Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр

Система захисту мережі малого офісу з віддаленим доступом до ресурсів

КРКБ. 190106.19.01.07 ПЗ

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Виконав студент 4 курсу, група КБ-19-1 07.06.23 Лакоценін З.Є.
Підпис, дата Ініціали, прізвище

Керівник канд. техн. наук, доцент 07.06.23 Орленко В.С.
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

Нормконтролер старший викладач 7.06.23 Мостовий С.В.
Науковий ступінь, вчене звання Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки Кльоц Ю.П.
Підпис, дата Ініціали, прізвище

7 06 2023р.

Хмельницький, 2023

Форма	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
А4		1	КРКБ.190106.19.01.07 ПЗ	Система захисту	64	
				мережі малого офісу		
				з віддаленим доступом		
				до ресурсів		
				Пояснювальна записка		
А4		2	КРКБ. 190106.19.01.07 Е8	Логічна топологія мережі	1	
А4		3	КРКБ. 190109.19.01.10 Е8	Фізична топологія мережі	1	
А4		4	КРКБ. 190106.19.01.07 Е8	Результати тестування	2	
				мережі		

Зм.	Арк.	№ Докум.	Підп.	Дата	КРКБ.190106.19.01.07 ВП		
Розробив		Лаконецнін З.Є.		7.06.23	Система захисту мережі малого офісу з віддаленим доступом до ресурсів Відомість проєкту	Літера	Аркуш	Аркушів
Перев.		Орленко В.С.		07.06.23		и	1	1
Н. контр.		Мостовий С.В.		7.06.23		ХНУ, КБ-19-1		
Затв.		Кльоц Ю.П.		7.06.23				

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень Бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 125 Кібербезпека

Освітня програма Освітньо-професійна програма підготовки бакалаврів

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

"1" 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Лакоценін З. Є.

Прізвище, ім'я, по батькові студента

1. Тема роботи Розробка системи захисту мережі малого офісу з віддаленим доступом до ресурсів

Керівник роботи к.т.н., доц. Орленко В.С.

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 01 березня 2023 р. №5

2. Строк подання студентом роботи на кафедру 01 червня 2023р.

3. Вихідні дані до проекту (роботи) спроєктувати та змоделювати систему захисту мережі малого офісу з віддаленим доступом до ресурсів. Вибрати програмне забезпечення для забезпечення проходження дозволеного та блокування забороненого трафік. Провести тестування мережі.

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Дослідження комп'ютерної мережі з розмежуванням доступу користувачів та постановка задачі. Проектування комп'ютерної мережі малого офісу з розмежуванням доступу користувачів. Реалізація та тестування комп'ютерної мережі малого офісу з розмежуванням доступу. Висновки.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Логічна топологія мережі», «Фізична топологія мережі», «Результат симуляції трафіку».

6. Консультанти розділів курсового проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прий

7. Дата видачі завдання 1 березня 2023р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи	Термін виконання етапів проекту (роботи)	Примітк
1	Ознайомлення з предметною областю	Лютий	–
2	Пошук теоретичної інформації про проектування системи захисту мережі малого офісу з віддаленим доступом до ресурсів	Березень	–
3	Дослідження існуючих рішень	Березень	–
4	Постановка задачі	Березень	–
5	Пошук теоретичної інформації про рішення для покращення системи захисту мережі малого офісу з віддаленим доступом до ресурсів	Квітень	–
6	Початок впровадження покращень до системи захисту мережі малого офісу з віддаленим доступом до ресурсів	Квітень	–
7	Завершення реалізації впровадження покращень до системи захисту мережі малого офісу з віддаленим доступом до ресурсів	Квітень\Травень	–
8	Оформлення пояснювальної записки згідно вимог	Травень	–
9	Оформлення графічної частини	Травень	–
10	Захист КП	09.06.2023	

Студент _____ З. С. Лакоценін
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ В.С. Орленко
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система захисту мережі малого офісу з віддаленим доступом до ресурсів»

Автор роботи: Лакоценін Захар Євгенійович.

Керівник роботи: Орленко Вікторія Сергіївна.

Пояснювальна записка: 65 с., 2 додатка, 25 рис., 3 таблиці, 41 джерело.

Графічна частина: 12 презентаційних слайдів.

СИСТЕМА ЗАХИСТУ МЕРЕЖІ МАЛОГО ОФІСУ, ВІДДАЛЕНИЙ ДОСТУП ДО РЕСУРСІВ, ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ.

Метою роботи є розробка системи захисту мережі малого офісу з віддаленим доступом до ресурсів, яка дозволить підвищити захист інформації і ресурсів в мережі.

У цій роботі було досліджено і проаналізовано предметну область, теоретичну інформацію про проектування системи управління інформаційною безпекою, а також створено і розроблену таку систему, яка дозволяє протестувати впровадження певних правил або методів захисту інформації в лімітованому середовищі, перш ніж вводити виправлення до всієї системи, що спрощує роботу системних адміністраторів та адміністраторів мережі малого офісу, щодо модерування системи та її захисту.

07/06/23

ANNOTATION

Theme of the qualification work: "Small office network security system with remote access to resources"

Author of the work: Lakotsenin Zakhar Evgenievich.

Head of work: Orlenko Viktoriia Serhiivna.

Explanatory note: 65 p., 2 appendices, 25 figures, 3 tables, 41 sources.

Graphic part: 12 presentation slides.

SMALL OFFICE NETWORK SECURITY SYSTEM, REMOTE ACCESS TO RESOURCES, NETWORK INFORMATION PROTECTION.

The aim of the work is to develop a system for protecting a small office network with remote access to resources, which will increase the protection of information and resources in the network.

In this work, the subject area, theoretical information about the design of an information security management system was researched and analyzed, and a system was created and developed that allows testing the implementation of certain rules or methods of information protection in a limited environment before introducing corrections to the entire system, which simplifies the work of system administrators and small office network administrators in moderating the system and protecting it.

07/06/23

ЗМІСТ

ВСТУП

Кібербезпека є однією з найбільш актуальних тем нашого часу, оскільки віртуальний простір стає все більш важливим та значущим для суспільства. В сучасних умовах віддалений доступ до ресурсів є необхідністю для багатьох організацій, що дозволяє працювати з будь-якого місця та за будь-якого часу. Однак, збільшення кількості з'єднань з мережею Інтернет збільшує ризик порушення безпеки інформації. У зв'язку з цим, розробка ефективної системи захисту мережі малого офісу з віддаленим доступом є актуальною й важливою задачею, яка вимагає комплексного підходу до вирішення.

Метою моєї кваліфікаційної роботи є розробка системи захисту мережі малого офісу з віддаленим доступом до ресурсів. Для цього, необхідно провести дослідження існуючих рішень та визначити найбільш ефективні методи захисту, розробити концепцію системи та її структуру, реалізувати та протестувати розроблену систему, а також провести аналіз її ефективності.

Дослідження теми моєї роботи є важливим не тільки для практичного застосування віддаленого доступу до ресурсів, але й має наукове значення. Розробка та впровадження ефективної системи захисту мережі малого офісу з віддаленим доступом допоможе зменшити ризики порушення безпеки інформації, що є надзвичайно важливим завданням у сучасному світі.

Для виконання даної кваліфікаційної роботи було обрано тему "Система захисту мережі малого офісу з віддаленим доступом до ресурсів". Оскільки в сучасному світі інформаційні технології займають все більш вагому роль у бізнесі та повсякденному житті людей, захист інформації є актуальною проблемою, особливо в контексті малого бізнесу.

В рамках даної роботи було розглянуто теоретичний аспект захисту мережі та ресурсів, а також розроблено практичний проект системи захисту мережі малого офісу з віддаленим доступом до ресурсів.

1 ДОСЛІДЖЕННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ З РОЗМЕЖУВАННЯМ ДОСТУПУ КОРИСТУВАЧІВ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Концепція комп'ютерної мережі з розмежуванням доступу та архітектурні принципи

Концепція побудови мережі з розділеним доступом є ключовим аспектом безпеки мережі невеликих офісів. Відповідно до цієї концепції мережа складається з окремих частин, які можуть мати різні рівні доступу до ресурсів мережі [1]. Це означає, що кожен користувач мережі може отримати доступ лише до ресурсів, необхідних для виконання своїх обов'язків. Сегментацію доступу можна здійснити за допомогою мережевих пристроїв, таких як маршрутизатори та комутатори, а також за допомогою різних рівнів автентифікації та авторизації для користувачів мережі.

При побудові мережі з обмеженим доступом також необхідно враховувати фізичний захист мережевих пристроїв і дотримуватися принципу найменших привілеїв для користувачів мережі. Це означає, що користувачі повинні мати лише ті права, які необхідні для виконання своїх обов'язків, що дозволить уникнути несанкціонованого доступу до мережевих ресурсів і знизити ризик інцидентів безпеки мережі.

Відповідно до потреб користувачів і вимог безпеки мережі, різні топологічні структури можуть бути використані для побудови мережі з розділеним доступом. Однією з можливих топологій є зірка, де всі комп'ютери з'єднані з центральним комутатором [2]. Така топологія забезпечує швидку передачу даних і дозволяє легко додавати нові пристрої в мережу. Однак якщо центральний комутатор виходить з ладу, усі комп'ютери втрачають зв'язок.

Інша можлива топологія – це топологія гілок і зірок, де центральний комутатор залишає кілька гілок, до яких підключаються комп'ютери. Така топологія забезпечує більшу надійність, оскільки відмова однієї гілки не

призводить до повної втрати зв'язку в мережі. Однак додавання нових пристроїв може спричинити проблеми з налаштуваннями адресації та маршрутизації [3].

Локальна мережа (LAN) – це частина комп’ютерної мережі, яка охоплює обмежену територію, наприклад окремий будинок, окремий відділ або підприємство, яка зображена на рисунку 1.1. Виходячи з топології та протоколів передачі даних, локальні мережі можна класифікувати на кілька типів [4]. Одним із найпоширеніших типів локальних мереж є Ethernet, який базується на технології передачі даних по дротових мережах. Він забезпечує швидкість передачі даних від 10 до 100 Мбіт/с або навіть вище, залежно від використовуваного стандарту. Іншим типом локальної мережі є Wi-Fi, яка використовує технологію бездротової передачі даних. Його можна використовувати для підключення до мережі різних пристроїв, таких як комп’ютери, смартфони, планшети тощо.

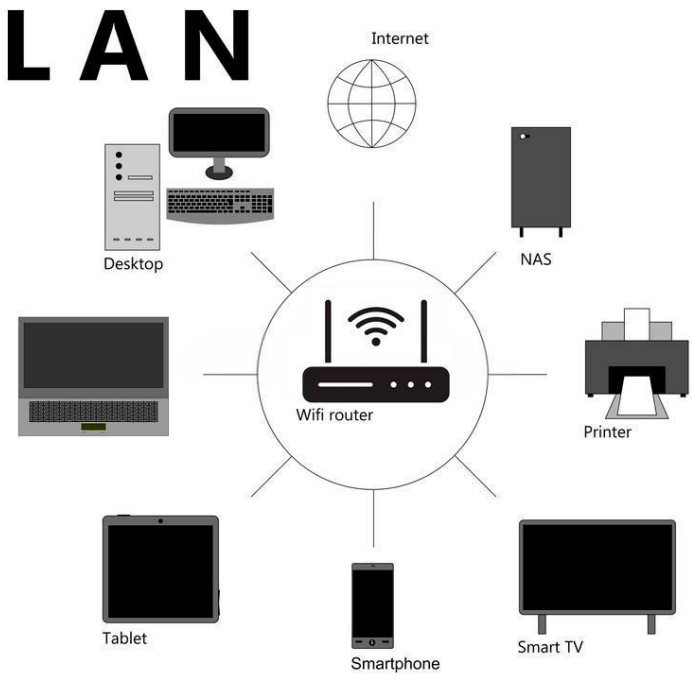


Рисунок 1.1 – Карта локальної мережі (схема)

Класифікація локальних мереж дозволяє зробити правильний вибір топології та типу мережі для конкретної організації чи підприємства, що забезпечить оптимальне функціонування мережі та забезпечить необхідний рівень безпеки та захисту.

Інтернет – ще один тип комп'ютерної мережі, яка об'єднує комп'ютери та інші пристрої по всьому світу. Інтернет є основним джерелом спілкування та обміну даними в сучасному світі.

Крім того, існують інші типи мереж, наприклад міські, глобальні та міжнародні мережі, які забезпечують зв'язок між комп'ютерами та пристроями, розташованими в різних країнах світу.

Ви також можете розрізняти мережі на основі топології, такої як зіркова, кільцева, деревоподібна, лінійна та сітчаста топології. Кожна мережа має свої переваги та недоліки, тому перед вибором певного типу потрібно враховувати такі фактори, як вимоги до мережі, кількість користувачів, відстань між вузлами тощо.

Мережеві пристрої є важливою частиною інфраструктури комп'ютерної мережі, що забезпечує передачу даних між різними пристроями. До активних мережевих пристроїв належать маршрутизатори та комутатори з «розумними» можливостями. Пристрої виконують такі завдання, як передача даних між пристроями користувача, об'єднання та розширення кабельних з'єднань, перетворення даних з одного формату в інший і керування передачею даних.. Вони здатні аналізувати заголовки пакетів даних і приймати рішення про їх подальшу передачу відповідному пункту призначення [5].

До активних мережевих пристроїв належать повторювачі, концентратори, мости, комутатори та маршрутизатори. Кожне з цих пристроїв має свої особливості та функції, які дозволяють ефективно керувати трафіком і забезпечують безпеку та надійність передачі даних. До мережевих пристроїв належать повторювачі, концентратори, мости, комутатори та маршрутизатори.

Повторювач – пристрій, який підсилює мережеві сигнали, щоб вони могли поширюватися на великі відстані через середовище, зображений на рисунку 1.2.

Рисунок 1.2 – Повторювач

Мережевий міст – це пристрій, призначений для фільтрації потоку даних у локальній мережі, щоб локалізувати передачу даних і підтримувати здатність спілкуватися з іншими частинами мережі для перенаправлення потоку даних туди. Міст збирає інформацію про те, на якому порту знаходиться певна MAC-адреса, і приймає рішення про пересилання даних на основі відповідного списку MAC-адрес. Міст виконує лише фільтрацію потоку даних відповідно до MAC-адреси вузла та може швидко пересилати дані.

Концентратор – це простий пристрій у комп’ютерній мережі, який використовується для з’єднання пристроїв у мережу. Однак невідомо, який вузол використовується для певного повідомлення, оскільки його основною функцією є передача електричних сигналів від одного порту до всіх інших портів.

Концентратор отримує сигнали даних від одного порту та дублює їх для всіх інших підключених до нього портів. Це означає, що коли пристрій надсилає повідомлення до концентратора, воно поширюється на всі підключені пристрої в мережі.

Комутатор – це пристрій, який можна назвати «розумним» концентратором, оскільки він передає дані лише безпосередньо одержувачу, зображений на рисунку 1.4.

Рисунок 1.4 – комутатор

Маршрутизатор – це мережевий пристрій, який пересилає пакети даних між мережами на основі адрес, зображений на рисунку 1.5. Маршрутизатори можуть вибрати найкращий шлях у мережі для передачі даних.

Рисунок 1.5 – маршрутизатор

Маршрутизатор може приймати рішення на основі мережевих адрес замість використання індивідуальних MAC-адрес другого рівня. Ця здатність маршрутизаторів робить їх основною магістраллю глобальної мережі Інтернет.

Мережева карта (мережевий інтерфейс) – це пристрій, який дозволяє комп’ютеру підключатися до мережі за допомогою мережевого кабелю або радіозв’язку. Не тільки мережеві карти, а й спеціальні пристрої для підключення до бездротових мереж.

Архітектурні принципи є важливою складовою побудови комп'ютерних мереж. Вони визначають, яким чином пристрої в мережі повинні комунікувати між собою та яким чином мережа повинна функціонувати в цілому. Існує кілька архітектурних принципів, які використовуються при побудові комп'ютерних мереж.

Однією з основних архітектур є клієнт-серверна архітектура. У цій архітектурі сервер забезпечує певні послуги та ресурси, які можуть бути доступні клієнтам у мережі. Клієнти в свою чергу звертаються до сервера, щоб отримати необхідні ресурси або послуги [6].

Іншою архітектурою є P2P (Peer-to-Peer). У такій мережі всі пристрої мають однакові можливості та вони можуть комунікувати між собою без необхідності використання централізованого сервера. Кожен пристрій може одночасно виступати як клієнт і як сервер, що забезпечує рівномірне розподілення навантаження та підвищує надійність мережі.

Ще одним важливим архітектурним принципом є орієнтованість на сервіс (Service Oriented Architecture, SOA). У цій архітектурі кожен сервіс представляє собою окрему функцію, яку можна використовувати як частину більш складного додатку. Сервіси можуть бути розташовані на різних серверах та взаємодіяти між собою для забезпечення більш складних функцій.

Принцип масштабовності (Scalability). Він передбачає можливість розширення мережі, щоб вона могла працювати з більшою кількістю вузлів та забезпечувати достатню швидкість передачі даних. Для цього використовуються різні технології та архітектури, такі як розподілені мережі та хмарні обчислення.

Принцип безпеки (Security). Він передбачає захист мережі від несанкціонованого доступу та захист даних, які передаються по мережі. Для цього використовуються різні захисні технології, такі як мережеві файрволи та шифрування даних.

Також важливим принципом є принцип ефективності (Efficiency), що означає максимальне використання ресурсів мережі. Це досягається за допомогою оптимізації маршрутизації, використанням протоколів з низьким рівнем задержки та мінімізацією втрат даних.

1.2 Демілітаризована зона (DMZ): принцип роботи, переваги та вразливості

Демілітаризована зона (DMZ) - це підмережа, яка знаходиться між зовнішньою мережею та внутрішньою мережею певної організації, яка зображена на рисунку 1.7. Ця зона зазвичай містить публічно доступні ресурси, такі як веб-сервери, електронна пошта, FTP-сервери та інші, які потребують зовнішнього доступу. Однак, ці ресурси не повинні мати прямого доступу до внутрішньої мережі [7].

Основний принцип роботи комп’ютерної мережі з DMZ полягає у створенні фізичного та логічного бар’єру між зовнішньою та внутрішньою мережами. Цей бар'єр забезпечується за допомогою файервола, який фільтрує трафік та відбиває спроби несанкціонованого доступу до внутрішньої мережі.

Крім того, сервери, які розміщені в DMZ, повинні бути налаштовані з дотриманням принципів безпеки, зокрема, у них повинні бути відключені всі непотрібні служби та порти, що можуть бути використані для атак.

Для створення DMZ на мережевому пристрої необхідно налаштувати правила пересилання портів (port forwarding) або використати функції NAT (Network Address Translation). Правила пересилання портів дозволяють пересилати мережевий трафік з одного порту мережевого пристрою на інший порт в зоні DMZ. Функції NAT, у свою чергу, дозволяють перетворювати IP-адреси та порти мережевих пакетів.

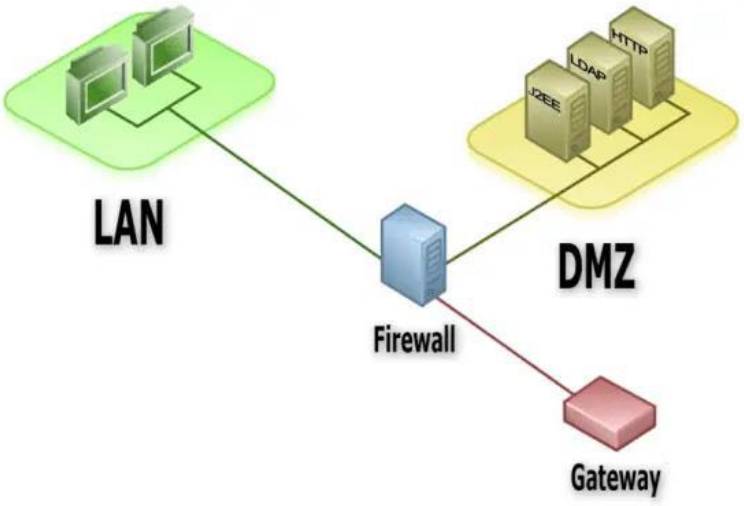


Рисунок 1.7 - Карта мережі з DMZ (схема)

Демілітаризована зона має декілька переваг, які роблять її корисною у використанні в комп'ютерних мережах:

По-перше, вона дозволяє підвищити рівень безпеки мережі. Демілітаризована зона може бути використана для розміщення різноманітних захисних систем, які будуть перевіряти трафік, що надходить з Інтернету до внутрішньої мережі. Таким чином, якщо зловмисники спробують здійснити атаку на мережу, вони спочатку потраплять до демілітаризованої зони, де захисні системи зможуть виявити та заблокувати їх [8].

По-друге, демілітаризована зона може бути використана для забезпечення рівня доступності мережі. Наприклад, внутрішня мережа може бути розділена на дві частини, з яких одна буде використовуватися для роботи з даними, а інша - для підключення зовнішніх користувачів. Таким чином, в разі, якщо зовнішній користувач здійснює атаку на мережу, вона не вплине на роботу внутрішньої мережі, що забезпечить її доступність та стабільність.

По-третє, демілітаризована зона дозволяє підвищити рівень контролю за доступом до ресурсів мережі. Внутрішні користувачі можуть мати різний рівень доступу до ресурсів мережі, в залежності від їх потреб та прав. Зовнішній користувач, який знаходиться в демілітаризованій зоні, може мати

обмежений рівень доступу до ресурсів мережі, що дозволить зменшити ризик несанкціонованого доступу до цих ресурсів.

Інформація може бути піддана чотирьом діям, які потенційно можуть становити загрозу: збір, модифікація, витік та знищення. Ці дії є базовими та потребують подальшого аналізу.

Відповідно до прийнятої класифікації, всі джерела загроз можна розділити на зовнішні та внутрішні. До джерел внутрішніх загроз можна віднести співробітників організації, програмне забезпечення та апаратні засоби.

Внутрішні загрози можуть мати наступні форми прояву: помилки користувачів та системних адміністраторів, порушення співробітниками фірми встановлених регламентів збору, обробки, передачі та знищення інформації, помилки в роботі програмного забезпечення, відмови та збої в роботі комп'ютерного обладнання.

До зовнішніх джерел загроз відносяться комп'ютерні віруси та шкідливі програми, дії організацій та окремих осіб, стихійні лиха.

Формами прояву зовнішніх загроз є: зараження комп'ютерів вірусами або шкідливими програмами, несанкціонований доступ (НСД) до конфіденційної інформації, інформаційний моніторинг з боку конкуруючих структур, розвідувальних та спеціальних служб, дії державних структур та служб, що супроводжуються збиранням, модифікацією, вилученням та знищенням інформації, аварії, пожежі, техногенні катастрофи [9].

Усі види загроз можна розділити на свідомі та несвідомі форми прояву. За даними Інституту захисту комп'ютерів (CSI) та ФБР, більше 50% вторгнень є результатом дій власних співробітників компаній. У той же час, 21% опитаних повідомили про повторні напади. Найпоширенішою формою нападу є несанкціонована зміна даних, яка в основному спрямована проти медичних та фінансових установ. Більше 50% респондентів розглядають конкурентів як можливе джерело нападів. Найбільшу значимість респонденти приділяють фактам прослуховування, проникнення в інформаційні системи та "нападам",

під час яких зловмисники фальсифікують зворотну адресу, щоб перенаправити пошук на непричетних осіб. Найчастіше такими зловмисниками є співробітники та конкуренти [10].

Існують такі види вразливостей:

- несанкціонований доступ може бути здійснений з використанням різних видів вразливостей;
- наслідки зараження комп'ютера шкідливою програмою можуть бути як явними, так і неявними. До неявних зазвичай відносять зараження програмами, які є вірусами, але через помилки в своєму коді або нестандартне програмне забезпечення цільового комп'ютера не можуть виконати своє шкідливе навантаження. При цьому вони ніяк не виражають свою присутність в системі. З ростом числа вірусів клас явних наслідків постійно збільшується [11].
- створення фальшивого потоку, яке називається порушенням автентичності, полягає у намаганні підробити свою сутність під іншу особу або організацію. З поширенням Інтернету та з'явленням несанкціонованого доступу до файлів, документів та персональної інформації, користувачі почали використовувати всі можливі програми своїх систем для захисту власної інформації. Іноді атаки відбуваються не ззовнішніх користувачів, а наприклад, зі збоїв в операційній системі.
- DDoS-атака (розподілена атака на доступність служб) - це набір дій, які можуть повністю або частково відключити інтернет-ресурс. Майже будь-який інтернет-ресурс може бути жертвою, такий як веб-сайт, графічний сервер або державний ресурс. В даний час практично неможлива ситуація, коли хакер самостійно організовує DDoS-атаку. У більшості випадків зловмисник використовує мережу комп'ютерів, що заражені вірусом. Вірус надає зловмиснику необхідний та достатній віддалений доступ до зараженого комп'ютера. Мережа таких комп'ютерів називається ботнетом [12].

1.3 Порівняльний аналіз архітектурних рішень для систем з розмежованим доступом

Архітектурні рішення для проектування систем з розмежованим доступом мають свої переваги та недоліки. Однією з найбільш поширених архітектур є демілітаризована зона, яка використовується для розмежування доступу між внутрішньою та зовнішньою мережами. До переваг такої архітектури належать підвищення рівня безпеки, забезпечення доступності та стабільності мережі, а також контроль доступу до ресурсів мережі.

Однак, демілітаризована зона має й свої недоліки, зокрема, можливість атаки на зону саму по собі, а також складність управління та підтримки.

Іншою архітектурою, яка використовується для розмежування доступу, є мультизональна архітектура. Вона дозволяє створювати кілька зон з різними рівнями безпеки та різними правами доступу до ресурсів мережі. Ця архітектура має переваги в тому, що забезпечує більший рівень безпеки, контролю та гнучкості управління доступом до ресурсів мережі.

Однак, мультизональна архітектура має свої недоліки, зокрема, складність в розгортанні та налаштуванні, високі вимоги до обладнання та програмного забезпечення, а також потребує більш високої кваліфікації персоналу [13].

Ще однією архітектурою, яка використовується для розмежування доступу, є мережевий периметр. Ця архітектура передбачає створення області, яка відділяє внутрішню мережу від зовнішньої, але не містить додаткових зон з різними рівнями безпеки. Перевагами мережевого периметру є його простота в налаштуванні та управлінні, а також менша складність у впровадженні порівняно з іншими архітектурами. Однак, така архітектура може бути менш ефективною в захисті внутрішніх ресурсів мережі від зовнішніх загроз. Також необхідно враховувати, що мережевий периметр може бути менш ефективним у разі збільшення кількості точок доступу до мережі та зростання складності

ресурсів, які потрібно захищати. Тому, при виборі архітектури для розмежування доступу, необхідно уважно враховувати всі переваги та недоліки кожного варіанту та обирати той, який найбільш ефективно відповідає потребам мережі та організації.

Отже, при проектуванні систем з розмежованим доступом необхідно ретельно аналізувати переваги та недоліки різних архітектурних рішень та вибирати те, яке найбільш відповідає вимогам та потребам конкретної мережі та компанії.

Малі офіси з віддаленим доступом до ресурсів є дуже популярними серед бізнесу з усього світу. Однак, такі системи також є досить вразливими до кібератак. Розглянемо основні загрози безпеці малого офісу з віддаленим доступом до ресурсів та можливі шляхи їх запобігання.

Однією з основних загроз є атака хакерів, які можуть намагатися використовувати слабкі місця в системі безпеки, щоб отримати доступ до конфіденційної інформації. Це може стати результатом використання застарілих програм або вразливих пристроїв, які використовуються в мережі.

Додатково, необхідно регулярно оновлювати програмне забезпечення та пристрої, щоб запобігти використанню вразливостей.

Іншою загрозою є атака на мережу через віддалений доступ. Зловмисники можуть використовувати різноманітні програмні засоби для зламу пароля та отримання доступу до мережі. Для запобігання таким атакам рекомендується встановлювати надійні програмні засоби для віддаленого доступу та регулярно оновлювати їх. Крім того, важливо встановлювати обмеження на доступ до ресурсів мережі для зовнішніх користувачів та вимагати складних паролів [14].

Варто також звернути увагу на захист бездротових мереж. Бездротові мережі є дуже зручними для роботи в малому офісі з віддаленим доступом, проте вони також є досить вразливими до атак. Для запобігання загрозам необхідно встановлювати надійні паролі для бездротової мережі,

використовувати шифрування та регулярно оновлювати програмне забезпечення.

Також, необхідно використовувати надійне програмне забезпечення для захисту комп'ютерів та серверів від вірусів, шпигунського ПЗ та інших загроз. Важливо регулярно оновлювати це програмне забезпечення, щоб забезпечити його ефективність у боротьбі з новими загрозами.

Взагалі, безпека малого офісу з віддаленим доступом до ресурсів є дуже важливою проблемою для бізнесу. Забезпечення безпеки мережі потребує витрат часу та коштів, проте воно є необхідним для захисту конфіденційної інформації та запобігання значним втратам для бізнесу.

Комп'ютерні мережі з розмежуванням доступу є дуже важливим інструментом для забезпечення безпеки даних та захисту від кібератак. Основним завданням таких мереж є забезпечення відмежування різних груп користувачів від доступу до конфіденційної інформації та ресурсів мережі.

Однією з переваг використання комп'ютерних мереж з розмежуванням доступу є можливість контролювати рівень доступу до ресурсів мережі. Це дозволяє зменшити ризик несанкціонованого доступу до конфіденційної інформації та забезпечити захист від зловмисних дій.

Крім того, комп'ютерні мережі з розмежуванням доступу дозволяють ефективно управляти ресурсами мережі. За допомогою таких мереж можна встановити права доступу до ресурсів для різних груп користувачів, що дозволить ефективніше використовувати ресурси мережі та зменшити навантаження на сервери.

Однак, мережі з розмежуванням доступу не є універсальним рішенням для всіх компаній та організацій. Вони можуть бути дорогими у впровадженні та підтримці, особливо для невеликих компаній з обмеженим бюджетом. Крім того, вони можуть вимагати додаткових знань та навичок для налаштування та управління, що може бути складним для менеджерів без технічної освіти.

1.4 Постановка задачі.

Метою даного дослідження є розробка системи захисту комп’ютерної мережі, яка зможе забезпечити невеликі офіси обмеженням доступу та віддаленим доступом до ресурсів. Для досягнення поставлених цілей необхідно:

- дослідити основні поняття, принципи роботи та методи, що лежать в основі концепції комп’ютерної мережі. Детальне розуміння цих аспектів допоможе в розробці ефективних систем захисту.
- дослідити принципи роботи DMZ, як вона забезпечує розмежування доступу між зовнішньою та внутрішньою мережами. Також необхідно визначити переваги, які надає DMZ, а також уразливі місця, які необхідно усунути та захистити.
- провести порівняльний аналіз архітектурних рішень систем з обмеженим доступом. Необхідний детальний аналіз різних архітектурних рішень для систем обмеження доступу. Варто розглянути такі аспекти, як різні топології мережі, механізми автентифікації та авторизації, протоколи шифрування тощо. Цей аналіз допоможе визначити найкраще рішення для невеликих офісів з віддаленим доступом.
- розробити систему захисту мережі з обмеженням доступу. Щоб забезпечити надійний і безпечний доступ до ресурсів, необхідно розробити систему, яка включає механізми автентифікації, авторизації, шифрування даних і контролю доступу. Розроблена система має забезпечувати високий рівень безпеки та контролю доступу до ресурсів та забезпечувати простоту та ефективність роботи.

2 ПРОЕКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАЛОГО ОФІСУ З РОЗМЕЖУВАННЯМ ДОСТУПУ КОРИСТУВАЧІВ

2.1 Вимоги по проектуванню та вибір топології мережі малого офісу

Створення локальної мережі в корпоративному офісі є одним з першочергових завдань, які постають перед керівництвом організації. Головне усвідомити, що до цих робіт мають бути залучені справжні професіонали. Робіть ставку не лише на ефективність вашої офісної мережі, а й на її потенціал для майбутнього розширення.

Одним із найважливіших аспектів є кібербезпека комп'ютерних мереж. Він повинен мати надійні рішення для захисту корпоративних даних і конфіденційної інформації. Тому вкрай важливо знайти надійну компанію, яка надає послуги з проектування мереж, має авторитетне та широке портфоліо продуктів і має досвід інтеграції мереж за подібних умов, як ваш офіс [15].

Розробка будь-якої інженерної системи починається з вивчення умов її функціонування. Наступний крок – дизайн. Без правильно складеного проекту неможливо врахувати всі фактори, що впливають на ефективність обладнання та комунікацій. Крім того, проект дозволяє уникнути розбіжностей між експертами різних спеціальностей, які беруть участь у розгортанні мережі. Список експертів великий, від будівельників до айтішників.

Крім основних завдань, пов'язаних з обміном, зберіганням і обробкою інформації, комп'ютерні мережі також повинні відповідати вимогам економії ресурсів для обслуговування та експлуатації.

Для цього необхідно визначити, які пристрої майбутньої мережі вимагають найбільше ресурсів, мінімізувати їх кількість і розвивати інфраструктуру комп'ютерної мережі таким чином, щоб мінімізувати їх навантаження [16].

Для невеликого офісу досить придбати потужний мережевий пристрій, бажано комбінований, до якого можна підключити весь відділ. Варто пам'ятати,

що сучасні хмарні технології також дозволяють економити носії інформації та зробити їх зберігання більш безпечним.

Рекомендується знайти провайдера, який надає вашому офісу єдине хмарне сховище та багатоцільові хмарні сервіси з безпечним доступом. Розвиток IT-технологій та програмного забезпечення дозволяє налагодити «безпаперовий» документообіг у невеликих офісах.

Правильно спроектована мережа також може зменшити кількість дорогих серверів (за рахунок хмарних технологій), комунікаційного, розподільчого та іншого обладнання, що використовується для побудови комп'ютерних мереж.

Ще один фокус – створення публічного кіберпростору. Мережеві диски корпоративної мережі обміну даними утворюють своєрідну «інформаційну скарбницю» для зберігання та віддаленого обміну файлами між співробітниками [17].

Крім того, WiFi можна використовувати для створення окремої мережі Ethernet для бездротового доступу. Переваги мереж WiFi включають такі функції, як усунення необхідності прокладати довгі кабелі. Тому його можна облаштувати навіть після завершення оздоблювальних робіт в кімнаті з мінімальною шкодою для дизайну. Таким же чином, легко змінити розташування більшості видів обладнання та робочих місць. І підключитися до нової мережі також легко.

Недоліком WiFi-мереж є те, що важко скоординувати роботу кількох таких мереж, якщо вони належать одному офісу. І більша «відкритість» мережі WiFi для хакерів (якщо власник вирішить заощадити і на заходах безпеки). Крім того, канали WiFi дуже чутливі до перешкод, особливо електромагнітних.

Дротові мережі є дуже гнучкими та більш захищеними від несанкціонованого доступу. Її можна розширювати практично нескінченно, на відміну від WiFi мережі, можливості якої обмежені потужністю та можливостями підключення до точки доступу, роутера тощо.

У правильно спроектованій дротовій мережі з сучасним і ефективним обладнанням швидкість і стабільність обміну даними також вище, ніж у мережі WiFi. Однак для невеликих офісів ця різниця може бути незначною. Тому головною перевагою «кабелів» є більша надійність і стабільність зв'язку.

При організації комп'ютерної мережі надзвичайно важливим є вибір топології, тобто розташування мережевого обладнання та кабельної інфраструктури. Необхідно вибрати структуру топології, яка може забезпечити надійну та ефективну роботу мережі та зручне керування мережевими потоками даних. Також сподіваються, що мережа має бути дешевою з точки зору витрат на створення та обслуговування, але вона все ще має можливість розширюватися далі, бажано шляхом переходу на технології зв’язку з більшою швидкістю [18].

Більшість мереж побудовано на трьох основних топологіях:

«Шина» — у цій топології всі комп’ютери з’єднані один з одним одним кабелем, яка зображена на рисунку 2.1. Дані, надіслані в таку мережу, передаються на всі комп'ютери, але обробляються тільки цим комп'ютером, апаратна MAC-адреса мережевого адаптера, яка записується в кадрі як адреса одержувача.

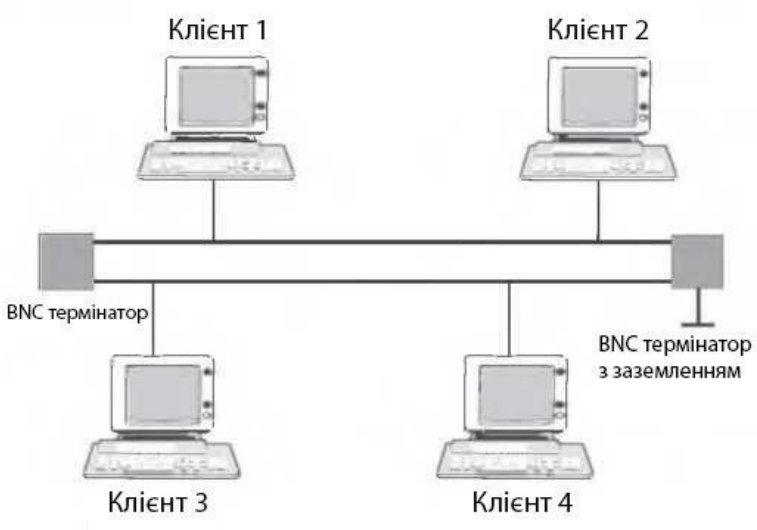


Рисунок 2.1 - Мережа з топологією «шина»

Ця топологія виключно проста в реалізації та дешева (вимагає найменше кабелю), проте має ряд істотних недоліків:

- розширити такі мережі (збільшивши кількість комп’ютерів у мережі та кількість сегментів – окремих ділянок кабелів, що їх з’єднують) важко;
- оскільки шина спільна, лише один комп’ютер може передавати в будь-який момент часу. Якщо два або більше комп’ютерів починають передачу одночасно, виникає спотворення сигналу (зіткнення або колізія), що спричиняє пошкодження всіх кадрів. Потім комп’ютер змушений призупинити передачу та по черзі повторно передавати дані. Чим більш виражений ефект зіткнення, тим більший обсяг інформації передається по мережі і тим більше комп'ютерів підключено до шини. Ці два фактори природно знижують максимально можливу продуктивність і загальну продуктивність мережі, уповільнюючи її. «Шина» є пасивною топологією – комп’ютери тільки «слухають» кабель і не можуть відновлювати затухаючі при передачі по мережі сигнали. Щоб подовжити мережу, потрібно використовувати повторювачі (репітери), які посилюють сигнал перед його передачею у наступний сегмент;
- низька надійність мережі в топології «шина». Коли електричний сигнал досягає кінця кабелю, він (якщо не вжито спеціальних заходів) відбивається, порушуючи роботу всього сегмента мережі. Щоб запобігти подібним відбиттям сигналу, на кінцях кабелів встановлюють спеціальні резистори (осадні резистори), які поглинають сигнали. Якщо в будь-якій частині кабелю стався розрив — наприклад, при порушенні цілісності кабелю або від’єднанні роз’єму — з’являються два незакінчені сегменти, сигнали починають відбиватися на їхніх кінцях, і вся мережа перестає функціонувати.

«Кільце» — у цій топології кожен комп’ютер з’єднаний з двома іншими комп’ютерами, щоб отримувати інформацію від одного комп’ютера та передавати її іншому комп’ютеру, яка зображена на рисунку 2.2. Останній комп'ютер підключається до першого, і кільце замикається.

У такій топології інформація циркулює в одному напрямку, проходячи по черзі кожен комп’ютер. Якщо будь-який комп’ютер у кільці втрачає з’єднання або відмовляється, усі інші комп’ютери в кільці припиняють передачу даних. Для вирішення цієї проблеми часто використовуються механізми контролю доступу, такі як кільця маркерів, де доступ до передачі даних контролюється маркерами, що передаються від одного комп’ютера до іншого [19].

Таким чином, кільцева топологія може забезпечити надійну передачу даних у мережі, але в той же час вона вимагає додаткових механізмів для контролю доступу та обробки втрат зв’язку.

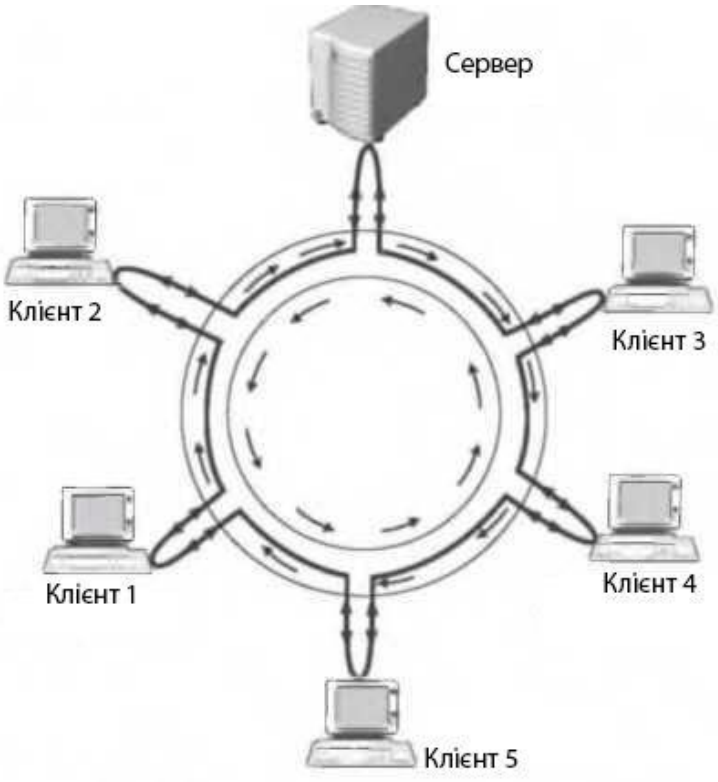


Рисунок 2.2 - Мережа з топологією «кільце»

Тут недоліки трохи переважують переваги для мереж з топологією «шина», тому популярні раніше кільцеві мережі зараз використовуються рідко, відображені у таблиці 2.1.

Таблиця 2.1 - Переваги та недоліки мереж з топологією «кільце»

Переваги	Недоліки
оскільки кабелі в цій мережі не мають вільних кінців, термінатори тут не потрібні	сигнал в «кільці» повинен пройти через усі комп'ютери послідовно (і тільки в одному напрямку), кожен комп'ютер перевіряє, чи надіслано йому інформацію, тому час передачі може бути дуже довгим.
кожен комп'ютер виконує роль ретранслятора, підсилюючи сигнал, що дозволяє будувати міжміські мережі	підключення нового комп'ютера до мережі зазвичай вимагає його зупинки, що перериває роботу всіх інших комп'ютерів; вихід з ладу хоча б одного комп'ютера або пристрою перериває роботу всієї мережі
завдяки відсутності колізій топологія має високу стійкість до перевантажень, забезпечуючи ефективну роботу в ситуаціях, коли в мережі передаються великі обсяги інформації	розрив або коротке замикання в будь-якому кабелі в кільці призведе до непрацездатності всієї мережі
	щоб уникнути зупинки мережі в разі збою комп'ютера або обриву кабелю, зазвичай прокладають два кільця, що значно збільшує вартість мережі

«Active Star» (Активна зірка) - Ця топологія виникла на зорі комп'ютерної техніки, коли всі інші користувачі мережі були підключені до одного потужного центрального комп'ютера. У такій конфігурації весь потік даних

проходить тільки через центральний комп'ютер, який відповідає виключно за управління обміном інформацією між усіма учасниками мережі.

Для такої мережі взаємодіючих організацій зіткнення малоймовірні, але центральний комп’ютер настільки сильно завантажений, що зазвичай цей комп’ютер не бере участі ні в чому, крім обслуговування мережі. Його збій спричиняє збій усієї мережі, тоді як збій або втрата зв’язку з периферійним комп’ютером не впливає на решту мережі. Сьогодні такі мережі зустрічаються дуже рідко.

Більш поширеною топологією сьогодні є подібний варіант – «Зірковий автобус», або «Пасивна зірка», відображена на рисунку 2.3. Тут периферійні комп'ютери підключені не до центрального комп'ютера, а до пасивного концентратора або концентратора. Останній, на відміну від центрального комп’ютера, жодним чином не відповідає за керування обміном даними, натомість виконує ту ж функцію, що й повторювач, а саме відновлення вхідних сигналів і пересилання їх на всі інші комп’ютери та пристрої, підключені до нього. Тому ця топологія, хоча фізично виглядає як «зірка», логічно є топологією «шина» (що відображено в її назві).

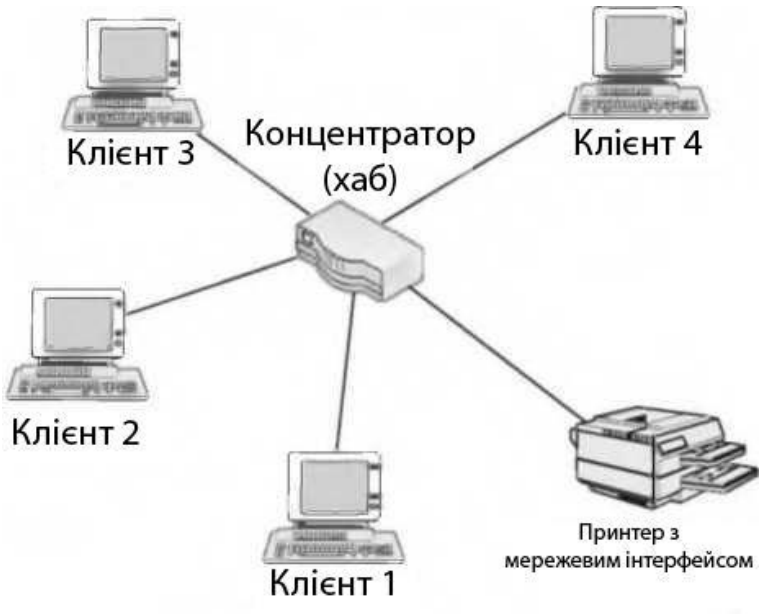


Рисунок 2.3 - Мережа з топологією «зірка-шина»

Незважаючи на високе споживання кабелю, характерне для зіркоподібної мережі, ця топологія має значні переваги перед іншими топологіями, що зумовило її найбільш широке використання в сучасних мережах [20].

Переваги мережі «Star Bus»:

– надійність підключення та відключення комп’ютера від центрального концентратора жодним чином не впливає на решту мережі, обірваний кабель впливає лише на один комп’ютер, термінатор не потрібен;

– простота обслуговування та усунення несправностей, усі комп’ютери та мережеве обладнання під’єднані до центрального пристрою підключення, що значно спрощує технічне обслуговування та ремонт мережі;

– безпека точки підключення централізовані в одному місці, що дозволяє легко обмежити доступ до важливих об'єктів мережі.

Слід зауважити, що при використанні більш "розумних" мережевих пристроїв, таких як мості, комутатори і маршрутизатори, замість концентраторів, отримуємо "проміжний" тип топології, що перебуває між активною та пасивною зіркою. У такому випадку пристрій зв'язку не лише ретранслює вхідні сигнали, але й керує обміном ними. До прикладу можна скористатись топологією «Дерево», яка зображена на рисунку 2.4.

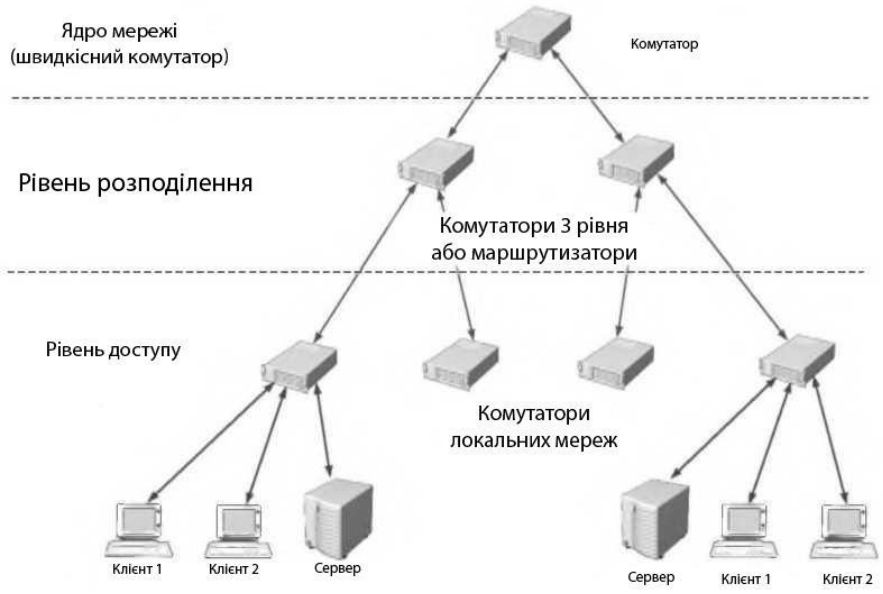


Рисунок 2.4 - Мережа з топологією «дерево»

Реальні комп'ютерні мережі постійно розширюються та модернізуються, тому часто вони мають гібридну топологію, яка є комбінацією кількох базових топологій. Наприклад, можна уявити гібридну топологію, що складається з комбінації зіркової та шинної або кільцевої та зіркової топологій.

Нарешті, слід згадати сітчасті топології, в яких усі або багато комп’ютерів та інших пристроїв безпосередньо з’єднані один з одним, відображену на рисунку 2.5. Така топологія дуже надійна - при перериванні будь-якого каналу передача даних не припиняється, оскільки можливі кілька шляхів доставки інформації. Топології мережі (зазвичай не повні, а часткові) використовуються там, де необхідно забезпечити максимальну відмовостійкість мережі, наприклад, при об'єднанні кількох частин великої корпоративної мережі або підключенні до Інтернету, хоча, звичайно, за це потрібно платити. Вартість: значно збільшена витрата кабелю, складне мережеве обладнання та його налаштування [21].

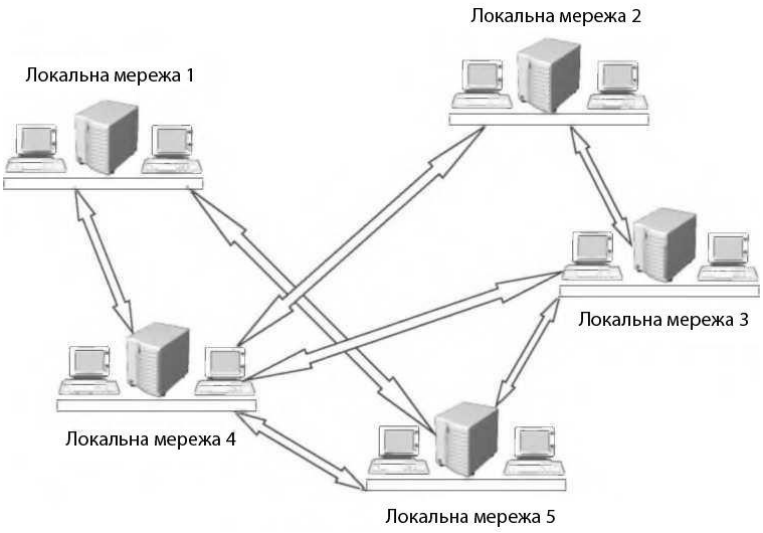


Рисунок 2.5 - Мережа з сітчастою топологією

З топологією мережі тісно пов’язана концепція методу доступу до транспортного середовища, що розуміється як набір правил, які визначають, як комп’ютер повинен надсилати та отримувати дані через мережу.

Основними підходами є:

- множинний доступ з контролем несучої та виявленням колізій;
- множинний доступ з контролем перевізника та запобіганням зіткненням;
- перекази токенів.

Завдяки множинному доступу з розпізнаванням несучої з виявленням зіткнень (CSMA/CD) усі комп’ютери (множинський доступ) «слухають» кабель (перевірка несучої), щоб визначити, чи передаються дані по ньому. Якщо кабель вільний, будь-який комп’ютер може розпочати передачу; тоді всі інші комп’ютери повинні дочекатися, поки кабель звільниться. Якщо комп’ютери починають передачу одночасно та стикаються, вони обидва припиняють передачу (виявлення зіткнення), кожен на різний час, а потім повторно передають дані [22].

Серйозним недоліком цього методу доступу є те, що при великій кількості комп'ютерів і високому навантаженні на мережу збільшується кількість колізій і зменшується пропускна здатність, іноді дуже помітно.

Однак цей спосіб дуже простий в технічній реалізації, тому він використовується в найпопулярнішій сьогодні технології Ethernet. Щоб зменшити кількість колізій, у сучасних мережах використовуються такі пристрої, як мости, комутатори та маршрутизатори.

Метод множинного доступу з визначенням несучої з уникненням зіткнень (CSMA/CA) відрізняється від попереднього методу тим, що комп’ютер надсилає в мережу спеціальний невеликий пакет даних перед передачею даних, щоб повідомити інші комп’ютери про те, що він має намір почати трансляцію. як інші комп'ютери "знають", що передача готова, таким чином уникаючи конфліктів. Звичайно, ці повідомлення збільшують загальне навантаження на мережу та зменшують її пропускну здатність (ось чому метод CSMA/CA працює повільніше, ніж CSMA/CD), але вони безперечно необхідні для таких операцій, як бездротові мережі [23].

Розглянувши найбільш часто використовувані сьогодні мережеві топології та методи доступу, обговоримо й інші чинники, що визначають вибір потрібного типу мережі.

При цьому слід враховувати:

- вже наявну кабельну систему та обладнання;
- як розташовані комп'ютери і де ви збираєтеся розмістити мережеве обладнання;
- розміри планованої мережі;
- обсяг і тип інформації для спільного використання.

У більшості сучасних мереж використовується топологія «зірка» або гібридна топологія, тобто комбінація кількох «зірок» (наприклад, топологія «дерева»), а спосіб доступу до середовища передачі — CSMA/CD (з контролем несучої та виявленням конфліктів). багаторазовий доступ).

2.2 Вимоги до програмного забезпечення та обґрунтування вибору мережевих пристроїв

Вибір мережевого обладнання є важливою частиною забезпечення ефективної та безпечної роботи мережі невеликого офісу з віддаленим доступом до ресурсів. Основними пристроями, які слід розглянути, є комутатори та маршрутизатори.

Вибір комутатора є критично важливим кроком у створенні мережевої інфраструктури невеликого офісу. При виборі комутатора слід враховувати такі фактори, як пропускна здатність, підтримка VLAN, безпека та масштабованість. Пропускна здатність має бути достатньою для задоволення поточних і майбутніх потреб мережі. Підтримка VLAN дозволить логічно розділити мережу на різні сегменти мережі, забезпечуючи безпеку та оптимізацію трафіку. Безпека комутатора включає такі функції, як контроль доступу до портів, захист від атак ARP-спуфінгу та механізми захисту від

переповнення буфера. Крім того, варто звернути увагу на масштабованість комутатора, щоб забезпечити можливість розширення мережі в майбутньому.

Основне завдання цього пристрою - забезпечити користувачам безперебійне підключення до мережі Інтернет. Комутатор призначений для простої та швидкої передачі даних на певні пристрої. Перед вибором обладнання необхідно розглянути основні типи вимикачів, які використовуються для організації вашого локального простору [24].

Комутатори Ethernet є важливою частиною мережевої інфраструктури, і їх вибір повинен бути обґрунтованим і залежати від потреб і вимог системи захисту мережі для невеликих офісів з віддаленим доступом до ресурсів. Вимикачі можна класифікувати за типом керування та конструктивними особливостями.

Некеровані комутатори популярні в домашніх мережах і на малих підприємствах. Вони прості у використанні та не вимагають складного налаштування.

Напівкеровані комутатори дозволяють налаштувати базовий рівень безпеки та мають простий інтерфейс налаштування. Вони корисні в мережах, які потребують додаткових заходів безпеки.

Керовані комутатори є найкращим вибором для компаній з великими локальними мережами. Вони мають розширені параметри налаштування та забезпечують високий рівень безпеки для передачі даних.

Крім того, вимикачі також можна класифікувати за конструктивними особливостями. Модульні комутатори характеризуються складною технічною реалізацією і високою вартістю, але можуть гнучко розширювати кількість портів і функцій. Стаціонарні комутатори мають обмежену кількість портів, але є більш економічним варіантом.

Вибираючи комутатор Ethernet для системи безпеки мережі невеликого офісу, яка отримує віддалений доступ до ресурсів, слід враховувати такі фактори, як вимоги до мережі, рівень безпеки, масштабованість і можливості

пристрою. Варто вибрати комутатор, який максимально відповідає вимогам системи захисту мережі невеликого офісу для віддаленого доступу до ресурсів. Керовані модульні комутатори можуть бути найкращим вибором, оскільки вони надають можливість налаштовувати, покращувати продуктивність і розширювати функціональність мережі [25].

Також важливо враховувати масштабованість комутатора, особливо можливість розширення портів і функцій. Щоб запобігти майбутнім проблемам, виберіть комутатори, здатні обробляти зростаючі обсяги даних і трафік.

Остаточний вибір комутаторів Ethernet і вимог до програмного забезпечення має ґрунтуватися на унікальних потребах і характеристиках невеликих офісних мереж, які мають віддалений доступ до ресурсів. Забезпечення надійності, безпеки та ефективності мережевої інфраструктури є основними цілями при виборі відповідного мережевого обладнання та програмного забезпечення.

Крім того, важливо визначити програмні вимоги для комутатора. Такі корисні параметри, як якість обслуговування (QoS) і протокол керування мережею (SNMP), покращують продуктивність мережі та керованість. Слід також переконатися, що програмне забезпечення сумісне з іншими компонентами інфраструктури та має можливість оновлюватися для забезпечення безпеки та усунення вразливостей.

Вибираючи комутатори Ethernet і встановлюючи вимоги до програмного забезпечення, ми створюємо надійну та безпечну мережеву інфраструктуру для невеликих офісів, які можуть отримувати віддалений доступ до ресурсів. Це допоможе забезпечити безпеку мережі, ефективну передачу даних і задовольнити вимоги користувачів [26].

Комутатор PoE (Power over Ethernet) — це особливий тип комутатора, який може не тільки передавати дані, але й подавати живлення на пристрої по одному кабелю, що спрощує процес розгортання мережі, зображений на рисунку 2.6. Вони дозволяють живити різні пристрої, такі як IP-телефони,

бездротові точки доступу, камери тощо, безпосередньо через мережеві кабелі, заощаджуючи час і ресурси при живленні кожного пристрою окремо.

Рисунок 2.6 - Свічі PoE з портом Gigabit Ethernet

Використання комутатора PoE є зручним і ефективним рішенням для мереж з великою кількістю пристроїв, які потребують живлення через мережевий кабель. Вони спрощують кабельну інфраструктуру, зменшують необхідну кількість електроенергії та покращують керування мережею. Вибираючи комутатори PoE, зверніть увагу на їх потужність, підтримку стандартів PoE, таких як IEEE 802.3af або IEEE 802.3at, і додаткові функції, такі як керування трафіком, безпека та масштабованість.

Вибираючи комутатор PoE для системи захисту мережі в невеликому офісі, де доступ до ресурсів здійснюється віддалено, слід враховувати конкретні потреби та характеристики мережі. По-перше, важливо визначити потужність, необхідну для комутатора, виходячи з кількості пристроїв, які будуть живитися від PoE. Кожен пристрій має власне визначене енергоспоживання, і загальна потужність комутатора має бути достатньою для підтримки всіх пристроїв [27].

Другий аспект — підтримка стандарту PoE. Переконайтеся, що комутатор PoE підтримує такі стандарти, як IEEE 802.3af або IEEE 802.3at, щоб забезпечити сумісність з різними пристроями. Це важливо, оскільки для живлення різних пристроїв може знадобитися різна кількість енергії.

2.3 Вимоги до захисту мережевих пристроїв та план виконання роботи

Вимоги до захисту мережевих пристроїв у системі захисту мережі малого офісу з віддаленим доступом до ресурсів є критичними для забезпечення безпеки та надійності мережевої інфраструктури.

Реалізація фізичного захисту мережевих пристроїв, включаючи маршрутизатори, комутатори та сервери, є важливим аспектом системи захисту мережі малого офісу з віддаленим доступом до ресурсів. Для забезпечення фізичної безпеки мережевих пристроїв можна виконати наступні заходи:

- мережеве обладнання слід розміщувати в спеціально обладнаних місцях з обмеженим доступом і контрольованими умовами. Це можуть бути серверні або спеціальні мережеві шафи, де обладнання захищене від несанкціонованого фізичного доступу;
- використовуйте різні механізми фізичної безпеки, такі як замки на шафах, контроль доступу за допомогою ідентифікаційних карток або біометричні методи, можна використовувати для забезпечення додаткової фізичної безпеки пристрою;
- встановіть систему моніторингу та сповіщення для виявлення будь-якої неправомірної поведінки або вторгнення в приміщення, де розташоване мережеве обладнання. Це можуть бути системи відеоспостереження, датчики руху або системи оповіщення у разі незвичайної активності;
- забезпечте фізичну безпеку кабелів, підключених до мережевих пристроїв. Вони можуть бути піддані фізичному пошкодженню або несанкціонованому доступу. Фізичну безпеку мережі можна підвищити за допомогою контрольованих захищених кабельних каналів або шифрування даних, що передаються по кабелю [28].

Мережеві пристрої повинні мати механізми автентифікації для перевірки ідентичності користувачів і авторизації для доступу до ресурсів. Важливими аспектами є використання надійних паролів, двофакторної автентифікації,

регулярне оновлення прав доступу та інші заходи безпеки. Для забезпечення надійності автентифікації та авторизації мережевих пристроїв можна вжити таких заходів:

- належним чином налаштуйте мережеві пристрої на вимогу надійних паролів, які містять комбінацію літер, цифр і спеціальних символів. Слабкі або очевидні паролі заборонені та потребують регулярної зміни пароля;
- регулярно переглядайте та оновлюйте дозволи доступу до ресурсів на мережевих пристроях. Видаліть непотрібні облікові записи користувачів, змініть рівні доступу за потреби та за принципом найменших привілеїв;
- створіть механізми моніторингу та журналювання для запису подій, пов’язаних з автентифікацією та авторизацією. Це дозволить виявити аномальну активність, спроби несанкціонованого доступу та забезпечити належний контроль системи.

Важливо використовувати шифрування для захисту конфіденційності та цілісності передачі даних на мережевих пристроях. Використання протоколів шифрування, таких як SSL/TLS, IPSec тощо, запобігає перехопленню та злому даних. Деякі можливі заходи для ефективного шифрування даних на мережевих пристроях включають [29]:

- налаштуйте SSL/TLS для шифрування даних, що передаються між веб-сайтами та користувачами. Це важливо для захисту конфіденційності персональних даних, таких як паролі, банківські реквізити та інша конфіденційна інформація;
- налаштування протоколу IPSec для шифрування трафіку між мережевими пристроями та створення захищених тунелів забезпечує конфіденційність і цілісність даних під час їх переміщення по мережі;
- установіть безпечне з’єднання VPN, щоб забезпечити безпеку під час підключення користувачів до віддалених ресурсів. Це дозволяє шифрувати трафік і забезпечує безпеку під час передачі даних між користувачами та мережевими пристроями;

– якщо ви отримуєте фізичний доступ до пристрою, використовуйте шифрування на рівні даних (наприклад, шифрування файлів або дискового простору), щоб захистити конфіденційну інформацію.

Регулярне оновлення програмного забезпечення мережевого пристрою є важливим аспектом безпеки. Використання найновішої версії та патчів допомагає усунути виявлені вразливості та забезпечує захист від відомих атак. Деякі можливі кроки для ефективного оновлення програмного забезпечення мережевого пристрою включають:

– налаштуйте автоматичне оновлення програмного забезпечення на мережевих пристроях, щоб вони отримували регулярні оновлення безпеки. Це дозволить вам швидко встановлювати нові версії прошивки та патчів і підтримувати безпеку вашої мережі;

– слідкуйте за виробниками мережевого обладнання та підписуйтесь на сповіщення про оновлення безпеки, це дозволить бути сповіщеним про оновлення версії;

– перед встановленням нових версій ПЗ та виправлень рекомендується провести тестування в тестовому або резервному середовищі. Це допоможе уникнути можливих проблем або втрати налаштувань під час оновлення;

– постійно відстежуйте оновлення безпеки виробників мережевого обладнання та вчасно їх оновлюйте. Це запобіжить можливим зломам і забезпечить надійний рівень безпеки мережі.

Якщо використовується віддалений доступ до мережевих пристроїв, мають бути задіяні механізми безпеки, щоб забезпечити безпечні з’єднання та обмежити адміністративний доступ. Можливі заходи, пов'язані із віддаленим керуванням, які сприяють забезпеченню безпеки мережевих пристроїв:

– встановлення з’єднання VPN забезпечує безпечний тунель даних між віддаленими та мережевими пристроями. Це дозволяє уникнути перехоплення та злому даних під час передачі;

– використовуйте такі протоколи, як SSH (Secure Shell) або HTTPS (HTTP Secure), щоб забезпечити шифрування з’єднання та запобігти перехопленню та злому даних під час віддаленого керування;

– налаштуйте доступ до віддаленого керування, щоб обмежити привілеї користувачів і визначити їхній рівень доступу до різних функцій і операцій;

– переконайтеся, що операції дистанційного керування регулярно реєструються та контролюються для виявлення можливих аномалій або несанкціонованого доступу;

– для підвищення безпеки віддаленого доступу потрібні надійні паролі та механізми двофакторної автентифікації.

Встановлення та налаштування відповідних механізмів безпеки для віддаленого керування допоможе захистити мережеві пристрої та запобігти несанкціонованому доступу та злому.

Для успішної реалізації системи захисту мережі малого офісу з віддаленим доступом до ресурсів необхідно декілька етапів.

Провести аналіз поточного стану мережі є першим кроком у впровадженні системи мережевої безпеки для невеликих офісів, які отримують доступ до віддалених ресурсів.

Під час цього етапу детально перевірити існуюче мережеве обладнання та конфігурації, щоб виявити потенційні вразливості та ризики, пов’язані з віддаленим доступом до ресурсів. Виявляючи наявні мережеві пристрої, ретельно дослідити кожен пристрій, щоб визначити його номер моделі, версію ПЗ, налаштування мережевого інтерфейсу та застосовану політику безпеки. Це дає повний огляд наявного обладнання та його поточний стан [30].

Після визначення мережевих пристроїв оцінити потенційні вразливості та ризики, пов’язані з віддаленим доступом до ресурсів. Це включає перевірку наявності захищених з’єднань для віддаленого доступу, перевірку використання механізмів автентифікації та авторизації, оцінку використання

шифрування для передачі даних та аналіз ризиків, які можуть виникнути через незахищений доступ до ресурсів. Крім того, перевірити наявність оновлень програмного забезпечення для своїх мережевих пристроїв і переконатися, що вони встановлені та налаштовані відповідно до останніх рекомендацій виробника. Також варто перевірити, чи є необхідні механізми моніторингу безпеки для виявлення потенційних загроз і реагування на них [31].

Аналіз поточного стану вашої мережі може надати цінну інформацію про сильні та слабкі сторони наявної інфраструктури, виявити потенційні вразливості та ризики, а також розробити системи безпеки мережі для віддаленого доступу невеликих офісів, а також основи впровадження. Дані, отримані на цьому етапі, будуть використані для розробки стратегій захисту та вибору необхідних заходів безпеки для забезпечення надійності та конфіденційності мережі.

Наступним етапом, необхідно розробити стратегію захисту мережі невеликого офісу з віддаленим доступом до ресурсів. Під час цього етапу розробити вимоги щодо захисту мережевих пристроїв і визначити необхідні заходи безпеки, такі як автентифікація, шифрування, оновлення програмного забезпечення тощо.

Наступним кроком є встановлення механізмів автентифікації та шифрування на мережевих пристроях. Це включає налаштування безпечних методів автентифікації, наприклад використання надійних паролів, двофакторної автентифікації або використання сертифікатів. Шифрування також налаштовано для забезпечення конфіденційності та цілісності даних, що передаються через мережеві пристрої. Після встановлення механізмів автентифікації та шифрування протестуйте та перевірте, чи система безпеки функціонує належним чином. Це включає перевірку правильності налаштувань, виявлення можливих проблем, перевірку функціональності механізмів автентифікації та шифрування, а також виконання тестів на проникнення для перевірки стійкості системи до можливих атак. Результати тестової перевірки

допоможуть виявити та усунути можливі проблеми безпеки та забезпечити ефективність та надійність системи захисту. У разі виявлення вразливостей або помилок їх слід виправити та перевірити повторно, щоб переконатися, що мережа малого офісу є достатньо безпечною. Виконання цього кроку реалізує заплановану політику безпеки та допомагає створити безпечну та надійну мережеву інфраструктуру для невеликих офісів, які можуть отримувати віддалений доступ до ресурсів [32].

Підтримка та моніторинг є невід'ємними частинами системи захисту мережі невеликого офісу, яка отримує віддалений доступ до ресурсів. Під час цього етапу безперервно контролюється безпека мережі та вживаються заходи для запобігання та виявлення потенційних загроз, програмне забезпечення регулярно оновлюється, а стратегії захисту переглядаються для забезпечення відповідності та ефективності. Постійний моніторинг безпеки мережі включає регулярний аналіз трафіку, моніторинг подій і виявлення аномалій. Це дозволяє своєчасно виявляти аномальну діяльність, атаки або порушення, які можуть загрожувати безпеці мережі. Крім того, виконуються перевірки відповідності, такі як перевірка того, що мережеві пристрої налаштовані правильно, з використанням найновіших механізмів автентифікації та шифрування, а також перевірка того, що політики безпеки виконуються. Для забезпечення безпеки мережевих пристроїв необхідні регулярні оновлення програмного забезпечення. Крім того, стратегії збереження регулярно переглядаються для оцінки їх ефективності та актуальності. Враховуйте зміни в загрозах, нові технології та рекомендації щодо безпеки. За необхідності внесіть корективи в стратегії захисту для забезпечення відповідності сучасним стандартам і вимогам безпеки. Підтримка та моніторинг — це постійний процес, який дозволяє підтримувати оптимальний рівень безпеки мережі для вашого невеликого офісу та ефективно реагувати на нові загрози та вразливості за допомогою віддаленого доступу до ресурсів [33].

2.4 Висновки

У цьому розділі детально проаналізовано та розроблено проект комп’ютерної мережі малого офісу з урахуванням вимоги щодо обмеження доступу користувачів.

Починаючи з вимог до проектування, були визначені необхідні вимоги до мережі малого офісу з поділом доступу, особливо щодо топології мережі. Вибір правильної топології дозволяє ефективно організувати роботу користувачів і забезпечити безпеку та захист даних.

Він також визначає вимоги до програмного забезпечення та обґрунтовує вибір мережевого обладнання для мережі малого офісу. Це включає в себе вибір правильного обладнання на основі функціональності, масштабованості та безпеки. Оптимальний вибір мережевого обладнання є важливим аспектом успішного проектування мережі.

Крім того, визначаються вимоги до захисту мережевого обладнання та розробляється план захисту. Це включає встановлення вимог безпеки для пристроїв, використання механізмів автентифікації, шифрування та регулярне оновлення програмного забезпечення. Ефективне впровадження плану безпеки допоможе забезпечити безпеку та надійність мережі вашого малого офісу.

Підводячи підсумок, можна сказати, що цей розділ є важливим етапом для створення системи захисту мережі. Результати цього розділу створюють необхідну основу для подальшого впровадження та тестування комп'ютерної мереж з обмеженням доступу в невеликих офісах.

3 РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ МАЛОГО ОФІСУ З РОЗМЕЖУВАННЯМ ДОСТУПУ

3.1 Проектування комп'ютерної мережі малого офісу з розмежованим доступом та розробка топології

У процесі проектування комп'ютерної мережі малого офісу з віддаленим доступом до ресурсів було враховано основні вимоги, такі як надійність, безпеки й ефективність.

Було проведено ретельний аналіз потреб малого офісу щодо мережевих ресурсів, використовуваних додатків, кількості користувачів й очікуваних навантажень.

Мережа офіс поділена на такі зони:

- робоча зона, яка включає в себе комп'ютери та інші пристрої, які використовуються співробітниками офісу для їх роботи. Усі пристрої підключені до комутатора, який має зв'язок з маршрутизатором і надає доступ до спільних ресурсів, такі як файли та спільно використовувані пристрої;
- гостьова зона, яка призначена для відвідувачів та гостей офісу, які можуть потребувати обмеженого доступу до мережевих ресурсів. У гостьовій зоні розташована окрема точка доступу, яка надає обмежений доступ до виходу в мережу Інтернет та обмежені можливості взаємодії з іншими зонами мережі. Це допомагає запобігти можливим загрозам безпеки, які можуть виникнути від зовнішніх користувачів;
- демілітаризована зона, яка є проміжною між зовнішнім інтернетом та внутрішньою мережею офісу. Вона містить пристрої, такі як сервери й маршрутизатор. Ця зона дозволяє розмежувати доступ та забезпечувати безпеку внутрішніх ресурсів [34];
- віддалена зона, яка дозволяє співробітникам отримувати віддалений доступ до ресурсів офісу поза його межами. Вона включає в себе використання приватної мережі (VPN), яка забезпечує зашифроване з'єднання між

віддаленим користувачем й внутрішньою мережею офісу. Це дозволяє безпечно працювати з ресурсами підприємства навіть поза його межами.

Зони мережі відображені на рисунку 3.1.

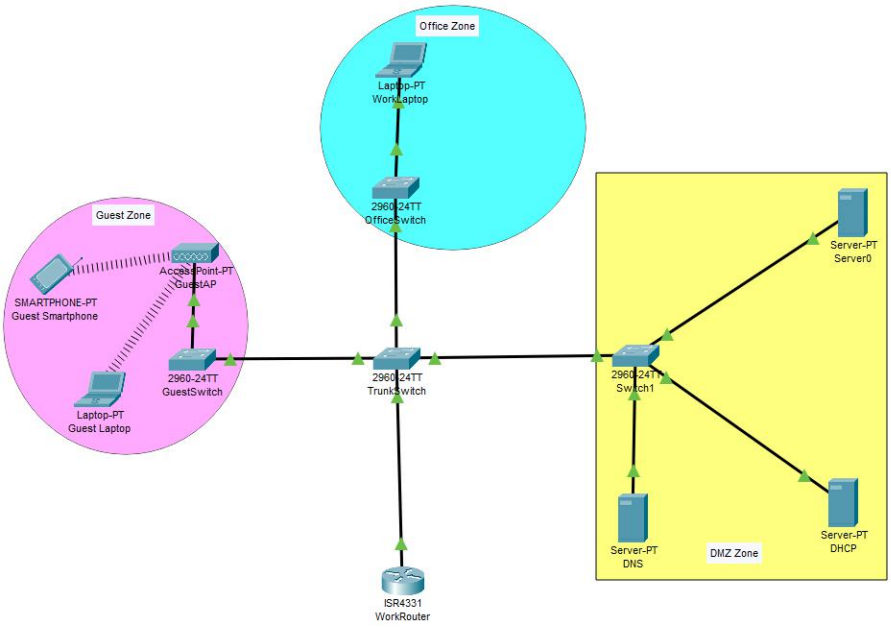


Рисунок 3.1 – Логічна схема розміщення пристроїв в малому офісі

Під час процесу вибору мережевого обладнання були враховані вимоги офісу, що дозволило забезпечити оптимальну функціональність та безпеку мережі. Важливо відмітити, що правильний вибір мережевого обладнання є ключовим для ефективності та безпеки комп'ютерної мережі [35].

Маршрутизатори були обрані з урахуванням їхньої пропускної здатності та підтримки безпеки, зокрема можливості налаштування VPN-з'єднань. Це дозволяє забезпечити захищену комунікацію для віддаленого доступу до ресурсів офісу.

Було обрано маршрутизатор Cisco ISR 4331, він є потужним маршрутизатором, розробленим для малих та середніх підприємств з вимогами до продуктивності та безпеки, зображений на рисунку 3.2.

Рисунок 3.2 – Маршрутизатор Cisco ISR 4331

Характеристики маршрутизатору:

- має пропускну здатність до 1000 Мбіт/сек, що дозволяє обробляти значні обсяги мережевого трафіку;
- має різні конфігурації портів, включаючи порти Gigabit Ethernet та порти SFP (Small Form-Factor Pluggable) для підключення зовнішніх пристроїв;
- пропонує високий рівень безпеки, включаючи вбудований файрвол, захист від атак типу DDoS, VPN-з'єднання та підтримку протоколів шифрування даних;
- маршрутизатор підтримує різні протоколи маршрутизації, включаючи OSPF, BGP, EIGRP та RIP. Це дозволяє ефективно маршрутизувати трафік в складних мережних середовищах;
- підтримує різні методи управління, включаючи командний рядок (CLI), веб-інтерфейс та протоколи управління мережею, такі як SNMP. Також доступні інструменти для моніторингу мережі та відладки;
- має можливості масштабування, що дозволяє додавати додаткові модулі та інтерфейси для розширення функціональності та підтримки більшого числа пристроїв в мережі;
- має вбудований модуль DSP, що дозволяє підтримувати голосові послуги через IP-мережу. Це робить його ідеальним вибором для підтримки голосового трафіку та впровадження IP-телефонії в офісному середовищі;
- має функцію оптимізації WAN-трафіку, яка дозволяє зменшити витрати на пропускну здатність та підвищити продуктивність за рахунок стиснення даних, кешування та управління пропускною здатністю;

– підтримує різні режими розгортання, включаючи самостійний режим та режим інтеграції з централізованою системою управління Cisco DNA Center. Це забезпечує гнучкість управління та масштабування мережі відповідно до потреб підприємства;

– підтримує функції високої доступності, такі як дублювання маршрутизаторів, SSO (Stateful Switchover) та NSF (Non-Stop Forwarding). Це забезпечує неперервну роботу мережі та відсутність відмов в разі виникнення проблем з одним з пристроїв.

Комутатори були вибрані з урахуванням кількості потрібних портів, їхньої швидкості передачі даних та можливості налаштування VLAN для розмежування мережевого трафіку. Це забезпечує ефективну комутацію даних у мережі та контрольоване розподіл ресурсів [36].

Комутатор Cisco 2960 є потужним комутатором для підприємств, що пропонує надійну комутацію та підтримку безпеки мережі, зображений на рисунку 3.3.

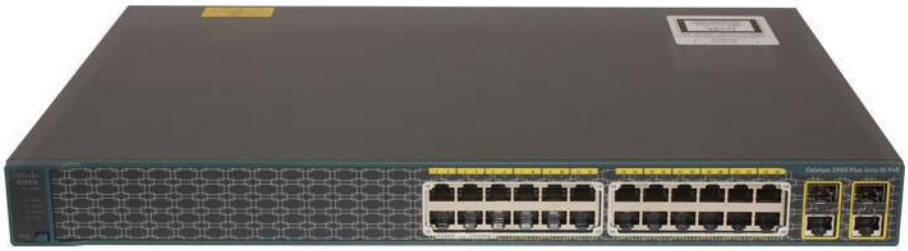


Рисунок 3.3 – Комутатор Cisco Catalyst 2960

Характеристики цієї моделі:

– доступний у різних конфігураціях з різною кількістю портів Ethernet. Він може мати від 8 до 48 портів Ethernet, що дозволяє підключати велику кількість пристроїв до мережі;

– підтримує швидкості передачі даних 10/100/1000 Мбіт/с на кожному порту Ethernet, що забезпечує високу продуктивність та швидку передачу даних в мережі;

− підтримує віртуальні локальні мережі (VLAN), що дозволяє розділити мережу на логічні сегменти та забезпечити ефективну комутацію даних та безпеку;

− пропонує різні функції безпеки, включаючи фільтрацію трафіку, списки керування доступом (ACL), захист від атак типу MAC-флуд або ARP-атак, а також підтримку протоколів шифрування даних;

− підтримує різні методи управління, включаючи командний рядок (CLI), веб-інтерфейс та протоколи управління мережею, такі як SNMP. Також доступні інструменти для моніторингу мережі та відладки;

− пропонує функції енергозбереження, які дозволяють ефективно використовувати електроенергію та знижувати витрати на операції мережі;

− підтримує функції QoS, що дозволяє пріоритезувати трафік у мережі. Це дозволяє надати пріоритети для важливих даних, таких як голосовий трафік або відео, забезпечуючи їх високу якість обслуговування;

− підтримують технологію PoE, що дозволяє живити пристрої, підключені до комутатора, через Ethernet-кабель. Це зручно для підключення IP-телефонів, відеокамер або точок доступу без додаткового джерела живлення;

− має можливість розширювати функціональність та кількість портів шляхом додавання модулів розширення або використання стекінгової технології. Це дозволяє збільшити мережеві можливості та підтримувати зростаючі потреби підприємства;

− є популярним рішенням, що має широку підтримку та доступність на ринку. Це означає, що він легко доступний для придбання та підтримки, що забезпечує зручність для підприємств у реалізації своїх мережних проектів.

Комутатор Cisco 2960 є надійним рішенням для побудови швидких та безпечних мереж для підприємств.

Точки доступу до мережі були обрані залежно від потреб офісу щодо бездротового доступу. Вибір точок доступу до мережі враховував їхню

сумісність з безпроводовими стандартами, дальність покриття та можливості налаштування безпеки, яка була зображена на рисунку 3.4.

Рисунок 3.4 – Точка доступу WI-FI CISCO CBW240AC-E

Точка доступу Wi-Fi Cisco CBW240AC-E є потужним пристроєм, розробленим для надання швидкого та надійного бездротового з'єднання.

Характеристики цієї моделі:

- підтримує стандарти бездротового зв'язку 802.11ac Wave 2 та 802.11n, що дозволяє швидке та стабільне підключення до мережі Wi-Fi;
- забезпечує швидкість передачі даних до 1,7 Гбіт/сек, що дозволяє ефективно передавати великі обсяги даних та стрімінгове відео;
- працює в діапазоні частот 2,4 ГГц та 5 ГГц, що дозволяє отримувати стабільне з'єднання та уникати перешкод від інших пристроїв;
- пропонує різні функції безпеки, включаючи шифрування WPA2/WPA3, автентифікацію користувачів, фільтрацію MAC-адрес та захист від несанкціонованого доступу;
- може підтримувати багатокористувацьку обробку даних та до 200 одночасних підключень, що дозволяє задовольнити потреби великих обсягів трафіку;

− підтримує централізоване управління через програмне забезпечення Cisco Mobility Express або контролери мережі. Крім того, доступні інструменти моніторингу та відладки для покращення продуктивності мережі Wi-Fi;

− використовує технологію Beamforming, яка спрямовує бездротовий сигнал безпосередньо до підключених пристроїв. Це дозволяє поліпшити якість з'єднання та забезпечити кращий охоплення сигналом в мережі Wi-Fi;

− використовує технологію MIMO, що дозволяє одночасно передавати та отримувати дані по кількох антенах. Це покращує продуктивність та стабільність бездротового зв'язку;

− дозволяє налаштовувати окрему гостьову мережу з обмеженим доступом до ресурсів основної мережі. Це зручно для надання безпечного бездротового з'єднання для відвідувачів та гостей офісу;

− може бути встановлена як самостійна точка доступу або як частина централізованої системи управління Cisco Mobility Express або контролером мережі. Це дозволяє зручне управління та масштабування мережі Wi-Fi;

− використовує технологію керування ресурсами AirTime Fairness, яка розподіляє багатокористувацький трафік рівномірно між пристроями. Це дозволяє уникнути перевантаження мережі та забезпечити рівномірний доступ до ресурсів.

Точка доступу Wi-Fi Cisco CBW240AC-E є надійним та ефективним рішенням для побудови бездротової мережі з високою швидкістю передачі даних та безпекою.

Для демілітаризованої зони було обрано два сервери ARTLINE Business R13 v11, зображений на рисунку 3.5, а також для доступу до ресурсів - ARTLINE Business R35 v19, зображений на рисунку 3.6.

Рисунок 3.5 – Сервер ARTLINE Business R13 v11

Сервер ARTLINE Business R13 v11 - це потужне рішення, розроблене для бізнесу з високими вимогами до продуктивності та надійності.

Таблиця 3.1 - Характеристики серверу ARTLINE Business R13 v11

Материнська плата	Asus Prime H570-PLUS
Процесор	Intel Pentium Gold G6400 (2 ядра, 4 потоки, 4.0 ГГц)
Оперативна пам'ять	8 ГБ DDR4-2666 МГц (можливий апгрейд до 128 ГБ)
Жорсткий диск	1 ТБ
Інтерфейси	PCIe 4.0, 2 слоти M.2, 1G Ethernet (Intel контролер), USB 3.2 Gen2 Type-C, внутрішній роз'єм Thunderbolt 4

У сервері ARTLINE Business R13v11 використовується один із найкращих на сьогодні блоків живлення Seasonic потужністю 400 Вт із сертифікатом 80+ Bronze. Якість продуктів Seasonic перевірено часом і підтверджується тисячами систем, складених на їхній основі.

Професійне складання сервера ARTLINE і наявність двох 80 мм вентиляторів забезпечать оптимальний повітряний потік усередині корпусу з форм-фактором 2U, а отже, і якісне охолодження всіх компонентів.

Рисунок 3.6 - Сервер ARTLINE Business R35 v19

Таблиця 3.2 - Характеристики серверу ARTLINE Business R35 v19

Материнська плата	P12R-M
Процесор	Intel Xeon E-2336 (6 ядер, 2.9 – 4.8 ГГц)
Оперативна пам'ять	32 ГБ ECC DDR4-3200 МГц
Жорсткий диск	SSD - 3 x 500 ГБ
Роз'єми	2 x USB 3.2 Gen 2 порти, 2 x USB 2.0 порти, 1 x VGA порт, 1 x HDMI порт, 2 x LAN (RJ-45), 1 x LAN для конфігурації
Швидкість LAN	1 Гбіт/с
Кількість LAN (RJ-45)	3
Чіпсет	Intel C252

Одна з унікальних особливостей сервера ARTLINE Business R35v19 - це можливість використання IPMI 2.0 для організації віддаленої роботи. Це дозволяє адміністраторам здійснювати віддалений доступ до сервера через мережу Ethernet, використовуючи технологію KVM-over-IP. Такий підхід

дозволяє уникнути необхідності фізично присутнього адміністратора біля сервера, що допомагає знизити витрати на операційні втручання.

Програмне забезпечення сервера контролює різні параметри, такі як напруга силових ланцюгів, температура, робота системи охолодження та підключена периферія. Це забезпечує необхідний контроль та моніторинг роботи сервера.

Зручний веб-інтерфейс працює незалежно від операційної системи сервера і дозволяє адміністраторам виконувати різні завдання, такі як управління живленням, моніторинг апаратних компонентів, установка ОС, налаштування, оновлення, запис відео, реєстрація критичних помилок та ведення журналу логів.

В комп'ютерній мережі малого офісу була обрана гібридна схема топології.

3.2 Налаштування демілітаризованої зони та захисту на мережевому обладнанні

Демілітаризована зона (DMZ) підприємства включає декілька серверів, кожен з яких виконує певні функції у мережі:

1. Сервер для доступу до ресурсів:

Цей сервер забезпечує доступ до різних ресурсів у мережі, таких як веб-сторінки (HTTP), налаштування якого зображені на рисунку 3.7 або файли для обміну (FTP), налаштування якого зображені на рисунку 3.8. Він забезпечує стабільну та безпечну передачу даних між клієнтами та сервером, надаючи необхідні сервіси для ефективного обміну інформацією [37].

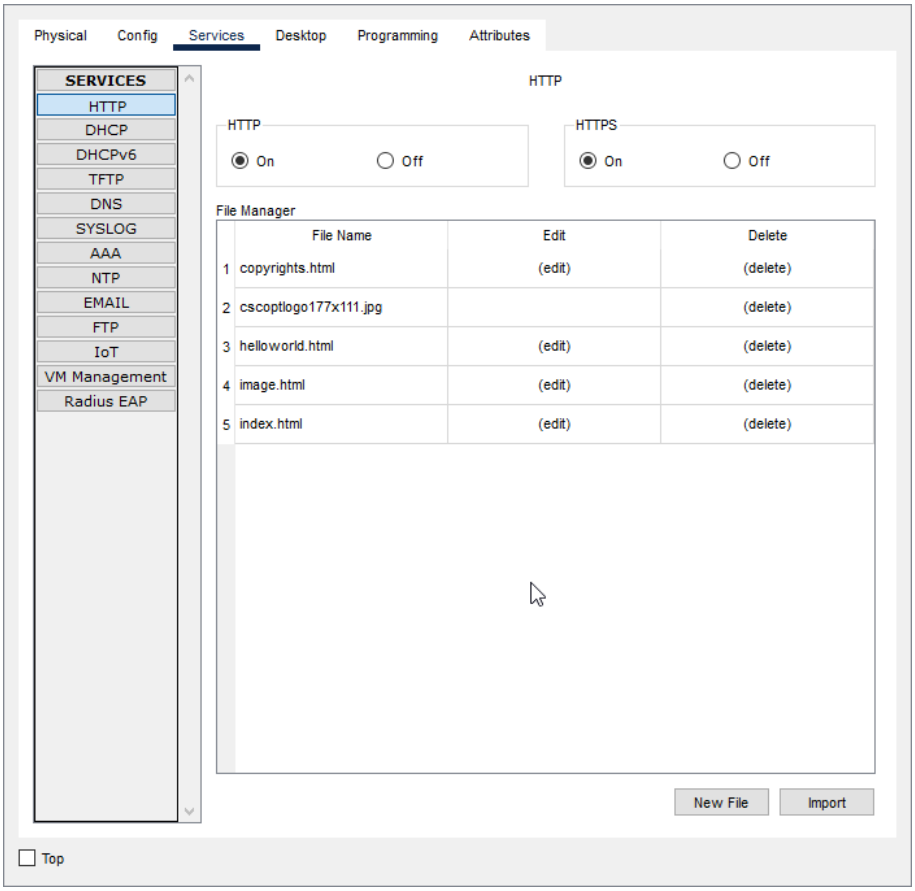


Рисунок 3.7 – Демонстрація налаштування HTTP сервісу на сервері

HTTP (Hypertext Transfer Protocol) є протоколом передачі гіпертексту, який використовується для обміну інформацією між веб-серверами та веб-клієнтами. У дипломній роботі використовується HTTP сервіс, який надає можливість доступу до веб-ресурсів через інтернет-протокол.

HTTP сервіс дозволяє користувачам переглядати веб-сторінки, завантажувати та відправляти дані на сервер, виконувати різноманітні операції, такі як заповнення форм, отримання динамічного вмісту та взаємодія з веб-додатками.

Використання HTTP сервісу дозволяє забезпечити зручну та надійну передачу веб-даних, що важливо для забезпечення функціональності та доступності веб-ресурсів для користувачів у мережі.

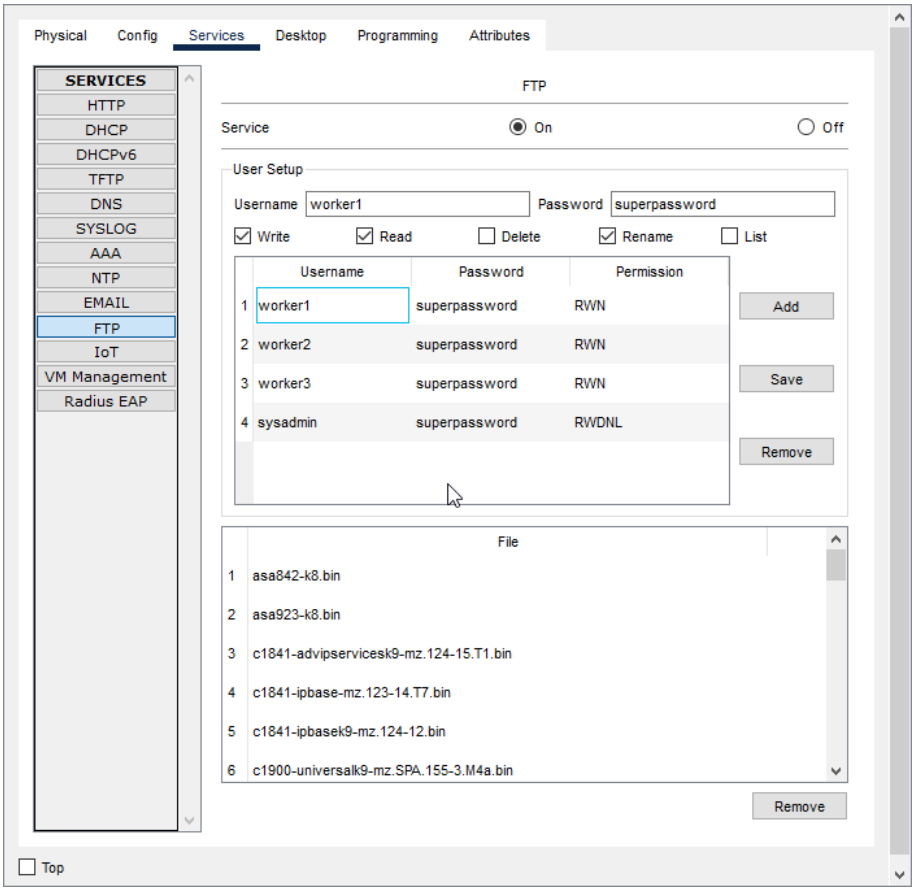


Рисунок 3.8 – Демонстрація налаштування FTP сервісу на сервері

FTP (File Transfer Protocol) є протоколом передачі файлів, що використовується для обміну файлами між різними комп'ютерами у мережі. У дипломній роботі використовується FTP сервер, який надає можливість зберігання та надання доступу до файлів для користувачів у мережі.

FTP сервер забезпечує швидку та безпечну передачу файлів між клієнтами та сервером. Користувачі можуть завантажувати та вивантажувати файли на FTP сервер, виконувати копіювання, переміщення та видалення файлів з використанням FTP клієнта.

Завдяки FTP серверу, робота з файлами стає зручною та ефективною, забезпечуючи доступ до необхідної інформації для користувачів у мережі [38].

2. DNS (Domain Name System) сервер відповідає за перетворення доменних імен на відповідні IP-адреси, налаштування якого зображено на рисунку 3.9. Він забезпечує надійну та швидку роботу доменної системи, що

дозволяє клієнтам в мережі знаходити й доступатися до різних ресурсів за допомогою доменних імен.

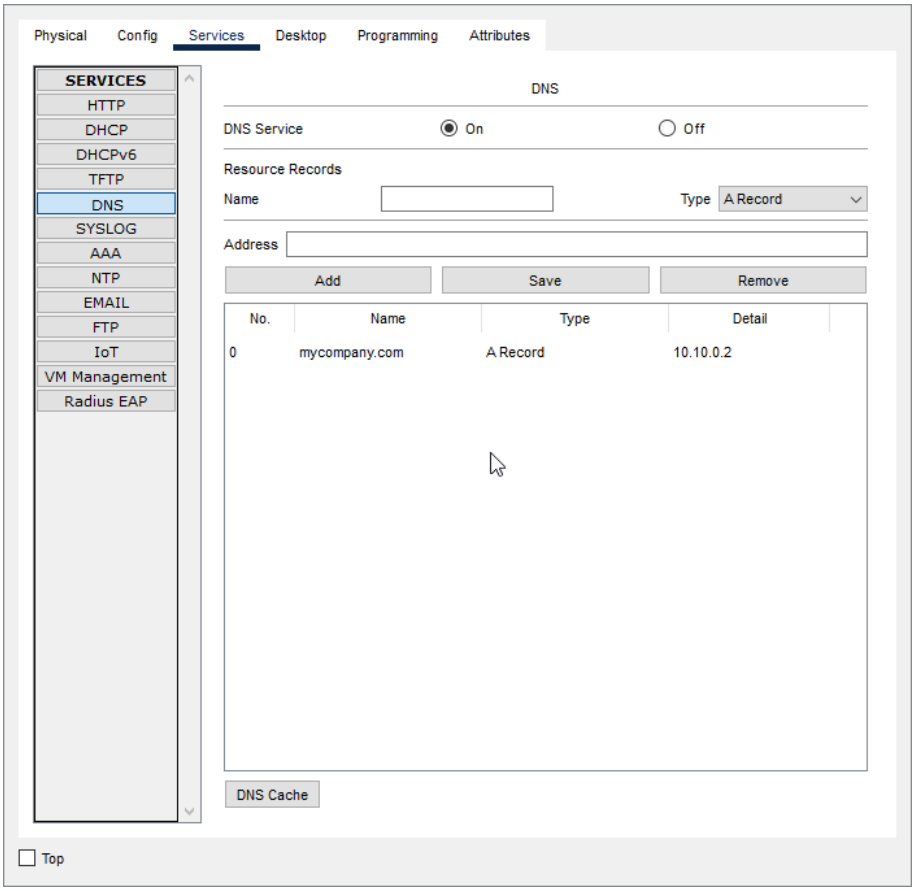


Рисунок 3.9 – Демонстрація налаштування DNS сервісу на сервері

3. DHCP (Dynamic Host Configuration Protocol) сервер автоматично надає мережевім пристроям IP-адреси, підмережі, шлюзи, DNS-сервери та інші мережеві налаштування, налаштування якого зображено на рисунку 3.10. Це дозволяє ефективно керувати розподілом IP-адрес у мережі та спрощує налаштування нових пристроїв, що приєднуються до мережі.

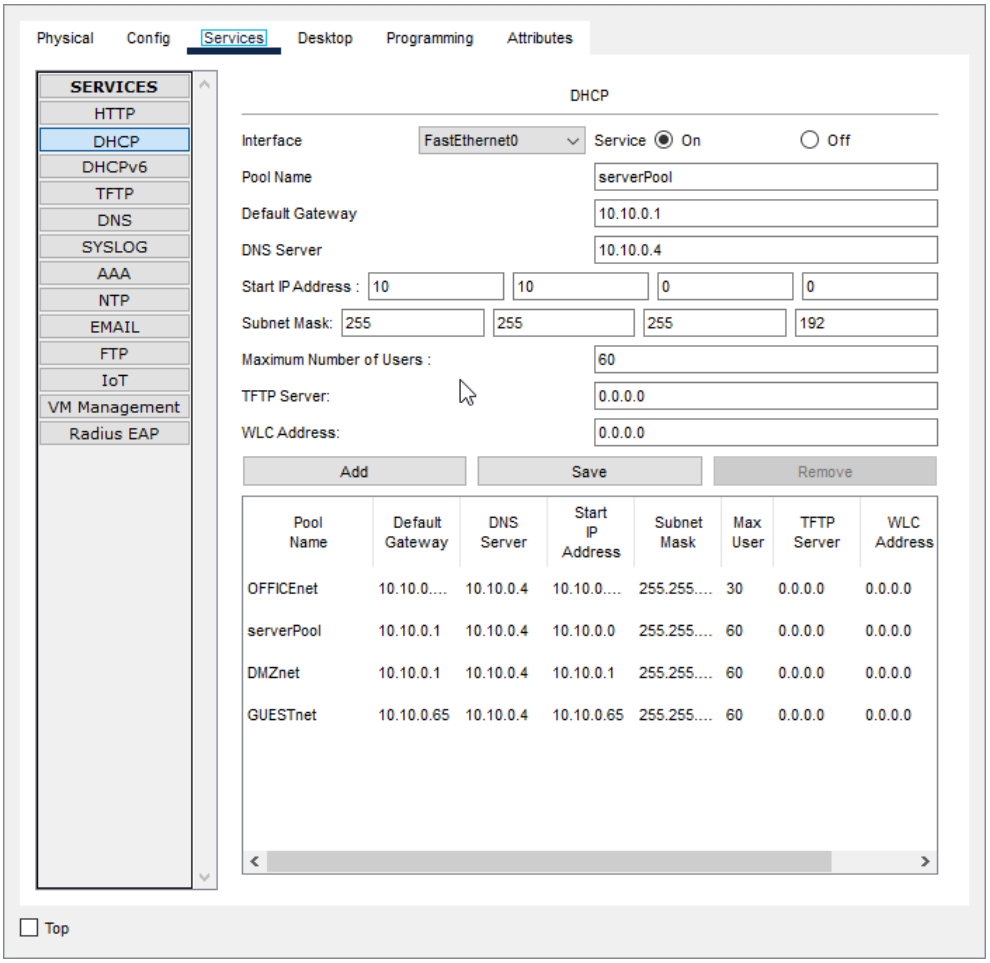


Рисунок 3.10 – Демонстрація налаштування DHCP сервісу на сервері

Для забезпечення комунікації між демілітаризованою зоною та іншими частинами мережі, використовується маршрутизатор з додатковими інтерфейсами.

Цей маршрутизатор відповідає за передачу пакетів даних між різними підмережами та забезпечує безпеку мережі шляхом налаштування правил фільтрації трафіку та захисту від потенційних загроз.

Така архітектура демілітаризованої зони дозволяє забезпечити безпеку мережі, розділивши різні функції на окремі сервери та контролюючи доступ до них. Крім того, застосування маршрутизатора дозволяє ефективно керувати комунікацією між різними частинами мережі та забезпечити надійність та швидкість передачі даних.

На маршрутизаторі налаштований VPN-тунель, який забезпечує безпечне віддалене з'єднання з користувачем, налаштування якого зображено на рисунку 3.11. VPN (Virtual Private Network) створює захищену тунельну з'єднання через відкриту мережу, що дозволяє користувачеві отримати доступ до ресурсів внутрішньої мережі з будь-якого місця.

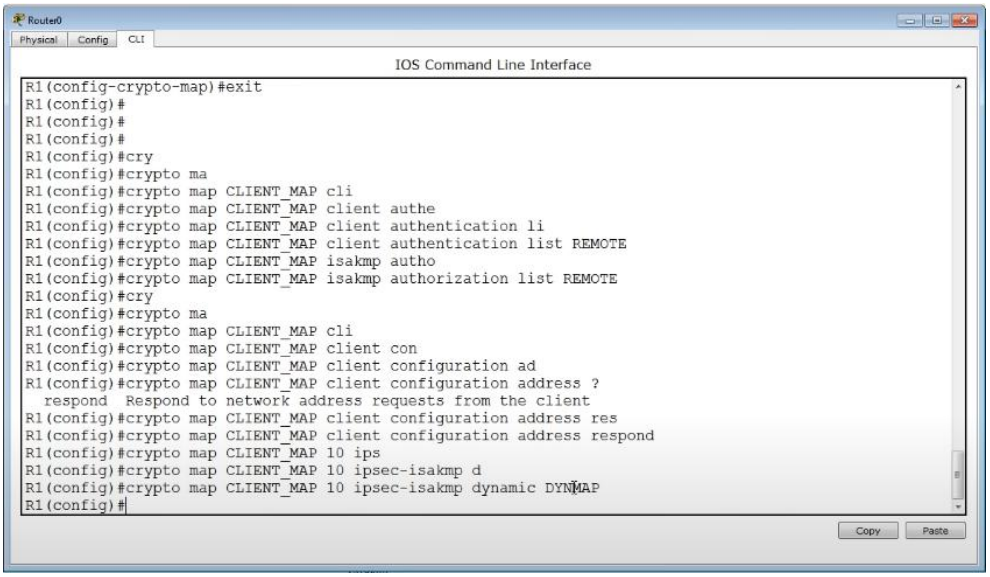


Рисунок 3.11 – Процес налаштування VPN-тунелю

За допомогою VPN-тунелю забезпечується конфіденційність, цілісність та доступність передачі даних. Користувач може безпечно підключатися до мережі, використовуючи захищене з'єднання і здійснювати роботу з внутрішніми ресурсами, незалежно від свого місцезнаходження, процес підключення зображено на рисунку 3.12.

VPN-тунель на маршрутизаторі гарантує захищений доступ до мережевих ресурсів та забезпечує зручну та безпечну комунікацію для віддалених користувачів.

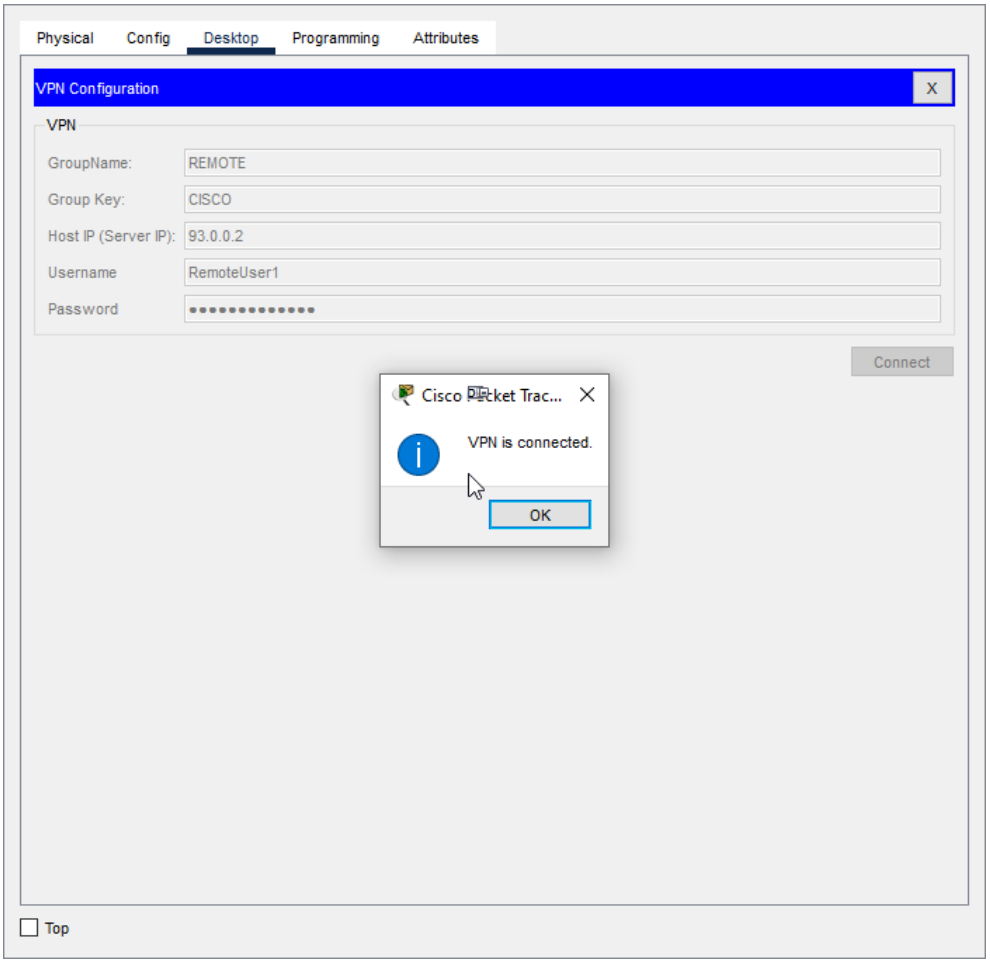


Рисунок 3.12 – Підключення до серверу

3.3 Розгортання, налаштування та тестування комп'ютерної мережі малого офісу з розмежуванням доступу

Після створення логічної схеми мережі, зображеної на графічному плакаті №1, було налаштовано магістральний комутатор, який об’єднує підмережі комп’ютерної мережі.

Магістральний комутатор — це мережевий пристрій, який використовується для передачі даних між різними віртуальними локальними мережами (VLAN) у комп’ютерній мережі. Він відіграє важливу роль у забезпеченні ефективного управління трафіком і розподілу доступу до різних ресурсів у мережі.

Основною функцією Trunk Switch є передача пакетів даних між різними портами VLAN. Він здатний передавати дані, що належать до різних VLAN, через одне фізичне з'єднання за допомогою технології тегування пакетів. Це дозволяє заощадити на фізичних підключеннях і зменшити складність вашої мережевої інфраструктури.

Магістральні комутатори використовують стандартні протоколи тегування пакетів, такі як тегування VLAN (802.1Q), щоб ідентифікувати та розподіляти пакети між різними VLAN. Цей процес дозволяє розділяти трафік і ефективно керувати обміном даними між VLAN [39].

Після успішного налаштування маршрутизатора провайдера в системі наступним кроком буде налаштування DHCP-сервера. DHCP (Dynamic Host Configuration Protocol) — це протокол, який дозволяє автоматично надавати параметри мережі, такі як IP-адреси, маски підмережі, шлюзи за замовчуванням і DNS-сервери, для пристроїв, підключених до мережі.

Налаштування сервера DHCP дозволяє ефективно керувати призначенням IP-адрес та іншими налаштуваннями для пристроїв у вашій мережі. Це спрощує процес налаштування та обслуговування мережевих пристроїв.

Після успішного налаштування сервера DHCP було налаштовано підінтерфейси на маршрутизаторі. Підінтерфейси — це логічні інтерфейси, які дозволяють розділити фізичний інтерфейс на логічні підмережі. Це важливий крок у розподілі трафіку на транзитні комутатори та забезпеченні ефективного обміну даними в мережі.

Налаштування підінтерфейсів дозволяє відокремлювати трафік на основі певних критеріїв, таких як VLAN (віртуальні локальні мережі) або підмережі, що допомагає забезпечити мережеву безпеку, ефективність і керованість. Кожен підінтерфейс має власну конфігурацію мережевих параметрів, таких як IP-адреса та маска підмережі, для розподілу трафіку на відповідний сегмент мережі.

Налаштування підінтерфейсів на маршрутизаторі дозволяє керувати мережевим трафіком за допомогою різних методів комутації та розподілу даних. Це робить мережу більш масштабованою, ефективною та безпечною, дозволяє оптимізувати використання ресурсів і забезпечує надійну передачу даних у мережах невеликих офісів із розмежуванням доступу.

Після успішного налаштування доступу до мережі відокремленого малого офісу наступним кроком є тестування служби та сервера з комп’ютера віддаленого користувача. Цей етап дозволяє переконатися, що налаштування правильні та відповідають функціональним вимогам системи.

Під час тестування віддаленого доступу до сервісів і серверів перевіряється підключення, швидкість передачі даних, стабільність підключення та очікувані результати. Виконуйте різні сценарії використання, щоб перевірити, як працює система за різних умов і навантажень.

Тестування віддаленого доступу до сервісів і серверів є важливою частиною впровадження системи захисту для мереж невеликих офісів з обмеженим доступом. Це дозволяє переконатися, що системи запущені та працюють, і що користувачі можуть отримати доступ до ресурсів з будь-якої точки світу.

Для цього я встановлював VPN-тунель між комп'ютером віддаленого користувача і мережею офісу, щоб забезпечити безпечне з’єднання.

Після успішного підключення я перевірив налаштування тунелю за допомогою команди ipconfig /all. Результат цієї команди показаний на малюнку 3.13, де показано IP-адресу, підмережу та інші параметри тунелю.

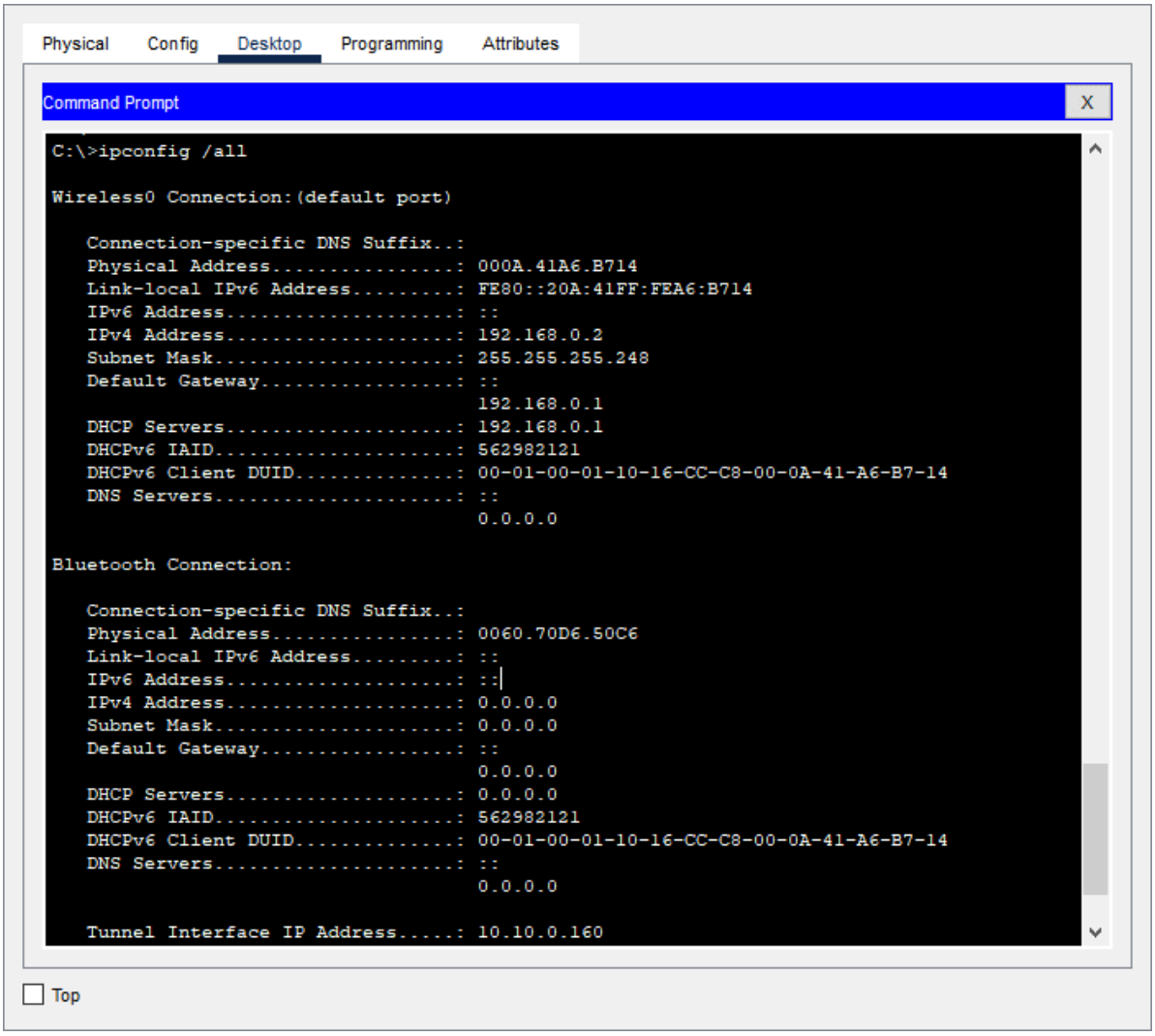


Рисунок 3.13 – Результат використання команди ipconfig /all

Цей крок підтвердив, що VPN-тунель був успішно налаштований і має вірні налаштування IP-адрес та мережевих параметрів. Це підтверджує наявність з’єднання між моїм комп'ютером віддаленого користувача та мережею офісу та гарантує безпечну передачу даних через тунель.

Після успішного налаштування тунелю я використовував команду PING з командного рядка комп'ютера віддаленого користувача, щоб перевірити з’єднання та доступність ресурсів, що відобразив на рисунку 3.14.

Команда PING дозволяє надіслати сигнал (запит ICMP) на вказану IP-адресу та отримати відповідь (відповідь ICMP). Під час виконання команди PING я перевіряв зв'язок між моїм комп'ютером та мережевими ресурсами

офісу. Якщо отримував відповідь на запит PING, це свідчило про наявність з’єднання та доступність ресурсів.

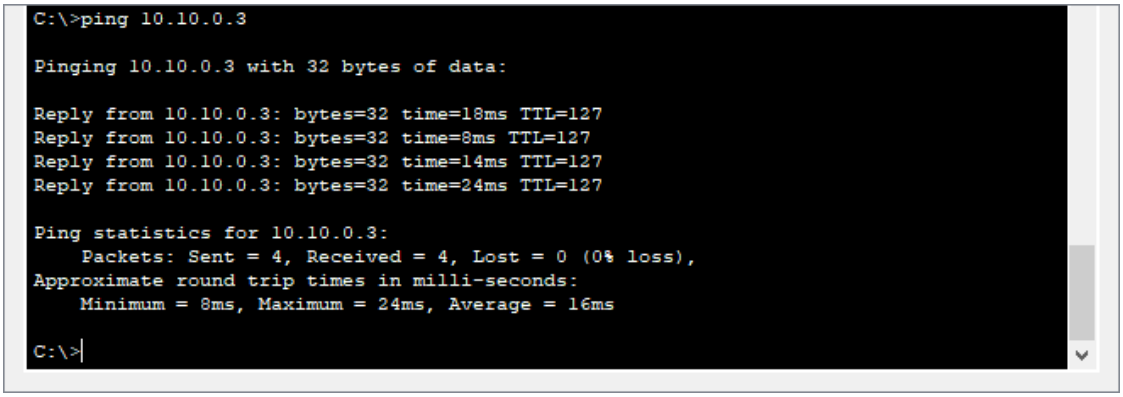


Рисунок 3.14 – Використання команди PING з командного рядку

Тестування за допомогою команди PING дозволило мені переконатися, що VPN-тунель працює належним чином та забезпечує зв’язок між моїм комп'ютером і офісною мережею [40]. Це дозволило мені перевірити швидкість передачі даних, стабільність з’єднання та підтвердити, що моя система захисту мережі з віддаленим доступом працює належним чином.

Наступним етапом була перевірка доступності HTTP сервера. Для цього я скористався встановленим веб-браузером на комп'ютері віддаленого користувача. Спробував перейти за адресою mycompany.com, щоб отримати доступ до веб-ресурсів офісу.

Результат цієї перевірки відображено на рисунку 3.15, де видно, що веб-сторінка mycompany.com була успішно завантажена у веб-браузері. Це підтверджує доступність HTTP сервера та правильну роботу моєї системи з віддаленим доступом до ресурсів офісу [41].

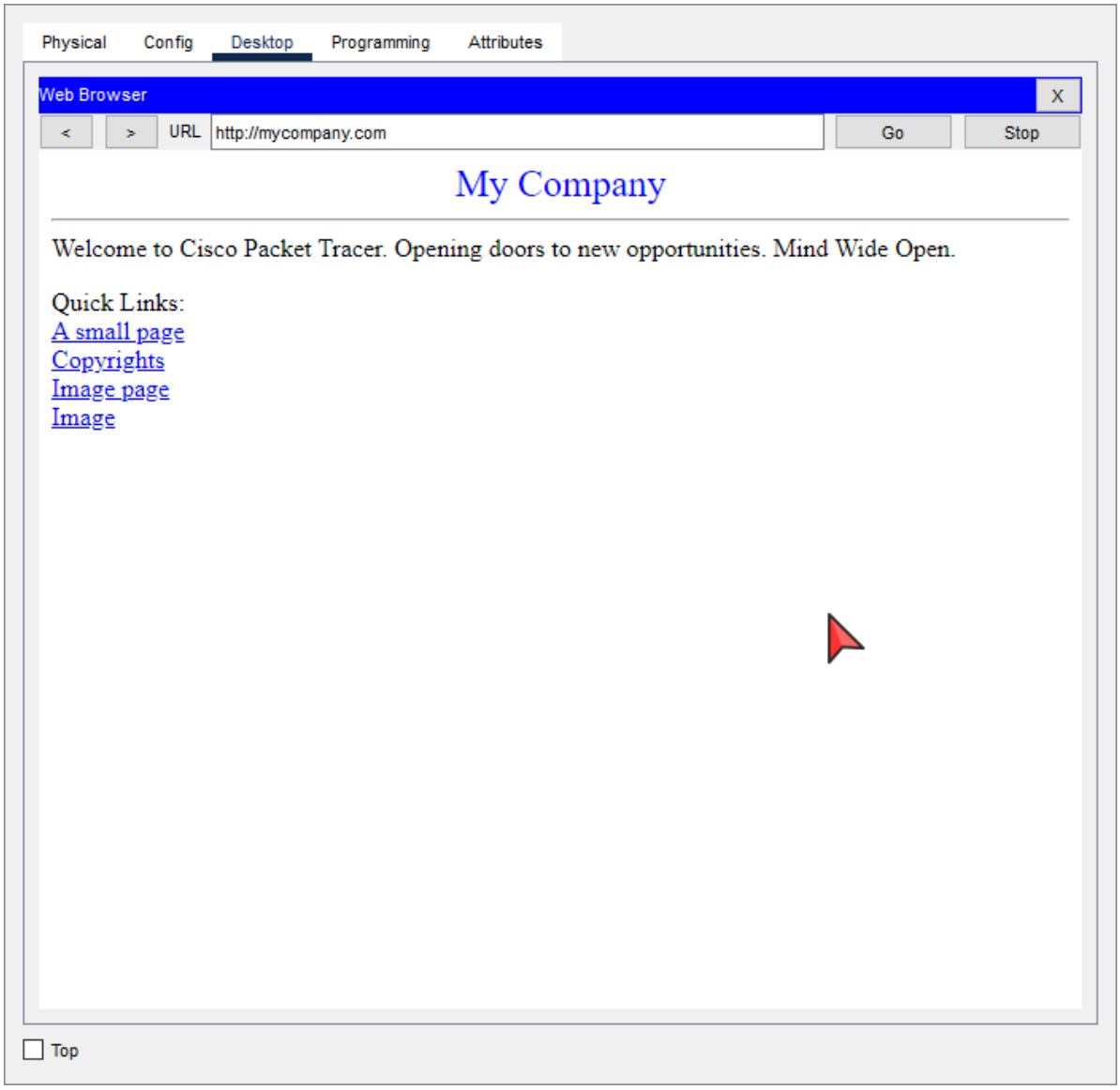


Рисунок 3.15 – Відкриття веб-сторінки

Цей етап дозволив перевірити, що зв'язок з HTTP сервером був успішно встановлений і можна безперешкодно отримувати веб-сторінки та ресурси, доступні в офісній мережі. Це підтверджує належне функціонування мережі малого офісу з розмежуванням доступу та ефективне забезпечення віддаленого доступу до ресурсів.

Додатково проведемо тестування FTP серверу. За допомогою командного рядка на комп'ютері віддаленого користувача виконаємо команду "ftp 10.10.0.2" для підключення до FTP серверу. Після успішного підключення введемо команду "delete <ім'я_файлу>", щоб спробувати видалити файл на сервері.

Після виконання команди "ftp 10.10.0.2" в командному рядку з'явилось підтвердження підключення до FTP серверу. Потім, за допомогою команди "delete <ім'я_файлу>", була спроба видалити вказаний файл на сервері, що відображено на рисунку 3.16.

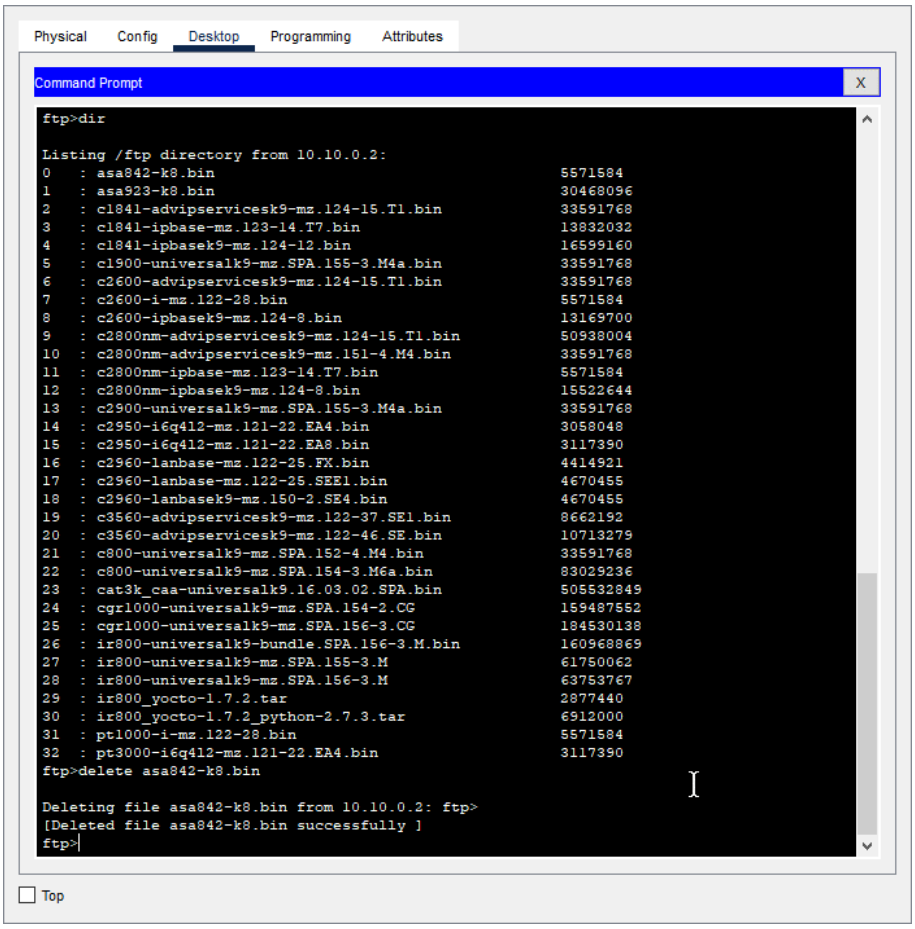


Рисунок 3.16 – Результати спроби видалення файлу на FTP-сервері

3.4 Висновки

В даному розділі виконано роботи з проектування, налаштування та тестування комп’ютерної мережі малого офісу з ресурсами віддаленого доступу. Завдяки цій роботі були отримані наступні результати.

Починаючи з проектування, розробляється топологія мережі для невеликого офісу з обмеженим доступом, що дозволяє ефективно організувати роботу внутрішніх і зовнішніх мережевих пристроїв. Демілітаризовані зони

(DMZ) належним чином налаштовані та захищені на мережевих пристроях, щоб забезпечити безпеку під час зовнішнього доступу до ресурсів. Розгортання, налаштування та тестування комп'ютерної мережі в невеликому офісі проведено успішно з урахуванням принципів обмеження доступу та встановлених вимог безпеки.

Таким чином, впровадження та тестування комп’ютерної мережі малого офісу з обмеженими правами доступу є важливим етапом у системі захисту мережі. Цей етап дозволяє створити безпечну та ефективну інфраструктуру, яка забезпечує віддалений доступ до ресурсів, захищаючи їх від потенційних загроз. Результати досліджень у цьому розділі закладають основу для подальшого розвитку та вдосконалення системи захисту мережі малого офісу для ресурсів віддаленого доступу.

ВИСНОВКИ

В ході даної кваліфікаційної роботи було проведено дослідження та розробку системи захисту комп'ютерної мережі малого офісу для ресурсів віддаленого доступу. Проаналізовано концепцію комп'ютерної мережі з обмеженим доступом, досліджено принципи функціонування демілітаризованої зони (ДМЗ), виконано порівняльний аналіз різних архітектурних рішень.

У результаті дослідження встановлено, що концепція комп'ютерної мережі з обмеженим доступом є ефективним інструментом захисту мережі малого офісу з віддаленим доступом до ресурсів. Обмеження доступу дозволяють контролювати та обмежувати дозволи користувачів, зменшуючи ризик несанкціонованого доступу та зовнішніх атак.

Демілітаризовані зони (DMZ) виявилися важливою частиною системи захисту. Це дозволяє розміщувати загальнодоступні ресурси за межами основної мережі, зберігаючи їх ізольованими від внутрішньої мережі.

Порівняльний аналіз різних архітектурних рішень показує, що існує кілька способів забезпечення безпеки мережі малого офісу з віддаленим доступом, де кожен підхід має свої переваги та недоліки.

Детально досліджено поняття комп'ютерних мереж з обмеженим доступом, принципи роботи DMZ, порівняльний аналіз різних архітектурних рішень. Отримані результати стали основою для розробки ефективної системи захисту мережі малого офісу з віддаленим доступом до ресурсів.

Для досягнення поставленої мети були поставлені та успішно виконані завдання. Досліджено концепцію комп'ютерної мережі з обмеженнями доступу, вивчено принципи роботи DMZ, проведено порівняльний аналіз архітектурних рішень, реалізовано систему захисту мережі малого офісу з віддаленим доступом до ресурсів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Коробейнікова Т. І., Захарченко С. М. Комп'ютерна мережа. Львів : Вид-во Львів. політехніки, 2022. 228 с.
2. Задерейко О., Логінова Н., Толокнов А. Комп’ютерні мережі: навчальний посібник. Одеса : Од. юрид. акад., 2022. 249 с.
3. Жураковський Б., Зенів І. Комп’ютерні мережі. Київ : Київ. політехн. ін-т ім. Ігоря Сікорського, 2020. 328 с.
4. Компютерні мережі, Internet. URL: https://sites.google.com/site/tehnikakomp/home/lekciie/komputerni-merezi-internet
5. Руденко В.Д, Макарчук О.М, Патланжоглу М.О. Практичний курс інформатики. Київ : Феникс, 2001. 304 с.
6. Шестопалов Є.А. Internet для початківця. Шепетівка : Аспект, 2005. 112 с.
7. Що таке демілітаризована зона (DMZ)?. URL: https://uk.itpedia.nl/2023/01/28/wat-is-een-demilitarized-zone-dmz.
8. DMZ – що це в роутері, налаштування демілітаризованої зони, як включити режим, сервер і хост, порти і зони. URL: http://teg.com.ua/dmz-shho-tse-v-routeri-nalashtuvannya-demilitarizovanoyi-zoni-yak-vklyuchiti-rezhim-server-i-host-porti-i-zoni-dmz-v-router-tp-link.
9. DMZ in networking. URL: https://www.techtarget.com/searchsecurity/definition/DMZ.
10. DMZ Network: How It Works, Its Uses, and Benefits in Network Security. URL: https://www.linkedin.com/pulse/dmz-network-how-works-its-uses-benefits-security-valdemar-závadský.
11. What is a demilitarized zone (DMZ)? Definition, examples, working, and importance in 2022. URL: https://www.spiceworks.com/it-security/network-security/articles/what-is-demilitarized-zone/.

12. Принципи побудови і призначенння комп’ютерних мереж. URL: https://tdmuv.com/kafedra/internal/informatika/classes_stud/uk/nurse/and/03.Принципи%20побудови%20і%20призначення%20компютерних%20мереж.html

13. Царенко О.М. Економіка розвитку. Дніпродзержинськ : Дніпродзерж. держ. техн. ун-т, 2015. 166 с.

14. Валецька Т.М. Комп'ютерні мережі. апаратні засоби. навчальний посібник. 2002. 208 с.

15. Основні вимоги до проектування кампусних мереж. URL: https://studfile.net/preview/5199546/page:2/.

16. Тарбаєв С.І. Проектування інфокомунікаційних мереж. 2015. 268 с.

17. Комп’ютерні мережі. URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6.

18. Топологія комп'ютерних мереж. URL: https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh.

19. Топології комп’ютерних мереж. URL: http://blogkkzshnika.blogspot.com/2017/10/blog-post_10.html.

20. Топологія локальних мереж. URL: https://ua5.org/lan/125-topologja-lokalnikh-merezh.html.

21. Організація комп'ютерних мереж. URL: http://nickshevtsov.blogspot.com/2017/10/blog-post.html.

22. Топологія мережі: 6 пояснених та порівняних мережевих топологій. URL: https://instagalleryapp.com/chistij-administrator-2/topologija-merezhi-6-pojasnenih-ta-porivnjanih/.

23. Топологія комп’ютерних мереж. Класифікація комп’ютерних мереж з топології. URL: https://creativnost.com.ua/topologiya-kompyuternix-merezh-klasifikaciya-kompyuternix-merezh-z-topologii/.

24. Інформаційні мережі / Полоневич О.В та ін. Київ, 2019. 94 с.

25. Докучаєв А.В, Засов А.В, Казакевич П.В. Інформаційна безпека комп'ютерних систем: навчальний посібник. Київ : Наук. думка, 2017. 152 с.

26. Whitman M. E, Mattord H. J. Principles of information security. 7-ме вид. Cengage Learning, 2018. 658 p.

27. Pfleeger C.P, Pfleeger S.L, Margulies J.A. Security in computing. 5-те вид. Pearson, 2015. 944 p.

28. Bosworth S, Kabay M.E. Computer security handbook. Wiley, 2018. 189 p.

29. Мельник С.М, Висоцька І.В. Мережеві технології: підручник. Київ : Видавничо-полігр. центр "Київ. ун-т", 2016. 316 с.

30. Ліхтарников О.М, Хорошко М.П, Слободяник В.О. Основи комп'ютерних мереж: навчальний посібник. Київ : Ленвіт, 2018. 320 с.

31. Tanenbaum A.S, Wetherall D.J. Computer networks. Pearson, 2010. 960 p.

32. Odom W. Cisco networking essentials. Cisco Press, 2015. 368 p.

33. Alani A.M, Mohammed M.A, Hussein R.H. Network design cookbook: architecting cisco networks. Packt Publishing, 2017. 328 p.

34. Chappell L.C. DMZs: how to secure your internal network with a DMZ. Lulu, 2019. 84 p.

35. Jankowski B. Demilitarized zone (DMZ): definition, benefits, and best practices. CTC Press, 2019. 174 p.

36. Kim D.J, Solomon, M.G. Network security bible. Wiley, 2019. 816 с.

37. Chappell L.C. DMZs: how to secure your internal network with a DMZ. Lulu, 2019. 84 p.

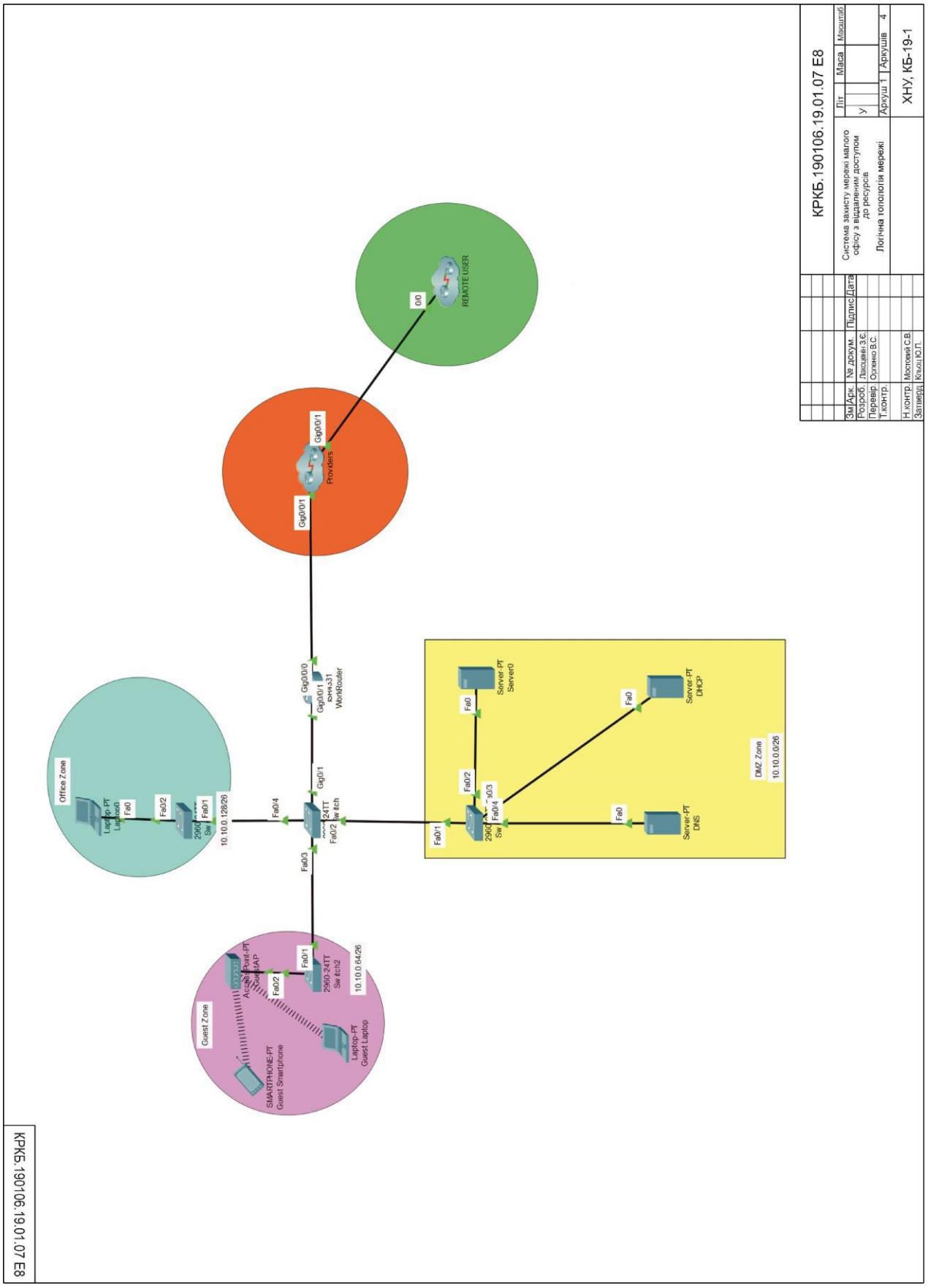
38. Jankowski B. Demilitarized zone (DMZ): definition, benefits, and best practices. CTC Press, 2019. 174 p.

39. Kim D.J, Solomon, M.G. Network security bible. Wiley, 2019. 816 p.

40. Kurose J. F, Ross K. W. Computer networking: a top-down approach. Pearson, 2017. 864 p.

41. Comer D. E. Computer networks and internets. Pearson, 2018. 912 p.

ДОДАТОК А Копія графічної частини



КРКБ.190106.19.01.07 Е8

Зм.	Арк.	№ докум.	Підпис	Дата
Розроб.		Лакшин З.Є.		
Перевір.		Оглєнко В.С.		
Т.контр.				
Н.контр.		Мостовий С.В.		
Затверд.		Кльоц Ю.П.		

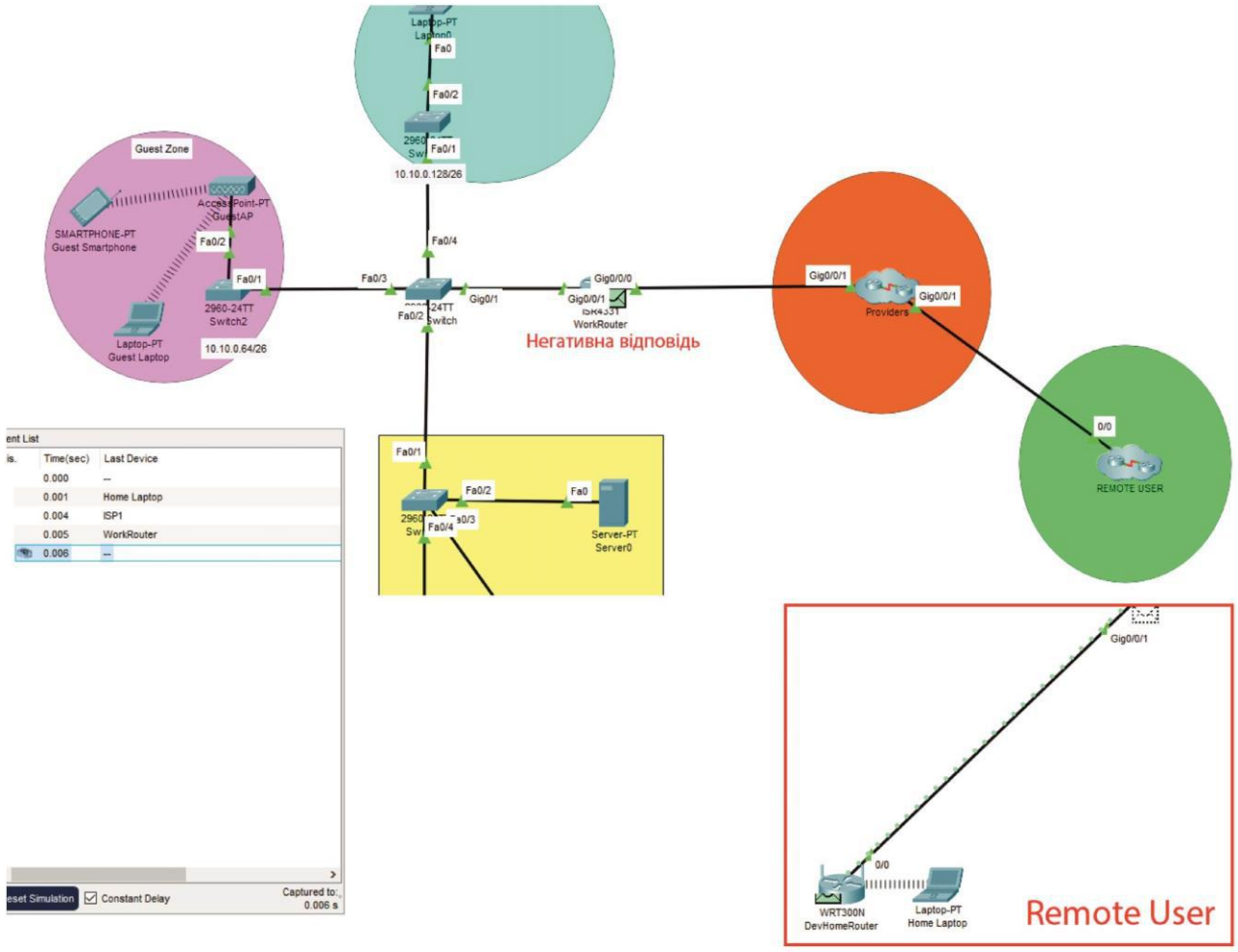
Система захисту мережі малого офісу з віддаленим доступом до ресурсів

Фізична топології мережі

Літ	Маса	Масштаб
У		
Аркуш 2	Аркушів	4

ХНУ, КБ-19-1

КРКБ.190106.19.01.07 Е8*

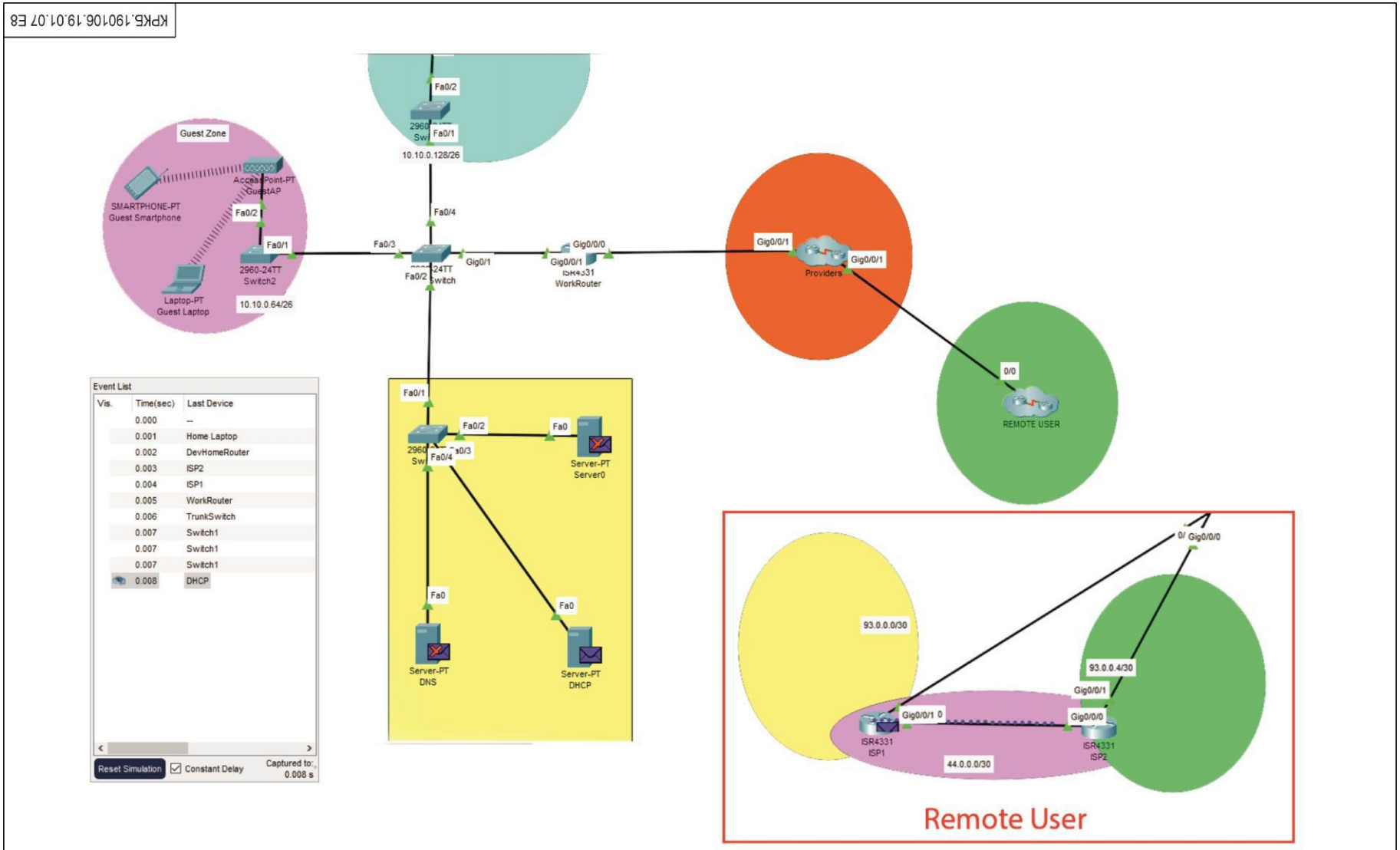


					КРКБ.190106.19.01.07 Е8
Зм.	Арк.	№ докум.	Підпис	Дата	
Розроб.		Лакоценін З.Є.			Система захисту мережі малого офісу з віддаленим доступом до ресурсів
Перевір.		Орленко В.С.			Результат симуляції трафіку
Т.контр.					
Н.контр.		Мостовий С.В.			
Затверд.		Кльоц Ю.П.			

Літ	Маса	Масштаб
У		
Аркуш 3	Аркушів 4	

ХНУ, КБ-19-1

Зм.	Арк.	№ докум.	Підпис	Дата	КРКБ.190106.19.01.07 ПЗ	Арк.
						68



					КРКБ.190106.19.01.07 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата		
Розроб.		Лакоценін З.Є.			Система захисту мережі малого офісу з віддаленим доступом до ресурсів	Літ. / Маса / Масштаб
Перевір.		Орленко В.С.				У
Т.контр.					Результат симуляції трафіку	Аркуш 4 / Аркушів 4
Н.контр.		Мостовий С.В.				ХНУ, КБ-19-1
Затверд.		Кльоц Ю.П.				

ДОДАТОК Б Налаштування мережевих пристроїв

Налаштування маршрутизатора:

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Router
!
aaa new-model
!
aaa authentication login REMOTE local
!
aaa authorization network REMOTE local
!
ip cef
no ipv6 cef
!
username RemoteUser1 secret 5 $1$mERr$aRfPYlsUfv7rVGAwRp8XV.
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 2
 lifetime 21600
!
crypto isakmp client configuration group REMOTE
 key CISCO
```

```
 pool MYPOOL
!
crypto ipsec transform-set MYSET esp-aes 256 esp-md5-hmac
!
crypto dynamic-map DYNMAP 10
 set transform-set MYSET
 reverse-route
!
crypto map CLIENT_MAP client authentication list REMOTE
crypto map CLIENT_MAP isakmp authorization list REMOTE
crypto map CLIENT_MAP client configuration address respond
crypto map CLIENT_MAP 10 ipsec-isakmp dynamic DYNMAP
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0/0
 ip address 93.0.0.2 255.255.255.252
 duplex auto
 speed auto
 crypto map CLIENT_MAP
!
interface GigabitEthernet0/0/1
 description Trunk port for Catalyst
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0/1.10
 description SubInterface for DMZ Network on vlan 10
```

```
 encapsulation dot1Q 10
 ip address 10.10.0.1 255.255.255.192
 ip helper-address 10.10.0.3
!
interface GigabitEthernet0/0/1.20
 description SubInterface for Guest Network on vlan 20
 encapsulation dot1Q 20
 ip address 10.10.0.65 255.255.255.192
 ip helper-address 10.10.0.3
!
interface GigabitEthernet0/0/1.30
 description SubInterface for Office Network on vlan 30
 encapsulation dot1Q 30
 ip address 10.10.0.129 255.255.255.192
 ip helper-address 10.10.0.3
!
interface GigabitEthernet0/0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip local pool MYPOOL 10.10.0.160 10.10.0.190
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0/0
```

```
!
ip flow-export version 9
!
line con 0
!
line aux 0
!
line vty 0 4
!
end
```

Налаштування магістрального комутатора:

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname TrunkSwitch
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 description Watch at Office Network
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
```

```
 description Watch at Guest Network
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/4
 description Watch at Office Network
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet0/1
 description Watch at router
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description DMZ Network
 no ip address
!
interface Vlan20
 description Guest Network
 no ip address
!
interface Vlan30
```

```
 description Office Network
 no ip address
!
line con 0
!
line vty 0 4
 login
line vty 5 15
 login
!
end
```

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Бакалавр Лакоценін Захар Євгенійович

Тема Система захисту мережі малого офісу з віддаленим доступом до ресурсів

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4 ; кількість сторінок записки 65

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та налаштовано комп'ютерну мережу малого офісу з віддаленим доступом до ресурсів із необхідними параметрами безпеки по трафіку.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, У першому розділі проведено огляд та аналіз сучасних корпоративних мереж за захисту даних у них, виконана постановка задачі. В другому розділі виконано аналіз наявних засобів й вимог для проектування та моделювання роботи мереж. В третьому розділі розроблено фізичну та логічну топологію мережі, обрано схему адресації та маршрутизації, проведено конфігурацію всіх мережних пристроїв, налаштовано VPN-тунель, а також налаштовано HTTP, DHCP, DNS сервери, протестовано проходження трафіку через мережу.

4. Позитивні сторони роботи Кваліфікаційна робота має практичну цінність. Практична цінність результатів дослідження полягає в обгрунтуванні вибору засобів та їх налаштуванню для побудови захищених мереж невеликих

5. Негативні сторони роботи В роботі відсутній деталізований опис розробки схеми адресації.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження

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

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Нічепорук Андрій Олександрович, доцент кафедри комп'ютерної інженерії та інформаційних систем, к.т.н.

« 7 » 06 2023р. _____ (підпис)

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: Система захисту мережі малого офісу з віддаленим доступом до ресурсів

Автор: Лакоценін Захар Євгенійович

Спеціальність: 125 – Кібербезпека

Освітня програма: Освітньо-професійна

Науковий керівник: Орленко В.С.

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 методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) 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 5.87% і адресується до 241 першоджерела, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ В.С. Орленко

Завідувач кафедри КБ, гарант ОП _____ Ю.П. Кльоц

Дата: 07.06.2023

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015458395

Дата перевірки:
06.06.2023 13:50:33 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
06.06.2023 13:51:12 EEST

ID користувача:
100008300

Назва документа: **Лакоценін**

Кількість сторінок: **65** Кількість слів: **12359** Кількість символів: **96947** Розмір файлу: **1.24 MB** ID файлу: **1015117769**

5.87%
Схожість

Найбільша схожість: **1.81%** з джерелом з Бібліотеки (ID файлу: **1015105543**)

3.79% Джерела з Інтернету	159	Сторінка 67
3% Джерела з Бібліотеки	82	Сторінка 68

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 10%**

	Документ		Сумарний збіг по Базі Даних	
ID: 114921 Назва: Система захисту мережі малого офісу з віддаленим доступом до ресурсів Додано в БД: 2023-06-06 Автора: Лакоценін З.Є. Керівники: Орленко В.С. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	74306	1156	978 (1%)	13 (1%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми