Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Пастушкова Дмитра Сергійовича

на здобуття ступеня вищої освіти Бакалавра

Розподілена інформаційно-телекомунікаційна система торгівельного підприємства

Галузь знань 12 – Інформаційні технології
Спеціальність 123 – Комп'ютерна інженерія
Освітня програма Програмування та захист комп`ютерних систем і мереж

Шифр КРБКІ. 2001120.20.01.04 ПЗ

Виконав студент 4 курсу група КІ-20-1 Дмитро ПАСТУШКОВ
Керівник канд. техн. наук, доцент Володимир ДЖУЛІЙ
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ
19 06 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Комп'ютерна інженерія

Освітня програма Програмування та захист комп`ютерних систем і мереж

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Пастушкову Дмитру Сергійовичу

1 Тема роботи Розподілена інформаційно-телекомунікаційна система торгівельного підприємства

Керівник роботи Володимир Джулій
Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи розроблено модель розподіленої інформаційно-телекомунікаційної мережі для торгівельного підприємства в програмі cisco packet tracer

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Аналіз розроділеної інформаційно-телекомунікаційної системи торгівельного підприєства, основні типи загроз розподілених інформаційно-телекомунікаційних систем, актуальність та передумови створення систем захисту комп'ютерних мереж, засоби для створення моделі розподіленої інформаційно-телекомунікаційної мережі в cisco packet tracer, моделювання мережі для торгівельного приміщення, моделювання мережі для головного офісу, тестування змодельованої розподіленої інформаційно-телекомунікаційної мережі торгівельного підприємства, реалізація змодельованої мережі, висновки, перелік джерел, додатки

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Логічна схема мережі, фізична схема мережі, фізична схема мережі, торгівельного підприємства, фізична схема мережі головного офісу

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прий
Нормоконтроль	Мостовий С.В., старший викладач кафедри кібербезпеки		

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Січень-Лютий	Виконано
Ознайомлення з предметною областю	Лютий	Виконано
Дослідження існуючих рішень	Лютий	Виконано
Постановка задачі	Березень	Виконано
Визначення загальних принципів рішення задачі	Березень	Виконано
Деталізація принципів рішення задачі	Квітень	Виконано
Розробка проєктних рішень	Квітень	Виконано
Апробація проєктних рішень	Травень	Виконано
Оформлення пояснювальної записки згідно вимог	Травень	Виконано
Оформлення графічної частини	Червень	Виконано
Захист КР	Червень	Виконано

Студент Дмитро ПАСТУШКО

Керівник кваліфікаційної роботи Володимир ДЖУЛ

АНОТАЦІЯ

Тема кваліфікаційної роботи: Розподілена інформаційно-телекомунікаційна система торгівельного підприємства.

Автор роботи: Пастушков Дмитро Сергійович.

Керівник роботи: Джулій Володимир Миколайович.

Пояснювальна записка: 61 с., 4 додатка, 18 рис., 1 табл., 38 джерел.

Графічна частина: 4 плакати.

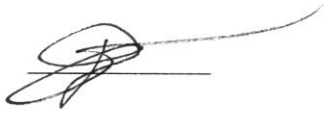
CISCO ASA, CISCO PACKET TRACER, ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНА СИСТЕМА, КІБЕРЗАХИСТ, МАРШРУТИЗАТОР, РОЗПОДІЛЕНА СИСТЕМА, ТОРГІВЕЛЬНЕ ПІДПРИЄМСТВО.

Метою цієї роботи була розробка моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства. Головним завданням було забезпечити високий рівень безпеки та швидкодії мережі.

Для досягнення цих цілей було проведено дослідження і аналіз інструменів наявних в програмі cisco packet tracer, а також теоретичної інформації про такі системи і їх моделі створення.

Розроблено модель розподіленої інформаційно-телекомунікаційної системи для торгівельного підприємства за допомогою програмного забезпечення cisco packet tracer та здійснено налаштування мережевих пристроїв для забезпечення захисту та швидкодії мережі.

11.06.2024



Зм						
Розробив	Пастушков Д.С.			Розподілена інформаційно-телекомунікаційна система торгівельного підприємства Пояснювальна записка	Літера	Аркуш 2	Аркушів
Перевірив	Джулій В.М.				Н		
Н.контр.	Мостовий С.В.				ХНУ, КІ1-20-1		
Затвер.	Кльоц Ю.П.						

ANNOTATION

Course project: Distributed information and telecommunication system of a trading enterprise.

Author of the work: Pastushkov Dmitry Sergeevich.

Supervisor: Dzhulii Volodymyr Mykolaiovych.

Amount: 61 p., 5 appendices, 18 figures, 1 table, 38 sources.

Graphic part: 4 slides.

CISCO ASA, CISCO PACKET TRACER, INFORMATION AND TELECOMMUNICATION SYSTEM, CYBER DEFENSE, ROUTER, DISTRIBUTED SYSTEM, COMMERCIAL ENTERPRISE.

The purpose of this work was to develop a cybersecurity model for a distributed information and telecommunication system of a trading enterprise. The main task was to ensure a high level of security and network performance.

To achieve these goals, we studied and analyzed the field of access control systems, existing methods of protection based on Bluetooth technology, as well as theoretical information about such systems and their creation models. Based on the analysis, a system was developed that can detect data leaks in access control systems using Bluetooth technology.

To achieve these goals, we studied and analyzed the tools available in the cisco packet tracer program, as well as theoretical information about such systems and their creation models.

A model of a distributed information and telecommunication system for a trade enterprise was developed using cisco packet tracer software and network devices were configured to ensure network security and performance.

11.06.2024

ЗМІСТ

ВСТУП

У сучасному суспільстві комп'ютерні мережі є однією з основних складових будь-якого підприємства. Комп'ютерна мережа - це складна система, що складається з апаратного та програмного забезпечення, яка забезпечує обмін даними між комп'ютерними пристроями (наприклад, ПК, серверами, комутаторами, маршрутизаторами та пристроями зберігання даних). Мережі є важливим елементом сучасної глобалізації, а передача інформації є не тільки зручним засобом комунікації, але й одним з основних елементів комфорту в розумінні людини 21-го століття.

Комп'ютерні мережі широко використовуються в державних і комерційних організаціях через їх широкий спектр функцій і можливостей. Інтеграція ключових функціональних підрозділів, ресурсів та інших пристроїв в єдину систему дозволяє значно оптимізувати і прискорити багато процесів, а також централізувати управління та адміністрування.

У той же час, зростання ролі та поширення мережевих технологій поставило на порядок денний питання забезпечення безпеки інформаційних систем. Разом з розвитком комп'ютерних мереж, впровадженням сучасних рішень та загальним процесом модернізації, зловмисники розробляють нові способи отримання несанкціонованого доступу до системних ресурсів, шукають нові вразливості в програмному та апаратному забезпеченні та створюють спеціальні програми для різних протиправних дій [1].

З початку збройного вторгнення російської федерації у 2014 році потреба та актуальність захисту інформаційних систем України багаторазово зросла, а після повномасштабного вторгнення у 2022 році інформаційні атаки з боку держави-окупанта, на відміну від мережевих атак окремих осіб чи груп, характеризуються більшою потужністю та небезпекою, а тому стали загальною стали загальною необхідністю. Саме тому створення добре спланованої, якісної та комплексної системи інформаційної безпеки є не лише важливим, але й

необхідним елементом корпоративного управління.

Забезпечення не лише працездатності системи, а й безпеки її окремих складових, зокрема ресурсів, пов'язаних з інформацією з обмеженим доступом, є надзвичайно важливим та актуальним завданням сьогодення. У цьому контексті важливим є проектування багаторівневих систем захисту інформації в корпоративному середовищі.

Об'єктом дослідження є інформаційно-комунікаційні системи торговельних підприємств.

Предметом дослідження є комплекс програмно-технічних засобів, спрямованих на забезпечення кібербезпеки досліджуваних інформаційно-комунікаційних систем.

Для досягнення поставленої мети необхідно було вирішити наступні завдання:

− вивчити поняття розподілених інформаційно-комунікаційних систем та їх безпеки;

− систематизувати основні причини виникнення проблем безпеки в інформаційно-комунікаційних системах;

− розглянути основні види загроз для розподілених інформаційно-комунікаційних систем;

− проаналізувати безпеку досліджуваних розподілених інформаційно-комунікаційних систем;

− розробити проект розподіленої інформаційно-комунікаційної системи, що досліджується, з урахуванням вимог кіберзахисту;

− виконати базову конфігурацію засобів захисту в моделі кіберзахисту запропонованої інформаційно-комунікаційної системи; Розробити базову конфігурацію засобів захисту в моделі кіберзахисту запропонованої інформаційно-комунікаційної системи.

1 АНАЛІЗ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ТОРГІВЕЛЬНОГО ПІДПРИЄМСТВА

1.1 Розподілена інформаційно-телекомунікаційна система торгівельно підприємства

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1].

При цьому під інформаційною системою розуміється організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів [1]. А під телекомунікаційною системою − сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [1].

Також під інформаційно-телекомунікаційною системою розуміють сукупність каналів, об’єктів і засобів зв’язку, а також інформаційні ресурси у вигляді інформації і апаратно-програмних засобів, призначених для прийому, передачі, накопичення, обробки і зберігання даних.

Розподілена інформаційно-телекомунікаційна система – це набір незалежних комп’ютерів, які користувач сприймає як єдину об’єднану систему. Всі робочі станції автономні, а в якості програмного забезпечення користувачами використовується єдина система [3].

Наявність у торгівельного підприємства телекомунікаційної системи, її подальша модернізація та розвиток створюють нові можливості інтеграційного характеру:

− єдину інформаційно-мережеву взаємодію всіх учасників торгівельного процесу;

− використання загальносистемних сервісів, до яких відносяться мережевий друк, використання спеціальних додатків для колективної роботи фахівців торгівельного підприємства;

− рішення задач торгівлі за рахунок спеціалізованих прикладних програмних продуктів;

− можливість створення дієвих механізмів інформаційної безпеки в процесі комунікації фахівців підприємства.

Якщо порівнювати розподілені інформаційно-телекомунікаційні системи з корпоративними мережами з доступом до Інтернет, то до перших вищі вимоги з точки зору кібербезпеки. Для корпоративних мереж стандартні засоби безпеки зазвичай добре показують себе при вирішенні питання захисту внутрішньої мережі від зловмисників.

Зазвичай в розподілених інформаційних системах використовуються відкриті канали передачі даних, тому для них типовими і найпоширенішими є віддалені атаки. При цьому зловмисник має змогу здійснювати не лише пасивний збір інформації, яка циркулює в системі, але й змінювати, підміняти чи якимось іншим чином впливати на неї [2].

Захищеність інформаційно-телекомунікаційних систем як правило розуміють як [4]:

− набір технологічних прийомів та засобів, які використовуються для забезпечення захисту компонентів інформаційної системи;

− зведення до мінімуму ризику для складових інформаційно-телекомунікаційної системи;

− сукупність логічних і фізичних заходів, які направлені на захист від загроз інформації та складових інформаційно-телекомунікаційної системи.

Вимоги до кібербезпеки розподілених інформаційних систем необхідно формально визначати. Дотримання вимог гарантує, що у разі появи загроз різної

природи, які були передбачені в вимогах до кібербезпеки, система збереже свою функціональність в повному обсязі. Якщо технічні умови функціонування системи були правильно визначені, то безпека системи має бути оцінена та забезпечена під час проектування шляхом детальної розробки архітектури системи, використанні спеціальних засобів та не може порушуватися у разі появи передбачених обставин.

Практичне виконання механізмів забезпечення захищеності розподіленої інформаційно-телекомунікаційної системи є залежним від множини факторів: розміру бізнесу, напрямку діяльності компанії, типу інформаційної системи, міри її складності та розподіленості, топологічної схеми мереж, програмного забезпечення, що використовується і т. д [5].

Управління інформаційною безпекою та визначення засобів захисту інформаційно-телекомунікаційної системи є нелегким динамічним процесом. З огляду на те, що розподілена інформаційно-телекомунікаційна система – це складна система з багаторівневою архітектурою, то при прийнятті рішення про методи та засоби забезпечення її захисту необхідно ділити її та складові частини. Правила, процеси і процедури, які використовуються для ефективного управління мають бути формалізовані для кожного сегмента цієї системи. Це дає змогу прийняти оптимальне рішення щодо найбільш прийнятного компонента захисту певної складової частини системи [6].

Згідно із Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» захист інформації — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі [1].

Доступ до внутрішньої мережі, віддалений доступ і доступ в Інтернет сьогодні використовуються достатньо широко, що породжує певний ризик і ставить цілий ряд питань безпеки. Мережа і апаратні засоби, що використовуються для доступу в мережу, можуть містити дефекти захисту, можуть бути неправильно встановлені чи налаштовані, а також можуть неправильно використовуватись [7].

Проведений аналіз літературних джерел дозволяє систематизувати основні причини виникнення загроз захисту мережі. До основних з них відносять:

− технологічні недоліки – кожна мережа і кожна комп'ютерна технологія мають свої проблеми захисту (недоліки, притаманні TCP/IP, операційним системам і мережевому обладнанню) [7];

− недоліки конфігурування – навіть сама надійна технологія захисту може бути неправильно реалізована чи використана, в результаті чого може виявитися проблема захисту (недостатній захист, який забезпечується налаштуванням за замовчуванням, неправильна конфігурація мережевого обладнання, незахищені облікові записи користувачів, облікові записи користувачів з простими паролями, неправильне налаштування служб Інтернет) [7];

− недоліки політики захисту мережі – неправильно реалізована політика захисту може зробити вразливою навіть найкращу технологію мережевого захисту (відсутність документованої політики захисту, внутрішні протиріччя політик, відсутність логічного контролю доступу до мережевого обладнання, невідповідність програмного забезпечення і апаратних засобів прийнятої політики, необізнаність про можливі атаки) [7];

− нестабільна робота обладнання – будь-які збої в роботі кабельної системи, серверів, персональних комп'ютерів, а також перебої в електроживленні негативно впливають на рівень захищеності системи від загроз) [8];

− дефекти програмного забезпечення – при наявності вразливостей програмного забезпечення, а також при несвоєчасному встановлені оновлень безпеки інформація в системі може бути втрачена чи пошкоджена через помилки програмного забезпечення чи зараження вірусами [8];

− несанкціоновані дії сторонніх осіб – порушення конфіденційності інформації шляхом її викрадення, підміни, пошкодження чи знищення, порушення роботи інформаційної системи чи вивід з ладу обладнання [8];

− помилки користувачів – випадкові її, які можуть призвести до знищення чи зміни даних, порушення роботи системи внаслідок некоректного використання програмного та апаратного забезпечення [8];

− навмисні дії користувачів – поєднує в собі все, що описано в попередніх двох пунктах, та включає поширення конфіденційної інформації [8].

Якщо при втручанні в роботу системи втрати чи викрадення інформації не відбулося, то це також класифікується як порушення безпеки інформаційної системи [8].

Кіберзахист має бути головним елементом організації мережі. Правильне рішення проблем захисту дозволить:

мінімізувати витрати впровадження і експлуатації засобів мережевого захисту;

відкрити можливість використання нових мережевих додатків і послуг;

зробити Інтернет недорогим і безпечним засобом глобальних комунікацій [7].

У положеннях чинного законодавства, а саме в Законі України «Про основні засади забезпечення кібербезпеки України» визначається, що кіберзахист – це сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [9].

1.2. Основні типи загроз розподілених інформаційно-телекомунікаційних систем

Розподілені інформаційно-комунікаційні системи є привабливими для багатьох загроз, як ненавмисних, так і зловмисних. Це пов'язано як з високим

професійним потенціалом зловмисників, так і з вразливістю всіх комп'ютеризованих систем [10].

Дослідження та аналіз інформаційної безпеки в різних розподілених обчислювальних системах показали, що, незалежно від використовуваного мережевого протоколу, топології та інфраструктури розподіленої обчислювальної системи, механізми реалізації загроз в розподілених інформаційно-комунікаційних системах не залежать від конкретної системи Підтверджено факт їх інваріантності щодо своїх характеристик. Це пов'язано з тим, що розподілені інформаційно-комунікаційні системи проектуються за однаковими принципами і тому проблеми безпеки практично ідентичні [10].

Розглянемо більш детально найпоширеніші типи загроз та способи захисту від них.

Почнемо з аналізу мережевого трафіку. Це метод пасивного моніторингу мережевого трафіку за допомогою пристроїв або утиліт. Інформація, зібрана шляхом перехоплення, може бути використана для підготовки інших видів мережевих атак або для крадіжки інформації [7].

Цей метод може бути використаний для атаки на мережевий трафік з метою виявлення структури потоків даних або збору інформації для подальшої крадіжки, наприклад, паспортні дані, ідентифікаційні номери, дані про роботу мережі або фінансові дані.

Для перевірки та перехоплення пакетів даних зловмисники можуть використовувати різні програми, залежно від місяця місцезнаходження. Сучасні сніфери, призначені для діагностики мереж, можуть бути використані для злому. Сніфферне програмне забезпечення може аналізувати перехоплені пакети і перетворювати інформацію в статичні дані, які можна зберігати або детально досліджувати [11].

В результаті таких атак неавторизовані особи можуть отримати доступ до даних.

Для захисту від цієї атаки можна використовувати такі методи:

– спроектувати системи безпеки на етапі розробки архітектури мережі;

– вимкнути режим безладного доступу до мережевого інтерфейсу;

– використовувати протокол IPSec для захисту пакетів, що передаються за допомогою шифрування.

Технологія IPSec використовується для шифрування та захисту даних і підтримується більшістю сучасних маршрутизаторів, брандмауерів та іншого мережевого обладнання [11].

Наступними атаками, які слід розглянути, є DoS та DDoS-атаки - Атаки на відмову в обслуговуванні (DoS) - це злочинні атаки, які виводять з ладу сервер або персональний комп'ютер користувача, що ускладнює доступ власника обладнання або системи чи користувача до файлів чи серверів або підключення до мережі. Це створює всілякі ситуації, які роблять файли та сервери недоступними або ускладнюють підключення до них.

Як правило, мережеві хости атакують, щоб порушити стабільну роботу мереж і серверів та вивести їх з ладу.

Такі атаки мають на меті перевантажити мережевий канал трафіком, що ускладнює або унеможливлює передачу корисної інформації.

Для захисту від таких атак необхідно дотримуватися певних правил безпеки:

– проектування систем безпеки на етапі розробки мережевої архітектури;

– відключення невикористовуваних мережевих функцій та використання SSH для мінімізації ризику з боку пристроїв, підключених до Інтернету;

– використання спеціального програмного забезпечення;

– фільтрація та блокування трафіку.

Існують також методи підміни довірених мережевих об'єктів (спуфінг). Довірені об'єкти - це мережеві елементи (наприклад, комп'ютери, брандмауери, маршрутизатори), які мають легітимні з'єднання і яким призначено право доступу до мережевих ресурсів інформаційної системи.

Метою атаки є порушення конфіденційності та цілісності інформації на сервері або хості.

Процес атаки передбачає присвоєння прав довірених користувачів, що дозволяє зловмиснику проводити сеанси роботи з об'єктами системи від імені довірених користувачів. Для генерації підроблених TCP-пакетів зловмиснику потрібно лише знайти відповідне поточне значення ідентифікатора TCP-пакета для даного TCP-з'єднання. Цей тип атаки може також включати надсилання службових повідомлень, які помилково змінюють дані маршруту або адреси від імені пристрою керування мережею (наприклад, маршрутизатора). Такі повідомлення легко підмінити, оскільки вони ідентифікуються лише за мережевою адресою відправника [11].

Як наслідок, такі атаки призводять до витоку даних та зараження програмного забезпечення.

Для захисту від цього типу атак необхідно впровадити наступні засоби безпеки:

− контроль доступу;

− мінімізація підміни IP-адрес. Суть полягає в контролі доступу. Весь трафік із зовнішніх мереж повинен бути заблокований. Це знижує ефективність підміни IP-адрес;

− фільтрація RFC2827 - застосовується до вихідного трафіку і блокує підміну зовнішніх мереж користувачами нашої мережі; фільтрація RFC2827 фільтрує вихідний трафік, який не містить адресу джерела, прийняту для даного інтерфейсу Фільтрація RFC2827 фільтрує вихідний трафік, який не містить адресу джерела, прийняту для цього інтерфейсу;

− аутентифікація - для зменшення наслідків спуфінгу необхідно впроваджувати методи аутентифікації, відмінні від аутентифікації на основі IP-адреси [25].

Комп'ютери та сервери не обов'язково повинні бути мішенню. Необхідні дані можна отримати від людей. Для цього існує метод, який називається

соціальною інженерією. Соціальна інженерія - це використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації [11].

Зловмисники намагаються отримати бажану інформацію шляхом прямого контакту з тим, хто володіє потрібною їм інформацією (наприклад, телефонні розмови, поштове листування, конфіденційні розмови в кафе).

Джерелами загрози є електронні листи, текстові повідомлення в будь-якому месенджері, SMS-повідомлення та телефонні дзвінки. Шахраї можуть видавати себе за працівників банків та інших фінансових установ, державних службовців, правоохоронців, інтернет-провайдерів, представників поштових служб, великих веб-ресурсів тощо [12].

Такі атаки можуть призвести до порушення конфіденційності даних та зараження програмного забезпечення.

Щоб захистити дані, слід дотримуватися наступних заходів захисту:

− навчати співробітників;

− попередити всіх співробітників компанії про небезпеку розголошення особистої або конфіденційної інформації компанії та про те, як запобігти витоку даних;

− використовувати сучасне антивірусне програмне забезпечення на комп'ютерах співробітників;

− використовувати спеціалізоване програмне забезпечення для виявлення та запобігання атакам;

− обмежити права користувачів у системах.

В результаті аналізу було узагальнено кілька варіантів кіберзахисту від мережевих атак:

− навчати співробітників поведінці, яка ускладнює здійснення мережевих атак;

− обмежити використання Інтернету працівниками;

− постійно оновлювати антивірусне програмне забезпечення;

− проектувати системи безпеки на етапі розробки мережевої архітектури;

− використовувати сучасні маршрутизатори при проектуванні та розробці моделей кіберзахисту мережі;

− відключення режиму promiscuous на мережевих інтерфейсах;

− використання IPSec-шифрування для захисту вихідних пакетів.

1.3 Актуальність та передумови створення систем захисту комп’ютерних мереж

Основними завданнями побудови багаторівневих систем безпеки для локальних мереж є захист інформаційного середовища від навмисного або випадкового втручання, спроб руйнування компонентів, несанкціонованого доступу та забезпечення працездатності системи в разі виникнення непередбачуваних подій.

У сучасному світі інформаційні системи відіграють важливу роль у функціонуванні організацій та підприємств. Метою інформаційних систем є задоволення потреб користувачів у виконанні їхніх завдань. За допомогою комп'ютерних мереж працівники компанії можуть швидко та ефективно обмінюватися інформацією, зберігати та створювати файли віддалено, спілкуватися електронною поштою, мати доступ до всесвітньої мережі Інтернет та її ресурсів, а також безпосередньо взаємодіяти з виробничими процесами. Можливості та ефективність використання мереж неможливо переоцінити і вони є невід'ємною частиною сьогоднішньої реальності.

Найбільш поширеною практикою на сучасних підприємствах є впровадження єдиної корпоративної інформаційної системи, яка централізує управління і в той же час інтегрує все обладнання в єдине середовище для ефективного функціонування та взаємодії різних підрозділів.

Зі зростанням ролі інформаційних систем в управлінні підприємством зростає і загроза несанкціонованого доступу до інформації в системах, спотворення інформації, протиправного впливу з метою знищення, атак та інших методів. Масштаби шкідливих наслідків варіюються від системних збоїв і фінансових втрат для комерційних підприємств до серйозної шкоди інтересам України, наприклад, розголошення державної таємниці. Тому інформаційна безпека завжди займала особливо важливе місце при проектуванні будь-якого підприємства.

Загалом, інформаційну безпеку можна описати як стан захищеності систем обробки та зберігання даних, що забезпечує відповідність основним критеріям оцінки інформаційної безпеки. Самі критерії являють собою сукупність методів визначення вимог до безпеки системи, створення компонентів безпеки та оцінки рівнів безпеки. [17]

Система визначає декілька характеристик інформаційної безпеки. Першою з них є конфіденційність - характеристика інформації, яка означає, що певна інформація доступна лише авторизованим користувачам. Наступною характеристикою є цілісність, яка є властивістю інформації, що означає, що інформація може бути змінена або модифікована лише авторизованими користувачами. Останньою характеристикою є доступність. Це властивість інформації, яка означає, що тільки авторизовані користувачі можуть використовувати ресурс без очікування, що перевищує визначений часовий інтервал, згідно з правилами, встановленими політикою безпеки.

Основною функцією існуючих систем інформаційної безпеки є попередження та ліквідація наслідків загроз інформаційному середовищу. Для кращого розуміння цього питання необхідно знати загальні поняття та види існуючих загроз. [3]

Загроза - це ситуація або подія, яка потенційно може призвести до порушення інформаційної безпеки та/або нанесення шкоди корпоративному

середовищу. Іншими словами, загроза - це все, що може негативно вплинути на існуючі системи.

Загалом, до загроз відносяться:

− навмисні дії порушників ІБ;

− помилки персоналу різного роду, що виникають в процесі експлуатації ресурсу;

− наслідки помилок проектування автоматизованих систем;

− стихійні лиха та непередбачувані надзвичайні ситуації.

Під час експлуатації інформаційних систем найпоширенішим видом порушника є віддалена мережева атака, яка являє собою деструктивний вплив на систему, що здійснюється через канали зв'язку. Залежно від характеру впливу мережеві атаки можна класифікувати як активні або пасивні. Активні впливи - це такі, що безпосередньо втручаються в роботу системи і призводять до порушення роботи системи або її окремих вузлів, взаємодії з компонентами системи, зміни конфігурації тощо. Пасивні впливи характеризуються тим, що такі впливи безпосередньо не впливають на роботу системи. Цей тип атак складніше виявити. [До найпоширеніших мережевих атак відносяться:

− атаки на переповнення буфера - це тип мережевих атак, спрямованих на переповнення буфера даних програми більшою кількістю даних, ніж передбачалося автором програми. В результаті такої атаки можуть бути виконані інструкції, написані зловмисником;

− підміна DNS - тип мережевої атаки, при якій IP-адреса помилково зіставляється з доменним ім'ям у кеш-файлі DNS-сервера.13 В результаті успішної підміни дані на DNS-сервері підміняються, і користувачеві сервера надається неправдива інформація про доменне ім'я та IP-адресу некоректна інформація про доменне ім'я та IP-адресу;

− сніфінг - це підслуховування каналів передачі даних в локальній мережі. Атака полягає в перехопленні пакетів даних, адресованих іншим авторизованим пристроям в мережі. Ця атака використовується для ефективного аналізу

захищеності системи та отримання інформації про наявне програмне та апаратне забезпечення. При використанні сніферів у пасивному режимі зловмисник може отримувати сеансовий трафік для протоколів SSL, TLS, TCP і UDP, IP-адреси та номери портів, що використовуються різними пристроями, і залишатися невиявленим програмними засобами захисту;

− DoS-атаки - це атаки на комп'ютерні системи, метою яких є зробити комп'ютерні ресурси недоступними для законних користувачів. Один з найпоширеніших методів атаки - насичення атакованого комп'ютера або мережевого обладнання великою кількістю зовнішніх запитів, що значно уповільнюють або повністю виводять з ладу пристрій або сервіс в процесі атаки; ефективність DoS-атаки підвищується, коли атака запускається одночасно з великої кількості IP-адрес стає більш ефективною. Внаслідок цього такі атаки отримали назву DDoS (Distributed Denial of Service attacks - розподілені атаки на відмову в обслуговуванні).

Для запобігання та проактивної протидії зловмисникам використовуються системи виявлення вторгнень (IDS) - програмне або апаратне забезпечення, призначене для виявлення несанкціонованого доступу, певних аномалій та інших незвичних станів в інформаційних системах. Деякі системи виявлення вторгнень можуть також виявляти ініціювання мережевих атак (IPS). Аналіз інформації всередині системи є фундаментальним елементом сучасних систем виявлення вторгнень та захисту Системи IDS можна класифікувати на схеми виявлення загроз на основі сигнатур та схеми виявлення аномалій. [18]

Методи виявлення аномалій засновані на профілюванні завдань і процесів в системі. Іншими словами, вони розпізнають інформацію та події, що циркулюють в системі, як нормальні робочі шаблони і порівнюють їх з новою поведінкою. Цей метод виявлення є дуже інноваційним, оскільки він використовує певні аспекти машинного навчання і може виявляти невідомі типи атак, але в той же час він має ряд недоліків. Цей недолік особливо помітний при

використанні специфічного програмного забезпечення, яке може залишати особливі підписи в інформаційній системі.

Методи виявлення сигнатур засновані на простому порівнянні послідовностей даних з шаблонами. Вхідні набори переглядаються, аналізуються і послідовно порівнюються з сигнатурами - характерними рядками програм, які відповідають характеристикам шкідливого трафіку. Самі сигнатури - це логічні фрази, команди або окремі фрагменти коду. Якщо збіг знайдено, системний адміністратор встановлює тригер. На відміну від методів виявлення аномалій, сигнатурний підхід може виявити лише ті загрози, які присутні в базі даних сигнатур, тому цей метод не може виявити нові та невідомі атаки взагалі. [18]

Використання систем виявлення вторгнень, а також діагностики має фундаментальне значення для забезпечення безпеки в мережі. Ретельно аналізуючи системні журнали та записи, фахівці з ІБ можуть впроваджувати ефективні процедури для посилення та подальшого розвитку безпеки системи.

1.4 Постановка задачі

Метою бакалаврської роботи є розробка моделі розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства.

Об’єктом дослідження виступає інформаційно-телекомунікаційна система торгівельного підприємства.

Предметом дослідження є сукупність засобів програмно-технічного характеру, які можуть бути спрямовані на забезпечення кібербезпеки інформаційно-телекомунікаційної системи об’єкта дослідження.

Поставлена мета обумовила необхідність вирішення наступних завдань:

− розглянути поняття розподіленої інформаційно-телекомунікаційної системи та її захищеності;

– систематизувати основні причини виникнення проблем захисту інформаційно-телекомунікаційних систем;

– розглянути основні типи загроз розподілених інформаційно-телекомунікаційних систем;

– проаналізувати захищеність розподіленої інформаційно-телекомунікаційної системи об’єкта дослідження;

– розробити проект розподіленої інформаційно-телекомунікаційної системи об’єкта дослідження з урахуванням вимоги кіберзахисту; здійснити основні налаштування пристроїв забезпечення безпеки в запропонованій моделі кіберзахисту інформаційно-телекомунікаційної системи.

2 РЕАЛІЗАЦІЇ МОДЕЛІ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1 Засоби для створення моделі розподіленої інформаційно-телекомунікаційної мережі в cisco packet tracer

Для досягнення поставленої мети використовувався комплекс загальнонаукових методів [13]:

− методи теоретичного узагальнення – при описі предметної області дослідження;

− аналізу та синтезу – при дослідженні захищеності діючої розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства;

− формалізації – при створенні проектів розподіленої комп'ютерної мережі в симуляторі Cisco Packet Tracer;

− системного аналізу та експерименту– при розробці моделі кіберзахисту розподіленої інформаційно-телекомунікаційної системи та налаштуванні пристроїв забезпечення безпеки.

Для розробки моделі інформаційно-телекомунікаційної системи торгівельного підприємства в дипломній роботі прийнято рішення використати симулятор Cisco Packet Tracer.

Cisco Packet Tracer – це програма, створена компанією Cisco для відтворення роботи власного обладнання: роутерів, комутаторів, бездротового обладнання, серверів, ПК і т.д. Даний симулятор дає можливість здобути досвід в налаштуванні реальної мережі, яка може містити необмежену кількість пристроїв. Налаштування обладнання здійснюється декількома способами: введення команд в операційну систему Cisco IOS, через графічний веб-інтерфейс, командами та графічним меню операційної системи. В Packet Tracer режим віртуалізації дає можливість користувачу відстежити переміщення пакетів даних та отримати повну інформацію про них на всіх пристроях мережі.

За допомогою симулятора можна виявити слабкі місця, несправності та надійність мережі [14, 15].

Переваги:

- зрозумілий графічний інтерфейс;
- можливість моделювання фізичної і логічної топології;
- наявність режиму симуляції, в якому наглядно зображені всі процеси що проходять в мережі;
- можливість додавання/видалення коментарів [16].

Недоліки:

- підтримуються не всі команди реального Cisco IOS;
- можливість створення імітаційної моделі лише для обладнання компанії Cisco Systems;
- Cisco Packet Tracer доступний для скачування лише для інструкторів, студентів, випускників та адміністраторів Мережевої академії Cisco [16].

З урахуванням недоліків програмного забезпечення Cisco Packet Tracer, його можливостей достатньо для використання в якості засобу реалізації моделі розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства для досягнення поставленої мети дипломної роботи.

Класи в Packet Tracer є важливими засобами для організації мережевих конфігурацій та управління ними. Класи це набір правил і налаштувань, які дозволяють керувати мережевим трафіком і взаємодією пристроїв у мережі. Кожен клас може мати власні параметри і налаштування, що дозволяє створювати різні політики для обмеження або керування трафіком.

Види класів [20, 21]:

- Class-Based Quality of Service (CBQoS). Використовується для налаштування якісного обслуговування в мережі. Може встановлювати пріоритети для різних видів трафіку;
- Access Control List (ACL) Class. Використовується для налаштування списків керування доступом для фільтрації IP-адрес та портів;

− Firewall Class. Дозволяє налаштовувати правила брандмауера для захисту мережі від небажаних підключень та атак;

− Quality of Service (QoS) Class. Використовується для налаштування якості обслуговування, такої як пріоритети для важливого трафіку, уникнення перевантажень мережі тощо;

− IP SLA Class. Використовується для налаштування IP Service Level Agreement (IP SLA) для моніторингу та керування продуктивністю мережі.

Класи дозволяють обмежувати або пріоритизувати певні види трафіку в мережі, дозволяють налаштовувати правила безпеки для фільтрації трафіку та захисту мережі від атак, дозволяють забезпечити необхідний рівень продуктивності для різних видів даних [20, 21].

Кожен клас може мати свої параметри, такі як пріоритети, швидкості, фільтри трафіку тощо. Налаштування класів зазвичай виконується за допомогою інтерфейсу командного рядка або графічного інтерфейсу в Packet Tracer.

При налаштуванні класів у мережі важливо враховувати потреби конкретного додатку чи сервісу.

Списки контролю доступу (Access Control Lists) є невід'ємною частиною мережевої безпеки і управління трафіком в сучасних комп'ютерних мережах. Ці механізми фільтрації дозволяють адміністраторам мережі контролювати, який трафік дозволено або блоковано на основі різних параметрів, таких як IP-адреси, порти, протоколи тощо. Давайте розглянемо докладніше, як ACLs працюють та для чого вони використовуються [22].

Існує два основних типи ACLs. Першим є Standard ACLs. ACLs дозволяють фільтрувати трафік лише на основі джерела пакетів, зазвичай за IP-адресою відправника. Вони працюють на рівні мережевого шару OSI і використовуються для базового блокування або дозволу трафіку. Другим є Extended ACLs. Ці ACLs надають більшу гнучкість, оскільки дозволяють вказувати умови фільтрації на основі різних параметрів, таких як джерело,

призначення, порти, протоколи тощо. Вони працюють на рівні транспортного і прикладного шару OSI [23].

ACLs дозволяють обмежувати доступ до ресурсів мережі, таких як сервери, веб-сайти, сервіси тощо. Це допомагає уникнути несанкціонованого доступу до важливої інформації. Вони використовуються для захисту мережі від різних видів атак, таких як DDoS, переповнення буфера, перехоплення пакетів тощо, шляхом блокування небажаного трафіку. ACLs дозволяють налаштовувати пріоритети для різних видів трафіку, що є корисним для забезпечення якості обслуговування (QoS) в мережі [24].

ACLs складаються з набору правил, кожне з яких містить умови фільтрації трафіку і дії, які потрібно виконати для відповідного трафіку.

У стандартних ACLs, кожне правило зазвичай вказується за номером та містить умову фільтрації для джерела пакетів.

У розширених ACLs, крім джерела, можуть вказуватися інші параметри, такі як призначення, порти, протоколи тощо.

ACLs використовуються на маршрутизаторах, комутаторах, файрволах та іншому мережевому обладнанні для здійснення контролю над трафіком [23].

У маршрутизаторах, вони допомагають визначати шляхи маршрутизації та керувати рухом мережевих пакетів.

У файрволах, вони використовуються для захисту мережі від зовнішніх атак та контролю доступу до внутрішніх ресурсів. Перед використанням ACLs необхідно ретельно спланувати, який трафік потрібно блокувати чи дозволяти для забезпечення ефективності і безпеки мережі [24].

ACLs слід регулярно оновлювати та перевіряти, оскільки зміни у мережевій інфраструктурі можуть впливати на їх ефективність.

Перед впровадженням ACLs рекомендується провести тестування, щоб переконатися у їх правильному функціонуванні і відсутності недосконалостей чи конфліктів з іншими правилами [24].

У стандартних ACLs, для додавання правила можна використовувати команди, наприклад, access-list <номер> {permit|deny} <джерело> у режимі конфігурації маршрутизатора.

У розширених ACLs, додатково можна вказувати параметри, такі як призначення, порти, протоколи, за допомогою команд, наприклад, access-list <номер> {permit|deny} <протокол> <джерело> <призначення>.

ACL можна налаштувати так, щоб блокувати певні IP-адреси чи діапазони IP, які вважаються небажаними у мережі, можна використовувати для дозволу доступу до певних служб або серверів, наприклад, дозволяючи доступ до веб-сайту з певних IP-адрес [25, 26].

Для ефективного використання ACLs важливо моніторити їх роботу і аналізувати журнали трафіку, щоб виявити аномальні патерни чи несправжні атаки.

Можна використовувати спеціальні інструменти і системи моніторингу, які допомагають відслідковувати і аналізувати взаємодію з ACLs.

Загальна інформація про Access Control Lists (ACLs) в мережах показує їх важливість для безпеки, управління трафіком та контролю доступу до ресурсів. Для кожного конкретного випадку використання ACLs важливо ретельно планувати і налаштовувати їх, враховуючи потреби мережі та політику безпеки.

Ключі в Packet Tracer використовуються для налаштування різних параметрів на мережевих пристроях, таких як маршрутизатори, комутатори, файрволи тощо. Вони дозволяють встановлювати різні опції конфігурації та активувати різні функціональні можливості.

Існують такі види ключів [27]:

− Encryption Keys (ключі шифрування). Використовуються для налаштування шифрування трафіку між пристроями для забезпечення конфіденційності даних під час передачі;

− Access Keys (ключі доступу). Використовуються для обмеження доступу до певних ресурсів на мережевих пристроях, таких як веб-сайти, сервіси, зони адміністрування тощо;

− Security Keys (ключі безпеки). Використовуються для налаштування параметрів безпеки, таких як аутентифікація, авторизація, контроль доступу до сервісів тощо;

Encryption Keys дозволяють захищати конфіденційні дані в мережі, що особливо важливо для безпеки при передачі чутливої інформації.

Access Keys дозволяють обмежувати доступ до певних ресурсів чи сервісів у мережі, що допомагає уникати несанкціонованого доступу.

Security Keys дозволяють налаштовувати різні параметри безпеки, такі як аутентифікація користувачів, контроль доступу до мережевих служб тощо.

Для Encryption Keys можна вказати алгоритм шифрування та встановити ключі для захисту трафіку.

Access Keys використовуються для налаштування списків керування доступом (ACLs) на мережевих пристроях.

Security Keys дозволяють налаштовувати параметри безпеки, такі як аутентифікація за допомогою ключів, реєстрація користувачів тощо.

Ключі є важливим елементом у мережевій безпеці, оскільки вони дозволяють захищати дані від несанкціонованого доступу і забезпечувати безпеку мережі в цілому.

Правильні налаштування та управління ключами важливі для забезпечення високого рівня конфіденційності, цілісності та доступності даних у мережі.

Загалом, ключі в Packet Tracer є ключовими компонентами для забезпечення безпеки та управління мережею. Їх використання відображається в різних аспектах, від шифрування трафіку до контролю доступу та налаштування параметрів безпеки.

SSH (Secure Shell) є протоколом мережевого рівня, який забезпечує безпечне з'єднання та обмін даними між двома пристроями через небезпечну

мережу. У Packet Tracer, як і в реальних мережевих середовищах, SSH використовується для безпечного віддаленого керування мережевими пристроями, такими як маршрутизатори, комутатори та сервери [28, 29].

Однією з найбільших переваг SSH є його здатність до шифрування даних, що передаються між клієнтом і сервером. Це робить SSH надійним вибором для віддаленого керування мережевими пристроями.

SSH використовує різні методи аутентифікації, такі як пароль, ключі SSH (RSA, DSA), що робить процес входу у систему більш безпечним і захищеним в порівнянні зі стандартними протоколами, такими як Telnet.

SSH дозволяє налаштовувати різні параметри, такі як шифрування, версія протоколу, порт з'єднання, що робить його гнучким у використанні для різних вимог безпеки.

У Packet Tracer можна налаштувати SSH на маршрутизаторах, комутаторах та інших мережевих пристроях, що підтримують цей протокол.

Під час налаштування SSH, вам потрібно створити ключі (RSA або DSA), вказати параметри шифрування та аутентифікації, а також налаштувати користувачів, яким дозволено використовувати SSH для віддаленого керування.

Спочатку потрібно зайти у консоль мережевого пристрою через Packet Tracer. Для цього потрібно вибирати пристрій, натиснути "Desktop" або "Terminal" і ввести відповідні команди для входу.

Після входу у консоль потрібно переконатись, що SSH активовано та правильно налаштовано на пристрої.

Далі потрібно згенерувати ключі SSH (RSA або DSA) на пристрої і зберегти їх для подальшого використання, налаштувати параметри шифрування, аутентифікації та доступу для користувачів, які будуть використовувати SSH.

У сценаріях реального життя, SSH використовується для віддаленого керування серверами, маршрутизаторами, комутаторами, а також для доступу до віддалених обчислювальних ресурсів [30].

Це дозволяє адміністраторам мережі безпечно налаштовувати, моніторити та керувати мережевим обладнанням з будь-якого місця.

Безпека SSH також залежить від правильної конфігурації і управління ключами, паролями та доступом користувачів.

Завжди потрібно використовувати сильні паролі і ключі, обмежувати доступ до SSH тільки необхідним користувачам та періодично переглядати налаштування безпеки.

SSH є важливим протоколом для безпечного віддаленого керування мережевим обладнанням, і його налаштування в Packet Tracer може допомогти зрозуміти його роботу та застосування в реальних мережевих середовищах.

Пріоритизація у мережевих технологіях стосується управління мережевим трафіком для забезпечення певного рівня обслуговування різних типів даних. Це особливо важливо в умовах обмеженої пропускної здатності мережі, коли потрібно гарантувати, що важливі дані мають пріоритет над менш важливими.

Основні елементи пріоритизації [31]:

- quality of service;
- class of service;
- differentiated services;
- traffic shaping;
- bandwidth reservation.

Quality of Service — це набір технологій, які дозволяють управляти пропускною здатністю мережі, щоб забезпечити надійність та якість обслуговування для різних типів трафіку. QoS використовується для контролю затримок, втрат пакетів, і джиттера, особливо для трафіку, чутливого до затримок, такого як голосовий або відео трафік.

Class of Service — це метод маркування пакетів у мережі для визначення пріоритету трафіку. Наприклад, Ethernet-фрейми можуть містити поле CoS для визначення пріоритету [31].

Differentiated Services — це модель QoS, яка використовує поле Differentiated Services Code Point у заголовку IP-пакета для визначення пріоритету трафіку. Вона дозволяє класифікувати та управляти трафіком на основі попередньо визначених класів обслуговування [31].

Traffic Shaping — це метод управління трафіком, який обмежує швидкість вихідного трафіку, щоб запобігти перевантаженням мережі. Це допомагає розподілити мережеве навантаження рівномірніше.

Bandwidth Reservation — це метод резервування певної частини пропускної здатності мережі для конкретних типів трафіку або додатків [32].

Пріоритизація в Packet Tracer використовується для управління чергами пакетів в мережі з метою забезпечення належної якості обслуговування. Це особливо важливо в мережах, де одночасно передаються різні типи трафіку, такі як голосовий, відео та звичайний даний трафік. Пріоритизація дозволяє мережним адміністраторам забезпечувати якість обслуговування, управляти трафіком, покращувати продуктивність мережі та її безпеку [33].

Пріоритизація дозволяє гарантувати що важливі сервіси отримують достатньо ресурсів для безперебійної роботи, оптимізовувати використання пропускної здатності мережі шляхом надання більших ресурсів важливим додаткам та обмеження їх для менш критичних.

В Packet Tracer є багато різноманітних мережевих пристроїв, за допомогою яких можна змоделювати мережі різної складності.

Комутатор – мережевий пристрій, який використовується для з’єднання кількох пристроїв в одній мережі та ефективного управління трафіком в цих мережах. Він дозволяє пристроям в мережі обмінюватись даними без конфліктів та з достатньо високою швидкістю. Приклад використання комутатора в комп’ютерній мережі зображено на рисунку 2.1.

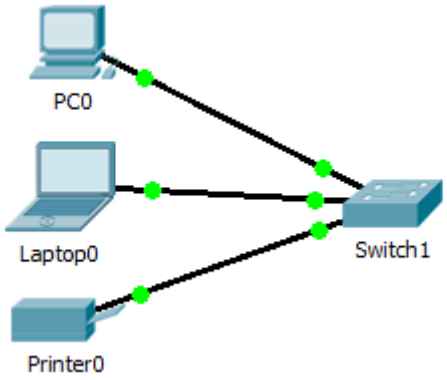


Рисунок 2.1 – приклад використання комутатора в комп’ютерній мережі

Роутер є мережевим пристроєм, який з’єднує різні мережі і маршрутизує дані між ними, забезпечуючи безпечне та надійне з’єднання. Він містить безліч вбудованих функцій для забезпечення безчного з’єднання між пристроями в мережі. Також він має різні типи інтерфейсів для підключення різноманітних пристроїв до нього. Крім того роутер підтримує переклад мережевих адрес, що забезпечує доступ до інтернету з внутрішньої мережі [34]. Приклад використання роутера зображено на рисунку 2.2.

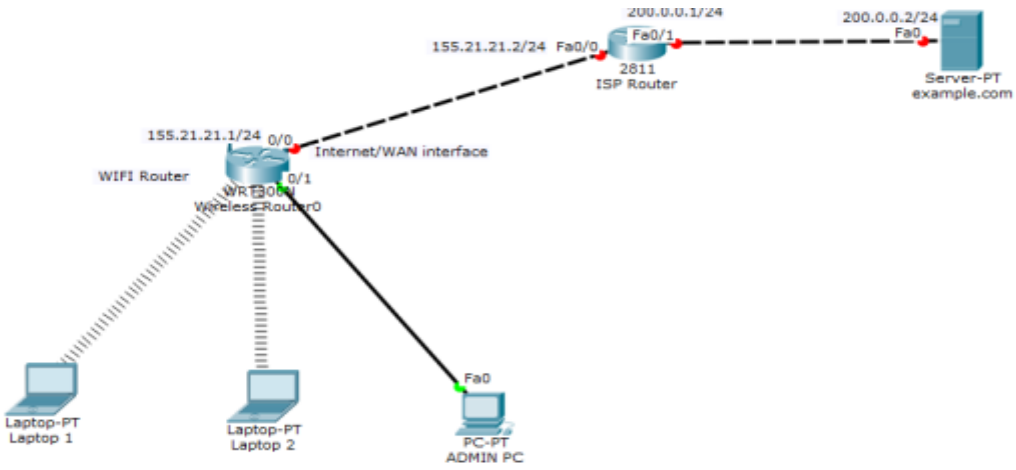


Рисунок 2.2 – Приклад використання роутера в комп’ютерній мережі

В комп’ютерній мережі також мають бути наявні кінцеві пристрої. Це такі пристрої, які є джерелами або одержувачами даних. Вони розташовані на кінцях мережі і використовуються кінцевими користувачами для доступу до ресурсів

мережі. До кінцевих пристроїв відносяться комп'ютери, телефони, принтери, сервери та інші пристрої, які взаємодіють з мережею [35].

Персональний комп'ютер є найпоширенішим кінцевим пристроєм в packet tracer. Він використовується для моделювання реальних сценаріїв використання комп'юетрів у мережі. Комп'ютер має багато інтерфейсів для підлкючення різноманітних пристроїв [35].

Сервер це потужний комп'ютер, що надає різні сервіси і ресурси іншим пристроям в мережі. Вони виконують ключову роль у функціонуванні межер і забезпечують цетралізоване керування, обробку та зберігання інформації. У packet tracer сервери представлені як спеціальні пристрої з можливістю налаштування різних сервісів, таких як DNS, DHCP, веб-сервери, файл-сервери та інше. Вони дозволяють моделювати реальні мережеві сценарії і тренуватись в налаштуванні різних мережевих служб.

Веб-камера в packet tracer це пристрій який моделює реальну мережеву ip-камеру. Цей пристрій використовується для захоплення відеозображень і передачі їх через мережу для моніторингу або інших цілей. Веб-камери зазвичай підключаються до локальної мережі через Ethernet або Wi-Fi і можуть бути налаштовані для віддаленого доступу через Інтернет. Їх використовують для моделювання різних сценаріїв, пов'язаних з відеомониторингом і безпекою [36].

Щоб пристроїв мережі могли обмінюватись даними та взаємодіяти між собою, їх потрібно з'єднати. З'єдання в мережі це процес підключення різних пристроїв один до одного для передачі даних. Воно забезпечує обмін інформацією між пристроями, дозволяючи їм взаємодіяти, ділитися ресурсами, мати доступ до інтернету та виконувати інші мережеві функції [37].

Дротове з'єднання використовує фізичні кабелі для з'єднання пристроїв. Його переваги включають в себе високу швидкість передачі даних, високий рівень безпеки, оскільки фізичне з'єдання до мережі зменшує ризик несанкціонованого доступу. З недоліків можна виділити обмеження мобільності пристроїв, оскільки вони мають бути фізично підключені до мережі та вартість і

трудомісткість прокладання кабелів, оскільки цей процес може бути дорогим, особливо в великих будівлях.

Бездротове з’єднання дозволяє підключатись пристроям до мережі без фізичного підключення кабелем. Це дозволяє переміщувати пристрої в межах зони покриття бездротової мережі без втрати з’єднання. Воно також не потребує прокладання великої кількості кабелів, що спрощує розгортання мережі. З недоліків можна підкреслити нижчу швидкість передачі даних, ніж через дротове з’єднання. Бездротові мережі більш вразливі до несанкціонованого доступу та перехоплення даних, що потребує додаткових заходів безпеки [38].

2.2 Моделювання мережі для торгівельного приміщення

Після аналізу наявних інструментів в програмі Packet Tracer, я визначив що з їх допомогою я успішно зможу змоделювати потрібну мені комп’ютерну захищену систему та правильно налаштувати її.

Спочатку спроектував декілька окремих приміщень, що будуть призначені для торгівлі. В кожному з приміщень має бути розташовані певні пристрої:

- камери відеонагляду;
- декілька комп’ютерів, що будуть розміщені на касах;
- принтер;
- комп’ютер адміністратора;
- свічі.

В результаті отримав логічну схему для торгівельного приміщення, яка зображена на рисунку 2.3. Таких приміщень в даному проекті буде три. Всі вони налаштовуються по одному принципу.

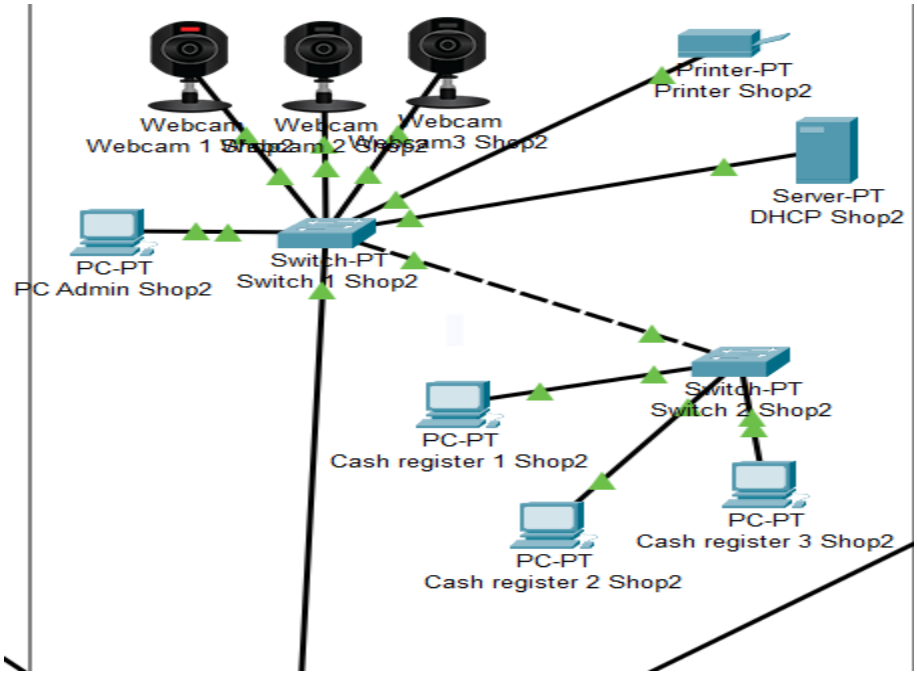


Рисунок 2.3 – Логічна схема торгівельного приміщення

В торгівельному приміщенні розташовано три каси, три камери відеонагляду, принтер, сервер, комп'ютер адміністратора. Усі пристрої з'єднані між собою за допомогою двох свічів.

Сервер роздає IP адреси для кожного з пристроїв в кімнаті. На рисунку 2.4 зображені налаштування сервера для коректного розподілення IP-адрес.

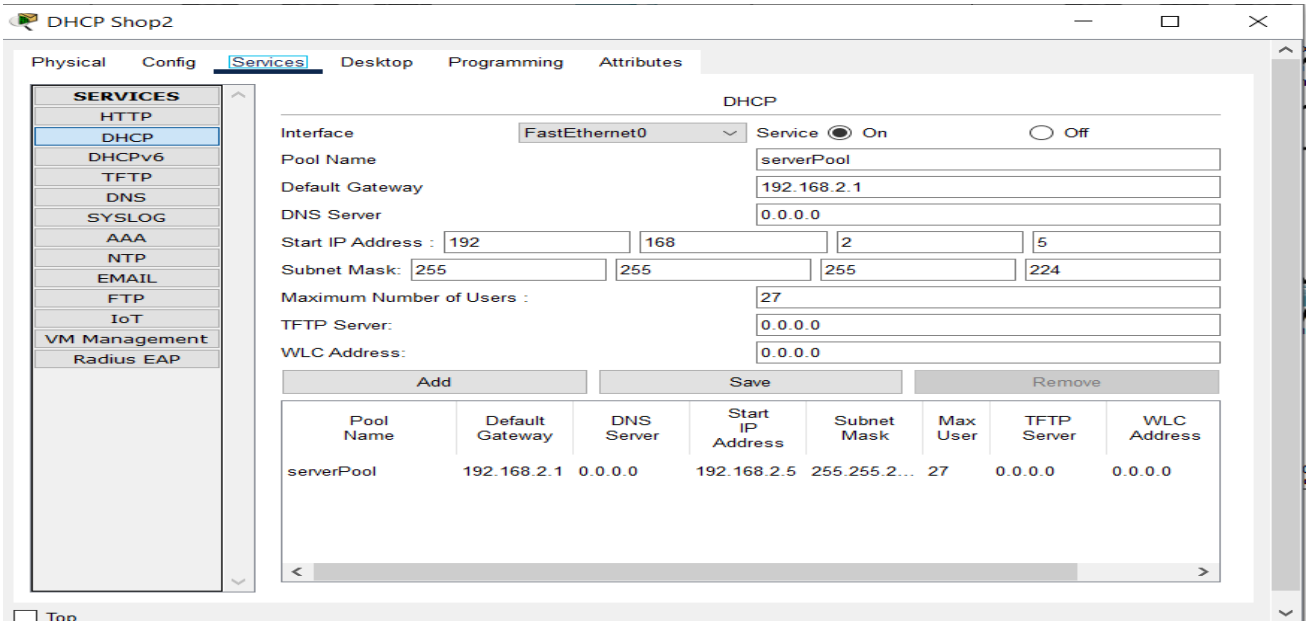


Рисунок 2.4 – Налаштування сервера в торгівельному приміщені

Далі налаштував свічі. Для цього перейшлов на вкладку «CLI». І за допомогою відповідних команд налаштував ім’я пристрою в мережі, встановив шифрування паролів, щоб вони зберігались в зашифрованому вигляді та встановив пароль для адміністратора. Для цього є декілька основних команд, які я використав. Щоб перейти в привілегійований режим EXEC, що надає доступ до конфігураційних командр, потрібно ввести команду «enable». Далі щоб зайти в режим глобальної конфігураціїї, потрібно ввести команду «configure terminal». За допомогою команди «hostname <ім’я>» задав ім’я пристрою. Щоб увімкнути шифрування паролів є команда «service password-encryption», вона дозволяє зберігати паролі в конфігурації в зашифрованому вигляді, щоб підвищи безпеку. Щоб встановити пароль потрібно ввести команду «password <пароль>», яка встановлює пароль для доступу в режим конфігураціїї. І щоб зберегти поточну конфігурацію, потрібно ввести команду «copy running-config startup-config». Повний список команд наведено в додатку А.

Далі налаштував камери. Кожній потрібно задати назву, пароль та IP-адресу.

Назва камери потрібна для ідетифікаціїї пристрою в мережі. IP-адреса потрібна для віддаленого доступу до неї. Пароль потрібен щоб захистити підключення до камери. Щоб виконати ці налаштування, потрібно перейти на вкладку «Config» і у відповідних полях вказати потрібні заначення.

Налаштування для камери зображено на рисунку 2.5.

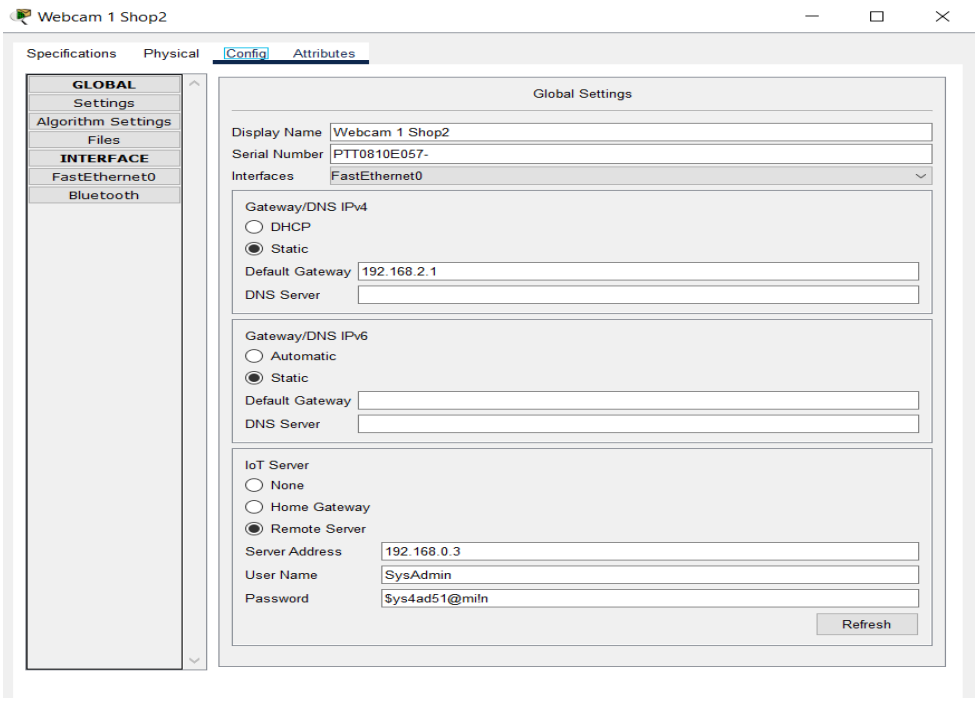


Рисунок 2.5 – Налаштування веб-камери

В результаті я отримав три торгових приміщення, в яких розміщені та відповідно налаштовані пристрої, необхідні для моделювання мережі.

2.3 Моделювання мережі для головного офісу

Після того як було змодельовано торгівельні приміщення, потрібно змоделювати головний офіс, з якого можна буде управляти всіма комп’ютерами та веб-камерами. Також це місце має бути захищене від стороннього проникнення та забезпечувати швидке та стабільне з’єднання з усіма пристроями в мережі.

У головному офісі буде розташоване таке обладнання:

- головний комп’ютер;
- роутер;
- сервер;
- свіч.

Головний комп’ютер повинен мати можливість підключатись до будь-якого приладу в мережі.

Після розміщення та під’єднання всіх приладів я отримав логічну схему, зображену на рисунку 2.6.

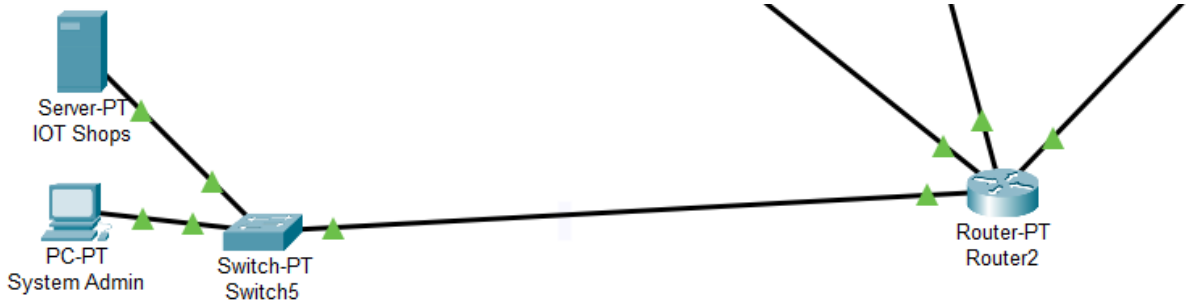


Рисунок 2.6 – Логічна схема головного офісу

Спочатку налаштував свіч. Задав йому ім’я хоста, включив шифрування паролів в конфігураційному файлі, встановив пароль, та включив вимогу входу до терміналу за допомогою пароля. Повний список команд наведено в додатку Б.

Тепер потрібно налаштувати роутер так, щоб він забезпечував ефективний та безпечний зв’язок між приладами в мережі.

В результаті роутер має рівномірно розподіляти та забезпечувати безпеку трафіку у мережі. Доступ до камер має бути лише з комп’ютера, що розташований в головному офісі, а інші комп’ютери або пристрої не мають мати доступу до головного офісу.

Я виділив декілька класів трафіку, які будуть мені потрібні. А саме:

- TCP;
- UDP;
- відеотрафік.

TCP та UDP це два основних транспортних протокола, які використовуються для передачі даних в мережі. Вони мають різні характеристики і підходять для різних типів трафіку.

Щоб створити клас трафіку, існує команда «class-map match-all <ім’я> match protocol <ім’я протоколу>», яка створює новий клас політики та додає правило до класу, яке вказує, що потрібно збігатись з вказаним протоколом. В мому випадку, я створив три класи і відповідно задав їм з якими протоколами вони мають збігатись. Для TCP я задав http протокол. Для UDP – https. Для відеотрафіку – протоколи rtp та h323.

Також буде корисним задати приорітети трафіку, для кращого розподілення ресурсів у мережі. Для цього я використав команду «policy-map <ім’я політики> class <ім’я класу> [команда]». Для TCP трафіку я задав приорітет в 15%, для UDP – 15% та для відеотрафіку – 30%.

Потім я прив’язав політику пріоритизації до інтерфейсів GigabitEthernet1/0, GigabitEthernet2/0 та GigabitEthernet3/0. Це я зробив за допомогою команди «interface <ім’я інтрефейсу> service-policy output <ім’я політики>»

Також потрібно налаштувати самі інтерфейси. Для інтерфейсу GigabitEthernet0/0 я задав механізм справедливого чергування за допомогою команди «fair-queue». Цей механізм розроділяє пропоскну здатність між потоками даних рівномірно, що запобігає домінуванню одного потоку над іншим.

Для інтерфейсу GigabitEthernet1/1 я встановив найвищий рівень безкеки за допомогою команди «security-level 100». Це означає що інтерфейс є внутрішнім і має найвищий рівень безпеки. Також задав йому ip-адресу з маскою підмережі за допомогою команди «ip address 192.168.0.1 255.255.255.240».

Для інтерфейсу GigabitEthernet1/2 я задав рівень безпеки рівний нулю, оскільки він може використовувати для підключення до зовнішніх мереж. Також задав йому ip-адресу та маску підмережі за допомогою команди «ip address 210.210.0.2 255.255.255.240».

Далі налаштував динамічний NAT (Network Address Translation) для перекладу внутрішніх адрес на зовнішній інтерфейс. Це допоможе покращити

безпеку мережі, оскільки NAT приховує внутрішню структуру мережі від зовнішніх мереж і користувачі не зможуть звертатись безпосередньо до внутрішніх ip-адрес.

Також налаштував списки контролю доступу. Вони дозволяють фільтрувати трафік, налаштувати управління доступами та підвищують продуктивність мережі шляхом блокування непотрібного та шкідливого трафіку до того як він досягне свого місця призначення. Для створення таких списків існує команда «access-list <ім’я списку> extended permit <ім’я протоколу> <джерело> <маска джерела>».

Крім того додав налаштування для політик інспекціїї трафіку. Вони дозволяють контролювати роботу різних додатків та протоколів, щоб забезпечити їх безпечне і правильне функціонування. Для цього командою «class-map inspection_default match default-inspection-traffic» створив клас для інспекції трафіку і вказав, що він відповідатиме за інспекцію трафіку за замовчуванням. Також створив та налаштував глобальну інспекцію. Для цього сворив політику за допомогою команди «policy-map global_policy class inspection_default» і за домогою команди «inspect <ім’я трафіку>» задав моніторинг для таких трафіків:

- dns;
- ftp;
- h323;
- http;
- icmp;
- tftp.

Крім цього є потреба налаштувати списки контролю доступу для конктретних підключень. Це потрібно для того, щоб забезпечити доступ до серверу для камер та комп’ютерів системних адміністраторів, а також заборонити трафік між магазинами та інший небажаний трафік. Для цього я використав команду «access-list <ім’я списку> < permit / deny> <ім’я протоколу>

<джерело> <маска джерела> <призначення> <маска призначення>». В результаті цих налаштувань було налаштовано наступне:

- дозволено камерам доступ до серверу;
- заборонено трафік між магазинами;
- дозволено доступ комп’ютеру системного адміністратора до магазинів.

Повний перелік команд для налаштування роутера наведено в додатку В.

В результаті я отримав мережу з трьох торгівельних приміщень та цетрального офісу, яка була налаштована так, щоб забезпечити безпеку мережі та її швидкодію. Логічна схема зображена в додатку Г. Фізична схема – в додатку Д.

2.4 Висновки

У другому розділі було проведено глибокий аналіз інструментів, доступних у Packet Tracer для моделювання та конфігурування мережі. Було детально розглянуто пріоритезацію трафіку, класи обслуговування, списки контролю доступу, кінцеві точки, мережеві пристрої та їхній взаємозв'язок. Кожен із цих аспектів має вирішальне значення для побудови ефективної та надійної мережі, особливо для ритейлерів, яким потрібен високий рівень безпеки та продуктивності.

Пріоритетність трафіку допомагає забезпечити пріоритет критично важливих даних над некритичними, що необхідно для безперебійної роботи критично важливих додатків і сервісів. Клас обслуговування допомагає розподілити мережеві ресурси таким чином, щоб забезпечити необхідний рівень якості обслуговування для різних типів трафіку.

Списки контролю доступу є невід'ємною частиною мережевої безпеки і дають змогу контролювати, які пристрої та користувачі можуть отримувати

доступ до різних мережевих ресурсів. Це важливо для запобігання несанкціонованому доступу та захисту конфіденційної інформації.

Під час аналізу кінцевих і мережевих пристроїв розглядалися різні типи обладнання, їхні можливості та способи взаємодії. Провідні з'єднання забезпечують швидкість і надійність, а бездротові - гнучкість і зручність розгортання мережі.

Після детального аналізу цих компонентів було зроблено висновок, що ці інструменти можна використовувати для моделювання та налаштування мережі роздрібної торгівлі, щоб забезпечити безпеку і високу продуктивність. Застосувавши принципи пріоритизації трафіку, розподілу ресурсів за класами обслуговування, використання списків контролю доступу та оптимального під'єднання кінцевих точок і мережевих пристроїв, я побудував мережу, яка відповідає всім вимогам сучасної роздрібної мережі та забезпечує надійність надійність роботи, безпеку даних і високу продуктивність.

3 ФІЗИЧНА РЕАЛІЗАЦІЯ РОЗПОДІЛЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ТОРГІВЕЛЬНОГО ПІДПРИЄМСТВА

3.1 Тестування змодельованої розподіленої інформаційно-телекомунікаційної мережі торгівельного підприємства

Одним з важливих аспектів розвитку мережі є тестування. На цьому етапі можна виявити потенційні проблеми та недоліки мережі ще до того, як вона почне функціонувати. Тестування також дозволяє перевірити безпеку мережі, виявити її вразливі місця і забезпечити захист від зовнішніх атак.

Мережа, змодельована програмним забезпеченням Package Tracer, може бути протестована за допомогою режиму симуляції. У цьому режимі можна імітувати різні аспекти мережі, спостерігати за взаємодією мережевого обладнання, аналізувати трафік і виконувати різні тестові сценарії без необхідності реалізації реальної мережі. У режимі моделювання можна імітувати реальний трафік між мережевими пристроями, включаючи передачу пакетів і взаємодію протоколів. Також можна перевірити, як мережа реагує на різні типи атак.

Для мене мета тесту - перевірити, чи правильно налаштована мережа. Вона повинна забезпечувати стабільний і швидкий зв'язок між пристроями і гарантувати безпеку з'єднання.

Для початку я перевіряю з'єднання між камерою та комп'ютером у головному офісі. Переконайтеся, що тільки цей комп'ютер має доступ до камери. Жодні інші пристрої в мережі не повинні мати до неї доступу. Для цього я використовую команду ping, яка є одним з основних інструментів для перевірки з'єднання між мережевими пристроями: вона надсилає ICMP-повідомлення з ехо-запитом на певний пристрій і отримує ехо-відповідь. Це дає змогу перевірити, чи доступний мережевий пристрій.

Щоб перевірити з'єднання між камерою і комп'ютером системного адміністратора, виберіть потрібний пристрій, виберіть програму Commang Promt

на вкладці "Робочий стіл", введіть команду "ping" і вкажіть IP-адресу пристрою. Результати виконання команди "ping" з комп'ютера системного адміністратора на камеру наведено на рисунку 3.1. Як видно з результатів виконання команди "ping", комп'ютер системного адміністратора з'єднаний з камерою. Комп'ютер системного адміністратора підтримує зв'язок з усіма камерами в мережі. Для перегляду всіх камер, підключених до мережі, необхідно зайти в додаток "веб-браузер" на вкладці "робочий стіл" комп'ютера системного адміністратора і ввести IP-адресу сервера, до якого підключена камера. Сторінка входу в систему показана на рисунку 3.2.

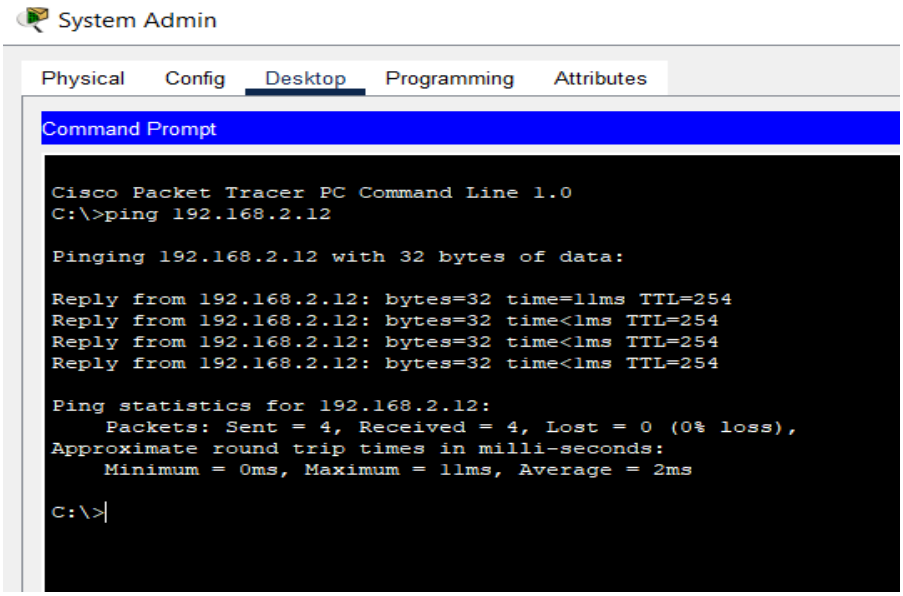


Рисунок 3.1 – Результат команди ping з комп’ютера системного адміністратора до камери

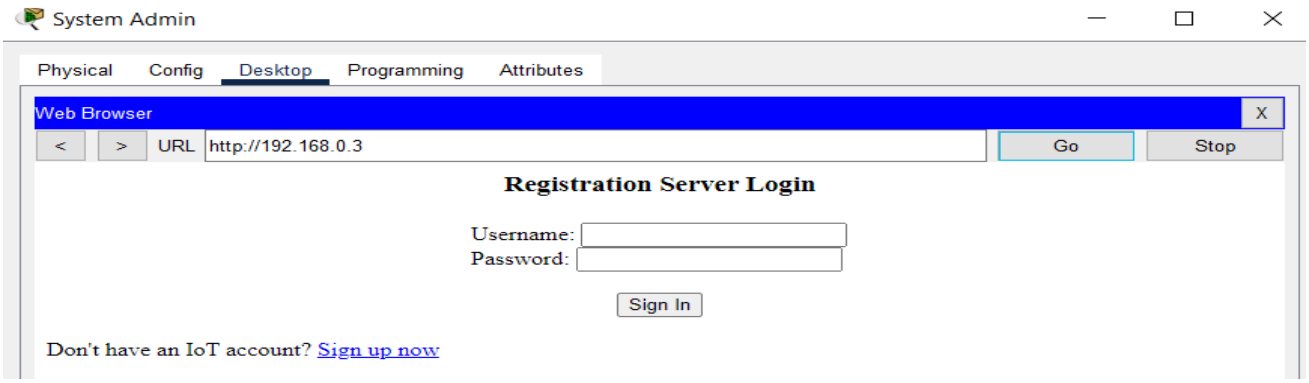


Рисунок 3.2 – Сторінка логіну

Для того щоб отримати доступ до всіх камер, потрібно залогінитись в систему за допомогою паролю і логіну. Після успішної автентифікації відобразиться список підлкючених камер, який зображено на рисунку 3.3.

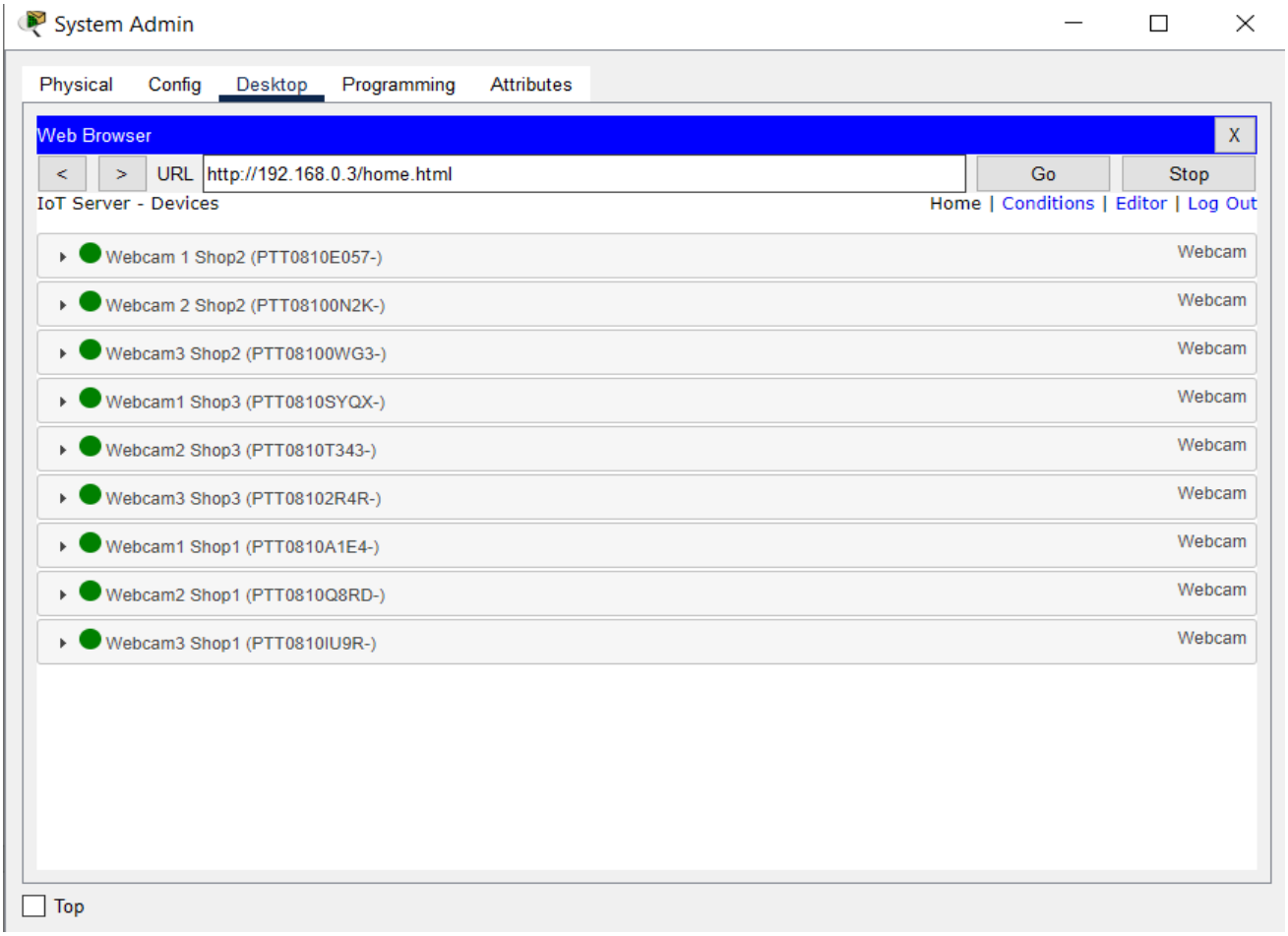


Рисунок 3.3 – Список камер що підключені до сервера

Зелені індикатори біля назв сигналізують що зі всіма камерами є зв'яок і вони працюють правильно.

Також за допомогою команди «ping» я перевірив чи є зв'язок між комп'ютером системного адміністратора та усіма іншими пристроями в мережі. Результат зображено на рисунку 3.4.

В результаті я перевірив зв'язок між камерами та комп'ютером системного адміністратора та переконався що він має доступ до всіх камер та інших пристроїв в мережі.

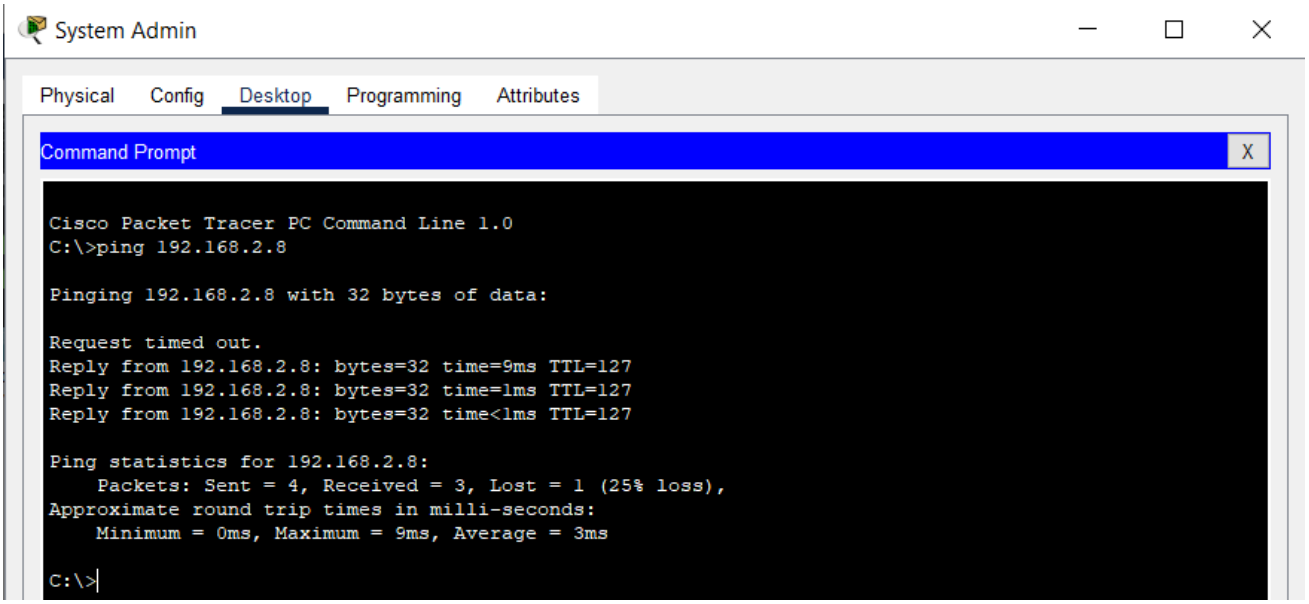


Рисунок 3.4 – перевірка з'язку між комп'ютером системного адміністратора та комп'ютером адміністратора магазину

Наступне, що потрібно протестувати це те що пристрої в мережі не повині мати доступ до камер та комп'ютера системного адміністратора. Це можна зробити за допомогою команди «ping» та програми «Web Browser». Я перевірю чи комп'ютер адміністратора магазину та комп'ютери на касах маю доступ до камер. Релузьтати перевірки зображено на рисунках 3.5 та 3.6.

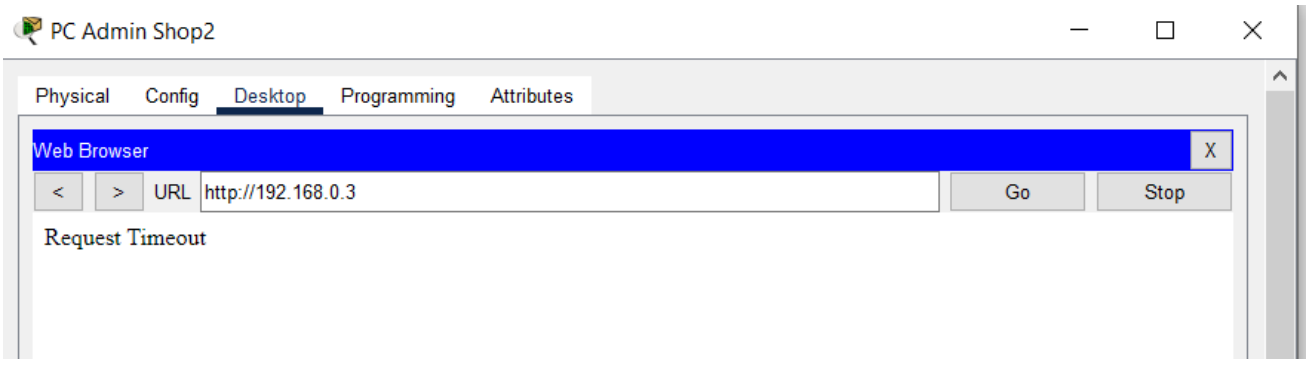


Рисунок 3.5 – перевірка доступу комп'ютера адміністратора магазину до камер

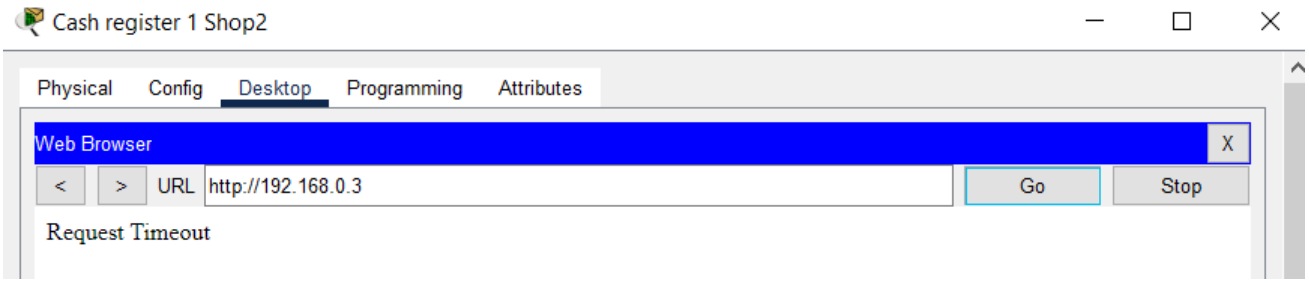


Рисунок 3.6 – Перевірка доступу комп’ютера на касі до камер

Після цієї перевірки я визначив що комп’ютери на касах та комп’ютери адміністраторів магазину не мають доступу до камер, отже налаштування виконані правильно.

Після завершення налаштувань мережі було проведено всебічне тестування для перевірки їхньої ефективності та правильності. Використовуючи режим симуляції в Packet Tracer, я змоделював різні сценарії мережевого трафіку, що дозволило переконатися у коректній роботі політики QoS та інших налаштувань. У процесі тестування були використані команди, такі як ping, та інші інструменти, що дозволило перевірити зв’язок між пристроями та їхню відповідність заданим параметрам.

Тестування також включало перевірку пріоритизації трафіку, що забезпечує необхідний рівень обслуговування для різних типів даних, таких як відео та звичайний трафік. Це дозволило переконатися, що високопріоритетні дані передаються швидше, що критично для додатків, що потребують низької затримки та високої пропускної здатності.

Окрім цього, була проведена перевірка налаштувань безпеки, включаючи списки контролю доступу (ACL) та політики інспекції. Ці перевірки підтвердили, що мережа захищена від несанкціонованого доступу та потенційних загроз.

Завдяки ретельному тестуванню стало очевидно, що налаштована мережа функціонує відповідно до всіх вимог. Всі компоненти мережі працюють гармонійно, забезпечуючи необхідний рівень продуктивності та безпеки. Це

дозволяє бути впевненими, що мережа готова до експлуатації в реальних умовах, де важливі стабільність, швидкість та захист даних.

3.2 Загальгі відомості про мережу та вибір обладнання

Після успішного тестування та виправлення недоліків можна переходити до фізичної реалізації такої розподіленої інформаційно-комунікаційної мережі торговельних підприємств.

В процесі фізичної реалізації мережі рітейлера були враховані всі вимоги до її впровадження та функціонування. Мережа складається з трьох торгових точок і головного офісу. Головний офіс виступає в ролі центрального вузла, з серверами для зберігання та обробки даних і мережевим обладнанням для управління трафіком. Кожен магазин підключений до головного офісу через маршрутизатор для забезпечення надійної та безпечної передачі даних.

При встановленні мережі було обрано надійне та ефективне обладнання для забезпечення високої продуктивності та надійності всієї системи. Вибір обладнання ґрунтувався на аналізі потреб мережі та специфічних характеристик обладнання.

Як показано на рисунку 3.7, для забезпечення централізованого зберігання та обробки інформації були обрані сервери Dell R720. Ці сервери характеризуються високою продуктивністю та надійністю. Вони оснащені процесорами Intel Xeon для досягнення високої швидкості обробки даних. Вони також оснащені великим об'ємом оперативної пам'яті і можуть зберігати великі обсяги даних, що робить їх ідеальними для використання в цій мережі. Для забезпечення резервування та високої надійності системи було розгорнуто чотири сервери DELL R720.

Рисунок 3.7 – Сервер DELL R720

Як показано на рисунку 3.8, для з'єднання між пристроями в мережі було обрано комутатор GREENVISION GV-017-AI-4. Комутатор забезпечує високу швидкість передачі даних і підтримує технологію Power over Ethernet (PoE), що дозволяє подавати живлення на пристрої через мережевий кабель. Комутатор має високу пропускну здатність і підтримує до п'яти портів, що дозволяє підключити велику кількість пристроїв; було встановлено чотири комутатори GREENVISION, що забезпечило надійний зв'язок у всіх приміщеннях.

Рисунок 3.8 – Свіч GREENVISION GV-017-AI-4

Для більш складних мережевих конфігурацій використовувався комутатор MikroTik CRS112-8G-4S-IN, показаний на рисунку 3.9. Цей комутатор підтримує до восьми портів Gigabit Ethernet і чотирьох портів SFP, до яких можна підключати оптоволоконні лінії. Він також підтримує ряд мережевих функцій, таких як VLAN і маршрутизація. Три з цих комутаторів були встановлені для забезпечення надійного зв'язку між роздрібними точками та головним офісом.

Рисунок 3.9 – Свіч MikroTik CRS112-8G-4S-IN

Як показано на рисунку 3.10, для відеоспостереження в цеху була використана камера Hikvision DS-2CE56H0T-IRMMF. Ця камера забезпечує високу якість зображення і сумісна з інфрачервоним підсвічуванням, що дозволяє здійснювати відеоспостереження в умовах низької освітленості. Вони також захищені від погодних умов і можуть використовуватися як в приміщенні, так і на вулиці. Дев'ять таких камер були встановлені для забезпечення повного покриття магазину.

Рисунок 3.10 – Камера Hikvision DS-2CE56H0T-IRMMF

Маршрутизатор MikroTik hAP AX3, показаний на рисунку 3.11, використовувався для маршрутизації трафіку та забезпечення зв'язку між торговими точками та головним офісом. Маршрутизатор підтримує високошвидкісний Wi-Fi 802.11ax, що забезпечує високу швидкість передачі даних і підтримку великої кількості підключених пристроїв. Вони також підтримують ряд мережевих функцій, таких як NAT, VPN та QoS. Ці маршрутизатори були встановлені для централізованого управління мережею.

Рисунок 3.11 – Маршрутизатор MikroTik hAP AX3

Персональні комп'ютери, зображені на рисунку 3.12, "все в одному" Artline Business B14 були обрані для підтримки адміністративного персоналу та управління мережею. Ці комп'ютери мають потужні процесори, достатньо оперативної пам'яті та великі екрани для комфортної роботи. Вони також мають інтегровані мережеві можливості, що дозволяє легко інтегрувати їх у загальну інфраструктуру. Загалом було встановлено 13 таких комп'ютерів для підтримки роботи адміністративного персоналу та касирів у всіх торгових точках і в головному офісі.

Рисунок 3.12 – Моноблок Artline Business B14

3.3 Реалізація змодельованої мережі в головному офісі

Головний сервер знаходиться в головному офісі і централізує зберігання та доступ до даних; сервери DELL R720 підключені до мережевих комутаторів і маршрутизаторів. Ці сервери характеризуються високою продуктивністю та надійністю і забезпечують безперебійну роботу всієї мережі: сервери DELL R720 оснащені процесорами Intel Xeon, які забезпечують високу обчислювальну

потужність і здатність обробляти численні запити одночасно. Він також оснащений великим об'ємом оперативної пам'яті, що дозволяє швидко маніпулювати даними і зберігати великі обсяги інформації, що робить його ідеальним для використання в нашій мережі. Завдяки цьому сервер може обробляти дані, що надходять з торгових точок, а також задовольняти потреби головного офісу.

На сервері було встановлено програмне забезпечення для обробки відеопотоків з IP-камер, встановлених у роздрібних магазинах; камери відеоспостереження Hikvision DS-2CE56H0T-IRMMF підключені до сервера через мережу і можуть приймати та обробляти відео в режимі реального часу. Камери оснащені системою камер з високою роздільною здатністю та інфрачервоними камерами. Ці камери забезпечують високу якість зображення завдяки високій роздільній здатності та інфрачервоному підсвічуванню, що дозволяє здійснювати відеоспостереження навіть у темних місцях. Сервер з програмним забезпеченням для обробки відео дозволяє централізовано зберігати всі відеозаписи та аналізувати події.

Для забезпечення безпеки та надійності з'єднання було застосовано шифрування даних і налаштовано VPN-з'єднання. Це захищає дані від несанкціонованого доступу і гарантує, що всі дані передаються захищеним каналом зв'язку; використання VPN-з'єднання забезпечує додатковий рівень безпеки, що особливо важливо для відеопотоків, які можуть містити конфіденційну інформацію.

Комп'ютер адміністратора в головному офісі використовується для моніторингу та управління відеокамерами, а також для налаштування та обслуговування мережі. Адміністратор має доступ до всіх камер відеоспостереження, що дозволяє йому контролювати умови в магазині в режимі реального часу. Комп'ютер адміністратора є важливим інструментом для моніторингу мережевої активності та швидкого реагування на будь-які проблеми, що можуть виникнути. Він також дозволяє конфігурувати мережеві

пристрої, забезпечуючи гнучкість і швидке реагування на мінливі вимоги та умови експлуатації.

Для забезпечення мережевої безпеки маршрутизатор MikroTik hAP AX3 налаштований за допомогою списків доступу, які можуть обмежувати доступ до певних ресурсів і фільтрувати небажаний трафік. Це ефективно захищає мережу від можливих атак і забезпечує безпеку переданих даних. Списки доступу дозволяють визначити, які пристрої та користувачі мають доступ до певних мережевих ресурсів, що значно підвищує рівень безпеки.

Крім того, для забезпечення високої якості відеопотоку та мінімізації затримок передачі даних налаштовано пріоритети та класи трафіку; створено кілька класів трафіку, включаючи TCP, UDP та відеотрафік, що дозволяє ефективно управляти навантаженням на мережу. . Пріоритезація трафіку гарантує, що важливі дані, такі як відеопотоки, мають пріоритет над менш важливим трафіком, таким як веб-серфінг та електронна пошта. Це допомагає підтримувати високу якість відео і мінімізувати затримки, що важливо для ефективного спостереження і безпеки.

Розгортання імітованої мережі в головному офісі є ключовим елементом у забезпеченні загальної функціональності та безпеки мережі в усьому ритейл-центрі. Використовуючи найсучасніше обладнання та ретельно налаштовуючи мережеві пристрої, ми змогли створити стабільну та надійну мережу, яка відповідала всім вимогам проекту.

3.4 Реалізація змодельованої мережі в торгівельних приміщеннях

Кожна торгова точка має сервер IP-адрес. Ці сервери відіграють важливу роль в автоматичному призначенні IP-адрес всім підключеним пристроям, що значно спрощує управління мережею і знижує ризик виникнення конфліктів IP-адрес. Сервери ретельно налаштовані для забезпечення стабільної роботи і

надійного функціонування; вони підключені до комутатора GREENVISION GV-017-AI-4, який забезпечує високошвидкісну передачу даних і підтримку Power over Ethernet (PoE), що дозволяє пристроям безпосередньо Живлення може подаватися безпосередньо на обладнання через мережевий кабель. Таке рішення мінімізує кількість кабелів і спрощує встановлення та обслуговування мережі.

Крім того, в кожному торговому залі встановлений комутатор MikroTik CRS112-8G-4S-IN для забезпечення надійного зв'язку між усіма пристроями. Комутатор підтримує до восьми портів Gigabit Ethernet, що дозволяє підключити велику кількість пристроїв, а також чотири порти SFP для оптоволоконних з'єднань. За допомогою цього комутатора можна легко інтегрувати оптоволоконні з'єднання для забезпечення високої пропускної здатності і стабільності мережі. Крім того, комутатор підтримує різні мережеві функції, такі як VLAN, маршрутизація і QoS для ефективного управління мережевим трафіком і забезпечення високого рівня безпеки.

Для відеоспостереження за приміщенням магазину було встановлено три камери Hikvision DS-2CE56H0T-IRMMF. Ці камери забезпечують високу якість зображення завдяки високій роздільній здатності та інфрачервоному підсвічуванню, що дозволяє вести відеоспостереження навіть у темних приміщеннях. Камери підключені через мережу до сервера в головному офісі, який отримує та обробляє зображення в режимі реального часу. Для забезпечення безпеки та стабільності передачі даних відеопотік було зашифровано та налаштовано VPN-з'єднання. Це запобігає несанкціонованому доступу до відеоданих і забезпечує високий рівень конфіденційності.

Кожен менеджер магазину має доступ до касових апаратів для налаштування та обслуговування. Комп'ютер адміністратора підключений до мережі через комутатор, що забезпечує надійне з'єднання та швидку передачу даних. Комп'ютер адміністратора не тільки забезпечує безперебійну роботу касового апарату, але й відіграє важливу роль у моніторингу та управлінні всіма мережевими пристроями в торговому приміщенні. Це дозволяє адміністратору

швидко реагувати на будь-які проблеми та вносити необхідні корективи, таким чином підтримуючи високу ефективність мережі та забезпечуючи якісне обслуговування клієнтів.

Для забезпечення високої продуктивності та надійності мережі було ретельно підібрано та налаштовано обладнання для кожної торгової точки. Кожен елемент мережі був протестований і налаштований на оптимальну роботу в реальних умовах навантаження. Це забезпечило стабільну та надійну роботу мережі, яка відповідає всім вимогам сучасного ритейлера.

3.5 Розрахунок вартості

Розрахунок вартості є критично важливим етапом при плануванні та впровадженні будь-якого мережевого проекту. Він дозволяє забезпечити раціональне використання фінансових ресурсів та уникнути перевитрат, що можуть негативно вплинути на загальний бюджет проекту. Правильний розрахунок вартості включає в себе детальний аналіз всіх компонентів та етапів проекту, таких як закупівля обладнання, ліцензії на програмне забезпечення, витрати на монтаж та налаштування, а також вартість обслуговування та підтримки мережі. Для точного розрахунку вартості необхідно врахувати вартість серверів, маршрутизаторів, комутаторів, кабелів, тощо. Також до уваги потрібно взяти вартість ліцензій на програмне забезпечення.

Правильний підхід до розрахунку вартості також включає використання сучасних методик та інструментів для фінансового планування та аналізу. Це допоможе забезпечити точність розрахунків та дозволить приймати обґрунтовані фінансові рішення, що сприятимуть успішній реалізації мережевого проекту.

Щоб реалізувати таку мережу буде потрібно таке обладнання:

− персональні комп’ютери (13 одиниць);

- роутер (1 одиниця);
- свічі (7 одиниць);
- сервери (4 одиниці);
- камери відеонагляду (9 одиниць);
- кабелі для з’єднання пристроїв.

Крім того на кожен з комп’ютерів потрібно буде встановити ліцензійне програмне забезпечення. Приблизний розрахунок вартості наведено в таблиці 3.1.

Таблиця 3.1 – Розрахунок вартості обладнання

Пристрій	Ціна, грн.	Кількість	Вартість, грн.
Персональний комп’ютер моноблок Artline Business B14	13000	13	169000
Роутер MikroTik hAP AX3	5500	1	5500
Свіч GREENVISION GV-017-AI-4 + 1P	2350	4	9400
Свіч MikroTik CRS112-8G-4S-IN	4000	3	12000
Сервер DELL R720	9000	4	36000
Камера відеонагляду Hikvision DS-2CE56H0T-IRMMF	1000	9	9000
Кабель UTP 5e (305м) Vinga CCA	1500	1	1500
Всього			242400

Ціни на обладнання акуальні на 06.06.2024.

В результаті підрахунків, щоб реалізувати таку мережу знадобиться бюджет в розмірі 242400 гривень.

3.6 Висновки

Завдяки використанню сучасного та надійного обладнання було побудовано ефективну та безпечну розподілену інформаційно-комунікаційну мережу для роздрібної торгівлі. Від аналізу вимог до фізичної реалізації, кожен етап проекту був ретельно спланований і виконаний для досягнення максимальної продуктивності та надійності мережі.

При виборі обладнання були враховані всі технічні вимоги та потреби компанії: використання серверів DELL R720 забезпечило високу продуктивність і надійність зберігання та обробки даних. Ці сервери підтримують роботу з великими обсягами інформації та забезпечують швидкий доступ до даних, що є критично важливим для ефективного функціонування роздрібної мережі.

Комутатори GREENVISION GV-017-AI-4+1P та MikroTik CRS112-8G-4S-IN забезпечують надійний зв'язок між усім мережевим обладнанням, дозволяючи ефективно управляти трафіком та швидко передавати дані Підтримка комутаторами GREENVISION технології PoE зменшує кількість необхідних кабелів і спрощує встановлення та обслуговування мережі.

Hikvision DS-2CE56H0T-IRMMF забезпечує високу якість зображення і відеоспостереження в умовах низької освітленості. Це забезпечує безпеку на об'єктах роздрібної торгівлі та дозволяє контролювати діяльність в режимі реального часу. Відеозаписи зберігаються на сервері в головному офісі, що дозволяє централізовано керувати відеопотоками та аналізувати події.

Маршрутизатор MikroTik hAP AX3 забезпечує надійне високошвидкісне з'єднання між торговими точками і головним офісом. Завдяки підтримці високошвидкісного Wi-Fi 802.11ax співробітники можуть використовувати

бездротові пристрої для роботи з клієнтами і швидкого доступу до мережевих ресурсів. Це значно підвищує ефективність роботи і забезпечує комфортні умови для співробітників.

Моноблочні комп'ютери Artline Business B14, встановлені в дилерських центрах і головному офісі, гарантують зручність і ефективність роботи адміністративного персоналу. Висока продуктивність цих комп'ютерів дозволяє швидко і комфортно виконувати необхідні операції, навіть при роботі з великими обсягами даних на великому екрані.

Мережа уможливила централізоване управління всіма процесами, що відбуваються в торгових точках і в головному офісі. Це включає управління касовими апаратами, відеоспостереження, розподіл IP-адрес і маршрутизацію трафіку. Пріоритезація трафіку та класифікація даних забезпечили високу якість відеопотоку, мінімізували затримки та забезпечили стабільну роботу мережі.

Одним з найважливіших аспектів розгортання мережі є забезпечення безпеки даних та захист від несанкціонованого доступу. Шифрування даних та налаштування VPN-з'єднань забезпечило високий ступінь захисту інформації. Обмеження доступу до певних ресурсів за допомогою списків доступу маршрутизатора дозволяє ефективно відфільтрувати небажаний трафік і захистити його від можливих атак.

Проект з побудови розподіленої інформаційно-комунікаційної мережі для торгової компанії був успішно завершений завдяки використанню найсучаснішого обладнання та ретельному плануванню кожного етапу робіт. Мережа відповідає всім вимогам проекту і гарантує ефективне управління торговим процесом, високий рівень обслуговування клієнтів та безпеку об'єктів магазину. Це дозволило компанії ефективно функціонувати та розвиватися, забезпечуючи високий рівень обслуговування своїх клієнтів.

ВИСНОВКИ

В результаті написання дипломної роботи було розглянуто та проаналізовано сутність поняття розподіленої інформаційно-телекомунікаційної системи та сформульовано її значення для торгівельних підприємств. Систематизовано основні причини виникнення проблем захисту інформаційно-телекомунікаційних систем та узагальнено існуючі методи їх попередження, в результаті чого можна зробити висновок, що кіберзахист має бути головним елементом організації мережі. Також було розглянуто основні типи загроз розподілених інформаційно-телекомунікаційних систем та узагальнено базові методи захисту від атак, а точніше методи зменшення ризику мережевих атак.

Для розробки моделі розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства було використано симулятор Cisco Packet Tracer. При проектуванні мережі акцент зроблено на використанні багатофункціональних пристроїв забезпечення безпеки Cisco ASA.

При створенні проекту розподіленої інформаційно-телекомунікаційної системи було здійснено основні налаштування пристроїв забезпечення безпеки Cisco ASA, а саме налаштування множини інтерфейсів, параметрів шифрування, списків контролю доступів та криптосхем. Для забезпечення шифрування даних, які передаються по міжмережевому протоколу IP, було здійснено налаштування засобів IPSec.

Запропонована модель розподіленої інформаційно-телекомунікаційної системи торгівельного підприємства може бути реалізована в будь-якій торгівельній мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text (дата звернення: 06.06.2024).

2. Корпань Я.В. Класифікація загроз інформаційній безпеці в комп'ютерних системах при віддаленій обробці даних. *http://dspace.nbuv.gov.ua/*. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/131565/04-Korpan.pdf?sequence=1 (дата звернення: 06.06.2024).

3. Глоба Л. Розробка інформаційних ресурсів та систем : підручник. Київ : Політехніка, 2023. 380 с.

4. Новіков М. В., Грайворонський О. М. Безпека інформаційно-комунікаційних систем : підручник. Київ : Вид. Група BHV, 2020. 698 с.

5. Сазонець О. М. Інформаційні системи та технології в управлінні зовнішньоекономічною діяльністю. Київ : Центр навч. Літ., 2023. 256 с.

6. Кузнецова М.Г. Застосування механізмів підвищення живучості для забезпечення захищеності інформаційного ресурсу в розподілених системах. Реєстрація, зберігання і обробка даних. 2022. Т.8. №3. С. 40-47. URL: http://dspace.nbuv.gov.ua/handle/123456789/50851.

7. Присяжнюк М., Рідей Н., Титова Н. Інформаційна безпека та кібербезпека держави. Дніпро : Ліра До, 2024. 224 с.

8. Романюк Б., Гавловський В., Гуцалюк М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій : Навчально –метод. Посіб. / ред. В. Бутузов. Одеса : Од. Юрид. Акад., 2024. 144 с.

9. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 06.06.2024).

10. Матов О.Я., Василенко В.С. Модель загроз у розподілених мережах. Реєстрація, зберігання і обробка даних. 2019. Т.10. №1. С. 91-102.

11. Ериксон Д. Хакінг: мистецтво експлойту. Київ, 2020. 240 с.

12. Сугестивні технології маніпулятивного впливу : Практ. Посіб. / Є. Скулиш та ін. Львів : Скіф, 2023. 248 с.

13. Важинський С., Щербак Т. Методика та організація наукових досліджень : навч. Посіб. Суми : СумДПУ ім. А.С. Макаренка, 2016. 260 с.

14. Cisco Packet Tracer. *https://www.cisco.com*. URL: https://www.cisco.com/c/ru_ua/trainingevents/netacad/training-courses/ciscopacket-tracer.html (дата звернення: 07.06.2024).

15. Киричек Г., Скрупський С. Методичні вказівки до виконання лабораторних робіт з дисципліни «Комп'ютерні мережі». Моделювання мереж в середовищі Packet Tracer. Запоріжжя : ЗНТУ, 2023. 378 с.

16. Рвачова Н., Павліченко В. Програмні засоби для моделювання NGN мереж. Харків : Скіф, 2020. 58 с.

17. Семенов А. Структуровані кабельні системи. 5-те вид. Київ : Print2print, 2019. 640 с.

18. Інформаційна та кібернетична безпека підприємства : підручник / Г. М. Гулак та ін. Львів : Магнолія, 2023. 370 с.

19. Роберто Рохас-Сесса. Interconnections for Computer Communications and Packet Networks. Apple Press, 2019. 296 p.

20. Едвард Тец. Cisco Packet Tracer. Wiley. John Wiley & Sons, LTD, 2020. 210 p.

21. Едвард Тец. Cisco Networking All-in-One For Dummies. Wiley. John Wiley & Sons, LTD, 2019. 720 p.

22. Рамський Ю. С., Олексюк В. М., Балик А. Адміністрування комп'ютерних мереж та систем : навч. посіб. Київ : НК-Клуб, 2020. 196 с.

23. Євсеєв С., Дженюк Н. Комп'ютерні мережі Книга 1 Технології комп'ютерних мереж. Львів : Новий світ-2000, 2024. 471 с.

24. Коробейнікова Т., Захарченко С. Комп’ютерні мережі. Львів : Львів. політехніка, 2022. 228 с.

25. Лунтовський А. О., Мельник І. В. Комп'ютерні мережі та телекомунікації. Київ : Ун-т "Україна", 2019. 274 с.

26. Струтинська О. Інформаційні системи та мережеві технології. Київ : Ун-т "Україна", 2019. 211 с.

27. Інформаційна безпека : підручник / М. Чеховська та ін. Київ : Ліра-К, 2021. 412 с.

28. Євсеєв С., Дженюк Н. Комп’ютерні мережі Книга 2 Архітектура комп’ютерів. Львів : Новий світ-і, 2024. 346 с.

29. Інформаційна безпека та кібербезпека держави : навч. посіб. / Н. Титова та ін. Київ : Ліра-К, 2024. 224 с.

30. Мельник А. Архітектура компю'тера : підручник. Луцьк : Вол. обласна друк., 2019. 470 с.

31. Палеха Ю., Оксіюк О., Мурейко Н. Документально-інформаційні комунікації : навч. посіб. Київ : Ліра-К, 2020. 386 с.

32. Буров Є. Комп’ютерні мережі : підручник. Київ : Магнолія, 2006. 256 с.

33. Остапов С., Король О., Євсеєв С. Технології захисту інформації : навч. посіб. Київ : Новий світ-2000, 2024. 678 с.

34. Технічний захист інформації / В. Богуш та ін. Київ : Ліра-К, 2022. 508 с.

35. Бобал Ю. Я., Горбатий І. В. Інформаційна безпека. Львів : Львів. політехніка, 2019. 580 с.

36. Пашорін В. І., Костюк Ю. В. Безпека інформаційних систем : навч. посіб. Київ : КНТЕУ, 2023. 376 с.

37. Хомуляк М. Адміністрування комп'ютерних систем і мереж : навч. посіб. Київ : Магнолія, 2023. 153 с.

38. Когут Ю. Корпоративна безпека : навч. посіб. Київ : Сідкон, 2021. 460 с.

Додаток А

Налаштування свічів в торгових приміщеннях

```
enable
configure terminal
hostname StoreSwitch3-1
service password-encryption
line console 0
password Admin
login
exit
line vty 0 15
password Admin
login
exit
enable secret Admin
exit
copy running-config startup-config
```

Додаток Б

Налаштування свіча в головному офісі

```
enable
configure terminal
hostname CentralSwitch
service password-encryption
line console 0
password Admin
login
exit
line vty 0 15
password Admin
login
exit
enable secret Admin
exit
copy running-config startup-config
```

Додаток В

Налаштування центрального роутера

```
enable
configure terminal
hostname CentralRouter
banner motd $Authorized access only!$
enable secret Adm1n$
service password-encryption
no ip domain-lookup
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.240
no shutdown
interface GigabitEthernet3/0
ip address 192.168.3.1 255.255.255.224
no shutdown
interface GigabitEthernet2/0
ip address 192.168.2.1 255.255.255.224
no shutdown
interface GigabitEthernet1/0
ip address 192.168.1.1 255.255.255.224
no shutdown
line console 0
password 0neS
login
logging synchronous
exec-timeout 60 0
ip domain-name central
crypto key generate rsa
```

2048
ip ssh version 2
username admin privilege 15 secret admin
line vty 0 4
transport input ssh
login local
logging synchronous
exec-timeout 60 0
exit
exit
copy running-config startup-config
enable
configure terminal
class-map match-all TCP
match protocol http
class-map match-all UDP
match protocol https
class-map match-any VIDEO-TRAFFIC
match protocol rtp
match protocol h323
exit
policy-map QOS-POLICY
class TCP
priority percent 15
class UDP
priority percent 15
class VIDEO-TRAFFIC
priority percent 30
class class-default

```
fair-queue
exit
exit
interface GigabitEthernet1/0
service-policy output QOS-POLICY
interface GigabitEthernet2/0
service-policy output QOS-POLICY
interface GigabitEthernet3/0
service-policy output QOS-POLICY
end
interface GigabitEthernet0/0
fair-queue
interface GigabitEthernet1/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.240
interface GigabitEthernet1/2
nameif outside
security-level 0
ip address 210.210.0.2 255.255.255.240
object network obj_any
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
route inside 0.0.0.0 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 210.210.0.1
access-list outside_access_in extended permit ip any any
access-list outside_access_in extended permit icmp any any
access-group outside_access_in in interface outside
class-map inspection_default
```

match default-inspection-traffic

policy-map type inspect dns preset_dns_map

parameters

message-length maximum 512

policy-map global_policy

class inspection_default

inspect dns preset_dns_map

inspect ftp

inspect h323

inspect http

inspect icmp

inspect tftp

service-policy global_policy global

access-list 101 permit ip host 192.168.1.11 host 192.168.0.3

access-list 101 permit ip host 192.168.1.12 host 192.168.0.3

access-list 101 permit ip host 192.168.1.13 host 192.168.0.3

access-list 101 permit ip 192.168.1.0 0.0.0.31 host 192.168.0.4

access-list 101 deny ip 192.168.1.0 0.0.0.31 192.168.2.0 0.0.0.31

access-list 101 deny ip 192.168.1.0 0.0.0.31 192.168.3.0 0.0.0.31

access-list 101 deny ip any any

interface GigabitEthernet1/0

ip access-group 101 in

access-list 102 permit ip host 192.168.2.12 host 192.168.0.3

access-list 102 permit ip host 192.168.2.13 host 192.168.0.3

access-list 102 permit ip host 192.168.2.14 host 192.168.0.3

access-list 102 permit ip 192.168.2.0 0.0.0.31 host 192.168.0.4

access-list 102 deny ip 192.168.2.0 0.0.0.31 192.168.1.0 0.0.0.31

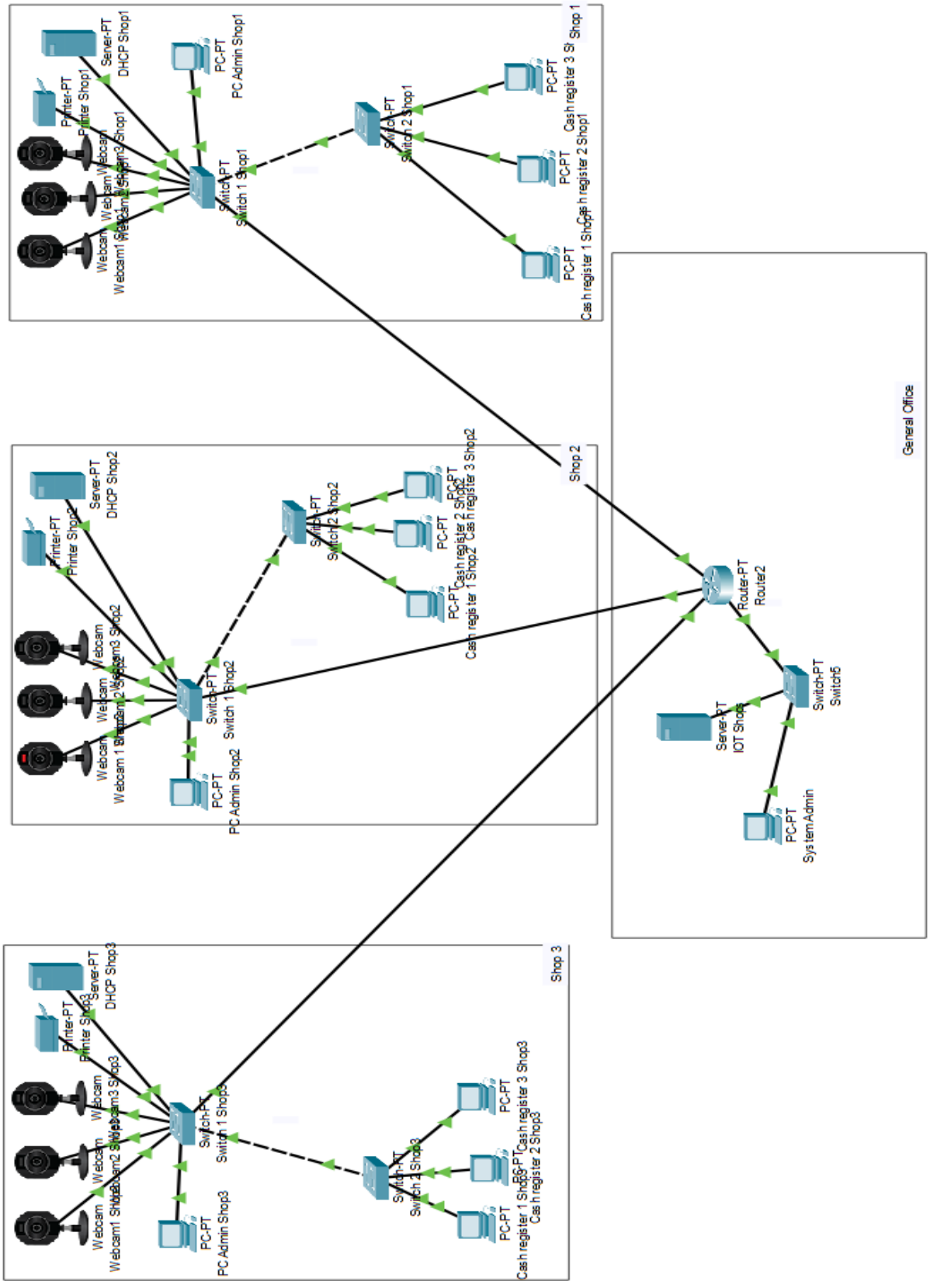
access-list 102 deny ip 192.168.2.0 0.0.0.31 192.168.3.0 0.0.0.31

access-list 102 deny ip any any

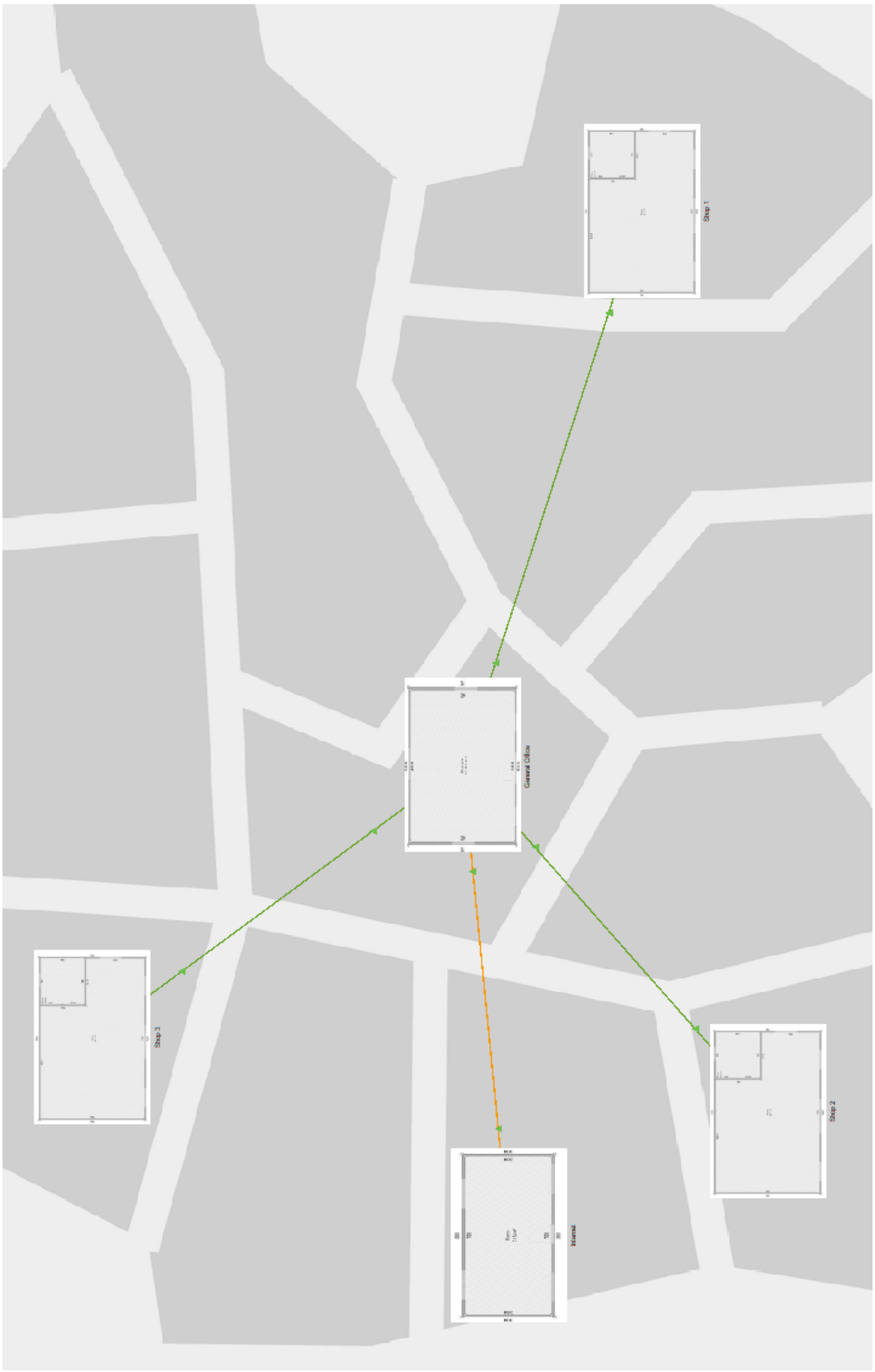
```
interface GigabitEthernet2/0
ip access-group 102 in
access-list 103 permit ip host 192.168.3.11 host 192.168.0.3
access-list 103 permit ip host 192.168.3.12 host 192.168.0.
access-list 103 permit ip host 192.168.3.13 host 192.168.0.3
access-list 103 permit ip 192.168.3.0 0.0.0.31 host 192.168.0.4
access-list 103 deny ip 192.168.3.0 0.0.0.31 192.168.2.0 0.0.0.31
access-list 103 deny ip 192.168.3.0 0.0.0.31 192.168.3.0 0.0.0.31
access-list 103 deny ip any any
interface GigabitEthernet3/0
ip access-group 103 in
```

Додаток Г

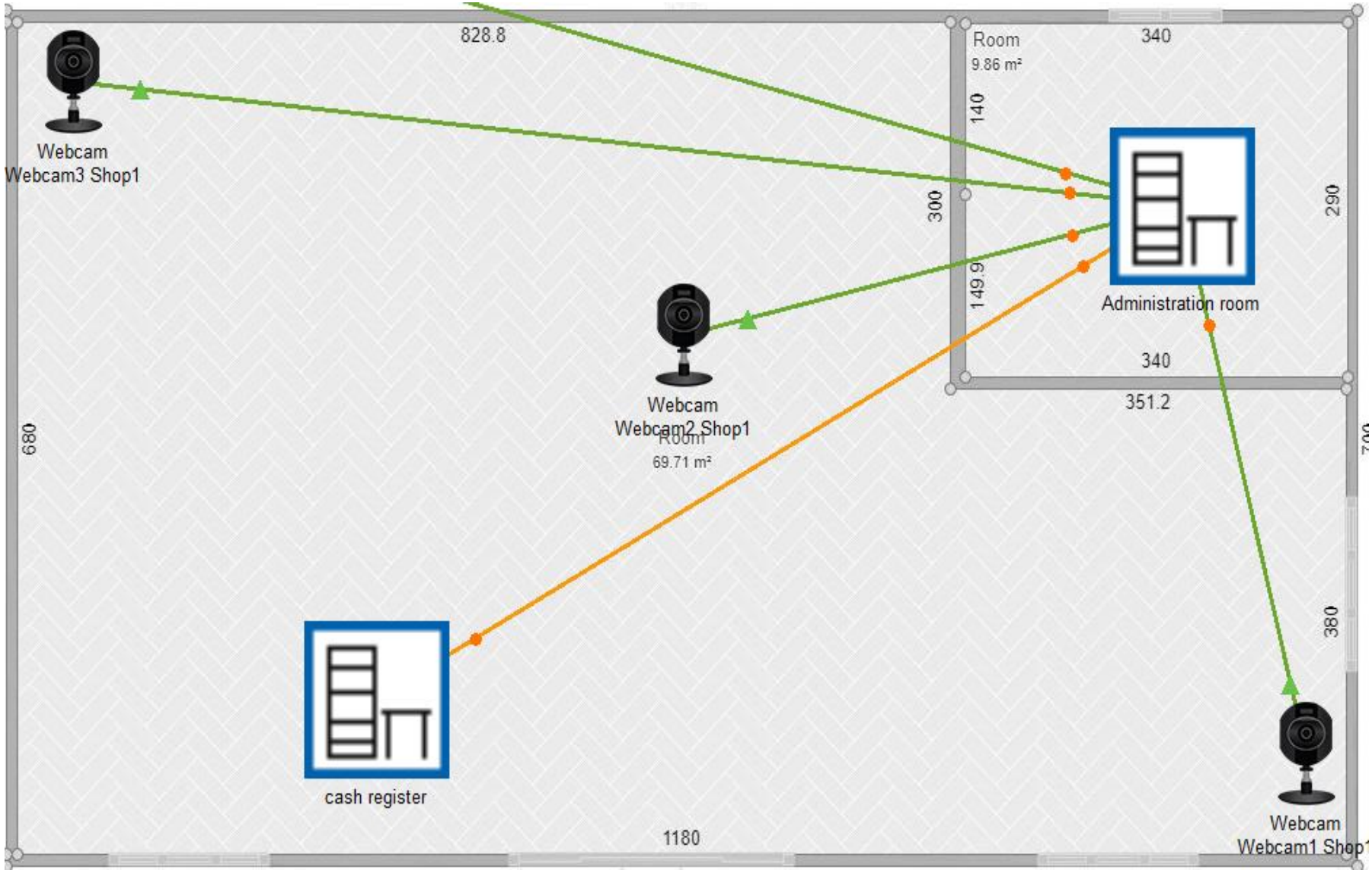
Копія графічної частини

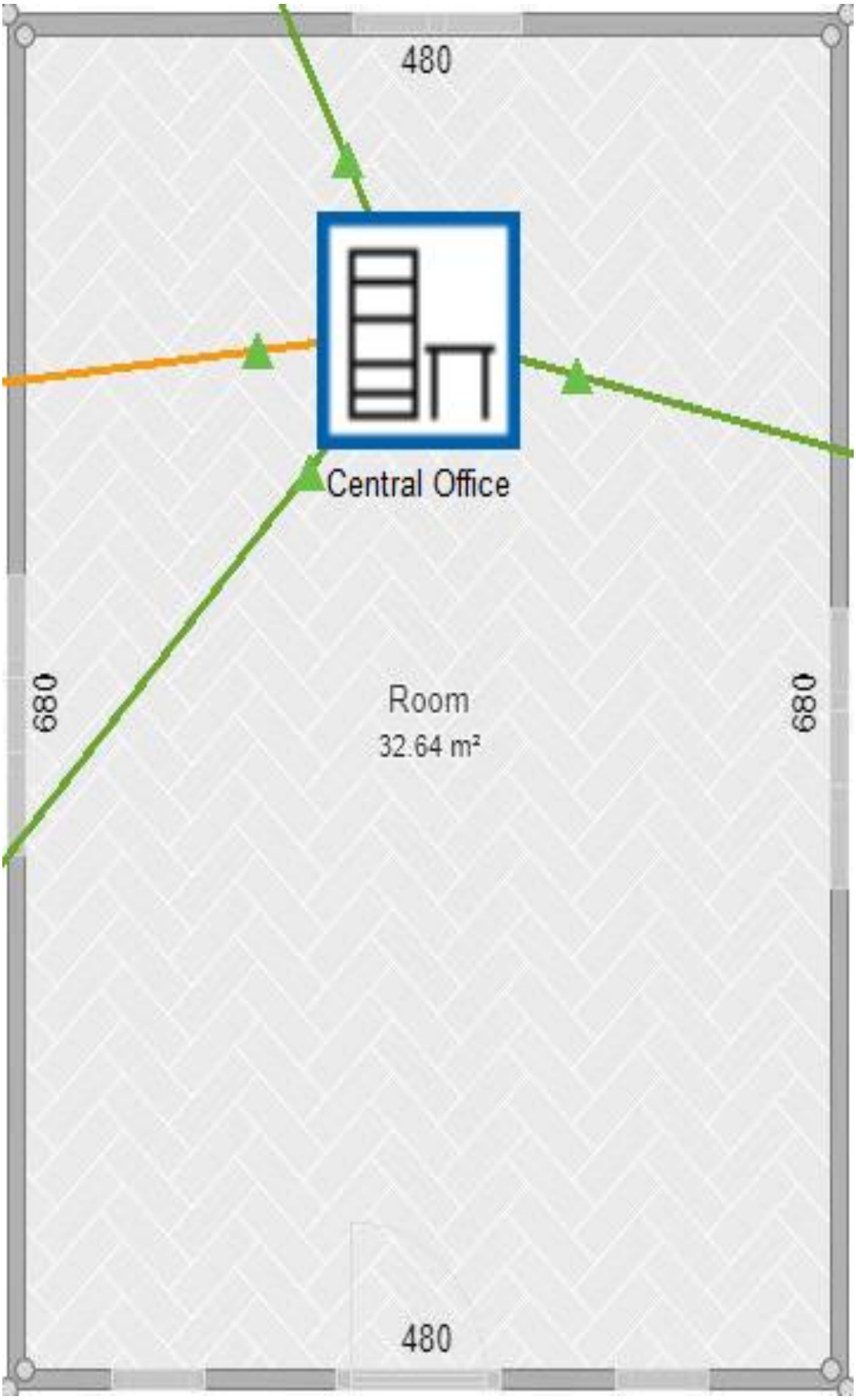


Зм.	Арк.	№ докум.	Підпис	Дата		Літера	Маса	Масштаб
Розроб.								
Перевір.						Аркуш	Аркушів	
Н. Контр.								
Т. Контр.								
Затв.								



Зм.	Арк.	№ докум.	Підпис	Дата		Літера	Маса	Масштаб
Розроб.								
Перевір.								
Н. Контр.						Аркуш	Аркушів	
Т. Контр.								
Затв.								


828.8
Room
9.86 m²
340
140
300
290
149.9
Webcam
Webcam3 Shop1
Administration room
340
351.2
Webcam
Webcam2 Shop1
Room
69.71 m²
680
380
cash register
1180
Webcam
Webcam1 Shop1



Зм.	Арк.	№ докум.	Підпис	Дата		Літера	Маса	Масштаб
Розроб.								
Перевір.						Аркуш	Аркушів	
Н. Контр.								
Т. Контр.								
Затв.								

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Пастушкова Дмитра Сергійович
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КІ1-20-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

19.06.24
дата


підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

Дата перевірки:
16.06.2024 21:32:11 EEST

Дата звіту:
16.06.2024 21:35:21 EEST

ID перевірки:
1016365916

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100008300

Назва документа: **Пастушков Антиплагіат**

Кількість сторінок: **62** Кількість слів: **11035** Кількість символів: **89310** Розмір файлу: **863.55 KB** ID файлу: **1016172050**

16.8%
Схожість

Найбільша схожість: **13.7% з Інтернет-джерелом** (https://www.essuir.sumdu.edu.ua/bitstream-download/123456789/804.

16.1% Джерела з Інтернету 738 ..... Сторінка 64

1.53% Джерела з Бібліотеки 128 ..... Сторінка 68

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 17

Sun Jun 16 20:04:13 EEST 2024, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 13%**

	Документ		Сумарний збіг по Базі Даних	
ID: 130856 Назва: Розподілена інформаційно-телекомунікаційна система торгівельного підприємства Додано в БД: 2024-06-16 Автора: Пастушков Д.С. Керівники: Джулій В.М. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	71357	1089	1651 (2%)	25 (2%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Розподілена інформаційно-телекомунікайна мережа торгівельного підприєства

Автор: Дмитро ПАСТУШКОВ
Спеціальність: 123 – Компютерна інженерія
Освітня програма: Програмування та захист комп`ютерних систем і мереж
Науковий керівник: Володимир ДЖУЛІЙ., к.т.н, доц.
Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 16.8% і адресується до 866 першоджерел, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Володимир ДЖУЛІЙ

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

Дата: 19.06.2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Пастушков Дмитро Сергійович

Тема Розподілена інформаційно-телекомунікаційна система торгівельного підприємста

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4; кількість сторінок записки 61.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі була розроблена розподілена інформаціно-телекомунікайна система торгівельно підприєства. Ця мережа налаштована таким чином, щоб забезпечувати високий рівень безпеки та швидкодії передачі даних. У процесі проєктування були розроблені такі компоненти: система контролю доступу, система відеоспостереження та система розміщення обладнання.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі було виконано поставлене завдання як у теоретичній, так і в практичній частині.

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі роботи наведена загальна характеристика задачі, визначені об'єкт, предмет та методи дослідження, а також сформульована мета. Зазначені задачі, що потрібно виконати для досягнення поставленої мети, проведений аналіз досліджуваної проблеми та обгрунтований підхід до її вирішення. У першому розділі розглядаються поняття розподіленої інформаціно-телекомунікайної системи, основні типи загроз і актак, а також методи для запобігання їм. Наступні розділи присвячені розробці комп'ютерної мережі і процесу налаштування для запебечення безпеки та швидкодії цієї мережі. Також був проведений економічний розрахунок системи.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Вона полягає у розробці моделі розподіленої інформаційно-телекомунікаційної системи торгівельного підприємстав, що забезпечує захист інформації та забезпечує високу швидкість передачі даних між пристоями в мережі. Завдяки цьому мережа є захищеною від витоку інформації та вторгнення зловмисників. При проєктуванні системи контролю доступу використане сучасне обладнання фірми ZKTeco.

5. Негативні сторони роботи В системі не передбачено резервне живлення на випадок зникнення електроенергії, що є надзвичайно актуальним в сучасних умовах, тому за відсутності електроенергії не будуть працювати пристрої, які знаходяться в мережі, що унеможливлює функціонування торгівельного підприємства.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень для досягнення мети.

8. Інші зауваження В переліку використаних джерел наявні посилання на популярні ресурси, такі, як Вікіпендія, які не рекомендовано використовувати при написанні кваліфікаціних робіт.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінки «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Бойко Юлій Миколайович,
доктор технічних наук, професор кафедри ТМІТ

«19» червня 2024. _____ (підпис)