановити для забезпечення централізованого керування паролями на мережеві пристрої. Для налаштування служби AAA потрібно налаштувати RADIUS сервер як на рис. 5.1.

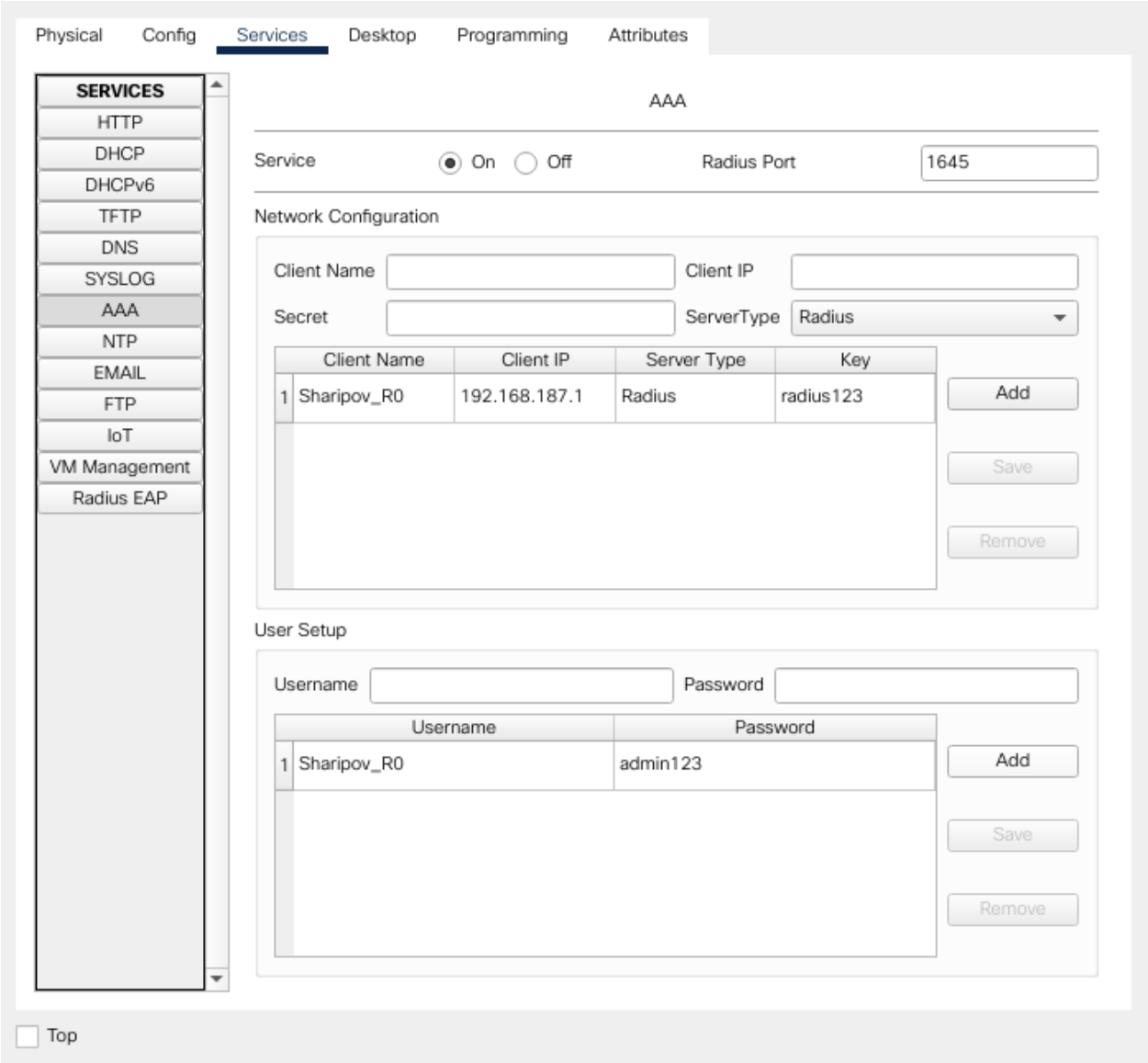

Рисунок 5.1 – Налаштування RADIUS сервера

Налаштування AAA:

Sharipov_R0*(config)#aaa*

Sharipov_R0*(config)#aaa new-model*

Sharipov_R0*(config)#radius-server host 192.168.187.223 key radius123*

Sharipov_R0*(config)#aaa authentication login default group radius local*

Sharipov_R0*(config)#line vty 0 5*

Sharipov_R0*(config-line)#login authentication default*

5.3 Налаштування мереж VLAN

Таблиця 5.1 – Назви VLAN для комерційного відділу

Номер VLAN	Ім’я VLAN	Примітка
1	default	Не використовується
33	Guard	Для охорони
43	Guest	Для гостей
53	Work	Для робітників
99	Management	Для управління
100	Native	Власна мережа

Налаштування VLAN тегів Sharipov_SW5.1:

Sharipov_SW5.1*(config-vlan)#vlan 33*

Sharipov_SW5.1*(config-vlan)#name* Guard

Sharipov_SW5.1*(config-vlan)#vlan 43*

Sharipov_SW5.1*(config-vlan)#name* Guest

Sharipov_SW5.1*(config-vlan)#vlan 53*

Sharipov_SW5.1*(config-vlan)#name* Work

Sharipov_SW5.1*(config-vlan)#vlan 99*

Sharipov_SW5.1*(config-vlan)#name Management*

Sharipov_SW5.1*(config-vlan)#vlan 100*

Sharipov_SW5.1*(config-vlan)#name Native*

Налаштування транку:

Sharipov_SW5.1*(config)#interface range f0/1-2*

Sharipov_SW5.1*(config-if-range)#switchport trunk native vlan 100*

Sharipov_SW5.1*(config-if-range)#switchport mode trunk*

Налаштування портів доступу:

Sharipov_SW5.1*(config)#interface range f0/5-10*

Sharipov_SW5.1*(config-if-range)#switchport mode access*

Sharipov_SW5.1*(config-if-range)#switchport access vlan 33*

5.4 Налаштування параметрів безпеки комутаторів та адресації ПК в мережах VLAN

5.4.1 Налаштування параметрів безпеки комутаторів

Налаштування безпеки портів на комутаторі Sharipov_SW5.1:

Sharipov_SW5.1*(config)#interface fastEthernet 0/9*

Sharipov_SW5.1*(config-if)#switchport mode access*

Sharipov_SW5.1*(config-if)#switchport port-security*

Sharipov_SW5.1*(config-if)#switchport port-security maximum 2*

Sharipov_SW5.1*(config-if)#switchport port-security mac-address 00FF.BA90.87AB*

5.4.2 Налаштування адресації ПК в мережах VLAN

Для забезпечення коректної роботи VLAN потрібно налаштувати адресацію. Для налаштування адресації потрібно налаштувати інкапсуляцію dot1Q.

VLAN 33:

Sharipov_R2*(config)#iinterface FastEthernet0/1.33*

Sharipov_R2*(config-subif)#encapsulation dot1Q 33*

Sharipov_R2*(config-subif)#ip address 192.168.186.1 255.255.255.224*

VLAN 43:

Sharipov_R2*(config-if)#interface FastEthernet0/1.43*

Sharipov_R2*(config-subif)#encapsulation dot1Q 40*

Sharipov_R2*(config-subif)#ip address 192.168.186.65 255.255.255.224*

VLAN 50:

Sharipov_R2*(config-if)#interface FastEthernet0/1.50*

Sharipov_R2*(config-subif)#encapsulation dot1Q 50*

Sharipov_R2*(config-subif)#ip address 192.168.186.129 255.255.255.224*

VLAN 99:

Sharipov_R2*(config)#interface fastEthernet 0/1.99*

Sharipov_R2*(config-subif)#encapsulation dot1Q 99*

Sharipov_R2*(config-subif)#ip address 192.168.186.193 255.255.255.224*

ВИСНОВКИ

В результаті виконання випускної кваліфікаційної роботи була спроектована і налаштована модель корпоративної мережі котеджного містечка Sun Coast Dnipro.

Були вирішені наступні завдання:

- Проведено аналіз існуючих рішень на основі якого був зроблений вибір;
- Вивчено базові настройки міжмережевої операційної системи Cisco IOS;
- Сформовано вимоги до отриманої системи
- Мережа спроектована і налаштована за всіма вимогами
- Проведено випробування роботи мережі, в ході яких були підтверджені вивчені теоретичні знання, а також відповідність віртуальних приватних мереж технічним завданням.

Таким чином, в результаті вирішення зазначених завдань можна сказати що поставлена в випускній кваліфікаційній роботі мета досягнута.

ПЕРЕЛІК ПОСИЛАНЬ

1 Воробьёва Н.И., Корнейчук В.И., Савчук Е.В. Надёжность компьютерных систем. – К.: «Корнійчук», 2002. – 144 с.

2 Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 172 с.

3 Цвіркун Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посіб. [Електронний ресурс] / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова ; під заг. ред. проф. Л.І. Цвіркуна ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». –

4 Цвіркун Л.І. Інженерна та комп'ютерна графіка. AutoCAD : навч. посіб. / Л.І. Цвіркун, Л.В. Бешта ; під. заг. ред. Л.І. Цвіркуна ; М-во освіти і науки України, НТУ “Дніпровська політехніка”. – Дніпро: НТУ “ДП” , 2018. – 209 с. – ISBN 978-966-350-663-0.

5 Цвіркун, Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с. – ISBN 978-966-350-595-4.

6 Цвіркун Л.І. Глобальні комп’ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с. – ISBN 978-966-350-417-9.

7 Дипломування. Методичні вказівки для бакалаврів галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова ; М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2016. – 56 с.

8 Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні 49 технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В.

Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с

9 Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.

10 Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

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

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

текст програми

804.02070743.21023-01 12 01

Листів 7

2021

АНОТАЦІЯ

Дана програма містить в собі частину коду для налаштування корпоративної мережі підприємства.

ЗМІСТ

Шифрування паролів

service password-encryption

Ім’я пристрою

hostname Sharipov_R0

Налаштування DHCP

ip dhcp pool dhcp

network 192.168.187.64 255.255.255.192

default-router 192.168.187.65

Налаштування WAN

interface FastEthernet0/0

ip address 10.0.23.2 255.255.255.252

duplex auto

speed auto

!

interface Serial0/0/0

ip address 10.0.23.9 255.255.255.252

clock rate 2000000

!

Налаштування LAN

interface FastEthernet0/1

ip address 192.168.187.65 255.255.255.192

duplex auto

speed auto

!

Налаштування EIGPR

router eigrp 23
network 10.0.23.0 0.0.0.3
network 10.0.23.8 0.0.0.3
network 192.168.187.64 0.0.0.63
!

Налаштування паролів на vty та привілейований режим
line con 0
password 7 0822455D0A16
login
!
line aux 0
!
line vty 0 4
password 7 0822455D0A16
login
transport input ssh

Налаштування паролів на ssh
line vty 5 15
password 7 0822455D0A16
login
transport input ssh

Налаштування AAA
aaa new-model
aaa authentication login 12317_Sharipov group radius local
aaa authentication login default local

Налаштування VPN

crypto isakmp policy 10

encryption aes

authentication pre-share

group 2

!

crypto isakmp key cisco address *209.165.202.2*

!

crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac

!

crypto map vpn 23 ipsec-isakmp

description VPN connection to Sharipov_R0

set peer *209.165.202.2*

set transform-set vpn-conf

match address 110

!

no ip domain-lookup

Налаштування VLAN

interface FastEthernet0/1.33

encapsulation dot1Q 33

ip address 192.168.186.1 255.255.255.224

interface FastEthernet0/1.43

encapsulation dot1Q 40

ip address 192.168.186.65 255.255.255.224

interface FastEthernet0/1.50

encapsulation dot1Q 50

ip address 192.168.186.129 255.255.255.224

interface fastEthernet 0/1.99

encapsulation dot1Q 99

ip address 192.168.186.193 255.255.255.224

Налаштування домену

ip domain-name Sharipov_R3

Налаштування банеру

banner motd # 123-17-1 Sharipov #

Налаштування ключу RSA

crypto key generate rsa general-keys modulus 1024