Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Кушніра Дмитра Олександровича

на здобуття ступеня вищої освіти Бакалавра

Корпоративна мережа із захистом доступу до ресурсів

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ.101004.20.01.04 ПЗ

Виконав студент 3 курсу група КІ1С-21-1 Дмитро КУШНІР
Керівник старший викладач Сергій МОСТОВИЙ
Нормоконтролер старший викладач Сергій МОСТОВИЙ

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

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 123 – Компютерна інженерія

Освітня програма Освітньо-професійна

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2024 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Кушніру Дмитру Олександровичу

1 Тема роботи Корпоративна мережа із захистом доступу до ресурсів

Керівник роботи

Затверджено наказом ректора університету від 15 лютого 2024 № 8

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи План приміщення і території підприємства. Перелік інформаційних ресурсів, перелік мережного обладнення. Політики безпеки організації.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Дослідити предметну область. Обрати категорію та вид мережних пристроїв та іншого обладнення. Розробити фізичну топологію. Розробити логічну топологію. Зконфігорувати мережні пристрої відповідно до політик безпеки. Протестувати розроблену мережу та провести аналіз отриманих результатів.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Логічна топологія мережі. Фізична топологія мережі. Результати тестування мережного трафіку.

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2024 р.

КАЛЕНДАРНИЙ ПЛАН

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

Студент Дмитро КУШНІР

Керівник кваліфікаційної роботи Сергій МОСТОВИЙ

Формат	Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
A4		1	КРБКБ.101004.20.01.04 ПЗ	Корпоративна мережа	56	
				із захистом доступу до		
				ресурсів		
A2		2	КРБКБ.101004.20.01.04 Е8	Логічна топологія мережі	1	
A2		3	КРБКБ.101004.20.01.04 Е8	Фізична топологія мережі	1	

Зм.	Арк.	№ Докум.	Підп.	Дата	КРБКБ.101004.20.01.04 ВП		
Розробив		Кушнір Д.О.		19.06.24	Корпоративна мережа із захистом доступу до ресурсів	Літера	Аркуш	Аркушів
Перев.		Мостовий С.В.		19.06.24		н	1	1
Н. контр.		Мостовий С.В.		19.06.24	Відомість проєкту	ХНУ, КІ1с-21-1		
Затв.		Кльоц Ю.П.		19.06.24				

АНОТАЦІЯ

Тема кваліфікаційної роботи: "Корпоративна мережа із захистом доступу до ресурсів".

Автор роботи: Кушнір Д.О.

Керівник роботи: Мостовий С.В.

Пояснювальна записка: 56 с., 14 рис., 3 таблиці, 41 джерело.

Графічна частина: 2 плакати, 13 презентаційних слайдів.

КОРПОРАТИВНА МЕРЕЖА, ВІДДАЛЕНИЙ ДОСТУП ДО РЕСУРСІВ, ЗАХИСТ ДОСТУПУ ДО МЕРЕЖІ, VPN

Мета кваліфікаційної роботи: проектування та розроблення архітектури корпоративної мережі із ефективним захистом доступ до ресурсів мережі як зсередини, так і ззовні.

У роботі було досліджено і проаналізовано предметну область, виділено задачі, що необхідно реалізувати для побудови корпоративної мережі. Було розроблено логічну та фізичну топологію мережі, схему адресації. Проведено налаштування відповідних мережних пристроїв та серверів. Протестовано мережу на предмет отримання доступу до ресурсів. Результати тестування показали, що поставлена задача виконана в повному обсязі.

19.06.2024р.

ABSTRACT

The topic of the qualification work: "Corporate network with protection of access to resources."

Author of the work: Kushnir D.O.

Head of work: Mostovy S.V.

Explanatory note: 56 pp., 14 figures, 3 tables, 41 sources.

Graphic part: 2 posters, 13 presentation slides.

CORPORATE NETWORK, REMOTE ACCESS TO RESOURCES, NETWORK ACCESS PROTECTION, VPN

The purpose of the qualification work: design and development of the corporate network architecture with effective protection of access to network resources from both the inside and the outside.

In the work, the subject area was researched and analyzed, the tasks that must be implemented to build a corporate network were highlighted. The logical and physical topology of the network and the addressing scheme were developed. Appropriate network devices and servers have been configured. Tested the network for obtaining access to resources. The results of the testing showed that the task was completed in full.

10.06.2024р

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

ІА – інформаційний актив

ІКСМ – інформаційно-комунікаційні системи та мережі

ІС – інформаційна система

МЕ – міжмережевий екран

ОС – операційна система

ПЗ – програмне забезпечення

ТЗ – технічні заходи

CERT – computer emergency response team

CVE – common vulnerabilities and exposure

CVSS – commom vulnerability scoring system

DDOS – disturbed denial of service

DES – data encryption standart

DOS – denial of service

DNS – domain name system

EIP – extended instruction pointer

ESP – extended stack pointer

ICMP – internet control message protocol

IDS – intrusion detection system

IDMEF – intrusion detection message exchange format

IPS – intrusion protection system

NGFW – next generation firewall

PAM – privilege access management

PPP – point to point protocol

RAM – random access memory

ROM – read only memory

SMB – small medium bussines

VPN – virtual private network

VTP – vlan trunkling protocol

ВСТУП

У сучасному світі корпоративні мережі зазнають стрімкого розвитку, що зумовлюється необхідністю інтеграції новітніх технологій для забезпечення високого рівня безпеки, масштабованості та ефективності роботи.

Однією з основних тенденцій є перехід до хмарних технологій та гібридних інфраструктур, які дозволяють компаніям більш гнучко управляти своїми ресурсами та забезпечувати безперебійний доступ до даних. Також значного поширення набуває використання технологій штучного інтелекту та машинного навчання для автоматизації процесів виявлення та реагування на загрози.

Іншою важливою тенденцією є підвищення рівня кібербезпеки шляхом впровадження багатофакторної аутентифікації (MFA), використання шифрування даних як у стані спокою, так і під час передачі, та застосування передових засобів захисту кінцевих точок (Endpoint Protection). Корпоративні мережі також все частіше використовують Zero Trust архітектуру, яка передбачає ретельну перевірку кожного користувача та пристрою, незалежно від їхнього місця розташування в мережі.

У контексті зростання кількості кіберзагроз та складності атак, підприємства стикаються з проблемою забезпечення надійного захисту своїх мережевих ресурсів.

Традиційні методи захисту, такі як міжмережеві екрани та антивірусні програми, стають недостатніми для протидії сучасним загрозам. Потрібні нові підходи до управління доступом до мережевих ресурсів та моніторингу безпеки.

Ця кваліфікаційна робота спрямована на розв’язання проблеми захисту доступу до ресурсів корпоративної мережі через розробку і впровадження інтегрованої системи захисту, яка поєднує в собі сучасні технології аутентифікації, авторизації та моніторингу мережевих активностей.

Виходячи з мети, поставлено такі завдання, які необхідно виконати:

а) провести аналіз поточного стану корпоративної мережі: виявити існуючі вразливості та проблеми в системі захисту доступу;

б) розробка політики доступу: створити детальну політику доступу до мережевих ресурсів з урахуванням ролей та прав користувачів;

в) впровадження багатофакторної аутентифікації (MFA): забезпечити підвищення рівня безпеки шляхом впровадження MFA;

г) Налаштування системи моніторингу та реагування на загрози: використати сучасні інструменти для моніторингу мережевих активностей та швидкого реагування на загрози;

д) тестування та оцінка ефективності: Провести тестування системи на вразливості та оцінити ефективність впроваджених заходів.

Метою дослідження є аналіз, проектування та розробка корпоративної мережі з захистом доступу до ресурсів.

Основна мета полягає у створенні безпечної та ефективної інфраструктури, яка забезпечує доступ користувачів до необхідних ресурсів та захищає мережеві активи від зовнішніх атак та внутрішніх загроз.

У роботі застосовуватимуться такі методи дослідження:

а) аналіз вимог: Дослідження потреб користувачів та бізнес-вимог до мережі;

б) проектування мережі: Розробка архітектури мережі, вибір необхідного обладнання та технологій;

в) розробка програмного забезпечення: Написання програмного коду для реалізації функціональності безпеки та управління мережею;

г) тестування та валідація: Проведення тестів для перевірки працездатності та безпеки розробленої мережі;

д) впровадження та підтримка: Розгортання мережі на підприємстві та надання подальшої підтримки.

Об'єктом дослідження є корпоративна мережа, яка включає в себе комп'ютери, сервери, мережеве обладнання, програмне забезпечення та інші мережеві ресурси.

Предметом дослідження є проектування та розробка системи безпеки для корпоративної мережі, включаючи захист від зовнішніх атак, ідентифікацію та

аутентифікацію користувачів, контроль доступу до ресурсів, шифрування даних, моніторинг та управління безпекою мережі.

Сучасний стан завдання захисту корпоративних мереж характеризується значною складністю та високими вимогами до безпеки. Більшість компаній усвідомлюють необхідність інтеграції комплексних систем захисту, однак впровадження таких систем часто потребує значних ресурсів та спеціалізованих знань. Актуальність цього завдання обумовлена постійним зростанням кількості та складності кіберзагроз, що робить питання безпеки пріоритетним для будь-якої організації.

Забезпечення надійного захисту доступу до ресурсів корпоративної мережі є критично важливим для збереження конфіденційності, цілісності та доступності інформації.

Невирішення цього завдання може призвести до серйозних фінансових втрат, компрометації даних та втрати довіри клієнтів. Крім того, з огляду на вимоги законодавства щодо захисту даних, підприємства зобов'язані дотримуватись певних стандартів безпеки, що також підкреслює важливість даного завдання.

Розробка, представлена в цій роботі, може бути застосована в різних галузях, де існує потреба у захисті конфіденційних даних та забезпеченні безпеки мережевих ресурсів. Це можуть бути фінансові установи, медичні заклади, державні організації, а також будь-які комерційні підприємства, що оперують великими обсягами критичної інформації.

Основне призначення розробки — підвищення рівня безпеки корпоративних мереж шляхом впровадження сучасних методів управління доступом та захисту інформації.

1 ДОСЛІДЖЕННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАХИСТОМ ДОСТУПУ ДО РЕСУРСІВ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Змістовний аналіз корпоративної мережі із захистом доступу до ресурсів, її структурних та функціональних особливостей

Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам. Залежно від масштабу підприємства, а також від складності і різноманіття вирішуваних завдань розрізняють мережі відділу, мережі кампусу і корпоративні мережі (рис 1.1) (термін «корпоративні» в даній класифікації набуває вузького значення — мережу великого підприємства).

Рисунок 1.1 – Приклад корпоративних мереж [13]

Користувачем корпоративної мережі повинен бути тільки співробітник компанії. На відміну від транспортних мереж, мереж компанії зазвичай не

доступні для інших користувачів або груп.

Розглянемо типову концепцію корпоративної мережі .Будь-яка організація - це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи зв'язані між собою функціонально, тобто вони виконують окремі види робіт в рамках єдиного бізнес процесу, а також інформаційно, обмінюючись документами, факсами, письмовими і усними розпорядженнями і так далі крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційною, так і функціональною. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися - для урядової установи, банку, промислового підприємства, комерційної фірми і так далі. [8,6]

Такий загальний погляд на організацію дозволяє сформулювати деякі загальні принципи побудови корпоративних інформаційних систем, тобто інформаційних систем в масштабі всієї організації.

Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP і використовує комунікаційні стандарти Інтернету, а також сервісні застосування, що забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків і інших службових документів. Службовці здійснюють доступ до необхідних документів за допомогою засобів перегляду Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послугам Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення і звукозаписи), надання необхідних ресурсів по запитах клієнтів Web, а також здійснення доступу до баз даних. У цьому керівництві всі служби публікації називаються “Службами Інтернету” незалежно від того, де вони використовуються (у Інтернеті або корпоративній мережі).

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднуючою офіси, підрозділи і інші структури, що знаходяться на значному віддаленні один від одного. Принципи, по яких будується корпоративна мережа,

досить сильно відрізняються від тих, що використовуються при створенні локальної мережі. Це обмеження є принциповим, і при проектуванні.

Корпоративна мережа є основою інформаційної інфраструктури будь-якого сучасного підприємства. Вона забезпечує зв'язок між співробітниками, доступ до корпоративних ресурсів та інформації, а також підтримує різноманітні бізнес-процеси. Захист доступу до ресурсів у корпоративній мережі є критичним завданням, що впливає на безпеку, цілісність та конфіденційність даних.

Розглянемо структурні особливості корпоративної мережі:

а) центральний офіс:

- дата-центр: У центральному офісі знаходяться основні сервери, системи зберігання даних та мережеве обладнання. Дата-центр забезпечує централізоване управління та зберігання інформації;

- основний маршрутизатор та міжмережевий екран (Firewall): Контролюють вхідний та вихідний трафік, забезпечують захист від зовнішніх загроз;

- сервери: Файлові сервери, сервери баз даних, веб-сервери та сервери додатків забезпечують функціональність та зберігання корпоративних даних;

- комутатори ядра мережі: Забезпечують з'єднання між різними сегментами мережі;

- безпровідні точки доступу (Wi-Fi): Забезпечують мобільність та доступ до мережі для бездротових пристроїв;

б) віддалені офіси:

- локальні маршрутизатори та міжмережеві екрани: Забезпечують безпеку та зв'язок віддалених офісів з центральним офісом;

- комутатори для локальної мережі: Забезпечують з'єднання пристроїв у віддалених офісах;

- безпровідні точки доступу: Забезпечують бездротовий доступ до мережі у віддалених офісах;

в) віддалені користувачі;

- VPN-клієнти: Забезпечують захищений доступ до корпоративної мережі для віддалених користувачів;

Розглянемо функціональні особливості корпоративної мережі:

а) міжмережеві екрани (Firewall);

- забезпечують контроль вхідного та вихідного трафіку;

- налаштовуються для обмеження доступу до критичних ресурсів та захисту від зовнішніх атак;

б) багатофакторна аутентифікація (MFA);

- Забезпечує додатковий рівень безпеки при вході користувачів до системи;

- Використовує комбінацію паролів, одноразових паролів (OTP) або біометричних даних для аутентифікації;

в) VPN (Virtual Private Network):

- захищає передавання даних між віддаленими користувачами та корпоративною мережею;

- шифрує трафік, що проходить через незахищені мережі, забезпечуючи конфіденційність.

г) контроль доступу на основі ролей (RBAC):

- визначає права доступу до ресурсів залежно від ролей користувачів;

- централізовано керується за допомогою LDAP або Active Directory.

д) сегментація мережі:

- поділ мережі на сегменти для ізоляції різних груп користувачів та ресурсів;

- використання VLAN для забезпечення безпеки та управління трафіком.

е) системи виявлення та запобігання вторгненням (IDS/IPS):

- виявляють та запобігають підозрілим активностям у мережі;

- постійно моніторять мережевий трафік для виявлення загроз.

є) моніторинг та управління мережею:

- використання систем управління інформаційною безпекою (SIEM) для централізованого збору та аналізу даних;

- автоматичне сповіщення про підозрілі активності.

ж) управління оновленнями та патчами:

- системи управління оновленнями забезпечують своєчасне встановлення патчів та оновлень;

- регулярне оновлення операційних систем та програмного забезпечення.

д) резервне копіювання та відновлення:

- системи резервного копіювання забезпечують збереження даних у випадку збоїв;

- плани відновлення перевіряються регулярно для забезпечення їх працездатності.

Сучасні корпоративні мережі стикаються з численними викликами, пов'язаними з безпекою та управлінням доступом до ресурсів. Зростання кількості кіберзагроз, розвиток віддаленої роботи та підвищення вимог до конфіденційності даних змушують підприємства інвестувати в надійні системи захисту. Актуальність даного дослідження полягає у необхідності розробки інтегрованих рішень, які забезпечують комплексний захист мережі, підвищують її стійкість та ефективність. [22]

Впровадження надійної системи захисту доступу до ресурсів у корпоративній мережі дозволяє:

- запобігти несанкціонованому доступу до конфіденційних даних;

- забезпечити безперебійну роботу бізнес-процесів;

- знизити ризики, пов'язані з кібератаками та внутрішніми загрозами;

- підвищити рівень довіри клієнтів та партнерів.

Розробка може бути використана в різних галузях, таких як:

- фінансові установи: для захисту банківських даних та транзакцій;

- медичні заклади: для збереження конфіденційності медичних записів;

- виробничі підприємства: для захисту інтелектуальної власності та виробничих секретів;

- освітні установи: для захисту персональних даних студентів та викладачів.

Корпоративна мережа із захистом доступу до ресурсів є ключовим елементом інформаційної інфраструктури будь-якого підприємства. Розробка та впровадження комплексної системи захисту дозволяє забезпечити надійність, безпеку та ефективність мережі, що є критично важливим у сучасному цифровому середовищі.

Розглянемо декілька варіантів корпоративних мереж із захистом доступу до ресурсів, що реалізовані в IT-компанія України.

а) Корпоративна мережа великої IT-компанії з розподіленою інфраструктурою- GlobalTech Solutions. GlobalTech Solutions є великою IT-компанією з офісами у різних містах України (Київ, Харків, Львів) та за кордоном. Основні завдання мережі включають забезпечення безпечного доступу до корпоративних ресурсів, управління великим обсягом даних та забезпечення безперервного обміну інформацією між різними офісами.

Основні компоненти мережі:

- VPN: Використовується для забезпечення безпечного з'єднання між офісами компанії та віддаленими працівниками;

- firewall: Розгорнутий для захисту від зовнішніх атак і контролю доступу до внутрішніх ресурсів;

- IDS/IPS: Система виявлення та запобігання вторгненням для моніторингу та захисту мережі;

- сервери: Централізовані сервери з базами даних, файловими сховищами та іншими корпоративними ресурсами;

Дана категорія мереж має наступні особливості застосування:

- високий рівень захисту: Використання VPN та IDS/IPS забезпечує високий рівень захисту даних;

- розподіленість: Важливо забезпечити високу продуктивність і мінімальну затримку між офісами;

- підтримка мобільності: Підтримка віддалених співробітників через VPN.

б) Корпоративна мережа середньої IT-компанії з акцентом на безпеку даних- DataSafe IT. DataSafe IT спеціалізується на розробці програмного забезпечення та наданні IT-консалтингових послуг. Компанія має високі вимоги до захисту даних через роботу з конфіденційною інформацією клієнтів.

Основні компоненти мережі:

- VPN: Для безпечного доступу до мережі для віддалених працівників;

- firewall з DPI: Глибока перевірка пакетів для детального контролю трафіку;

- антивірусні рішення: Захист робочих станцій та серверів від вірусів і шкідливого ПЗ;

- системи резервного копіювання: Автоматизовані системи резервного копіювання для забезпечення відновлення даних у разі інцидентів.

Дана категорія мереж має наступні особливості застосування:

- захист конфіденційності: Високий рівень захисту даних клієнтів є критично важливим;

- безперервність бізнесу: Системи резервного копіювання забезпечують можливість швидкого відновлення після інцидентів;

- забезпечення доступності мережі для віддалених працівників через VPN.

в) Корпоративна мережа стартапу з фокусом на гнучкість та масштабованість компанія InnovateIT. InnovateIT є стартапом, що спеціалізується на розробці інноваційних IT-рішень. Компанія швидко розширюється, тому їм необхідна гнучка і масштабована мережева інфраструктура.

Основні компоненти мережі:

- хмарні сервіси: Використання хмарних сервісів для зберігання даних та хостингу додатків;

- SD-WAN: Використання програмно визначеної широкомасштабної мережі для управління трафіком між офісами та хмарними ресурсами;

- VPN: Для забезпечення безпечного з'єднання віддалених працівників;

- zero Trust: Впровадження принципу Zero Trust для забезпечення безпеки доступу до ресурсів;

Дана категорія мереж має наступні особливості застосування:

- масштабованість: Використання хмарних сервісів та SD-WAN дозволяє легко масштабувати мережу відповідно до зростання компанії;

- гнучкість: Хмарні рішення забезпечують гнучкість у розгортанні нових сервісів та додатків;

- zero Trust: Підвищена безпека через впровадження принципу Zero Trust, який передбачає перевірку кожного доступу до ресурсів.

Проаналізувавши різноманітні варіанти корпоративних мереж із захистом доступу до ресурсів на прикладі розглянутих компаній. В цілому можна виділити наступні особливості по застосуванню цих мереж на території України.

а)юридичні вимоги та регуляції:

- компанії повинні дотримуватися українського законодавства щодо захисту даних (наприклад, Закону України "Про захист персональних даних");

- важливим аспектом є дотримання міжнародних стандартів захисту даних (наприклад, GDPR для європейських клієнтів).

б) інфраструктура Інтернет-провайдерів:

- якість інтернет-з'єднання може варіюватися залежно від регіону, що може вплинути на продуктивність мережі;

- важливо вибирати надійних інтернет-провайдерів для забезпечення безперебійного зв'язку.

в) вартість обладнання та послуг:

- вартість мережевого обладнання та послуг може бути високою, що впливає на бюджет малих та середніх компаній;

- альтернативні варіанти, такі як хмарні сервіси, можуть допомогти знизити витрати на інфраструктуру.

г) кваліфікація персоналу:

- наявність висококваліфікованих ІТ-спеціалістів є важливим фактором для управління та захисту корпоративних мереж;

- інвестиції в навчання та підвищення кваліфікації персоналу є критично важливими для ефективного управління мережею.

Впровадження корпоративних мереж із захистом доступу до ресурсів дозволяє українським ІТ-компаніям забезпечити високий рівень безпеки, гнучкість та масштабованість своїх ІТ-інфраструктур, що є ключовим фактором для успішного функціонування та зростання бізнесу.

1.2 Аналіз наявного програмно-апаратного забезпечення корпоративної мережі із захистом доступу до ресурсів

Перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям “інформація”. Це поняття сьогодні вживається дуже широко і різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Повсякденно під час здійснення різних видів діяльності користуються таким поняттям:

Інформація – нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення.

Інформація – це відомості, які є об’єктом зберігання, передавання і оброблення.

Відомо, що інформація може мати різну форму, зокрема, дані в комп’ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції, дисертації, судові документи й ін.

Як і всякий продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Відповідно до різноманітності поняття інформації, словосполучення “інформаційна безпека” в різних контекстах може мати різний сенс.

Так, у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” наводиться таке поняття інформаційної безпеки:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. [29]

Спеціальне законодавство в галузі безпеки інформаційної діяльності

представлено низкою законів. У їхньому складі особливе місце належить базовому Закону “Про інформацію, інформатизацію і захист інформації”, що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

– інформації та інформаційних систем;

– суб’єктів – учасників інформаційних процесів;

– правовідносин виробників – споживачів інформаційної продукції;

– власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб’єктам інформаційних відносин, зокрема, власникам і користувачам інформації та інфраструктури.

Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб’єктів інформаційних відносин та інтересів цих суб'єктів, пов’язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці – це зворотна сторона використання інформаційних технологій. [1]

Тут необхідно зауважити, що трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно різнитися. Для ілюстрації досить зіставити режимні державні організації і навчальні заклади. У першому випадку “хай краще все зламається, ніж ворог дізнається хоч один секретний біт”, у другому – “немає у нас жодних секретів, аби все працювало”. Отже, інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це поняття принципово ширше.

Суб’єкт інформаційних відносин може постраждати (зазнати збитки та/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій власне захист від несанкціонованого доступу до інформації

стоїть за важливістю зовсім не на першому місці.

Класифікацію : [19,24] загроз за ознаками наведено в таблиці 1.1.

Таблиця 1.1 — Класифікація загроз за ознаками

Ознака класифікації	Причини, спрямованість, характеристики загроз
1	2
Природа виникнення	Природні загрози (виникають через впливи на АС та її компоненти об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від людини). Штучні загрози (викликані діяльністю людини) Фізичний доступ: □ подолання рубежів територіального захисту і доступ до незахищених інформаційних ресурсів;
Принцип несанкціонованого доступу (НСД)	□ розкрадання документів і носіїв інформації; □ візуальне перехоплення інформації, виведеної на екрани моніторів і принтери; □ підслуховування; □ перехоплення електромагнітних випромінювань. Логічний доступ (доступ із використанням засобів комп'ютерної системи)
Мета НСД	Порушення конфіденційності (розкриття інформації). Порушення цілісності (повне або часткове знищення інформації, спотворення, фальсифікація, викривлення). Порушення доступності (наслідок — відмова в обслуговуванні).
Причини появи вразливостей різних типів	Недоліки політики безпеки. Помилки адміністративного керування. Недоліки алгоритмів захисту. Помилки реалізації алгоритмів захисту
Характер впливу	Активний (внесення змін в АС). Пасивний (спостереження).
Режим НСД	За постійної участі людини (в інтерактивному режимі) можливе застосування стандартного ПЗ. Без особистої участі людини (у пакетному режимі) найчастіше для цього застосовують спеціалізоване ПЗ.

Кінець таблиці 1.1

1	2
Місцезнаходження джерела НСД	Внутрішньосегментне (джерело знаходиться в локальній мережі). У цьому випадку, як правило, ініціатор атаки — санкціонований користувач. Міжсегментне: – несанкціоноване вторгнення з відкритої мережі в закриту; – порушення обмежень доступу з одного сегмента закритої мережі в інший.
Наявність зворотнього зв'язку	Зі зворотним зв'язком (атакуючий отримує відповідь системи на його вплив). Без зворотного зв'язку (атакуючий не отримує відповіді).

Для забезпечення безпеки доступу до ресурсів у корпоративній мережі використовується комплекс програмно-апаратних засобів, що включає мережеве обладнання, програмне забезпечення для управління та моніторингу безпеки, а також системи аутентифікації та авторизації. Аналіз наявного програмно-апаратного забезпечення дозволяє оцінити його відповідність сучасним вимогам безпеки та ефективності.

Розглянемо варіанти мережного обладнання корпоративних мереж:

а) маршитизатори та комутатори: Cisco, Juniper, Huawei: Високопродуктивні маршрутизатори та комутатори, що забезпечують надійну роботу мережі та підтримку різних протоколів маршрутизації. Вони забезпечують Підтримка VLAN, QoS (Quality of Service), управління трафіком, резервування каналів зв'язку;

б)міжмережеві екрани (Firewall): Fortinet, Palo Alto Networks, Check Point: Міжмережеві екрани наступного покоління (NGFW), що забезпечують комплексний захист від загроз. Вони дозволяють проводити: інспекція трафіку на прикладному рівні, реалізовувати захист від вторгнень (IPS), контроль доступу на основі політик, VPN-з'єднання.

в)Бездротові точки доступу (Wi-Fi): Cisco Meraki, Aruba, Ubiquiti: Вони забезпечують надійний та безпечний доступ до мережі, підтримують WPA3, управляють трафіком, сегментують мережі, гостьовий доступ.

Розглянемо варіанти системи аутентифікації та авторизації

а)Active Directory (AD) використовується для централізованого управління обліковими записами користувачів, політиками безпеки та доступом до ресурсів. Забезпечують підтримка групових політик (GPO), багатофакторна аутентифікація (MFA), інтеграція з іншими системами;

б) LDAP (Lightweight Directory Access Protocol) використовується для зберігання та пошуку інформації про користувачів, групи та інші об'єкти в мережі. Забезпечує підтримка централізованого управління доступом, інтеграція з різними додатками.

Розглянемо програмне забезпечення для моніторингу та управління безпекою:

а)SIEM (Security Information and Event Management):Splunk, IBM QRadar, ArcSight: Платформи для збору, аналізу та кореляції даних з різних джерел для виявлення та реагування на загрози. Забезпечують аеальний час аналізу подій, автоматизація реакцій на інциденти, генерація звітів.

б)Антивірусне та антишкідливе програмне забезпечення:Avast, Bitdefender, Avira, AVG: Програми для захисту кінцевих точок від вірусів, шкідливого ПЗ та інших загроз. Забезпечують постійне оновлення баз даних загроз, проактивний захист, сканування в реальному часі.

в)Системи виявлення та запобігання вторгнень (IDS/IPS): Snort, Suricata, Cisco IPS: Системи, що виявляють та запобігають підозрілим активностям у мережі. Вони дозволяють проводити аналіз мережевого трафіку, сигнатурний та поведінковий аналіз, реагування на інциденти.

Розглянемо варіанти захисту від витоку даних (DLP): Forcepoint, Digital Guardian, Symantec DLP: Системи для запобігання витоку конфіденційних даних з корпоративної мережі. Забезпечують моніторинг та контроль передачі даних, політики безпеки для різних каналів зв'язку (email, веб, USB).

Наявне програмно-апаратне забезпечення корпоративної мережі забезпечує високий рівень безпеки завдяки використанню сучасних технологій та інтеграції різних компонентів. Проте, існує декілька аспектів, які потребують постійної уваги та оновлення:

а) адаптація до нових загроз: Кіберзагрози постійно розвиваються, тому необхідно регулярно оновлювати ПЗ та обладнання для захисту від нових атак;

б) інтеграція нових технологій: Використання технологій штучного інтелекту та машинного навчання для виявлення аномалій та підозрілої активності;

в) автоматизація реакцій на інциденти: Розширення можливостей автоматизації для швидшого реагування на інциденти безпеки;

г) підвищення користувацької зручності: Спрощення процедур аутентифікації та авторизації без зниження рівня безпеки.

Наявне програмно-апаратне забезпечення корпоративної мережі забезпечує необхідний рівень захисту доступу до ресурсів. Проте, з огляду на швидкий розвиток кіберзагроз, необхідно постійно оновлювати та вдосконалювати інфраструктуру безпеки. Інтеграція новітніх технологій, регулярне оновлення програмного забезпечення та навчання персоналу є ключовими компонентами для підтримки високого рівня безпеки в корпоративній мережі.

1.3 Визначення вимог до системи автоматизації та розробка технічного завдання

Метою даної роботи є аналіз поточного стану корпоративної мережі, виявлення можливих вразливостей у системі захисту доступу до ресурсів та розробка заходів для підвищення безпеки.

Для реалізації поставленої задачі мають бути вирішені такі питання:

1. Аналіз поточного стану мережі:

- Огляд фізичної і логічної топології мережі.

- Ідентифікація критичних вузлів та ресурсів мережі.
- Перевірка поточних методів аутентифікації та авторизації.
- Огляд використання міжмережевих екранів (firewall) та систем запобігання вторгненням (IDS/IPS).

2. Перевірка політики доступу:

- Аналіз існуючих політик доступу до ресурсів.
- Перевірка ролей та прав користувачів.
- Визначення процедур управління доступом.

3. Аудит системи безпеки:

- Перевірка конфігурації мережевих пристроїв (роутери, комутатори, точки доступу).
- Оцінка використання VPN для віддаленого доступу.
- Аудит використання шифрування даних при передачі та зберіганні.

4. Тестування на вразливості:

- Виконання сканування мережі на наявність вразливостей.
- Проведення тестів на проникнення (penetration testing).
- Аналіз журналів подій (логів) для виявлення підозрілих активностей.

5. Оцінка безпеки кінцевих точок:

- Перевірка захисту робочих станцій, серверів та мобільних пристроїв.
- Оцінка використання антивірусного та антивірусного ПЗ.
- Перевірка процедур оновлення та патчінгу ПЗ.

6. Документування та рекомендації:

- Складання звіту з виявленими вразливостями та потенційними ризиками.
- Розробка рекомендацій для покращення системи безпеки.

Постановка задачі:

1. Збір даних про мережу

- Зібрати детальну інформацію про фізичну і логічну топологію корпоративної мережі.
- Визначити критичні вузли та ресурси мережі.

2. Аналіз політик доступу

- Перевірити існуючі політики доступу до мережевих ресурсів.
- Провести аудит ролей та прав користувачів.

3. Перевірка мережевих пристроїв

- Проаналізувати конфігурації мережевих пристроїв на предмет безпеки.
- Перевірити використання VPN та інших методів захисту для віддаленого доступу.

4. Тестування на вразливості

- Виконати сканування мережі для виявлення вразливостей.
- Провести тестування на проникнення.

5. Оцінка кінцевих точок

- Перевірити захист робочих станцій, серверів та мобільних пристроїв.
- Оцінити ефективність антивірусного та антивірусного ПЗ.

6. Складання звіту та розробка рекомендацій

- Підготувати звіт з виявленими вразливостями та потенційними ризиками.
- Надати рекомендації для покращення системи безпеки.

Перед початком розробки корпоративної мережі необхідно визначити основні вимоги:

1. Безпека: Забезпечення конфіденційності, цілісності та доступності даних.

2. Масштабованість: Можливість легкого розширення мережі.

3. Надійність: Висока доступність і стійкість до збоїв.

4. Продуктивність: Швидкий доступ до ресурсів та мінімальні затримки.

5. Керованість: Простота адміністрування та моніторингу мережі.

2. Топологія мережі

3. Захист доступу до ресурсів

3.1. Міжмережеві екрани (Firewall)

- Використання міжмережевих екранів для контролю вхідного та вихідного трафіку.

- Налаштування правил доступу для обмеження доступу до критичних ресурсів.

3.2. Багатофакторна аутентифікація (MFA)

- Впровадження багатофакторної аутентифікації для доступу до мережевих ресурсів.

- Використання додаткових факторів, таких як одноразові паролі (OTP) або біометрія.

3.3. VPN (Virtual Private Network)

- Налаштування VPN для захищеного доступу віддалених користувачів до мережі.

- Використання шифрування для захисту даних при передачі.

3.4. Контроль доступу на основі ролей (RBAC)

- Визначення ролей і призначення прав доступу відповідно до цих ролей.

- Використання LDAP або Active Directory для централізованого управління користувачами.

3.5. Сегментація мережі

- Поділ мережі на сегменти для обмеження доступу між різними частинами мережі.

- Використання VLAN для ізоляції різних груп користувачів і ресурсів.

3.6. Системи виявлення та запобігання вторгненням (IDS/IPS)

- Впровадження систем IDS/IPS для виявлення та запобігання загрозам.

- Моніторинг мережевого трафіку для виявлення підозрілих активностей.

4. Моніторинг та управління мережею

4.1. Система управління інформаційною безпекою (SIEM)

- Використання SIEM для централізованого збору та аналізу журналів подій.

- Налаштування автоматичних сповіщень про підозрілі активності.

4.2. Моніторинг мережевого трафіку

- Використання інструментів для моніторингу та аналізу мережевого трафіку.

- Визначення базових показників для виявлення аномалій.

4.3. Управління оновленнями та патчами

- Впровадження системи управління оновленнями для своєчасного встановлення патчів.

- Регулярне оновлення операційних систем та програмного забезпечення.

5. Забезпечення резервного копіювання та відновлення

- Налаштування систем резервного копіювання даних.

- Регулярне тестування планів відновлення після збоїв.

2 ПРОЄКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАХИСТОМ ДОСТУПУ ДО РЕСУРСІВ

2.1 Фізична топологія

Фізична топологія мережі (рис.2.1) відображає фактичне розташування та з'єднання мережевих пристроїв і кабелів у мережі. Вона визначає, як пристрої (комп'ютери, сервери, комутатори, маршрутизатори) фізично підключені один до одного. Фізична топологія впливає на продуктивність мережі, її масштабованість та надійність.

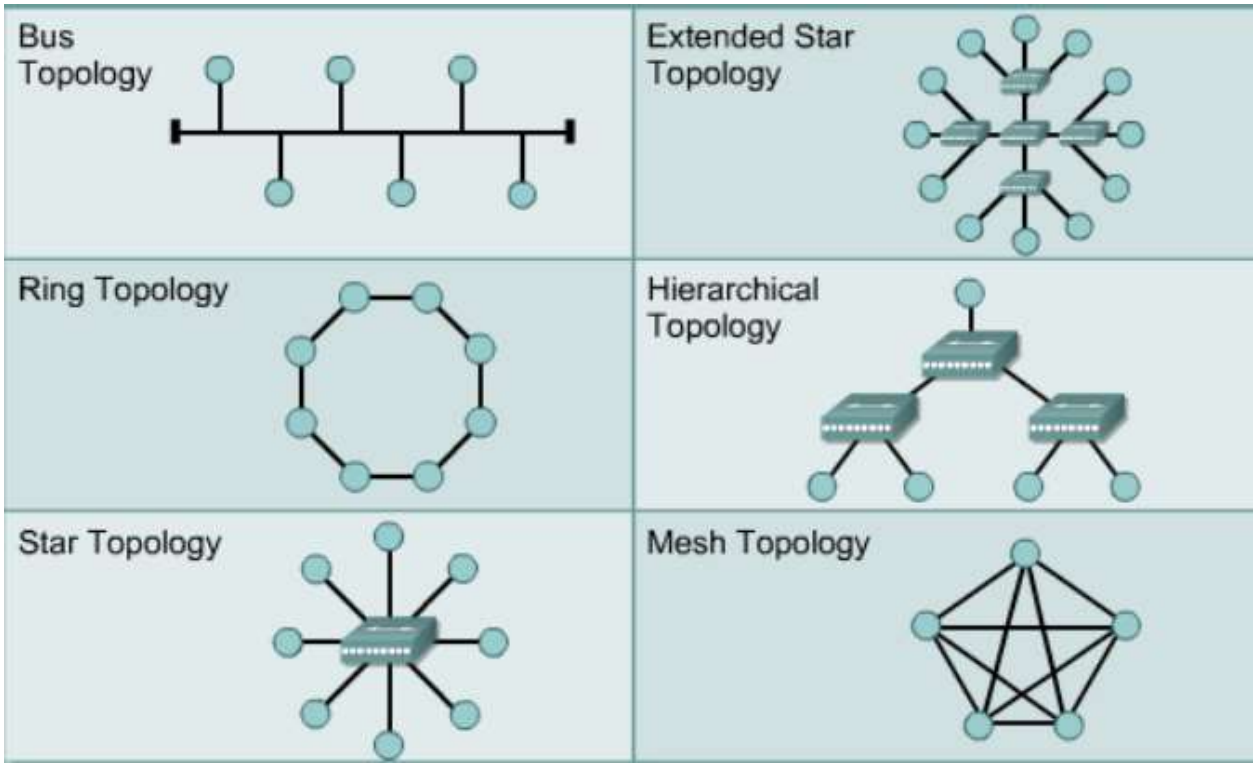


Рисунок 2.1 – Основні мережеві топології [17]

Основні типи фізичної топології:

а) шина (Bus):

- всі пристрої підключені до одного загального кабелю;
- простота установки, але уразлива до пошкоджень кабелю.

б) зірка (Star):

- всі пристрої підключені до центрального комутатора або концентратора;

- легке управління та виявлення проблем, але вразлива до відмови центрального пристрою;

в) кільце (Ring):

- пристрої підключені по колу, де кожен пристрій має два сусіди;

- рівномірний розподіл трафіку, але складність виявлення та усунення пошкоджень.

г) сітка (Mesh):

- кожен пристрій підключений до кількох інших пристроїв;

- висока надійність і стійкість до відмов, але висока вартість і складність установки.

д) дерево (Tree):

- ієрархічна структура, схожа на топологію зірки, але з додатковими рівнями;

- гнучкість і масштабованість, але складність управління.

Логічна топологія визначає, як дані передаються між пристроями у мережі, незалежно від їх фізичного розташування. Вона описує структуру потоків даних та методи доступу до мережі.

Основні типи логічної топології:

а) шина (Bus):

- дані передаються по одному загальному каналу;

- використовується в Ethernet з використанням широкомовних передач.

б) зірка (Star):

- всі дані проходять через центральний пристрій (комутатор/концентратор);

- поширена в сучасних Ethernet-мережах.

в) кільце (Ring):

- дані передаються по колу від одного пристрою до іншого;

- використовується в мережах Token Ring і FDDI;

г) сітка (Mesh):

- дані можуть передаватися по декількох шляхах;

- висока надійність та гнучкість.

д) дерево (Tree):

- ієрархічна структура з багатьма рівнями;

- підходить для великих корпоративних мереж.

Хоча фізична і логічна топології можуть бути різними, вони тісно взаємопов'язані. Наприклад, фізична топологія зірки може мати логічну топологію шини, якщо використовується спільний середовище передачі, як у випадку з деякими видами Ethernet. Правильне планування та вибір топології є критичними для забезпечення оптимальної продуктивності, надійності та масштабованості мережі.

Фізична топологія мережі визначає розміщення і з'єднання мережевого обладнання. Для нашої IT-компанії пропонується зіркоподібна топологія, оскільки вона забезпечує високу швидкість передачі даних та зручність у налаштуванні і підтримці. Основні елементи фізичної топології:

- центральний комутатор (Core Switch) – з'єднує всі сегменти мережі;

- комутатори доступу (Access Switches) – підключаються до центрального комутатора і забезпечують доступ до мережі для робочих станцій;

- маршрутизатор – забезпечує підключення до зовнішньої мережі (інтернету);

- точки доступу (Access Points) – забезпечують бездротовий доступ до мережі.

За наведеною на рис.2.2 топологієюовипливає, що:

а) центральний комутатор розташований у серверній кімнаті;

б) комутатори доступу розташовані у різних відділах компанії;

г) маршрутизатор підключений до центрального комутатора і до провайдера інтернету;

д) точки доступу розташовані по всьому офісу для забезпечення бездротового покриття.

2.2 Логічна топологія

Найбільш поширеним мережевим обладнанням для побудови мереж є обладнання компанії Cisco. Незважаючи на те, що ОС Cisco IOS підтримує аутентифікацію поновлень маршрутизації актуальною є задача побудови захищеної мережі на основі використання технології VPN.

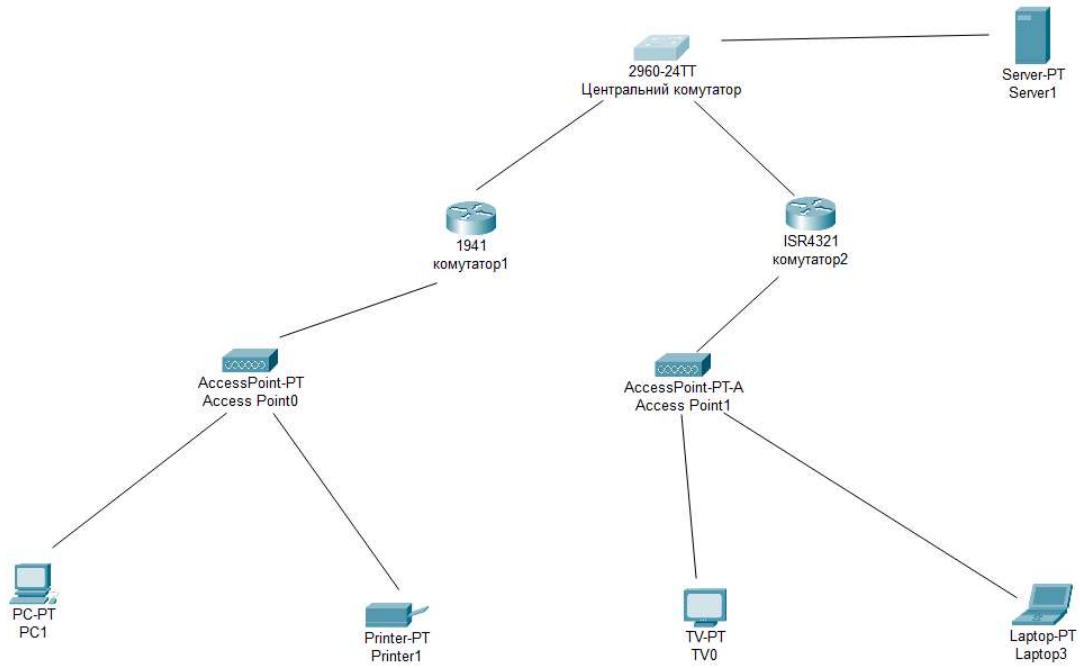


Рисунок 2.2 – Логічна топологія мережі

Об’єми створюваної, переданої по каналах зв’язку і збереженої інформації постійно зростають. Ефективність інформаційних систем і мереж забезпечується по двох основних напрямках — стиснення об’ємів і захист інформації. [2,9]

Одним із заходів захисту інформації в таких мережах є фіксація mac-адресів робочих станції користувачів, що підключаються до мережі. Портам комутатора прописують відповідну mac-адресу, і якщо в процесі роботи мережі, до цього порту буде підключено комп’ютер з мережевою картою у якої інша адреса, то він буде блокований даним портом. Іншими словами здійснюється «прив’язка» mac-

адресів комп'ютерів посадових осіб до портів комутатора на основі технології VLAN (Virtual LAN).

Виробники комутаторів випускають їх уже із фіксованою конфігурацією, коли всі порти прописані до VLAN1, тобто обмін між портами не розмежований і можна створювати дзеркальний порт, а також контролювати інформацію, що передається через будь-який із портів. Технологія VLAN дає можливість при конфігуруванні портів комутаторів і визначенні їх режимів роботи, здійснити групування портів по напрямкам діяльності посадових осіб, комп'ютери яких планується підключати. Причому, окремі порти різних комутаторів входять до однієї віртуальної мережі vlan10, vlan20 і т.д.

Пакети, що передаються від абонента не входять за межі конкретної VLAN. Така мережа повністю захищена він небажаного втручання. Для виходу із локальної мережі і підключення до інших мереж потрібний маршрутизатор (gateway), який працює на мережевому рівні

Логічна топологія описує шлях передачі даних у мережі. Для забезпечення безпеки і управління доступом використовуються віртуальні локальні мережі (VLAN).

Для нашої корпоративної мережі були виділені та спроектовані наступні підмережі (рис.2.3):

- VLAN для адміністрації – для управлінського персоналу та адміністраторів систем.

- VLAN для розробників – для відділу розробки програмного забезпечення.

- VLAN для тестувальників – для відділу тестування.

- VLAN для гостей – для відвідувачів компанії.

- VLAN для бездротових пристроїв – для пристроїв, що підключаються через Wi-Fi.

Кожен VLAN ізольований один від одного для підвищення безпеки і управління трафіком.

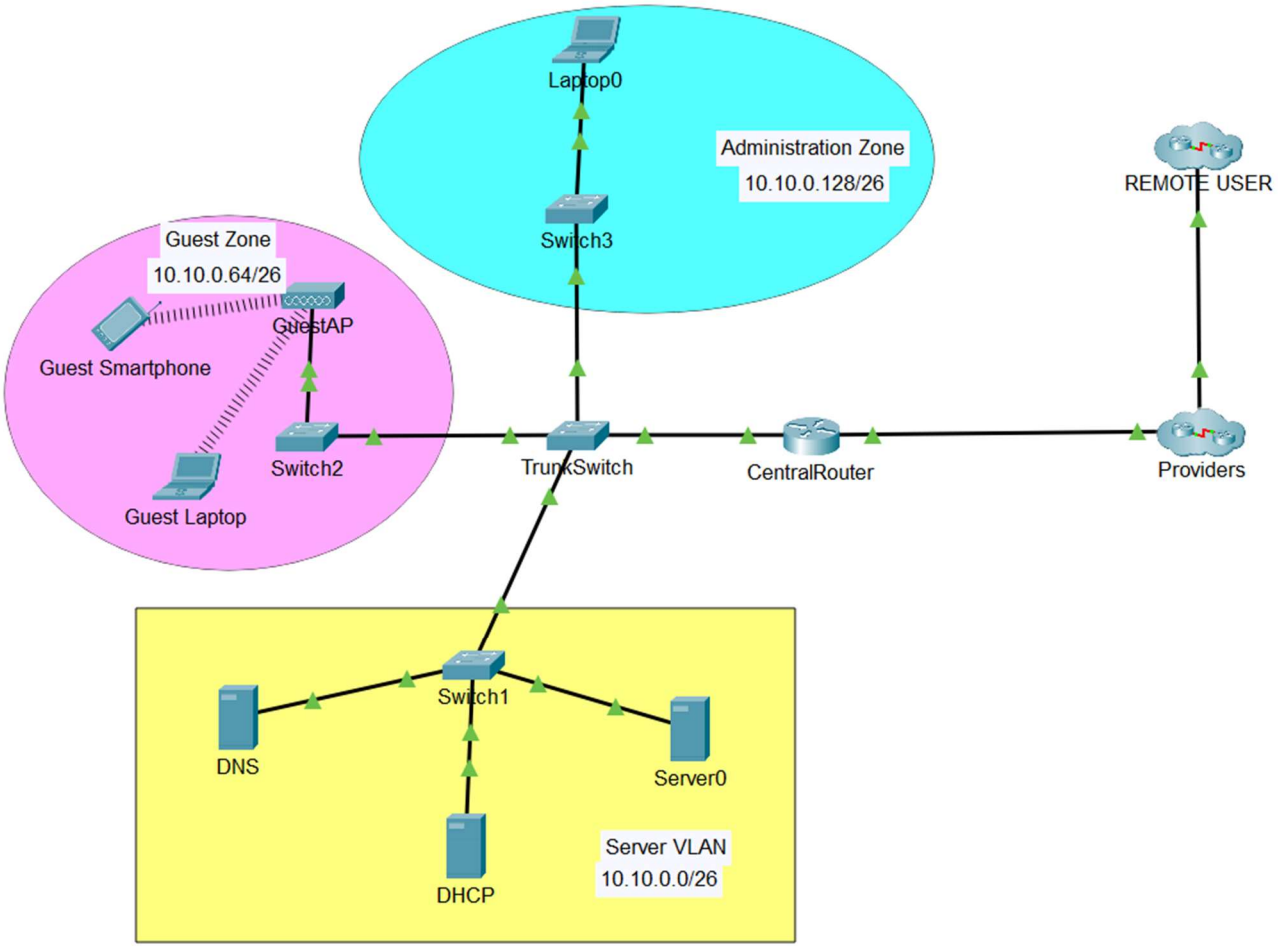


Рисунок 2.3 – Розподіл на підмережі

Така організація корпоративної мережі дає можливість в майбутньому масштабувати мережу, підключати нових користувачів у нові сегменти, міняти фізичне розташування об'єктів без значних змін у налаштуванні обладнання.

2.3 Схема адресації

Розрахунок адресного простору IP-адрес включає в себе визначення діапазону IP-адрес, які будуть використовуватись у мережі.

Основні кроки для розрахунку адресного простору IP-адрес наступні: Визначаємо версію протоколу IP (IPv4 або IPv6), залежно від потреб мережі. Більшість мереж зараз використовують IPv4 тому й в цій роботі буде використано

цю версію. Визначимо клас IPv4-адреси (A, B, C, D і E). Для менеджменту буде використано клас B. Це потрібно лише для семантичного виділення мережі.

Весь адресний простір використовуватись не буде. Але для мережі підприємства буде використовуватись весь клас C.

Розрахуємо скільки мереж потрібно. Це може бути важливо для масштабування мережі та організації сегментів мережі для покращення безпеки та продуктивності.

Потрібна наступна кількість мереж:

- 3 мережі для офісних працівників;
- 1 для взаємодії із зовнішніми користувачами;
- 1 мережа LAN для настільних роутерів;

Схема адресації визначає призначення IP-адрес для кожного пристрою в мережі. Використовується приватна адресація IPv4, щоб забезпечити ефективне використання адресного простору і підвищити безпеку.

Перелік схеми адресації наступний:

- Адміністрація: 10.10.0.128/26
- Розробники: 10.10.0.192/26
- Тестувальники: 10.10.0.0/26
- Гості: 10.10.0.64/26
- Бездротові пристрої: 192.168.5.0/24

Маршрутизатор використовує NAT (Network Address Translation) для забезпечення підключення внутрішніх пристроїв до інтернету.

2.4 Вибір компонентної бази

Обладнання включає:

1. Центральний комутатор(Cisco Catalyst 9500) (Core Switch):

Рисунок. 2.4 – Вигляд комутатора

Мережеві комутатори Cisco Catalyst 9500 серії забезпечують захист до, під час та після атаки. Підтримка високошвидкісних портів, VLAN, QoS (Quality of Service), висока продуктивність і надійність.

Серія Catalyst 9500 забезпечує впровадження Інтернету речей з провідним в індустрії рівнем масштабованості, забезпечують до 384 портів з потужністю до 60Вт для UPOE, а також POE+ та PoE, високу безпеку, підтримку протоколу AVB та стандарту IEEE 1588, аналіз сервісів та класифікацію для додатків Інтернету речей.

Також забезпечують високу доступність на основі частнічних оновлень, технологію GIR для безпечної установки та видалення ПЗ та обладнання, використовують механізми NSF/SSO, а також використовують високоефективні резервовані модулі вентиляторів та блоків живлення.

Крім того, вони підтримують розширені можливості для маршрутизації та надання мережевих сервісів. [14]

Таблиця 2.1 – Технічні характеристики комутатора Cisco C9500-48Y4C-E:

Характеристика	Значення
1	2
Опис продукту	Cisco Catalyst 9500 - Network Advantage - switch - 32 ports - managed - rack-mountable
Тип девайсу	Switch - 32 ports - L3 - managed
Тип корпусу	Rack-mountable 1U
Підтип	40 Gigabit Ethernet
Порти	32 x 40 Gigabit QSFP
Продуктивність	Switching capacity (full duplex): 3.2 Tbps ¦ Forwarding rate: 1 Bpps

Кінець таблиці 2.1

1	2
Ємність	Routing table entries: 80000 ¦ Indirect IPv4 routes: 212000 ¦ Host IPv4 routes: 90000 ¦ Indirect IPv6 routes: 212000 ¦ Host IPv6 routes: 90000 ¦ Multicast scale: 32000 ¦ QoS ACL scale: 16000 ¦ Security ACL scale: 270000 ¦ FNF entries: 96000 ¦ VLAN IDs: 4000 ¦ Switched virtual interfaces (SVIs): 4000
Розмір таблиуці MAC-адрес	64K entries
Підтримка Jumbo Frame	9198 bytes
Протокол маршутизації	OSPF, IS-IS, RIP-2, BGP, EIGRP, IGMP, VRRP, PIM-SM, PIM-SSM, MSDP, RIPng, MPLS
Протокол віддаленого керування	SNMP 1, RMON 1, RMON 2, SNMP, SNMP 3, SNMP 2c, TFTP, NETCONF, RESTCONF
Особливості	DHCP support, NAT support, PAT support, trunking, MPLS support, Non-Stop Forwarding (NSF), Stateful switchover (SSO), Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Spanning Tree Protocol (STP) support, Virtual Route Redundancy Protocol (VRRP) support, Access Control List (ACL) support, Quality of Service (QoS), Non-Stop Routing (NSR), Remote Switch Port Analyzer (RSPAN), Hot Standby Router Protocol (HSRP) support, Virtual Routing and Forwarding (VRF), Maximum Likelihood Demodulation (MLD), Flexible NetFlow (FNF), Multicast Source Discovery Protocol (MSDP), MACsec support, Control plane protection (CoPP), integrated Wireshark, VLAN Double Tagging (Q-in-Q), Ethernet over MPLS (EoMPLS), Hierarchical Virtual Private LAN Service (H-VPLS), Private VLAN, Layer 3 VPN (L3VPN) support, CoAP support, Switched Port Analyzer (SPAN)
Відповідність стандартам	IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.3ae, IEEE 802.1s, IEEE 802.1ae, IEEE 802.3ba
Потужність	AC 120/230 V (50 - 60 Hz)
Резервування живлення	Optional
Розмір	17.5 in x 18 in x 1.7 in
Вага	21.85 lbs

2. Комутатори доступу (Access Switches):

Модель: Cisco Catalyst 2960-X

Рисунок 2.5 – Вигляд комутатора

Особливості: Підтримка Power over Ethernet (PoE) для живлення точок доступу, управління VLAN, простота налаштування і адміністрування.

Cisco Catalyst 2960-X – лінійка стекування комутаторів з підтримкою технології доступу Gigabit Ethernet. Моделі Cisco Catalyst 2960-X забезпечують комутацію другого рівня (L2 layer) і оснащені одним основним блоком живлення з можливістю встановлення додаткового, резервного джерела живлення. Дані комутатори забезпечені 24 або 48 портами Gigabit Ethernet, підтримують технології Power over Ethernet/Power over Ethernet Plus (PoE/PoE+) і чотири канали Gigabit Ethernet Small Form-Factor Pluggable (SFP) або два канали 10 Gigabit Ethernet Small Form-Factor Pluggable Plus (SFP+). Комутатори працюють на базі двох ядерних процесорів 600МГц. Технологія FlexStack-Plus дозволяє зібрати стек з 8 комутаторів і забезпечує пропускну здатність 80 Гбіт/сек . Для забезпечення візуалізації та контролю трафіку різних програм у мережі, Cisco додали функцію NetFlow Lite, яка дозволяє інженерам моніторити та керувати потоками даних на всіх сегментах мережі.

Ця платформа, прийшовши на зміну пристроям із серії Catalyst 2960-S , розроблена з метою скорочення операційних витрат та сукупної вартості володіння. Вона забезпечує захист інвестицій завдяки можливості змішаного стекування FlexStack+ з комутаторами Cisco Catalyst 2960-S та 2960-SF (у цьому випадку в стек можна об'єднати до 4 комутаторів).

Використовуючи такі технології, як Cisco EnergyWise та Energy Efficient Ethernet, комутатори Catalyst 2960 серії X забезпечують кращу у своєму класі

енергоефективність, а механізм Switch Hibernation Mode дозволяє в окремих випадках домогтися радикального скорочення енергоспоживання з економією електроенергії до 80%.

Програмне забезпечення (feature set) комутаторів Cisco Catalyst2960-X випускається в образах LAN Base**i**Lan Lite Image**.** LAN Base має ширший функціонал, включаючи покращену безпеку (ACLs), DHCP Snoopingі додаткові функції контролю доступу - Web authentication і розширення 802.1x, додаткові можливості установок якості обслуговування QoS, підтримка надлишкового живлення RPS та великої кількості SFP-портів. Функції Flex Links та Link State Tracking, збільшена кількість підтримуваних VLANs (до 256), IPv6 Host, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, та IP SLA (responder) та інше. Образ LAN Lite підтримує базові функції Layer 2 і призначений в основному для використання в невеликих організаціях, а LAN Base повністю підтримує функції Layer 2 та розрахований на застосування в середніх та великих організаціях. Комутатори Cisco Catalyst 2960-XR випускаються з набором IP Lite. Набір функцій IP Lite підтримує вже Layer 3 (тобто має функції маршрутизації) та орієнтований так само на середні та великі організації. [24]

2. Маршрутизатор моделі Cisco ISR 4431

Рисунок 2.6 – Загальний вигляд маршрутизатора

Особливості: Підтримка NAT, VPN (Virtual Private Network), високий рівень захисту та масштабованість.

Таблиця 2.2 – Технічні характеристики маршрутизатора Cisco ISR 4431

Характеристика	Значення
1	2
Назва продукту	Isr 4431 Security Bundle
Номер деталі виробника	ISR4431-SEC/K9
Серія продуктів	4000
Модель продукту	4431
Тип	Router
Інтерфейси/порти	
Загальна кількість портів	4
Лінія електропередач	No
Порт керування	Yes
Розширення	
Загальні кількість слотів розширення	8
Мережа та звязок	
Мережеві технології	10/100/1000Base-T
Технологія Ethernet	Gigabit Ethernet
VoIP Supported	Yes
Живлення	
PoE (RJ-45) Port	No
Джерело живлення	Power Supply PoE
Фізичні характеристики	
Compatible Rack Unit	1U
Form Factor	Rack-mountable Wall Mountable
Height	1.7"
Width	17.3"
Depth	20"
Warranty	
Limited Warranty	90 Day
Other Information	
Product Family	4000
Token Ring Port	No
USB	Yes
Number of Network (RJ-45) Ports	4
Тип слота розширення	SFP Network Interface Module (NIM) Integrated Services Card (ISC)

Кінець таблиці 2.2

1	2
Технологія пам’яті	DRAM
Сертифікати та стандарти	Safety: • UL 60950-1 • CAN/CSA C22.2 No. 60950-1 • EN 60950-1 • AS/NZS 60950-1 • IEC 60950-1 • GB-4943 EMC: • 47 CFR, Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI V-3 • CNS 13438 • EN 300-386 • EN 61000 (Immunity) • EN 55024, CISPR 24 • EN50082-1 • KN22, KN24 Telecom: • TIA-968-B • CS-03 • ANSI T1.101 • ITU-T G.823, G.824 • IEEE 802.3 • RTTE Directive
Flash Memory	8 GB
Вхідна напруга	120 V AC 230 V AC
Максимальна пам’ять	16 GB
Стандартна пам’ять	4 GB

4. Точка доступу (Access Points) Модель: Cisco Aironet 2800 Series

Рисунок 2.7 – Загальний вигляд

Особливості: Підтримка останніх стандартів Wi-Fi (802.11ac), висока продуктивність, можливість управління через контролер.

5. Брандмауер (Firewall) моделі Cisco Firepower 2110

Рисунок 2.8 – Загальний вигляд

Особливості: Захист від атак, фільтрація трафіку, підтримка VPN.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ІЗ ЗАХИСТОМ ДОСТУПУ ДО РЕСУРСІВ

3.1 Конфігурація пристроїв

Перед виконанням завдання необхідно за тест-кейсом пройти всі етапи, перелічені нижче:

1. Збір даних про мережу

- Використати інструменти для аналізу мережі, такі як Nmap, Wireshark, та інші.

- Створити докладну схему мережі з визначенням критичних вузлів та ресурсів.

2. Аналіз політик доступу

- Перевірити налаштування політик доступу у системах управління доступом.

- Провести інтерв'ю з адміністраторами для розуміння існуючих політик та процедур.

3. Перевірка мережевих пристроїв

- Виконати аудит конфігурацій мережевих пристроїв на предмет відповідності стандартам безпеки.

- Перевірити налаштування VPN та інших методів віддаленого доступу.

4. Тестування на вразливості

- Використати сканери вразливостей, такі як Nessus, OpenVAS, для виявлення слабких місць.

- Провести penetration testing з метою імітації дій зловмисників.

5. Оцінка кінцевих точок

- Провести аудит безпеки робочих станцій, серверів та мобільних пристроїв.

- Перевірити ефективність антивірусного та антивірусного ПЗ.

6. Складання звіту та розробка рекомендацій

- Оформити звіт з результатами дослідження, включаючи виявлені вразливості та рекомендації.

- Розробити план дій для покращення системи безпеки та захисту доступу до ресурсів.

Після успішного затвердження тест-кейсу переходимо до реалізації розробки корпоративної мережі із захистом доступу.

З метою забезпечення усіх вузлів мережі офісу безперебійним доступом до мережі Інтернет до маршрутизатора PTMV1-GW здійснено підключення одночасно двох Інтернет провайдерів (основного і резервного).

Налаштування інтерфейсу центрального комутатора (Core Switch) - Cisco Catalyst 9500:

Подамо стартову конфігурацію:

enable

configure terminal

hostname AccessSwitch

interface range FastEtherneto/1-24

switchport mode access

switchport access vlan 10 (or 20, 30, 40, 50 depending on the department)

exit

interface GigabitEthernet1/0/1

switchport mode trunk

exit

2. Конфігуарація інтерфейсів VLAN:

enable

configure terminal

hostname Router

interface GigabitEtherneto/0

description Link to Core Switch

ip address 192.168.1.254 255.255.255.0

exit

interface GigabitEtherneto/1

description Link to Internet

ip address ‹ public _ip_address> « subnet_mask>

ip nat inside

exit

ip nat inside source list 1 interface GigabitEthernet0/1 overload

access-list 1 permit 192.168.0.0 0.0.255.255

exit

Комутатори доступу (Access Switches) - Cisco Catalyst 2960-X

1. Базова конфігурація:

enable

configure terminal

crypto isakmp policy 1

encr aes

authentication pre-share

group 2

exit

crypto isakmp key «shared_key› address ‹remote_peer_¡p>

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

exit

crypto map VPN-MAP 10 ipsec-isakmp

set peer ‹ remote peer_ip>

set transform-set VPN-SET

match address 101

exit

interface GigabitEtherneto/1

crypto map VPN-MAP

exit

access-list 101 permit ip 192.168.0.0 0.0.255.255 < remote network› ‹ subnet _mask»

Маршрутизатор - Cisco ISR 4431

В даній мережі маршрутизатори також будуть виконувати роль TFTP-серверів.

TFTP (англ. Trivial File Transfer Protocol — тривіальний протокол передачі файлів) — простий, покроково синхронізований протокол передачі файлів, який дозволяє клієнтам зчитувати або записувати файли сервера. Одним із основних використань протоколу є первинне завантаження бездискових робочих станцій у локальній мережі. Найчастіше TFTP використовується саме через простоту його реалізації. Протокол працює поверх протоколу UDP.

Тобто, з TFTP-сервера IP-телефони в даній мережі будуть отримувати свою прошивку (програмне забезпечення) при завантаженні.

1. Базова конфігурація:

```
webvpn gateway SSLVPN-GW
ip address 192.168.1.254 port 443
ssl trustpoint TP-self-signed -1234567890
inservice
exit
webvpn context SSLVPN
gateway SSLVPN-GW
ssl authenticate verify all
inservice
policy group PolicyGroup1
functions svc-enabled
svc address-pool "VPN-POOL"
sc split include 192.168.0.0 255.255.0.0
default-group-policy PolicyGroup1
exit
ip local pool VPN-POOL 192.168.10.1 192.168.10.254
```

Точки доступу (Access Points) - Cisco Aironet 2800 Series

1. Базова конфігурація (через контролер):

configure terminal

wlan WirelessNetwork 1 WirelessSSID

interface Vlan50

security wpa

authentication open

exit

interface range GigabitEthernet0/1-4

switchport mode access switchport access

vlan 50

exit

3.2 Налаштування захисту (VPN)

Маршрутизатор - Cisco ISR 4431

1. Конфігурація IPSec VPN:

configure terminal

crypto isakmp policy 1

encr aes

authentication pre-share

group 2

exit

crypto isakmp key < shared _key› address ‹ remote_peer_ip>

crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac

exit

crypto map VPN-MAP 10 ipsec-isakmp

set peer ‹ remote_peer_ip>

set transform-set VPN-SET

match address 101

exit

interface GigabitEtherneto/1

crypto map VPN-MAP

exit

access-list 101 permit ip 192.168.0.0 0.0.255.255 ‹ remote_network› ‹subnet mask›

2. Конфігурація SSL VPN (Cisco AnyConnect):

webvpn gateway SSLVPN-GW

ip address 192.168.1.254 port 443

ssi trustpoint TP-self-signed-1234567890

inservice

exit

webpn context SSLVPN

gateway SSLVPN-GW

ssl authenticate verify all

inservice

policy group PolicyGroup1

functions svc-enabled

svc address-pool "VPN-POOL"

svc split include 192.168.0.0 255.255.0.0

default-group-policy PolicyGroup1

exit

ip local pool VPN-POOL 192.168.10.1 192.168.10.254

3.3 Результати тестування

При тестуванні віддаленого доступу до сервісів і серверів перевіряються підключення, швидкість передачі даних, стабільність з'єднання і очікувані результати. Виконайте серію тестових перевірок, щоб побачити, як система працює в різних умовах і при різних навантаженнях.

Тестування віддаленого доступу до служб і серверів є важливою частиною впровадження системи безпеки для мереж невеликих офісів з обмеженим доступом. Це гарантує, що система готова до роботи і користувачі зможуть отримувати доступ до ресурсів з будь-якої точки світу.

Для проведення тестування мережі для кожного з'єднання відбувається відкриття VPN-тунелю між комп'ютером віддаленого користувача і мережею, щоб забезпечити безпечне з’єднання.

Після успішного підключення перевіряємо роботу тунелю з використанням команди ipconfig /all. Результат перевірки наведені на рисунку 3.1. Як видно з рисунку абонент отримав IP-адресу, маску підмережі та інші параметри відповідно до налаштувань тунельного зєднання:

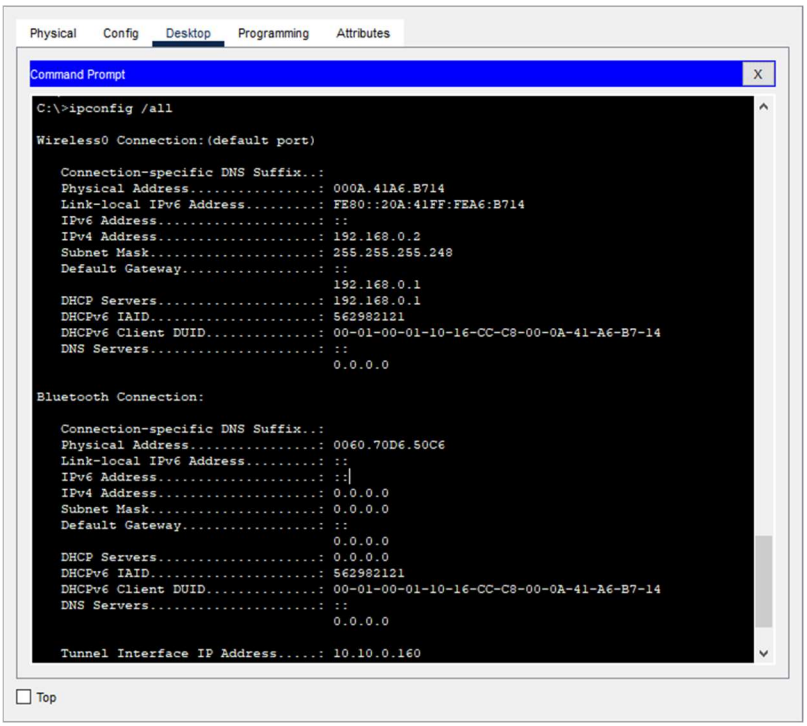


Рисунок 3.1 – Результат перевірки мережних налаштувань

На цьому кроці ви переконалися, що тунель VPN успішно налаштований і що у вас вказана правильна IP-адреса та налаштування мережі. Це гарантує, що між комп'ютером віддаленого користувача і офісною мережею є з'єднання, що забезпечує безпечну передачу даних по тунелю.

Після успішного налаштування тунелю ви можете скористатися командою PING з командного рядка на комп'ютері віддаленого користувача, щоб визначити підключення та доступність ресурсів, як показано на рисунку 3.2.

Ви можете використовувати команду PING для надсилання сигналу (ICMP-запиту) на вказану IP-адресу та отримання відповіді (ICMP response). Під час виконання команди PING було перевірено з'єднання між віддаленим комп'ютером і мережевими ресурсами компанії. Отримана відповідь на запит PING вказує на наявність з'єднання і доступність ресурсів, а отже, і на точність настройки.

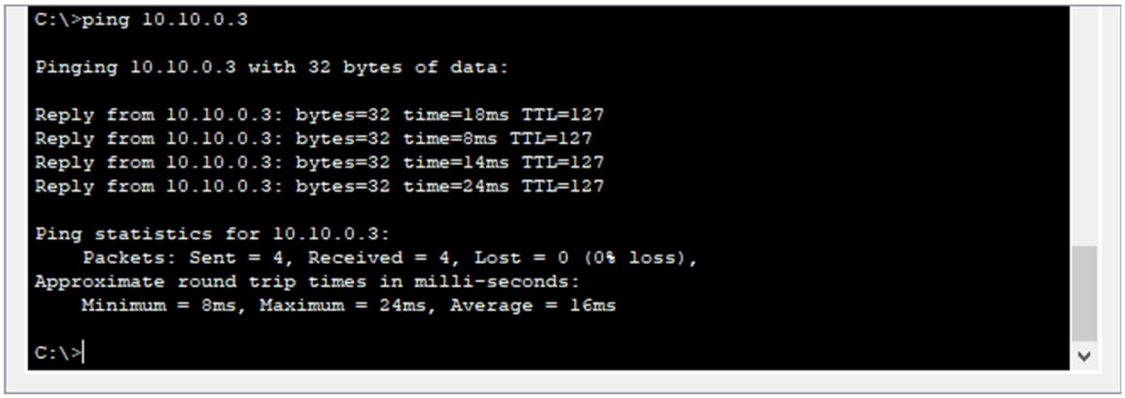


Рисунок 3.2 – Перевірка мережного з'єднання

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

Наступним етапом була перевірка доступності ресурсів компанії, а саме HTTP сервера. Для цього скористаємося встановленим веб-браузером на комп'ютері віддаленого користувача.

Результат цієї перевірки відображено на рисунку 3.3, де видно, що веб-сторінка mycompany.com була успішно завантажена у веб-браузері. Це підтверджує доступність HTTP сервера та правильну роботу системи з віддаленим доступом до ресурсів [41].

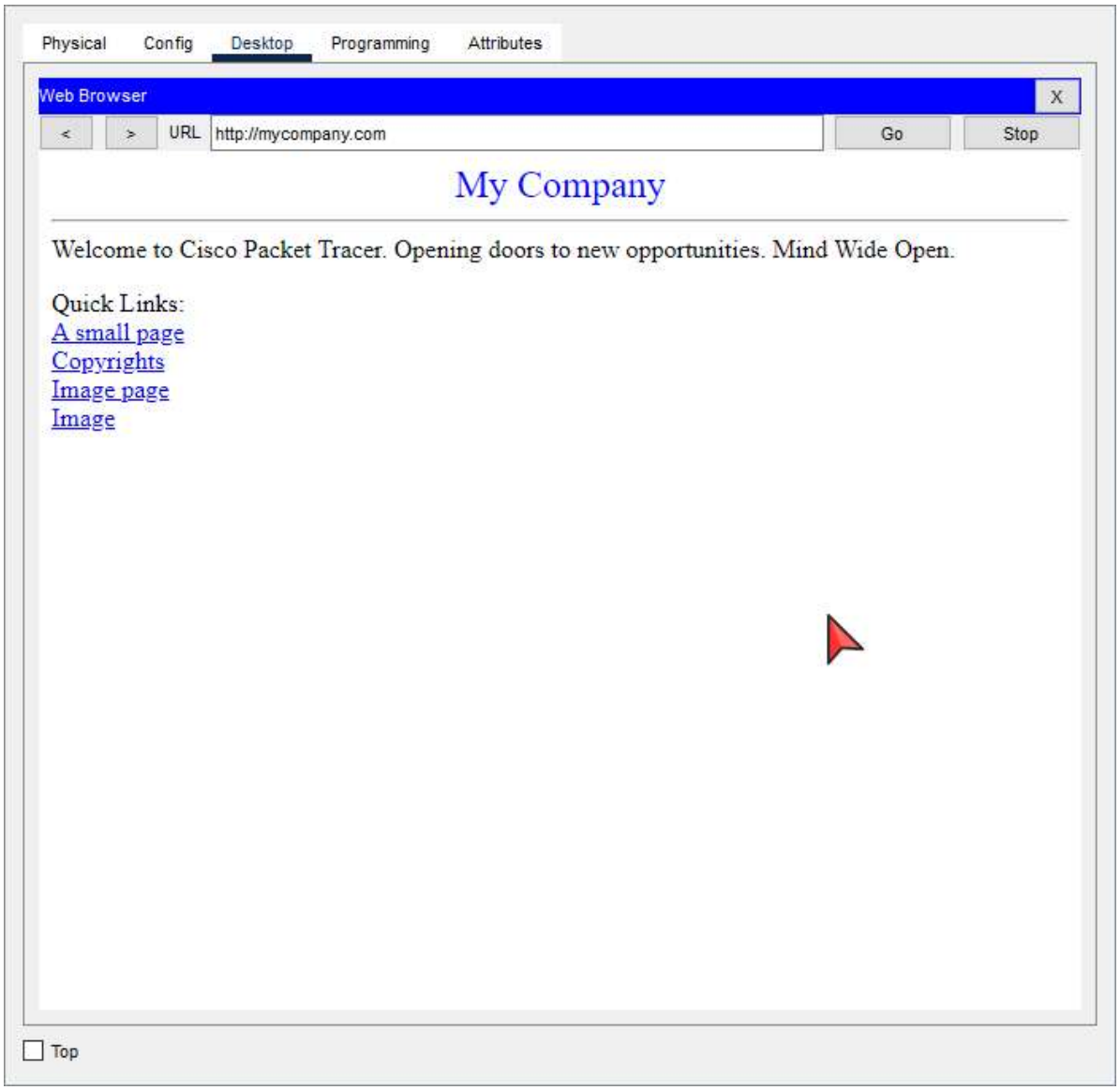


Рисунок 3.3 – Результати доступу до ресурсів корпоративної мережі

На цьому етапі можна буде переконатися в тому, що з'єднання з HTTP-сервером успішно встановлено, і безкоштовно отримувати веб-сторінки і ресурси, доступні в офісній мережі, що підтвердить належне функціонування мережі малого офісу з контролем доступу і ефективним наданням віддаленого доступу до ресурсів.

Крім того, протестуйте FTP-сервер. Використовуючи командний рядок комп'ютера віддаленого користувача, виконайте команду "ftp10.10. 0. 2" для підключення до FTP-сервера. Коли з'єднання буде успішно встановлено, введіть команду "Видалити<ім'я_файлу>", щоб спробувати видалити файл на сервері.

Після виконання команди "ftp10.10. 0. 2" в командному рядку з'явилося підтвердження підключення до FTP-сервера. Потім я спробував за допомогою команди "delete<ім'я_файлу>" видалити вказаний файл на сервері, як показано на рисунку 3.4.

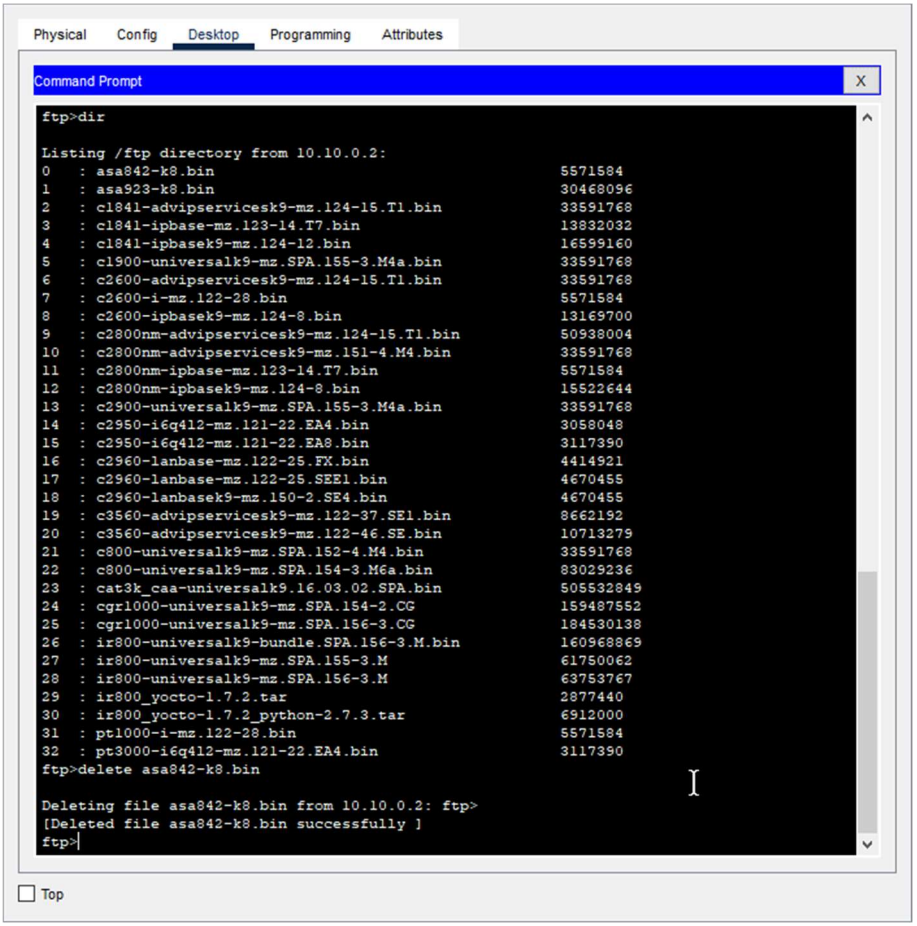


Рисунок 3.4 – Результати доступу до FTP-серверу

Додатково проводилось тестування з'єднання із ресурсами корпоративної мережі без встановлення VPN-зєднання (рис. 3.5). Як видно з результатів, спроба доступу виявляється невдалою, оскільки віддалений користувач надсилає запити із IP-адреси, що не є внутрішньо корпоративною.

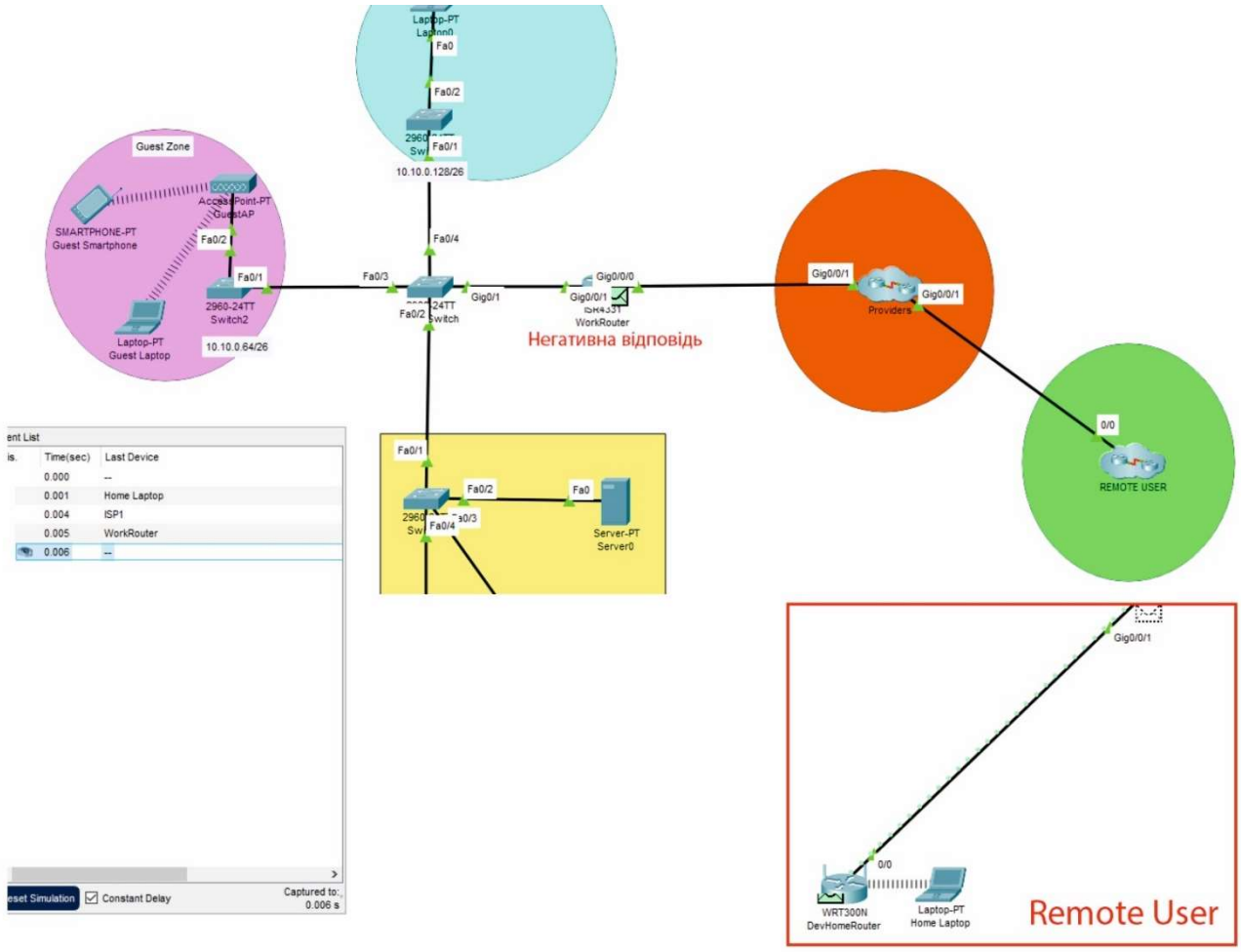


Рисунок 3.5 – Результати доступу без встановлення VPN-з'єднання

Отримані результати свідчать про правильність налаштувань мережі та дозволяють говорити про надійний захист ресурсів.

ВИСНОВКИ

Будь-яка організація – це сукупність взаємодіючих елементів (підрозділів), кожен з яких може мати свою структуру. Елементи пов'язані між собою функціонально, тобто вони виконують окремі види робіт у рамках єдиного процесу, а також інформаційно, обмінюючись документами, факсами, письмовими та усними розпорядженнями і т.д. Крім того, ці елементи взаємодіють із зовнішніми системами, причому їх взаємодія також може бути як інформаційним, так і функціональним. І ця ситуація справедлива практично для всіх організацій, яким би видом діяльності вони не займалися – для урядової установи, банку, промислового підприємства, комерційної фірми і т.д.

Корпоративна мережа — це мережа, головним призначенням якої є підтримка роботи конкретного підприємства, що володіє даною мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не надають послуг стороннім організаціям або користувачам.

Корпоративною мережею вважається будь-яка мережа, що працює по протоколу TCP/IP[1] і використовує комунікаційні стандарти Інтернету, а також сервісні застосування, що забезпечують доставку даних користувачам мережі.

Корпоративна мережа, як правило, є територіально розподіленою, тобто об'єднує офіси, підрозділи і інші структури, що знаходяться на значному віддаленні один від одного.

Корпоративні мережі дозволяють забезпечити колективну обробку даних користувачами підключених в мережу комп'ютерів і обмін даними між цими користувачами, сумісне використання програм, сумісне використання принтерів, модемів і інших пристроїв.

Використання обчислювальних мереж дає підприємству наступні можливості:

- розподіл ресурсів;
- вдосконалення комунікацій;

- поліпшення доступу до інформації;

- швидке і якісне ухвалення рішень;

- свобода в територіальному розміщенні комп'ютерів.

Концептуальною перевагою корпоративних мереж є здатність виконувати паралельні обчислення. За рахунок цього в системі з декількома оброблювальними вузлами в принципі може бути досягнута продуктивність, що перевищує продуктивність окремого процесора.

Ще одна очевидна і важлива перевага розподілених систем – це їх принципово вища відмовостійкість. Під відмовостійкістю розуміється здатність системи виконувати свої функції (можливо, не в повному об'ємі) при відмовах окремих елементів апаратури і неповної доступності даних. Основою підвищеної відмовостійкості розподілених систем є надмірність. Надмірність оброблювальних вузлів (процесорів в багатопроцесорних системах або комп'ютерів в мережах) дозволяє при відмові одного вузла передавати виконання завдань на інші вузли.

Також чинником використання мережі є прагнення забезпечити співробітникам оперативний доступ до обширної корпоративної інформації.

Наявність мережі приводить до вдосконалення комунікацій між співробітниками підприємства, а також його клієнтами і постачальниками. Мережі знижують потребу підприємств в інших формах передачі інформації, таких як телефон або звичайна пошта. Корпоративна мережа може використовуватися для організації аудіо- і відеоконференцій. Також на її основі може бути створена власна внутрішня телефонна мережа.

Структура комп’ютерної мережі залежить від її призначення, кількості користувачів, специфіки обладнання та технологій, які вона повинна підтримувати.

Розробка корпоративної мережі із захистом доступу до ресурсів є важливим етапом у забезпеченні інформаційної безпеки підприємства. Впровадження сучасних технологій захисту, таких як багатофакторна аутентифікація, VPN, контроль доступу на основі ролей, а також системи виявлення та запобігання

вторгненням, дозволяє значно підвищити рівень безпеки мережі. Моніторинг мережевого трафіку та управління інформаційною безпекою забезпечують своєчасне виявлення та реагування на загрози, що є критично важливим для захисту корпоративних ресурсів.

У цьому розділі було проведено ґрунтовний аналіз корпоративних мереж із захистом доступу до ресурсів, їхніх структурних та функціональних особливостей. Основною метою такого аналізу було виявлення ключових елементів мережі, які забезпечують її захищеність, ефективність та надійність. Було визначено, що важливими складовими корпоративної мережі є надійне програмно-апаратне забезпечення, ефективні засоби захисту даних та механізми управління доступом.

Було проведено детальний аналіз наявного програмно-апаратного забезпечення корпоративної мережі, яке використовується для захисту доступу до ресурсів. Розглянуто різні типи обладнання, такі як комутатори, маршрутизатори та точки доступу, а також програмні засоби для управління доступом та захисту даних. Це дозволило визначити переваги та недоліки існуючих рішень та сформувати вимоги до майбутньої системи.

На основі проведеного аналізу було визначено вимоги до системи автоматизації корпоративної мережі із захистом доступу до ресурсів. Розроблено технічне завдання, яке включає основні параметри та функціональні вимоги до системи, необхідні для забезпечення високого рівня безпеки та ефективності мережі.

Було розроблено фізичну топологію корпоративної мережі, яка враховує розташування всіх мережевих компонентів, таких як комутатори, маршрутизатори та точки доступу. Вибір оптимальної фізичної топології дозволяє забезпечити високу продуктивність та надійність мережі.

Описано логічну топологію мережі, яка визначає логічні зв'язки між різними компонентами мережі. Логічна топологія дозволяє ефективно організувати потоки даних та забезпечити надійний захист інформації.

Розроблено схему адресації для мережі, яка забезпечує унікальність IP-адрес для всіх пристроїв та дозволяє легко керувати мережею. Схема адресації є важливим елементом, який сприяє безперебійній роботі мережі.

Проведено вибір компонентної бази для мережі, враховуючи вимоги до продуктивності, надійності та захищеності. Було обрано сучасне обладнання, яке відповідає всім вимогам та забезпечує високу ефективність мережі.

Описано конфігурацію пристроїв, яка включає налаштування комутаторів, маршрутизаторів та точок доступу. Конфігурація пристроїв здійснюється з урахуванням вимог до безпеки та ефективності мережі.

Проведено налаштування захисту мережі з використанням технології VPN. Налаштування VPN дозволяє забезпечити безпечний доступ до корпоративних ресурсів для віддалених користувачів та підвищити загальний рівень безпеки мережі.

Проведено тестування корпоративної мережі з метою перевірки її працездатності та відповідності всім вимогам. Результати тестування показали високу ефективність мережі, надійність захисту даних та відповідність всім заданим параметрам.

Запропонована корпоративна мережа із захистом доступу до ресурсів забезпечує високу продуктивність, гнучкість та безпеку. Використання VLAN дозволяє розділити мережу на сегменти, що підвищує рівень захисту та зменшує ризики несанкціонованого доступу. Вибір високоякісного мережевого обладнання від компанії Cisco гарантує надійність і ефективність функціонування мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Наталенко П. П., Шолудько В. Г., доц., к.т.н.; Захист інформації в корпоративних мережах./ Національний технічний університет України «Київський політехнічний інститут», - К, 2022. - 222-223 с.

2. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка - К.: Юніор, 2003. – 400 с.

3. Коробейнікова Т. І., Захарченко С. М. Комп'ютерна мережа. Львів : Вид-во Львів. політехніки, 2022. 228 с.

4. Воробієнко П.П. Телекомунікаційні та інформаційні мережі [Навчальний посібник] / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченко – К.: Самміт-книга, 2010. – 708 с.

5. Городецька О.С. Комп'ютерні мережі: навчальний посібник / О.С. Городецька, В.А. Гикавий, О.В. Онищук. – Вінниця : ВНПУ, 2017. – 129 с.

6. Струтинська О.В. Інформаційні системи та мережі [Навчальний посібник для дистанційного навчання] /За наук.ред.М.І.Жалдака – К.: Університет «Україна», 2008. – 211 с.

7. Тарнавський Ю.А. Організація комп'ютерних мереж [Електронний ресурс]/ Ю.А. Тарнавський, І.М. Кузьменко – К.: КПІ ім. Ігоря Сікорського, 2018. – 259 с.

8. Міхунін С.В. Комп'ютерні мережі. Загальні принципи функціонування комп'ютерних мереж [Навчальний посібник] / С.В. Міхунін, С.В. Кавун, С.В. Знахур – Харків: Вид. ХНЕУ, 2008. – 210 с.

9. В. М. Базилевич, Д. Б. Мехед, Ю. М. Ткач. Комп'ютерні мережі. Протоколи, технології, обладнання : навч. посіб. для студ. спец. 125 «Кібербезпека»– Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. – 108 с.

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

11. Ромашко С.М. Конспект лекцій з дисципліни "Комп'ютерні мережі і телекомунікації" - Львів: ЛРІДУ НАДУ, 2006. - 61с.

12. Волосюк Ю. В. В68 Комп'ютерні мережі : курс лекцій / Ю. В. Волосюк. –

Миколаїв : МНАУ, 2019. – 203 с.

13. Організація комп’ютерних мереж : підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення» та 122 «Комп’ютерні науки» / КПІ ім. Ігоря Сікорського ; Ю. А. Тарнавський, І. М. Кузьменко. – Київ : КПІ ім. Ігоря Сікорського, 2018. – 259 с.

14. Азаров О. Д., Захарченко С. М., Кадук О. В. та ін. Комп’ютерні мережі : навчальний посібник. — Вінниця : ВНТУ, 2013. — 371 с.

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

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

17. Сандул Г. Д. Можливості технології Cisco IOS IP SLA. URL: http:// www.securitylab.ru/analytics/309557.php (дата звернення: 15.04.2024)

18. The Secure Real-time Transport Protocol (SRTP). URL: https://tools.ietf.org/html/rfc3711 (дата звернення: 05.05.2024)

19. Cisco Webex Plans and Pricing. URL: https://www.webex.com/pricing/index.html (дата звернення: 03.04.2024)

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

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

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

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

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

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

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

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

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

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

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

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

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

33. Основні вимоги до проектування кампусних мереж. URL: https://studfile.net/preview/5199546/page:2/ (дата звернення: 17.03.2024).

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

35. Комп'ютерні мережі. URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 (дата звернення: 20.04.2024).

36. Топологія комп'ютерних мереж. URL: https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh (дата звернення: 30.03.2024).

37. Топології комп'ютерних мереж. URL: http://blogkkzshnika.blogspot.com/2017/10/blog-post_10.html (дата звернення: 04.04.2024).

38. Топологія локальних мереж. URL: https://ua5.org/lan/125-topologja-lokalnikh-merezh.html (дата звернення: 07.04.2024).

39. Організація комп'ютерних мереж. URL: http://nickshevtsov.blogspot.com/2017/10/blog-post.html (дата звернення: 20.03.2024).

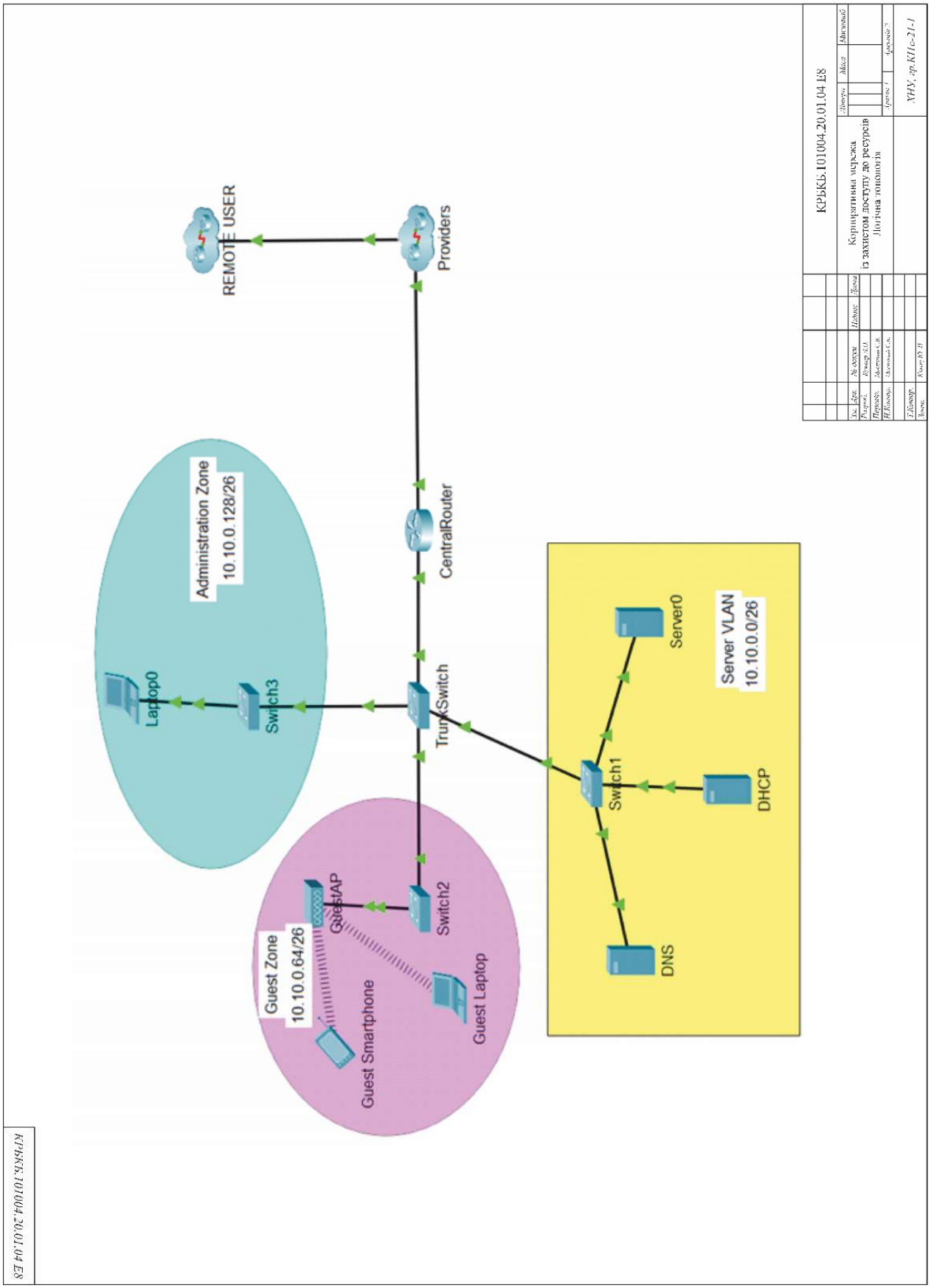
40. Топологія мережі: 6 пояснених та порівняних мережевих топологій. URL: https://instagalleryapp.com/chistij-administrator-2/topologija-merezhi-6-pojasnenih-ta-porivnjanih/ (дата звернення: 15.04.2024).

41. Топологія комп'ютерних мереж. Класифікація комп'ютерних мереж з топології. URL: https://creativnost.com.ua/topologiya-kompyuternix-merezh-klasifikaciya-kompyuternix-merezh-z-topologii/ (дата звернення: 10.04.2024).

Додаток А

(обовязковий)

Копія графічної частини



КРБКБ.101004.20.01.04 Е8

						КРБКБ.101004.20.01.04 Е8					
						Корпоративна мережа із захистом доступу до ресурсів Фізична топологія		Літера	Маса	Масштаб	
Зм.	Арк.	№ докум.	Підпис	Дата				Аркушів 1		Аркуш 1	
Розроб.		Кочур О.О.									
Перевір.		Дьяченко С.В.									
Н.контр.		Дьяченко С.В.									
Затверд.											
Інв.№		Кочур О.О.									

УНУ, гр. КІІс-21-1

Додаток Б

(обовязковий)

Конфігураційні файли мережного обладнення

Маршрутизатор Сутекфд:

```
Current configuration : 4280 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Office
!
enable password cisco
!
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.254
ip dhcp excluded-address 192.168.1.11
ip dhcp excluded-address 192.168.2.1
ip dhcp excluded-address 192.168.2.254
ip dhcp excluded-address 192.168.2.11
ip dhcp excluded-address 192.168.3.1
ip dhcp excluded-address 192.168.3.254
ip dhcp excluded-address 192.168.3.11
ip dhcp excluded-address 192.168.1.10
ip dhcp excluded-address 192.168.2.10
ip dhcp excluded-address 192.168.3.10
!
ip dhcp pool Managing0-pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.11
ip dhcp pool Accounting0-pool
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
dns-server 192.168.2.11
ip dhcp pool Client0-pool
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
dns-server 192.168.3.11
!
!
!
no ip cef
no ipv6 cef
!
username admin privilege 15 password 0 cisco
!
```

```
!
license udi pid CISCO2911/K9 sn FTX1524V8IB-
!
ip domain-name oficesecurity.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip access-group From-SCisco in
ip access-group OAL010 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.2.1 255.255.255.0
ip access-group From-SCisco in
ip access-group AAL020 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.3.1 255.255.255.0
ip access-group From-SCisco in
ip access-group CAL030 out
duplex auto
speed auto
!
interface Serial0/1/0
ip address 20.0.0.1 255.255.255.252
ip access-group From-outside in
clock rate 64000
!
interface Serial0/1/1
no ip address
clock rate 2000000
!
interface Serial0/2/0
ip address 10.10.10.6 255.255.255.252
ip access-group From-SCisco in
clock rate 64000
!
interface Serial0/2/1
ip address 10.10.10.2 255.255.255.252
ip access-group From-SCisco in
clock rate 64000
!
interface Vlan1
ip address 192.168.100.2 255.255.255.0
shutdown
!
```

```
router ospf 10
log-adjacency-changes
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
! router rip
version 2
network 10.0.0.0
network 20.0.0.0
network 192.168.1.0
network 192.168.2.0
network 192.168.3.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard OAL010
deny 192.168.2.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
ip access-list standard AAL020
deny 192.168.1.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list extended From-SCisco
permit tcp 192.168.1.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.2.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.3.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.4.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.5.0 0.0.0.255 host 192.168.50.2 eq www
permit tcp 192.168.6.0 0.0.0.255 host 192.168.50.2 eq www
deny ip 192.168.1.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.2.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.3.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.4.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.5.0 0.0.0.255 host 192.168.50.2
deny ip 192.168.6.0 0.0.0.255 host 192.168.50.2
permit ip any any
ip access-list extended From-outside
deny ip any 192.168.1.0 0.0.0.255
```

```
deny ip any 192.168.2.0 0.0.0.255
deny ip any 192.168.3.0 0.0.0.255
deny ip any 192.168.4.0 0.0.0.255
deny ip any 192.168.5.0 0.0.0.255
deny ip any 192.168.6.0 0.0.0.255
deny tcp any host 20.0.0.2 eq telnet
permit ip any host 20.0.0.2
ip access-list standard CAL030
deny 192.168.1.0 0.0.0.255
deny 192.168.2.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
!
no cdp run
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
!
!
end
```

Маршрутизатор Work:

```
Building configuration...

Current configuration : 2769 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Shop
!
!
!
enable password cisco2
!
!
ip dhcp excluded-address 192.168.4.1
ip dhcp excluded-address 192.168.4.254
ip dhcp excluded-address 192.168.5.1
ip dhcp excluded-address 192.168.5.254
ip dhcp excluded-address 192.168.6.1
```

```
ip dhcp excluded-address 192.168.6.254
ip dhcp excluded-address 192.168.6.10
ip dhcp excluded-address 192.168.5.10
ip dhcp excluded-address 192.168.4.10
!
ip dhcp pool Managing1-pool
network 192.168.4.0 255.255.255.0
default-router 192.168.4.1
dns-server 192.168.1.11
ip dhcp pool Accounting1-pool
network 192.168.5.0 255.255.255.0
default-router 192.168.5.1
dns-server 192.168.2.11
ip dhcp pool Client1-pool
network 192.168.6.0 255.255.255.0
default-router 192.168.6.1
dns-server 192.168.3.11
!
!
!
ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$yG9qv7LLYVv0YzwRYtdTM/
!
!
license udi pid CISCO2911/K9 sn FTX1524D21C-
!
ip domain-name shopsecurity.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.5.1 255.255.255.0
ip access-group AAC120 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.4.1 255.255.255.0
ip access-group MAL110 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.6.1 255.255.255.0
ip access-group CAC130 out
duplex auto
speed auto
```

```
!
interface Serial0/2/0
ip address 10.10.10.5 255.255.255.252
!
interface Serial0/2/1
ip address 10.10.10.9 255.255.255.252
!
interface Vlan1
ip address 192.168.100.3 255.255.255.0
shutdown
!
router ospf 10
log-adjacency-changes
network 10.10.10.4 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
!
router rip
version 2
network 10.0.0.0
network 192.168.4.0
network 192.168.5.0
network 192.168.6.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard MAL110
deny 192.168.2.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard AAC120
deny 192.168.1.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard CAC130
deny 192.168.1.0 0.0.0.255
deny 192.168.2.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
```

```
deny 192.168.7.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
end
```

Комутатори:

```
Current configuration : 2810 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Storage
!
!
!
enable password cisco1
!
!
ip dhcp excluded-address 192.168.9.1
ip dhcp excluded-address 192.168.9.254
ip dhcp excluded-address 192.168.8.254
ip dhcp excluded-address 192.168.8.1
ip dhcp excluded-address 192.168.7.1
ip dhcp excluded-address 192.168.7.254
ip dhcp excluded-address 192.168.7.10
ip dhcp excluded-address 192.168.8.10
ip dhcp excluded-address 192.168.9.10
!
ip dhcp pool Managing2-pool
network 192.168.7.0 255.255.255.0
default-router 192.168.7.1
dns-server 192.168.1.11
ip dhcp pool Accounting2-pool
network 192.168.8.0 255.255.255.0
default-router 192.168.8.1
dns-server 192.168.2.11
ip dhcp pool Client2-pool
network 192.168.9.0 255.255.255.0
default-router 192.168.9.1
dns-server 192.168.3.11
!
```

```
!
!
no ip cef
no ipv6 cef
!
!
!
username admin privilege 15 secret 5 $1$mERr$q.MA2tj.WFptzvbifq/1i.
!
!
license udi pid CISCO2911/K9 sn FTX1524Q23E-
!
ip domain-name storagesecurity.com
!
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
ip address 192.168.9.1 255.255.255.0
ip access-group CAL230 out
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.7.1 255.255.255.0
ip access-group MAC210 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 192.168.8.1 255.255.255.0
ip access-group MAC210 out
duplex auto
speed auto
!
interface Serial0/1/0
ip address 10.10.10.1 255.255.255.252
!
interface Serial0/1/1
ip address 10.10.10.10 255.255.255.252
clock rate 64000
!
interface Vlan1
ip address 192.168.100.1 255.255.255.0
shutdown
!
router ospf 10
log-adjacency-changes
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.8 0.0.0.3 area 0
network 192.168.9.0 0.0.0.255 area 0
network 192.168.8.0 0.0.0.255 area 0
```

```
network 192.168.7.0 0.0.0.255 area 0
!
router rip
version 2
network 10.0.0.0
network 192.168.6.0
network 192.168.7.0
network 192.168.9.0
!
ip classless
!
ip flow-export version 9
!
!
ip access-list standard MAC210
deny 192.168.2.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard AAC220
deny 192.168.1.0 0.0.0.255
deny 192.168.3.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.6.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.9.0 0.0.0.255
permit any
ip access-list standard CAL230
deny 192.168.1.0 0.0.0.255
deny 192.168.2.0 0.0.0.255
deny 192.168.4.0 0.0.0.255
deny 192.168.5.0 0.0.0.255
deny 192.168.7.0 0.0.0.255
deny 192.168.8.0 0.0.0.255
permit any
!
no cdp run
!
line con 0
!
line aux 0
!
line vty 0 4
login local
transport input ssh
!
end
```

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П
Кушніра Дмитра Олександровича
Студента ФІТ, 3 курсу, групи КІ1с-21-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а) та надаю свою згоду на обробку й збереження університетом моєї роботи в інституційному репозитарії Хмельницького національного університету.

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

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

19.06.2024р.
дата

підпис

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1016388854

Дата перевірки:
26.06.2024 11:00:32 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
26.06.2024 11:10:22 EEST

ID користувача:
100008300

Назва документа: **Кушнір_на_плагіат**

Кількість сторінок: **54** Кількість слів: **8641** Кількість символів: **70896** Розмір файлу: **1.59 MB** ID файлу: **1016201105**

24.8%
Схожість

Найбільша схожість: **2.73%** з Інтернет-джерелом (https://128gb.ru/uk/chto-takoe-korporativnaya-set-opredelenie-organ..

23.5% Джерела з Інтернету	299	Сторінка 56
3.17% Джерела з Бібліотеки	73	Сторінка 58

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

9.55%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за **8 слів** та **0%**)

9.55% Вилучення з Інтернету	175	Сторінка 59
0.09% Вилученого тексту з Бібліотеки	5	Сторінка 59

Модифікації

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

Замінені символи	19

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

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

ID: 132631 Назва: Корпоративна мережа із захистом доступу до ресурсів Додано в БД: 2024-06-26 Автора: Кушнір Д.О. Керівники: Мостовий С.В. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	59224	539	5014 (8%)	41 (8%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Корпоративна мережа із захистом доступу до ресурсів

Автор: Кушнір Дмитро Олександрович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Мостовий Сергій Володимирович

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. 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 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.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 75,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 99%.

Згідно з Положенням про систему забезпечення академічної доброчесності у ХНУ (https://khmnu.edu.ua/wp-content/uploads/normatyvni-dokumenty/polozhennya/pro-systemu-zabezpechennya-akademichnoyi-dobrochesnosti.pdf, Додаток В) кваліфікаційна робота, виконана за , освітньо-професійною програмою, кількісні показники рівня унікальності тексту у відсотках до загального обсягу матеріалу в якій складає 75-100 %, визнається роботою з високою унікальністю тексту: «Текст вважається унікальним і не потребує додаткових дій щодо запобігання неправомірним запозиченням».

Керівник роботи _____ Сергій МОСТОВИЙ

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Дипломник Кушнір Дмитро Олександрович

Тема Корпоративна мережа із захистом доступу до ресурсів

Спеціальність 123 – Комп'ютерна інженерія

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 2 ; кількість сторінок записки 56

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі спроектовано та налаштовано корпоративну мережу із ресурсами з відповідним захистом доступу до них, що дозволяє гарантувати безпеку при передачі даних по відкритих лініях з'єднання

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 технологій реалізації корпоративних мереж та безпеки даних у них. В другому розділі розроблено логічну та фізичну топології мережі, виконано аналіз наявних засобів для проектування та моделювання роботи мереж та обгрунтовано вибір пакету для роботи. В третьому розділі обрано схему адресації та маршрутизації, проведено конфігування всіх мережних пристроїв, протестовано проходження трафіку через мережу.

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

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 «задовільно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Мартинюк Валерій Володимирович, д.т.н., професор, завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки Хмельницького національного університету

« 20 » 06 2024р. (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.