Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

Захищена корпоративна мережа на основі концепції Zero Trust
Назва теми

Рівень вищої освіти *перший (бакалаврський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ.022058.22.04.01 ПЗ

Виконав здобувач IV курсу, група КІ2-22-1 — Підпис — Нікіта МЄЛЄЄВ (Ініціали, прізвище)

Керівник — канд.техн. наук, доц. (Науковий ступінь, учене звання) — Підпис — Дмитро МЕДЗАТИЙ (Ініціали, прізвище)

Нормоконтролер — канд.фіз.-мат. наук, доц (Науковий ступінь, учене звання) — Підпис — Тетяна КИСІЛЬ (Ініціали, прізвище)

До захисту допускаю:
завідувач кафедри КПС — підпис — Ольга ПАВЛОВА (Ініціали, прізвище)
«04» червня 2026 р.
дата

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ПЕРШИЙ (БАКАЛАВРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
_____ Ольга ПАВЛОВА
" 10 " 01 2026 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Мєлєєву Нікіті Борисовичу
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Захищена корпоративна мережа на основі концепції Zero Trust
Керівник проекту (роботи) Медзатий Дмитро Миколайович канд. техн. наук, доц.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 20.01.2026 р. № 7
2. Термін подання здобувачем роботи на кафедру 01.06.2026 р.
3. Вихідні дані до роботи Схема робочої захищеної корпоративної мережі на основі концепції Zero Trust.
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Теоретичні основи досліджуваної проблеми
Архітектура корпоративної мережі на основі концепції Zero Trust
Проектування захищеної корпоративної мережі на основі концепції Zero Trust
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Архітектура створюваної корпоративної мережі
Розділлення на підмережі всередині офісу корпоративної мережі
Результати тестування працездатності корпоративної мережі

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання « 10 » 01 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примі
1	Узгодження індивідуальної теми кваліфікаційної роботи з керівником	10.01.2026	виконан
2	Формулювання мети та задач дослідження; ознайомлення з предметною областю; визначення об'єкта та предмета дослідження	01.02.2026	виконан
3	Робота над першим розділом – збір матеріалу за темою дослідження, вимог та нормативів до виконуваного проекту та існуючих технічних рішень та постановка задачі	01.03.2026	виконан
4	Робота над другим розділом – визначення архітектури корпоративної мережі основаної на концепції «Нуль довіри»	01.04.2026	виконан
5	Робота над третім розділом – проєктування захищеної корпоративної мережі на основі концепції zero trust	29.04.2026	виконан
6	Оформлення пояснювальної записки відповідно до вимог	25.05.2026	виконан
7	Попередній захист ВКР	26.05.2026	виконан
8	Захист ВКР на засіданні ЕК	Червень 2026 року	

Здобувач _____ Нікіта МЄЛЄЄВ
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Дмитро МЕДЗАТИЙ
Підпис Ім'я, ПРІЗВИЩЕ

№ рядка	формат	Позначення	Найменування	Кіл.листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ 022058.22.04.01 ПЗ	Пояснювальна записка	64		
			Графічні матеріали			
2		КвРКІ 022058.22.04.01 Е8	Архітектура створюваної корпоративної мережі	1		
3		КвРКІ 022058.22.04.01 Е8	Розділення на підмережі всередині офісу корпоративної мережі	1		
4		КвРКІ 022058.22.04.01 Е8	Результати тестування працездатності корпоративної мережі	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ 022058.22.04.01 ВП		
Розробив		Мєлєєв			Відомість проекту	Літера	Аркуш	Аркушів
Перевір.		Медзатий				У	1	1
Н. контр.		Кисіль				ХНУ, КІ2-22-4		
Затв.		Павлова						

АНОТАЦІЯ

Тема «Захищена корпоративна мережа на основі концепції Zero Trust»

Автор роботи: Нікіта МЄЛЄЄВ.

Керівник роботи: Дмитро МЕДЗАТИЙ.

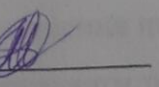
Пояснювальна записка: 73 с., 22 рис., 4 табл., 3 дод., 40 джерел.

Графічна частина: 2 креслення.

КОРПОРАТИВНА МЕРЕЖА, CISCO PACKET TRACER, ZERO TRUST

Кваліфікаційна робота бакалавра присвячена розробці та дослідженню Захищеної корпоративної мережі на основі концепції Zero Trust. Актуальність теми зумовлена зростаючими вимогами до надійності та безпеки функціонування комп'ютерних мереж, серверного обладнання та її кінцевих пристроїв. Своєчасне реагування на небезпеку та контроль доступу до ресурсів мережі дає змогу попереджати про проникнення в мережу, знижувати ризики небажаної взаємодії з мережею і підвищувати безпеку під час експлуатації технічних засобів.

Метою роботи є проектування та розробка захищеної корпоративної мережі на основі концепції Zero Trust з урахуванням усіх вимог та нормативів даного типу систем. Розроблено модель мережевої структури та симуляція використання відповідних протоколів виконана з використанням програмного забезпечення Cisco Packet Tracer. Тестування показало, що система забезпечує стабільне виконання вимог безпеки та своєчасне сповіщення про небезпеку, що є відповідним до поставлених задач.



Підпис здобувача

30.05.2026

Дата

ЗМІСТ

					КвРКІ. 022058.22.04.11 ПЗ		
Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Мелєєв Н.			Захищена корпоративна мережа на основі Zero Trust. Пояснювальна записка	Літ.	Арк. 4 / Акрушів 73
Перевір.		Медзатий Д.М.					
Реценз.						ХНУ, гр. КІ2-22-4	
Н. Контр.		Кисіль Т.М.					
Затверд.		Павлова О.О.					

ВСТУП

Впродовж декількох останніх років безпека інформаційних мереж досить впевнено посіла надзвичайно важливе місце в дедалі більшій кількості компаній від невеликого бізнесу, до корпоративних гігантів. Вона поширюються майже на всі сфери корпоративної діяльності, надаючи більшу безпеку.

Можливість мати часткову, а й інколи повну безпеку мережевих данних під час доступу до них є необхідністю в наш час. Також не слід забувати про зростання кількості кібератак та ускладнення IT-інфраструктури старі підходи (наприклад, побудова захищеного периметра з подальшою довірою до всіх всередині) більше не працюють.

У зв’язку з переходом до хмарних технологій та віддаленої роботи, традиційні периметрові моделі кібербезпеки втрачають ефективність. Концепція Zero Trust (нульової довіри), яка базується на принципі «ніколи не довіряй, завжди перевіряй», є критично необхідною для захисту сучасних корпоративних мереж від внутрішніх і зовнішніх загроз.. Дана модель безпеки передбачає необхідність постійного підтвердження автентичності користувачів, запитів до мережевої системи та пристроїв незалежно від місця їх надходження. Головними аспектами побудови захищеної системи є постійний моніторинг активності, ретельний контроль та дотримання інших принципів моделі Zero Trust.

1 ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖУВАНОЇ ПРОБЛЕМИ

1.1 Аналіз предметної області і виявлення наявних проблем і завдань

Типова модель мережевої безпеки часто надає широкий, плоский доступ до внутрішніх систем - набагато більше, ніж потрібно більшості користувачів. Це спадщина мережецентричного дизайну: опинившись «всередині», користувачі неявно отримують довіру. Сучасні моделі нульової довіри відкидають це. І, як показує практика, вони загалом кращі [32].

Початкова концепція нульової довіри Кіндервага була радикальною: довіру потрібно усунути як вразливість. Кіндерваг також запропонував три головні принципи нульової довіри [11]:

1. Усі джерела повинні бути перевірені та захищені;
2. Контроль доступу має бути обмежений та суворо контрольований;
3. Весь мережевий трафік має перевірятися та реєструватися.

Компанія Forrester також розширила своє початкове визначення Zero Trust за допомогою Zero Trust eXtended Framework3 або ZTX, яка ставить дані в центр захисту, оточені людьми, робочим навантаженням, мережею та пристроями. Серед основних моментів, які слід врахувати є: дані знаходяться в центрі систем, які впроваджуватимуть Zero Trust, робочі навантаження, що включає ресурси, які обробляють або, по суті, керують даними мережі, що зосереджується на сегментації на рівні мережі та охоплює загальний доступ з багатохмарних архітектур, даний момент охоплює точну сегментацію користувачів та управління ними для забезпечення точної ідентифікації та пристрої, який зосереджений на ідентифікації активів у середовищі та їх ізоляції [6].

Архітектура нульової довіри (ZTA) – це основа для впровадження нульової довіри в підприємстві. Нульова довіра зосереджена на автентифікації та авторизації, щоб зменшити неявну довіру, зберігаючи при цьому доступність. Метою ZTA є запобігання несанкціонованому доступу до даних і послуг, роблячи контроль доступу максимально точним і детальним [4].

Сучасна архітектура нульової довіри побудована на кількох основних принципах, які переорієнтовують мислення в галузі безпеки [15]. Серед яких є припущення про наявність порушення, тобто команди безпеки повинні діяти так, ніби зловмисники вже знаходяться всередині мережі, зосереджуючись на обмеженні горизонтального переміщення та мінімізації збитків.

Розташування створюваної мережі не має мати значення. Довіра не надається на основі місцезнаходження користувача, наприклад, чи знаходиться він у корпоративній локальній мережі, чи підключається віддалено.

Відсутність довіри обумовлюється тим, що кожна сутність будь то користувач, пристрій, програма чи служба - повинна бути перевірена та авторизована перед отриманням доступу, незалежно від їхнього положення відносно периметра мережі. Під час проведення будь-яких робіт з мережею вона має вважатись скомпрометованою або ворожою в будь-який час. В свою чергу, Доступ до ресурсів надається на основі «необхідності знати», дотримуючись принципу найменших привілеїв.

Також існує шість припущень з точки зору мережі, які кожен проект Zero Trust повинен враховувати [16]:

1. Приватна мережа підприємства не кваліфікується як зона неявної довіри.
2. Пристрої можуть не належати підприємству та не налаштовуватися ним.
3. Жоден ресурс не є довіреним за своєю суттю.
4. Не всі ресурси підприємства знаходяться на інфраструктурі, що належить підприємству.
5. Віддалені суб'єкти та підприємства не можуть повністю довіряти своєму локальному мережевому підключенню.
6. Активи та робочі процеси, що переміщуються між корпоративною та некорпоративною інфраструктурою, повинні мати узгоджену політику безпеки та режим роботи.

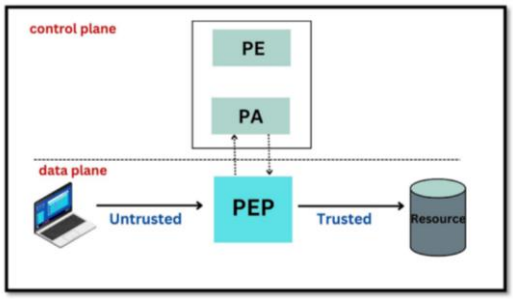


Рисунок 1.1 – Концепція архітектури нульової довіри [12, 33]

Логічні компоненти, показані на рисунку 1.1 [40]:

1. PE – механізм політик, що визначає рішення щодо доступу на основі політик підприємства.

2. PA – адміністратор політик, який тісно співпрацює з PE та надає або забороняє доступ на основі оцінки PE.

3. PEP – точка забезпечення дотримання політик, яка сприяє, контролює та, нарешті, розриває з'єднання між суб'єктом та ресурсом.

Компоненти архітектури мережі з нульовою довірою [10, 27]:

Керування ідентифікацією та доступом (IAM) – Централізоване керування ідентифікаторами, ролями та дозволами користувачів. Включає єдиний вхід (SSO), багатофакторну автентифікацію (MFA) та адаптивну автентифікацію.

Безперервний моніторинг та керування пристроями, що отримують доступ до мережі. Впровадження програмно-визначених периметрів (SDP) та мікросегментації. Контролює горизонтальне переміщення та ізолює конфіденційні ресурси.

Керування інформацією та подіями безпеки (SIEM) агрегує та аналізує журнали безпеки з усієї мережі. Забезпечує видимість потенційних загроз у режимі реального часу та підтримує пошук загроз. Інструменти, що запобігають несанкціонованому доступу, обміну або витоку конфіденційних даних (DLP). Постійна оцінка вразливостей та слабких місць конфігурації. Автоматизація завдання виправлення для підтримки безпечного стану (CDM). (CASB) – Розширює принципи ZTNA на хмарні середовища. Забезпечує прозорість, забезпечення відповідності та захист даних для хмарних додатків. Забезпечення

шифрування всіх даних під час передачі та зберігання. Використовування протоколу безпеки транспортного рівня (TLS) та інші стандарти шифрування.

Одним з принципів безпеки з нульовою довірою є контроль доступу на основі ідентифікації. Цей підхід надає доступ на основі перевірених ідентифікаційних даних користувачів або пристроїв, а не на основі місцезнаходження мережі [1, 7].

Другим є мікросегментація. Вона ізолює системи, робочі навантаження та дані в мережі, щоб мінімізувати горизонтальне переміщення, якщо один актив скомпрометовано [9]. Розширені постійні загрози (APT) – це ще одна область, де вплив ZTA відчутний. Шарма (2022) ілюструє, що мікросегментація – основний компонент ZTA – служить ефективним бар'єром проти горизонтального переміщення, яке використовують APT. Їхній аналіз показує, що поділ мереж на менші, безпечні зони обмежує зловмисників, тим самим зменшуючи потенційну шкоду від тривалих вторгнень [2].

Найменш привілейований доступ гарантує, що користувачі та служби мають лише мінімальні права доступу, необхідні для виконання призначених їм завдань. Привілеї надаються вчасно та за потреби.

Керування привілейованим доступом (PAM) – це поєднання інструментів і технологій, що використовуються для захисту, контролю та моніторингу доступу до критично важливої інформації та ресурсів організації. Приклади облікових записів на основі PAM включають наступне [8]:

1. Процедури безпеки, які включають реагування на інциденти, аварійне відновлення та плани забезпечення безперервності бізнесу.
2. Локальні облікові записи адміністраторів.
3. Будь-які програми або служби.
4. Облікові записи адміністраторів, що працюють з доменами та веб-програмами.

Безперервний моніторинг та аналітика забезпечують цю функцію. Вона постійно відстежує мережевий трафік, активи та поведінку користувачів на наявність аномалій, які можуть свідчити про загрози. Моніторинг у режимі

реального часу в сегментованих середовищах дозволяє негайно ідентифікувати та нейтралізувати аномальну поведінку, пов'язану з APT [2]. Для постійного моніторингу трафіку організаційних даних шлюзи та межі сервісів повинні бути захищені та моніторинговані. Безпечні межі сервісів дозволяють суворо контролювати доступ до API та інших зовнішніх точок контакту. Перевірка ідентифікації, дозволів та контексту кожного запиту.

Перевірка ідентифікації [20] – автентифікація користувача доводить, що це та сама особа, яка раніше зареєструвалася у вашому цифровому сервісі. Вона не обов’язково надає підтвердження особи користувача, і дуже часто це також не є критичною вимогою. Однак у деяких галузях, таких як фінансові програми, медичні системи, податкові системи або деякі урядові вебсайти, вам може знадобитися вагомий доказ автентичності користувача. Саме тоді вам потрібно використовувати автентифікатор для перевірки ідентифікації.

Цього можна досягти за допомогою сильної автентифікації [28]. В загальному існує п'ять типів сильної автентифікації, але в цьому випадку нам потрібно знати лише про два з них, а саме біометрію та багатофакторну аутентифікацію.

Біометрія – зазвичай вважається найсильнішим методом автентифікації. Її дуже важко зламати, але одним із недоліків є складність налаштування біометричної системи. Найпоширеніші типи біометрії включають: відбиток пальця, розпізнавання обличчя, розпізнавання фрази, розпізнавання голосу.

Багатофакторна автентифікація – це практика використання таких факторів, як те, що знає користувач (наприклад, пароль), що має користувач (наприклад, керований пристрій або сертифікат пристрою), хто є користувачем (наприклад, біометрія) та що користувач може вирішити (наприклад, капча з проблемами); це основоположний принцип нульової довіри [39].

Принцип нуль довіри може враховувати шифрування даних. Шифрування даних у стані спокою та під час передачі запобігає несанкціонованому доступу, навіть якщо система скомпрометована. Тому управління ключами та надійні політики є критично важливими.

Одним із найчастіш використовуваних методів шифрування даних є використання відкритого та закритого ключа [10]. Існує ряд важливих математичних алгоритмів шифрування використовуючи даний метод, таких, як алгоритм RSA, алгоритм Діффі-Хеллмана, Алгоритм теорії еліптичних хвиль.

Крім того, модель безпеки Zero Trust може включати збір даних, які дозволять приблизно визначити або розпізнати загрозу[18]. Серед типів даних які зазвичай включаються в збір є контекстуальні дані, що визначають ролі та пристрої користувачів, що можуть змінюватися з часом. Працівники можуть змінювати свою роль з різних причин, таких як зміна команди або отримання підвищення. Як наслідок, місце доступу до інформації також змінюється. Тип пристрою, операційна система та використовувані програми також можуть змінюватися. Важливо створити умови та налаштувати матеріальне забезпечення для можливості проведення збору всієї цієї інформації.

Додатково до збору можуть відноситись метадані підключення. Є важливим виконувати збір інформації про ролі користувачів та деталі пристрою під час входу в систему. Ролі користувачів можна легко зібрати з членства в групах Active Directory, а деталі пристрою можна зібрати під час оцінки стану.

Реєстрація підозрілих дій – оскільки раніше було встановлено базовий рівень довіри, важливо також створити базову поведінку користувачів у межах цього рівня довіри. Будь-яке відхилення від базового рівня необхідно фіксувати та аналізувати, і слід негайно вживати заходів.

Такі компанії, як GoodAccess пішли ще далі і пропонуть кілька додаткових типів запису даних з усієї мережі нульової довіри:

1. Записи доступу на рівні шлюзу – записи доступу на периметрі. Щоразу, коли пристрій підключається до периметра, створюється запис у журналі, який показує, хто підключається і коли, який пристрій вони використовують, з якого місця та скільки даних було передано.

2. Записи доступу на рівні системи – записи доступу до окремих критичних систем на мережевому рівні. Ці записи показують, хто підключається

і коли, який пристрій вони використовують, з якого місця та скільки даних було передано системі.

3. Записи блокувальника загроз – записи мережевого зв'язку з доменами з чорного списку, наприклад, шкідливе програмне забезпечення, фішинг, командні та контрольні системи тощо.

4. Записи перевірки стану пристроїв – записи стану безпеки пристроїв та записи кожної регулярної перевірки. Ці журнали автоматично оновлюються при будь-якому покращенні/погіршенні стану безпеки всіх пристроїв, які використовують співробітники.

5. Записи адміністратора – записи всіх змін, внесених адміністраторами до конфігурації мережі GoodAccess з нульовою довірою через панель керування.

Об’єднання моделі мережевої безпеки нульової довіри та штучного інтелекту створює новий метод впровадження кібербезпеки, який адаптується до нових загроз, залишаючись при цьому проактивним та стійким до атак. Численні організації почали впроваджувати рішення безпеки на основі штучного інтелекту з нульовою довірою у фінансовому, медичному та державному секторах, оскільки вони покращують зменшення кіберризиків [24, 29, 30].

Важливою частиною впровадження мережевої безпеки є врахування ризику може бути складним, тому слід почати з областей, які заслуговують на подальше дослідження, наприклад, сторонні особи та співробітники [22, 34].

Розуміння поведінки користувачів має вирішальне значення для розрізнення ризикованих та доброякісних дій. Цей аналіз вивчає закономірності нормальної поведінки, щоб потім визначити, коли поведінка є аномальною. Аналіз цих закономірностей та їх оцінка відповідно до політики компанії призводить до кращого визначення запитів на доступ.

Наведені нижче рекомендації щодо нульової довіри також можуть допомогти у розробці та розгортанні системи безпеки з нульовою довірою. Вони можуть допомогти створити надійну стратегію запобігання втратам даних (DLP) та уникнення порушень [5]:

1. Визначити область найбільшого ризику.

2. Впровадити засоби контролю мережевого трафіку.

3. Попереднє планування архітектури мережі з нульовою довірою.

4. Створити політику нульової довіри. Після того, як відбулось створення архітектури мережі,необхідно буде розробити політики нульової довіри. Найефективніше це зробити за допомогою методу Кіплінга. Він передбачає запитання: хто, що, коли, де, чому та як для кожного користувача, пристрою та мережі, які хочуть отримати доступ.

5. Моніторинг мережі.

Існує кілька підходів до впровадження ZTA. Одним із підходів при застосуванні моделі Zero Trust є п'ятиетапний підхід [21, 35]:

Перший крок полягає у визначенні захисної поверхні, тобто у визначенні даних, програм, активів та послуг, які потребують захисту. Активи з високою чутливістю включають не лише критичні дані, але й критичні служби, такі як Active Directory (AD), DNS та DHCP.

Другим кроком буде відображення потоку транзакцій. Ці потоки безпосередньо інформують про те, де слід розмістити відповідні елементи керування.

Третій крок – побудова архітектури нульової довіри. Це передбачає розробку архітектури нульової довіри, адаптованої до брандмауера або брандмауерів, визначених у кроках 1 та 2.

Четвертий крок – створення політики нульової довіри. Нульова довіра повинна бути встановлена як політика 7-го рівня.

П'ятий крок – моніторинг та обслуговування мережі. Весь трафік до 7-го рівня необхідно перевіряти та реєструвати.

Впровадження нульової довіри поетапний підхід [13, 38]:

Організації, які успішно впроваджують нульову довіру, зазвичай починають з оцінки та планування, визначення критично важливих активів даних, зіставлення потоків даних у середовищі та оцінки існуючих засобів контролю безпеки відповідно до принципів нульової довіри.

Після завершення оцінки організації зазвичай зосереджуються на управлінні ідентифікацією та доступом як на другому етапі. Це включає посилення механізмів автентифікації та впровадження контекстної авторизації, яка враховує кілька факторів під час надання доступу.

Трансформація мережі є важливою віхою у впровадженні Zero Trust, яка часто вимагає суттєвих архітектурних змін. Організації впроваджують мікросегментацію, щоб розділити мережі на безпечні зони та розгорнути засоби контролю безпеки на рівні додатків, які захищають ресурси незалежно від розташування мережі.

Заключний етап зосереджується на можливостях видимості та аналітики, постійно контролюючи екосистему безпеки. Організації розгортають комплексні інструменти моніторингу на мережевому, ідентифікаційному та прикладному рівнях, одночасно розробляючи можливості автоматизованого реагування, які можуть стримувати загрози без втручання людини.

Нам також потрібно враховувати недоліки даної системи та обмеження доступу. Фундаментальним аспектом нульової довіри є обмеження доступу, головним чином через створення білих списків. Це практика диктування того, що може статися, все інше заборонено за замовчуванням.

Таким чином, правильно виконана стратегія нульової довіри забезпечить баланс між безпекою та доступом. Вона також повинна знайти баланс між тим, чого можна ефективно досягти [3].

Окрім спроб досягти цього балансу, існують також технічні проблеми впровадження ZTA, такі як [14, 37, 36]:

Застарілі системи та інтеграція – Застарілі системи не побудовані з урахуванням сучасних потреб кібербезпеки, і багато підприємств змушені покладатися на них. Зазвичай ці системи не забезпечують необхідних для ZTA можливостей, таких як детальний контроль доступу або інтеграція з рішенням для управління ідентифікацією.

Проблеми масштабованості та продуктивності – Однак впровадження ZTA у великих розподілених середовищах є проблемою продуктивності, оскільки

організації масштабують свої операції. ZTA дозволяє здійснювати детальний контроль доступу та безперервну автентифікацію, але вони можуть погіршити взаємодію з користувачем. Організації повинні ретельно збалансовувати вимоги безпеки з міркуваннями зручності використання та продуктивності.[19].

Побудова системної схеми – це ще один важливий крок до реалізації мережі з нульовою довірою. Чітке уявлення про те, як відбувається як внутрішня, так і зовнішня мережева комунікація, буде корисним під час проектування каналів системного зв'язку.

Існує багато різних механізмів для реєстрації та аналізу мережевих потоків [26]: Wireshark, Cisco Secure Network Analytics та Datadog Network Performance Monitoring.

1.2 Порівняльний аналіз переваг та недоліків існуючих рішень

Wireshark залишається потужним і широко використовуваним аналізатором мережевих протоколів. Функціонал, що надає Wireshark є дуже схожим з можливостями програми tcpdump, але навідміну від попереднього Wireshark має графічний інтерфейс і значно більше можливостей для сортування інформації. Ця програма надає користувачеві можливість переглядати весь трафік, що проходить по мережі, в режимі реального часу.

Основні можливості Wireshark. Можливість використання фільтрів відображення для швидкого пошуку пакетів за портами, вмістом або IP. Здатність перегляду зашифрованих даних (SSL/TLS або WPA/WPA2) за наявності відповідних ключів. Перехоплення даних безпосередньо з мережевих інтерфейсів в реальному часі. Підтримка тисяч протоколів, від поширених (HTTP, TCP, DNS) до спеціалізованих. Працює на Windows, macOS, Linux, Solaris та інших ОС.

Основні недоліки Wireshark. Інструмент не підходить для моніторингу великих корпоративних мереж у реальному часі. Перехоплення та аналіз великих обсягів даних можуть суттєво навантажувати процесор та оперативну пам'ять. Wireshark не може показати повну картину, якщо трафік зашифровано (наприклад,

HTTPS). В порівнянні з комерційними продуктами, Wireshark потребує ручного розрахунку дельти часу між пакетами, що заважає швидко знайти причини затримок. При розборі тунельованого трафіку ,такого, як VPN, модулі можуть заміщати один одного, роблячи аналіз неможливим. Відновлені потоки не розглядаються як єдиний буфер, що ускладнює їх обробку.

Cisco Secure Network Analytics є чудовим рішенням для спостереження та аналізу мережевого трафіку, що використовує технологію NetFlow для виявлення загроз в режимі реального часу, моделювання поведінки та безпечної видимості мережі.

Основні можливості Cisco Secure Network Analytics. Створює «базову модель» нормальної поведінки для кожного хоста та сигналізує про будь-які аномалії. Використовує глобальну базу даних загроз від Cisco Talos для ідентифікації відомих ботнетів та атак. Виявляє шкідливе програмне забезпечення у зашифрованих потоках даних без потреби в їх розшифровці, зберігаючи їх конфіденційність. Використовує мережеву інфраструктуру як «сенсор», що дозволяє бачити всі дії користувачів та пристроїв без встановлення додаткових агентів.

Основні недоліки Cisco Secure Network Analytics. Налаштування системи та її інтеграція в існуючу інфраструктуру потребує високої кваліфікації інженерів. На початкових етапах система може генерувати велику кількість хибних сповіщень, що перевантажує службу безпеки. Вагомим недоліком також є висока вартість даного рішення, включаючи як ліцензії, так і необхідність у наявності потужної апаратної інфраструктури для збору та аналізу даних.

Datadog дозволяє візуалізувати мережеві потоки в режимі реального часу, що спрощує побудову системних діаграм та розуміння взаємодії між різними мережевими компонентами. Монітор продуктивності мережі (SaaS) – інструмент, що входить до платформи Datadog, призначений для відстеження продуктивності гібридних та хмарних мереж. Він забезпечує візуалізацію мережевого трафіку, корелює дані NetFlow з інфраструктурою та програмами, допомагаючи діагностувати затримки та збої.

Основні можливості Datadog Network Performance Monitoring**.** Дозволяє виявляти причини мережевих затримок та перевантажень, корелюючи мережеві показники з продуктивністю додатків. Виявлення вузьких місць у мережі за допомогою детальної карти взаємозв'язків. Перегляд потоків даних між хостами, контейнерами, сервісами та зонами доступності в реальному часі. Моніторинг як локальних мереж, так і хмарних інфраструктур (AWS, Azure, GCP). Інструмент дозволяє командам DevOps та мережевим інженерам оперативно знаходити та усувати проблеми з підключенням.

Основні недоліки Datadog Network Performance Monitoring. Агенти Datadog, які встановлюються на серверах для збору мережевих метрик, можуть споживати значну кількість оперативної пам'яті, що критично для продуктивних систем. Вартість базується на кількості хостів, що може зробити Datadog дуже дорогим для великих інфраструктур, особливо при активному моніторингу трафіку. Через великий обсяг даних, які збирає Datadog, виявлення справжньої причини інциденту серед тисяч попереджень може бути складним без детального налаштування оповіщень. Хоча інструмент показує взаємодію сервісів, глибокий аналіз фізичних мережевих пристроїв (SNMP/NetFlow) іноді поступається спеціалізованим "залізо-орієнтованим" рішенням, що означає обмежену видимість на закритому обладнанні.

1.3 Підходи до вирішення задачі за темою дослідження

Для виконання поставленої задачі було обрано Cisco Packet Tracer оскільки під час навчання було набуто досвід в його використанні. Для виконання проектної частини дипломної роботи було обрано пятиетапний підхід описаний раніше.

Виконувана схема буде мати в собі розділ на певні корпоративні відділи та можливість під’єднання сторонній пристроїв для симуляції систем мережевої безпеки Zero Trust. Також буде впроваджено віддалений доступ адміністрації мережі до її елементів по зашифрованому каналу SSH, віддалене збереження

облікових даних користувачів мережі, підтримка взаємодії кількох філій з головнм офісом компанії через під’єднання між комутаторами третього рівня та логування даних використання мережі двома окремими методами.

1.4 Висновки до першого розділу

В ході виконання першого розділу було досліджено принципи функціонування захищеної корпоративної мережі на основі концепції Zero Trust. Було проведено аналіз теоретичної інформаці пов’язаної з даною сферою та охарактеризовано базову модель та структуру предметної області. Також було описано уже існуючі механізми реалізації, виділено наявні проблеми в галузі та шляхи їх вирішення.

Таким чином подальшими завданнями виконуваної роботи будуть:

– використовуючи за основу виконані дослідження, визначити основні функції системи, розробити модель функцій, які система повинна виконувати, сформувати низку функціональних та нефункціональних вимог;

– підвести певні підсумки щодо необхідності розробки даної системи;

– сформувати мету та об’єкт для наступних досліджень;

– оцінити ступінь виконання поставлених завдань.

– На основі даного списку завдань створити працездатну мережеву систему, що використовує принцип безпеки “Zero Trust” та зробити висновки на основі виконаної роботи.

2 АРХІТЕКТУРА КОРПОРАТИВНОЇ МЕРЕЖІ ОСНОВАНОЇ НА КОНЦЕПЦІЇ ZERO TRUST

2.1 Архітктура мережі Zero Trust

Побудова мережі Zero Trust означає зміну основної філософії вашої безпеки з «довіряй, але перевіряй» на «ніколи не довіряй, завжди перевіряй». У середовищі Zero Trust просте підключення до мережі не дає доступу ні до чого; Кожен користувач, пристрій і додаток мають бути явно автентифіковані та авторизовані у будь-який час. Впровадження мережі Zero Trust проходить наступним чином.

Спочатку слід відобразити всі свої дані та їх потоки та ідентифікувати кожного користувача, пристрій (включаючи IoT та BYOD) та додаток. Також слід забезпечити строгу автентифікацію через Впровадження суворої багатофакторної автентифікації (MFA) та Single Sign On (SSO) для всіх точок доступу, щоб запобігти несанкціонованому доступу [1].

Багатофакторна автентифікація (MFA) – це модель безпеки, при якому користувач надає два або більше різних фактори верифікації особи для отримання доступу до облікового запису або додатку. Це додає важливі рівні захисту, окрім стандартного пароля, запобігаючи несанкціонованому доступу у разі компрометації ваших облікових даних [6].

Три основні фактори автентифікації, серед яких MFA вимагає перевірки щонайменше за двома окремими категоріями доказів [4]:

1. Щось, що є вже відомим: пароль, PIN-код або питання безпеки.
2. Щось, що є наявним у користувача: мобільний пристрій, смарт-карта або фізичний апаратний ключ.
3. Особисті данні: біометрія, така як відбиток пальця, розпізнавання обличчя або сканування голосу.

На практиці при вході в обліковий запис багатофакторна аутентифікація перетворює процес верифікації особи на багатокроковий процес в якому початковим кроком буде введення свого стандартного логіну та паролю. Далі буде необхідність ввести додатковий фактор, або надати другий доказ (наприклад,

ввести код з додатку автентифікатора, натиснути клавішу або просканувати обличчя). Після введення логіну та паролю і надання, якогось другорядного доказу особистості користувача система перевіряє всі фактори одночасно, і доступ дозволяється лише за умови успішху кожної перевірки [4, 6].

Для найвищого рівня безпеки експерти зазвичай рекомендують впорядковувати такі методи багато-факторної автентифікації. Додатки, такі як Microsoft Authenticator або Google Authenticator надають можливість генерувати тимчасові, захищені коди, які не надсилаються через перехоплювані мобільні мережі. Також є випадки використання апаратних ключів безпеки таких, як фізичні USB або Bluetooth-пристрої (наприклад, YubiKeys), які потрібно підключити до вашого комп'ютера [4].

Додатково, як підтвердження особистості можливо використовувати SMS або електронні коди, які будуть слугувати одноразовими паролями, які надсилаються на номер телефону або електронну скриньку. Хоча це краще, ніж відсутність MFA, цей метод трохи більш вразливий до «SIM-swapping» або перехоплення електронної пошти.

Корисним функціоналом також можна вважати Single-sign-on (SSO) [1, 35]. SSO базується на відносинах між довіреним застосунком, який ви хочете використовувати, та центральним провайдером ідентифікації (IdP). Автентифікація відбувається через вхід на центральний IdP (наприклад, Okta, Google, Microsoft), використовуючи ім'я користувача, пароль або багатофакторну автентифікацію (MFA). В подальшому IdP створює захищений цифровий токен, який підтверджує вашу особу. Після чого, коли виконується перехід до підключеного додатку, цей додаток перевіряє провайдер ідентифікації, розпізнає довірений токен і пропускає вас без додаткового пароля.

Кодова база SSO використовує специфічні протоколи галузевого стандарту для безпечної передачі ідентифікаційних даних користувачів між різними системами. Серец цих протоколів є SAML (Security Assertion Markup Language), що є широко використовуваною в корпоративних середовищах для передачі даних авторизації та автентифікації між мережами.

Також одним з даних протоколів можна назвати OIDC (OpenID Connect), що є легким протоколом автентифікації, побудованим на основі OAuth 2.0, що широко використовується для мобільних додатків та сучасного вебу [16].

Хоча Telnet був розроблений для простоти, він позбавлений сучасних методів захисту мережі, що робить його непридатним для використання в публічних або навіть сучасних приватних мережах. Через це для доступу до комутаторів ззовні в даній мережі було прийнято рішення використати протокол SSH. Основні переваги SSH включають в себе надійну безпеку, що гарантується через шифрування всього трафіку, включаючи імена користувачів і паролі. Telnet передає все у відкритому тексті, дозволяючи будь-кому з пакетним сніфером (наприклад, Wireshark) легко викрасти облікові дані. Також SSH підтримує кілька безпечних методів, включаючи аутентифікацію з відкритим ключем (усуваючи потребу в паролях) та багатофакторну автентифікацію.

SSH використовує функції хешування, щоб переконатися, що дані не були змінені або підроблені під час передачі. SSH здатне забезпечити основу для SFTP і SCP, дозволяючи безпечно переміщувати файли без необхідності окремого протоколу, такого як FTP. Також ви можете використовувати SSH для створення безпечних «тунелів» для іншого незахищеного трафіку (наприклад, X11 або з'єднання з базами даних), фактично виступаючи як легкий VPN.

Сучасні реалізації SSH краще справляються з мережевими «затримками», ніж Telnet. Якщо ваше інтернет-з'єднання ненадовго зникає, SSH часто може відновитися з того місця, де ви зупинилися, тоді як Telnet зазвичай одразу завершує сесію. SSH підтримує стиснення даних, що може зробити віддалені сесії командного рядка швидшими через повільні або високозатримкові лінії.

Далі слід впровадити доступ за найменшими привілеями (Least Privilege Access), що значить необхідність надавання користувачам і сервісам лише мінімальної можливості доступу, необхідні для виконання своєї роботи та впровадження обмеження на часовий вікно для цих дозволів [8, 15].

Щоб забезпечити мінімальний доступ до привілеїв у, ви можете призначити певні рівні привілеїв (рівні 0 – 15) користувачам і обмежити їх лише командами, необхідними для їхньої роботи.

Рівень 1 (за замовчуванням): використовується для стандартних користувачів, яким потрібен лише базовий доступ лише для читання (наприклад, ping, show). Рівні 2 – 14 (Custom): За замовчуванням не використовуються. Адміністратори можуть вручну визначати, які саме команди належать до цих рівнів. Рівень 15 (за замовчуванням): використовується для адміністраторів з повним доступом до читання та запису пристрою.

Необхідно встановлювати політики на основі ролей користувачів та конкретних атрибутів (наприклад, департаменту, проєкту або рівня допуску). Безпечні комунікації між машинами. Найменший привілей однаково застосовується до API, мікросервісів і автоматизованих скриптів. Використовуйте короткочасні токени та криптографічні сертифікати замість жорстко закодованих облікових даних або API-ключів, які легко вкрасти [35].

Слід розділити свою мережу на менші зони. Замість плоских мереж, які дозволяють бічний рух, бажано використовувати ZTNA (Zero Trusk Network Access), щоб з'єднувати користувачів безпосередньо з конкретними застосунками, які їм потрібні, а не з усією мережею.

Мікросегментація – це стратегія безпеки Zero Trust, яка розділяє мережі на ізольовані зони для обмеження розповсюдження загроз по мережі [18]. Хоча у випадку Cisco Packet Tracer не має підтримки корпоративного програмного мікросегментування, таких як Cisco ACI або Cisco Secure Workload, є можливість емулювання даної концепції за допомогою базової маршрутизації та комутації.

Основними елементами реалізації мікросегментації в Cisco Packet Tracer можуть слугувати такі налаштовувані аспекти мережі як приватні підмережі, списки контролю доступу та безпека портів.

Приватні підмережі (PVLAN) підтримуються на комутаторах Cisco Catalyst у Packet Tracer та дозволяють ізолювати кінцеві пристрої користувачів (ізольовані порти) один від одного, змушуючи їх спілкуватися лише з маршрутизатором або

default gateway за замовчуванням (Promiscuous ports), повністю запобігаючи горизонтальному переміщенню між пристроями.

Розміщені на комутаторах або маршрутизаторах третього рівня, розширені списки доступу можуть бути написані так, щоб за замовчуванням явно відмовлятися від трафіку між певними серверами або підмережами, дозволяючи лише необхідний зв'язок (наприклад, дозволяючи робочій станції отримувати доступ лише до порту 443 веб-сервера). Також є можливість обмежити MAC-адреси, дозволені на певних портах комутаторів, щоб запобігти підключенню несанкціонованих пристроїв до чутливих сегментів мережі.

Під час розробки даної мережі слід завжди припускати, що зловмисник уже в мережі та ввести безперервинй моніторинг. Є необхідним встановити постійний контроль мережевого трафіку і фіксацію всіч дій, щоб аномалії можна було миттєво виявляти та блокувати [6].

Для контролю мережевого трафіку найбільше, в даному випадку, підходять таки рішення як рагіше описане розділення мережі на підмережі та розділення мережі на зони (zone-based policies).

Розділення мережі на зони (zone-based policies), часто реалізовані через міжмережеві екрани, групують мережеві інтерфейси або VLAN у зони безпеки на основі рівня довіри. Замість традиційних правил на основі інтерфейсу, вони визначають поведінку трафіку між зоною джерела та зоною призначення, забезпечуючи високобезпечну, масштабовану та модульну сегментацію мережі.

Зони безпеки – це логічні групи мережевих інтерфейсів із подібними функціями, рівнями довіри або вимогами до безпеки. Поширені приклади включають LAN (довірений), DMZ (напівдовірений) та WAN/Internet (недовірений). Зони безпеки організовуються через зонові пари, як односторонні визначення трафіку. Наприклад, пара зон, що йде з LAN до WAN, відрізняється від пари зворотного трафіку WAN до LAN.

Політика за замовчуванням орієнтовані на зони, зазвичай за замовчуванням «відмовляють усіх». Будь-який трафік, що рухається між різними зонами, блокується, якщо це не дозволено явно. Трафік у межах однієї зони зазвичай

пропускається за замовчуванням. Одною з основних переваг є можливість легко ізолювати вразливі пристрої (наприклад, IoT або гостьові мережі) від основної інфраструктури.

Зменшення поширення правил усуває необхідність підтримувати незліченну кількість окремих IP-адрес або IP-списків контролю доступу (ACL) [3]. Якщо новий пристрій підключається до локальної мережі, він автоматично отримує права доступу LAN-зони.

Кращий логування даних мережі забезпечить адміністрації можливість швидко оцінити, які частини мережі можуть спілкуватися між собою на основі бізнес-логіки.

Серед варіантів дій для логування трафіку найкращими будуть Syslog та частина AAA, що відповідає за аккаунтинг [20]. Syslog (System Log Protocol) – це стандарт, який використовується для логування повідомлень. Він дозволяє різним мережевим пристроям, серверам і додаткам генерувати, форматувати та передавати повідомлення та сповіщення про події, на певному матеріальному обладнанні, на централізований сервер [3].

Адміністратори використовують його для моніторингу стану системи, усунення помилок і відстеження подій безпеки. Процес Syslog використовує просту клієнт-серверну архітектуру:

– клієнт (відправник) – пристрій (наприклад, маршрутизатор, фаєрвол або сервер) генерує повідомлення при виникненні події;

– протокол – форматує повідомлення у стандартизовану структуру, що містить початок події, часову мітку та опис події;

– сервер (приймач) – безпечно приймає, аналізує та зберігає журнали з кількох різних пристроїв в одному, зручному для пошуку місці.

Поширені випадки використання включають в себе централізування управління, що здійснюється за рахунок логування з сотень маршрутизаторів, комутаторів і серверів в одне місце. Відстежування несанкціонованих спроб входу, зміни конфігурацій та втрати міжмережевого екрану. Також syslog

допомагає інженерам точно відстежувати, коли система збоїла або додаток видав помилку.

Syslog передає свої дані через UDP-порт 514, але також може використовувати TCP для більш надійної доставки. Хоча спочатку він був створений для систем Unix/Linux, ви можете легко пересилати дані з Windows та інших платформ на сервер Syslog за допомогою сторонніх агентів.

AAA аккаунтинг є компонентом AAA (Автентифікація, Авторизація та Аккаунтинг). Він фіксує активність користувачів - таку як час входу/виходу з акаунтів та використані дані - щоб створити аудиторський слід для білінгу, аналізу безпеки та планування ресурсів.

Фреймворк AAA керує мережевим доступом через три послідовні кроки:

– автентифікація – перевіряє особу користувача або пристрою (наприклад, введення імені користувача та пароля);

– авторизація – визначає, до яких конкретних мережевих ресурсів, команд або даних користувач має доступ;

– аккаунтинг – Вимірює та фіксує точні дії користувачів під час підключення до мережі.

Аккаунтинг працює шляхом відстеження та надсилання конкретних метрик на централізований сервер. Вона базується на двох основних типах записів даних: Записи старту генеруються, коли користувач успішно встановлює мережеву сесію, фіксуючи точний час початку та параметри підключення. Записи зупинки, що генеруються, коли користувач відключається або сесія закінчується. Це включає час завершення, тривалість та загальну кількість надісланих і отриманих даних.

Одною з основних причин для використання AAA у виконуваній мережі можна назвати централізацію управління. Використання AAAдозволить об'єднати всі облікові дані користувачів і політики доступу в єдину централізовану базу даних. Замість налаштування користувачів на кожному окремому маршрутизаторі, комутаторі чи фаєрволі, адміністратори можуть керувати доступом з одного місця.

Серед причит також можна назвати покращену безпеку при автентифікації. Мережа буде перевіряти особу користувачів і пристроїв та їх рівень доступу перед його наданням. Це утримує несанкціонованих користувачів і захищає кінцеві точки за допомогою протоколів, таких як 802.1X, запобігаючи несанкціонованим дротовим або бездротовим з'єднанням.

Детальний контроль доступу є необхідним для забезпечення дотримання принципу найменших привілеїв. Після автентифікації користувача AAA точно визначає, до яких файлів, команд або мережевих сегментів йому дозволено мати доступ.

Підзвітність та аудит є необхідними для відстежування використання мережі, тривалість сесії та виконані дії. Це створює комплексний аудиторський слід, який є важливим для усунення несправностей, виявлення підозрілої активності та дотримання галузевих стандартів безпеки. • Масштабованість: Легко обробляє зростаючу кількість пристроїв, користувачів, віддалених працівників і гостьових мереж без втрати адміністративного контролю.

Поширеними протоколами при використанні AAA є RADIUS та TACACS+. RADIUS є найпоширенішим стандартом віддаленого доступу, що широко використовується підприємствами та провайдерами та передає данні простим текстом. В свою чергу TACACS+ є протоколом, розробленим Cisco, який забезпечує більш детальний облік, особливо для точного відстеження команд інтерфейсу командного рядка (CLI), введених адміністраторами.

Для даної мережі було прийнято рішення використати протокол TACACS+. Використання TACACS+ (Terminal Access Controller Access-Control System Plus) є стандартною практикою для безпечного адміністрування мережевих пристроїв. Він забезпечує централізований спосіб управління тим, хто може отримати доступ до вашої інфраструктури та що саме вони можуть робити.

Основні причини використання TACACS+ включають:

1. Детальна авторизація команд. На відміну від інших протоколів, TACACS+ дозволяє адміністраторам дозволяти або відхиляти конкретні команди. Наприклад, ви можете дозволити молодшому техніку запускати команди шоу, але

заборонити використовувати конфігурацію терміналу чи перезавантаження. Також ви можете визначати набори команд для різних груп користувачів Role Based Access Control (RBAC), гарантуючи, що персонал матиме лише необхідні для своєї ролі привілеї.

2. Повне шифрування корисного навантаження

TACACS+ шифрує весь пакетний вантаж. Натомість протоколи, такі як RADIUS, шифрують лише пароль, залишаючи імена користувачів і бухгалтерські дані видимими потенційним зловмисникам. Також це комплексне шифрування захищає чутливий адміністративний трафік від атак на перехоплення даних та повторних атак.

3. Розділення функцій AAA

TACACS+ розглядає автентифікацію (хто ви), авторизацію (що ви можете робити) та бухгалтерію (те, що ви зробили) як окремі процеси. Оскільки вони є окремими, ви можете використовувати різні методи для кожного кроку. Наприклад, ви можете автентифікуватися через центральний сервер, але здійснювати авторизацію локально або через інший сервіс.

4. Детальний аудит і бухгалтерський облік

TACACS+ фіксує кожну команду, введену адміністратором, разом із часовими мітками. Ці детальні аудиторські сліди є необхідними для дотримання регуляторних стандартів, таких як ISO 27001, PCI-DSS або HIPAA.

5. Надійне управління з'єднанням – TACACS+ використовує TCP (зазвичай порт 49) замість UDP. Це забезпечує більш надійне з'єднання, гарантуючи, що сервер миттєво підтверджує запити та може краще керувати кількома сесіями.

6. Централізоване управління – замість керування локальними акаунтами на сотнях окремих комутаторів або маршрутизаторів, ви керуєте всіма обліковими даними в одному центральному місці. Більшість серверів TACACS+ можуть інтегруватися з існуючими провайдерами ідентифікації, такими як Active Directory або LDAP, що спрощує налаштування та депровізацію користувачів.

2.2 Функціонал завдань які може виконувати дана система

Мережа з нульовою довірою (ZTN) – це модель безпеки, побудована на принципі «ніколи не довіряй, завжди перевіряй». Вона розроблена для виконання завдань, зосереджених на постійній автентифікації, найменш привілейованому доступі, мікросегментації мережі та суворому стримуванні загроз. Корректно працююча мережа Zero Trust має безперешкодно виконувати такі основні завдання:

Перевірка особи та доступу залучає безперервну автентифікацію, що значить, що система автентифікує та перевіряє кожного користувача, обліковий запис служби та машину незалежно від місцезнаходження або того, чи знаходяться вони всередині чи поза межами корпоративного периметра. Також велике значення в дані перевірці має контекстуальна оцінка на основі якої система приймає рішення щодо доступу на основі динамічних контекстуальних даних, таких як поведінка користувача, стан пристрою, місцезнаходження та чутливість запитуваних даних. Даний функціонал може бути втіленим на сервері через використання раніше описаного протоколу AAA.

Застосування доступу з мінімальними привілеями, що буде надавати користувачам мінімальний рівень доступу та привілеїв, необхідних для виконання конкретних завдань, і автоматично скасовує його після виконання завдання.

Ізоляція додатків і робочих навантажень забезпечує безпосередній доступ до хмарних додатків, SaaS-платформ і внутрішніх робочих навантажень, уникаючи необхідності широкого мережевого доступу (наприклад, заміни традиційних VPN).

Також дана ціль може бути досягнута за рахунок ZTNA (Zero Trust Network Access) – це фреймворк кібербезпеки, який замінює традиційні VPN, суворо перевіряючи ідентифікацію та контекст кожного користувача та пристрою перед надходженням доступу до конкретних додатків.

Основні принципи ZTNA визначаються наступним:

– доступ автоматично блокується, якщо це не дозволено явно;

– користувачі отримують лише мінімальну кількість доступу, необхідну для виконання своїх обов'язків;

– доступ перевіряється не лише при вході а постійно контролюється на основі ідентифікації користувача, безпеки пристрою та контексту;

– користувачі підключаються безпосередньо до потрібних додатків, а не до самої корпоративної мережі, захищаючи базову інфраструктуру від публічного інтернету.

Наступним завданням до виконання якого має бути придатна мережа є сегментація та ізоляція мережі. Мікросегментація на основі ідентичності для поділу мереж на сильно ізольовані, невеликі сегменти (часто до одного пристрою або робочого навантаження), щоб обмежити здатність скомпрометованого актива спілкуватися з рештою мережі.

Запобігання горизонтальному переміщенню для блокування несанкціонованих, недовірених потоків даних, що запобігає горизонтальному переміщенню зловмисником по системах для отримання чутливих «коронних перлин» даних [6].

Щоб запобігти горизонтальному переміщенню у Cisco Packet Tracer, потрібно ізолювати сегменти мережі, обмежувати несанкціоновані підключення пристроїв і суворо обмежувати міжVLAN-комунікацію. Наступний основний, багаторівневий підхід зупиняє шкідливе ПЗ або зловмисника від переходу між пристроями:

Найефективніший спосіб запобігти бічному переміщенню – впровадити суворі списки контролю доступу (ACL), та чітко визначити, які підмережі можуть і не можуть спілкуватися. Використовувати розширені списки доступу слід на маршрутизаторах або комутаторах. Також слід заборонити трафік із менш довірених зон (наприклад, гостьові або IoT-VLAN) у більш критичні зони (наприклад, серверний VLAN) [4].

Слід переконатися, що всі пристрої знаходяться у своїх логічних доменах широкомовлення (VLAN). Це створює чітку межу, тобто трафік не може просто переміщатися з однієї робочої станції на іншу без проходження маршрутизатора

або фаєрвола. Призначити конкретні порти призначеним VLAN за допомогою доступу в режимі switchport. Використовуйте маршрутизацію Router-on-a-stick або комутатор рівня 3, щоб увесь трафік між VLAN проходив точку перевірки безпеки (наприклад, ACL).

Під час впровадження безпеки портів слід запобігати підключенню шкідливих пристроїв до існуючих мережевих переривів. Це заважає зловмиснику від'єднати принтер, підключити ноутбук і використати цей доступ для проведення розвідки. Обмежити кількість дозволених MAC-адрес на порт до 1. Встановити режим порушення на вимкнення, щоб порт переходив у стан err-disabled, якщо підключено зловживаний пристрій.

Створювана мережа має давати видимість і аналітику. Система має бути спроможна здіснювати Безперервний моніторинг для інспекції та реєстрації всього мережевого трафіку, сесій користувачів і активності пристроїв у режимі реального часу. Також має бути можливість виявлення загроз для використання автоматизованої аналітики для виявлення аномалій, виявлення сигналів шкідливого ПЗ та ідентифікації несанкціонованих або скомпрометованих пристроїв.

Також система має бути здатно до негайного вимикання робочих процесів з пом'якшенням наслідків (наприклад, ізоляцію скомпрометованого пристрою або завершення активної сесії) при виявленні загрози чи витоку.

Адаптивні коригування політики безпеки , які автоматично оновлюють мережеві фільтри та коригують рівень довіри на основі оцінки політики в реальному часі.

2.3 Наявний функціонал попередньо обраного програмного забезпечення

Cisco Packet Tracer повністю підтримує віртуальні локальні мережі (VLAN). Він дозволяє моделювати майже всі необхідні VLAN-конфігурації, які ви виконуєте на реальному корпоративному обладнанні Cisco.

Ви можете створювати та називати VLAN за допомогою стандартних команд IOS (наприклад, VLAN 10). Ви можете налаштувати порти комутатора як порти доступу до конкретних VLAN. Підтримує транкінг 802.1Q для передачі кількох VLAN між комутаторами, включно з налаштуванням нативних і дозволених VLAN. Ви можете маршрутизувати трафік між різними VLAN за допомогою комутатора рівня 3 або конфігурації маршрутизатора на стику. Ви можете сегментувати голосовий трафік від трафіку даних або налаштовувати керуючі SVI (віртуальні інтерфейси комутатора).

Cisco Packet Tracer не підтримує налаштування MFA у межах симульованих мережевих середовищ (наприклад, на віртуальних маршрутизаторах або комутаторах). Потрібно використовувати зовнішні сервери RADIUS/TACACS+ (наприклад, Cisco ISE, Cisco Duo або TACACS.net) [6].

У Cisco Packet Tracer справжня багатофакторна автентифікація (MFA), що містить позасмугові коди (наприклад, SMS або push-сповіщення), не може бути симулявана, оскільки програмне забезпечення не підтримує зовнішнє інтернет-з'єднання для таких сервісів.

Однак ви можете імітувати багатокроковий процес входу, який функціонально імітує «два фактори» того, що ви знаєте (пароль) та інший рівень доступу поєднуючи аутентифікацію AAA сервера (RADIUS/TACACS+) з локальною автентифікацією за паролем. Спочатку слід налаштувати AAA-сервер [20].

Далі слід додати сервер до топології та присвоїти йому IP-адресую Перейти у вкладку «Послуги» обрати та увімкнути сірвіс AAA. Також слід додати конфігурацію мережі (клієнт), тобто введсти ім'я вашого маршрутизатора (наприклад, Router1). В налаштуваннях слід ввести IP інтерфейсу вашого роутера. Вводимо спільний ключ (наприклад, cisco123) та вибрати тип сервера між RADIUS або TACACS+. Додайте користувача з ім'ям користувача: user1 та паролем: pass123.

Додатково слід реалізувати «другий фактор» (локально увімкнути секрет). Щоб імітувати MFA, слід застосувати AAA-вхід до лінії VTY (SSH/Telnet), але

для повного доступу потрібен окремий увімкнення секрету. Встановіть локальний пароль і застосуйте до лінії VTY.

Для тестування слід скористатися командним рядком SSH у маршрутизатор: ssh -l user1. Введіть пароль, визначений на AAA-сервері (pass123), як перший фактор. Після входу в режим User EXEC введіть enable. Далі буде запропоновано ввести другий пароль - введіть секрет увімкнути (SecondFactorPass) як другий фактор.

Cisco Packet Tracer повністю підтримує AAA (автентифікацію, авторизацію та облік). Він дозволяє налаштовувати локальні AAA, а також серверні AAA (наприклад, RADIUS або TACACS+), використовуючи симульовані сервери у створюваній топології [20].

Можливість увімкнути AAA глобально можливо за допомогою команди aaa new-model. Пристрої можуть автентифікуватися безпосередньо за базами даних користувачів, що зберігаються в локальній пам'яті маршрутизатора. Це було зроблено для створення подальшої можливості використовувати вбудований пристрій "AAA/RADIUS Server" (у меню кінцевих пристроїв) як централізований сервер автентифікації, авторизації та бухгалтерії. Packet Tracer підтримує протоколи, такі як RADIUS і TACACS+, для зв'язку між мережевими пристроями та AAA-сервером.

Cisco Packet Tracer підтримує обмежену кількість AAA-команд, а специфічний синтаксис для обліку команд часто призводить до помилок «недійсного введення» через непідтримувані ключові слова або неправильний порядок параметрів.

Конкретні команди aaa з обліку aaa accounting commands <level> ... часто не повністю реалізований у Packet Tracer. В процесі розробки слід переконатися, що використовуються старі команди клавіш хоста tacacs-server і tacacs-server, оскільки новіший синтаксис сервера tacacs зазвичай не підтримується в Packet Tracer.

Cisco Packet Tracer підтримує логування syslog. Ви можете налаштувати віртуальні пристрої Cisco (маршрутизатори, комутатори, фаєрволи) для

надсилання лог-повідомлень на виділений Syslog Server у вашій мережевій топології.

Packet Tracer підтримує ведення логування базових подій, таких як зміни статусу інтерфейсу, зміни конфігурацій та повідомлення на рівні налагодження.

Хоча Packet Tracer дуже точний для навчальної програми CCNA, він має трохи спрощене середовище IOS порівняно з реальним апаратним забезпеченням. Дуже специфічні або просунуті функції syslog, такі як успішний або невдалий вхід у SSH або порушення ACL, можуть не завжди працювати ідеально залежно від моделювання версії IOS.

Версія iOS в Cisco Packet Tracer не підтримує деякі конкретні команди. Хоча вони стандартними командами безпеки на реальному обладнанні Cisco, Packet Tracer – це симулятор з обмеженим набором команд.

Packet Tracer часто не має розширених функцій безпеки та управління, таких як повний «Login Block» або специфічні параметри логування при вході при успіху, які використовуються у більш потужних фізичних маршрутизаторах і комутаторах. Симулятор емулює базовий Cisco IOS. Команди, такі як login on-success log, можуть бути частково розпізнані або повністю відсутні залежно від конкретної моделі пристрою, яку ви обрали у робочому просторі.

Cisco Packet Tracer підтримує міжмережеві екрани політики на основі зон (ZPF). Ви можете налаштовувати карти класів, карти політик, зони безпеки та пари зон для динамічної фільтрації трафіку за допомогою підтримуваних моделей маршрутизаторів.

ZPF зазвичай працює на інтегрованих сервісних маршрутизаторах (ISR) 2800 та новіших, таких як серія 2900. Деякі підінтерфейси (наприклад, VLAN-інтерфейси на комутаторах або старіших моделях маршрутизаторів) можуть не приймати команду zone-member. Можливо, доведеться призначати фізичні FastEthernet або GigabitEthernet інтерфейси для зон. Ви групуєте інтерфейси в зони і застосовуєте політику інспекції стану до пар зон, що переміщуються між ними. Весь міжзональний трафік за замовчуванням блокується, якщо це не дозволено явно.

Cisco Packet Tracer не має повністю автоматизованого «майстра» для компіляції складних мережевих політик. Натомість ви автоматизуєте розгортання політик за допомогою вбудованого API Network Controller, Activity Wizard (для шаблонування) або вставляючи скриптовані команди IOS, щоб обійти ручну конфігурацію.

Найпоширеніший спосіб автоматизації конфігурацій політик у Packet Tracer – це використання текстового файлу CLI. Замість того, щоб вводити команди одну за одною, ви копіюєте заздалегідь написані політичні команди з текстового документа і вставляєте їх безпосередньо в CLI-консоль пристрою.

Створити текстовий файл з усіма командами конфігурації (наприклад, розширені списки доступу, карти маршрутів або міжмережеві екрани на основі зон). Для цього слід відкрити цільовий пристрій (роутер або комутатор), введіть увімкнути, а потім налаштувати термінал. Клацніть правою кнопкою миші у вікні терміналу та виберіть «Вставити», щоб автоматично запустити всі політики одночасно.

Також окремим пунктом хотілось би зазначити режим симуляції Cisco Packet Tracer, що дозволяє уповільнити час і крок за кроком спостерігати, як пакети даних проходять через створену мережу. Це найкращий діагностичний інструмент для перевірки таблиць маршрутизації, перевірки поведінки протоколів та усунення проблем із підключенням рівнів за шаром. Для його використання слід переключіться з режиму реального часу на режим симуляції (у нижньому правому куті), щоб візуально перевірити, як несанкціоновані пакети переходять з режиму реального часу в режим симуляції (у нижньому правому куті), щоб візуально перевірити, як несанкціоновані пакети скидаються.

2.4 Теоретична модель мережі

Незважаючи на відсутність підтримки деяких команд у Cisco Packet Tracer, все ще є можливість відтворити головні принципи Zero Trust для створюваної мережі.

Щоб відтворити Zero Trust у Cisco Packet Tracer, потрібно налаштувати суворі списки контролю доступу (ACL) на маршрутизаторах і комутаторах, щоб відображати принципи «відмова за замовчуванням» та «мінімальні привілеї». Симуляція суворо запобігає бічному переміщенню, блокуючи будь-який трафік, який явно не дозволений.

Реалізація мікросегментації залежить від розділу мережі на ізольовані сегменти, щоб пристрої (наприклад, користувачі, сервери та гостьові мережі) не могли спілкуватися, якщо це не дозволено. В подільшому слід створити VLAN на обраному основному комутаторі, а у даному випадку одному з центральних комутаторів третього рівня та призначит порти доступу відповідним VLAN і налаштувати транкові порти для маршрутизації між VLAN.

Також слід застосувати список доступу до вашого маршрутизатора або комутатора рівня 3, який за замовчуванням обмежує весь трафік. Визначити правила розширеного списку доступів (наприклад, access-list 100 permit ip-хост 192.168.1.10 10.0.0.5), що будуть надавати доступ лише необхідному, перевіреному трафіку під час процесу комунікації. Слід додати будь-яке правило для заборони IP, щоб гарантувати, що спроби несанкціонального доступу не зазнають успіху. Далі слід прив'язати ACL до відповідного інтерфейсу за допомогою команди ip access-group in.

Теоретична модель створюваної мережі буде складатись з кількох комутаторів другого рівня двох серверів (перший для втілення деякого функціоналу з логуванням та збереження облікових записів користувачів та другий для імітації підключення до інтернету), одного комутатора третього рівня, який у данному випадку буде слугувати яу точка використання безпекових політик мережі та буде брати на себе функціонал роутера для легшого переміщення даних по мережі.

Беручи до уваги кінцеві пристрої, їх кількість не буде мати значення, оскільки використання безпекових політик мережі буде залежати від підмережі до якої є під’єднаним даний пристрій. Три комутатори другого рівня буде необхідно використати для налаштування відділів компанії і відповідно до цього лише один

порт комутатора другого рівня буде здатен передавати дані по кільком підмережам і це буде порт по якому виконується під'єднання до центрального комутатора в цілях можливості доступу до функціоналу серверу та доступу адміністрації до налаштування комутатора. Всі інші порти комутаторів другого рівня будуть налаштовані виключно на підмережу даного відділу.

З усієї мережі один з комутаторів другого рівня буде відведено виключно для адміністрації. Даному комутатору буде надано найбільше свободи у переміщенні по мережі оскільки у всіх списках доступів по всіх комутаторах трафіку підмережі адміністрації буде надано повний доступ на переміщення та можливість налаштування комутаторів. Недолік відносно можливості зловмисника використати доступ адміністрації буде обійдено через відсутність налаштувань портів комутаторів для підмережі адміністрації, та відсутність функціоналу сервісу DHCP на підмережі адміністрації.

В налаштуваннях всіх комутаторів другого рівня було передбачено зовнішній доступ через протокол SSH для якого буде попередньо налаштовано IP адреси двох наявних комп'юторів адміністрації через розширений список доступу в якому будуть записані IP-адреси адміністрації та буде записоно у віртальній консолі.

Як вже було написано раніше комутатор третього рівня буде слугувати як точка використання безпекових політик мережі та буде брати на себе функціонал роутера для легшого переміщення даних по мережі, і через це він буде розташований в центрі мережі і всі комутатори другого рівня будуть під'єднані до нього через порти GigabitEthernet. Також в ньому буде прописана основна частина списків доступу. Список доступу для адміністрації буде надавати доступ до передачу будь-якого трафіку через мережу. В свою чергу, списки доступів для інших відділів будуть практично ідентичні з забороною передачі даних між підмережами (відділами) та доступом до інтернету на портах 80 (www) і 443 (https) для доступу до програмного забезпечення даного відділу. Навідміну від інших, відділ охорони не буде мати доступу до інтернету.

До підмереж записаних у базу даних даного комутатора будуть входити всі попередньо зазначені підмережі з відповідними IP адресами на сабпортах для можливості застосування розширених списків доступу на всю підмережу навідміну від окремих портів, що дасть можливість більш ефективно фільтрувати вхідний трафік окремих підмереж. В даному випадку така схема буде мати такий вигляд:

1. 10 (Адміністрація), IP-адреса сабпорта – 192.168.10.254
2. 20 (Охорона), IP-адреса сабпорта – 192.168.20.254
3. 30 (Фінанси), IP-адреса сабпорта – 192.168.30.254
4. 40 (Загальний відділ), IP-адреса сабпорта – 192.168.40.254
5. 50 (Сервер), IP-адреса сабпорта – 192.168.50.254

Щоб гарантувати можливість адміністрації на використання SSH та облегшити маніпуляції з мережею подальший вибір IP-адрес для сабпортів комутаторів другого рівня буде відбуватись подібним чином у порядку спадання, тобто:

1. Адміністрація – 192.168.10.253
2. Охорона – 192.168.10.252
3. Фінанси – 192.168.10.251
4. Загальний відділ – 192.168.10.250

Список доступу для сервера буде надавати доступ до трафіку, що відповідає функціоналу серверів, на даний момент даний трафік передається на портах 49 (tacacs+) і 68 (DHCP).

Хоча основна більшість списків доступів буде створена та застосована на центральних комутаторах у даному випанку при комунікації всередині відділу обмежень на види трафіку введено не буде, хоча буде вимагатись введення облікових даних користувача, таким чином забезпечуючи функціонування внутрішніх структур відділу з певним рівнем безпеки.

Кожному відділу буде надаватись набір з певної початкової кількость комп’ютерів для особистого використання, який в подальшому можна буде розширити за допомогою використання попередньо налаштуваного сервісу

DHCP. Також поза особистими комп'ютерами буде надаватись додаткове обладнання відповідно до функції данного відділу в компанії (наприклад фінансовий відділ буде мати принтер, а відділ охорони буде мати камери).

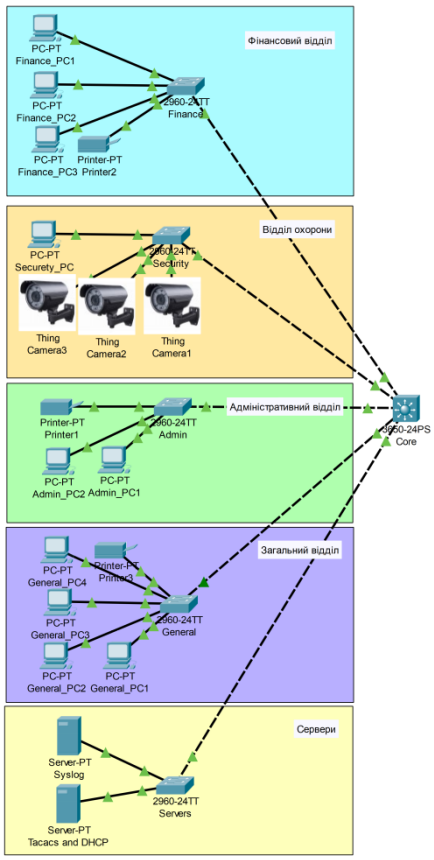


Рисунок 2.1 – Теоретична схема розділу відділу створюваної мережі на зони;

Розділ створюваної мережі на зони буде відбуватизь за рахунок розширених списків доступу, що будуть налаштовуватись індивідуально на кожнаму з наведених комутаторів. До налаштуваню кожного з комутаторів другого рівня буде створено зонову пару в якій серед умов буде зазначена необхідність у введенні облікових даних користувача для передачі будь-яких даних.

В свою чергу на комутаторі тертього рівня буде передбачений список доступу, що буде виконувати перевірку передачі трафіку на порті під'єднаному до інших філій. Подальша перевірка трафіку та передача інформації на сервер і з серверу буде виконуватись за рахунок списків доступу та налаштувань інших комутаторів.

2.5 Висновки до другого розділу

В ході виконання другого розділу, використовуючи за основу дослідження виконані у першому розділі, було визначено основні функції системи, розробено модель функцій, які система повинна виконувати та сформовано низку функціональних вимог, які виконувана мережа має дотримуватись.

Додатково було розроблено теоретичну модель виконуваної мережі включаючи розділ на підмережі, функціонал фільтрування трафіку при його переході між вищеназваними підмережами та приблизна модель налаштувань кожного з сервісів використовуваних на серверах мережі. У створюваній мережі даний функціонал буде нараховувати віддалене збереження і доступ до облкових записів користувачів, логування внутрішніх подій та трафік, що проходить на матеріальному забезпеченні. Також даний функціонал буде нараховувати автоматичну видачу IP-адрес на нові під’єднані кінцеві пристрої.

В ході створення теоретичну модель виконуваної мережі було дотримано вимог та функціоналу для створення мережі по принципу Zero Trust, що входить у функціонал попередньо обраного програмного забезпечення для її створення.

3 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ КОНЦЕПЦІЇ «НУЛЬ ДОВІРИ»

3.1 Розробка мережі

Безпечна корпоративна мережа потребує відповідної інфраструктури, що буде здатна забезпечити стабільність та безпеку для всіх її зон. Для розділення трафіку підмереж (VLAN) при використанні IP роутингу на комутаторі трецього рівня було вирішено використати списки доступу (ACL), що дозволить розподілити доступ працівників компанії до відповідних ресурсів в локальній мережі, покращити контроль доступу та захист даних.

Фінансовий та загальний відділ будуть приймати на себе основне робоче навантаження мережі, тому дані підмережі є ізольованими оскільки є найбільш легкодоступними для зовнішнього впливу.

Для загального та фінансового відділів мережу є необхідність у наявності провідного підключення до інтернету з швидкістю до 1 Гбіт/с з обмеженням лише до певних додатків. Така швидкість гарантуватиме відповідну нормі роботу елементів мережевої системи навіть при високих навантаженнях.

Централізація логування трафіку корпоративної мережі була виконана через сервер. Централізація керування мережею була виконана через виокремлення підмережі адміністрації з можливістю підключення до кожного комутатора мережі через зашифрований канал SSH. Цей метод надає можливість проведення досить простого обслуговування і контролю локальної мережі, дозволяючи адміністратору ефективно виявляти і усувати можливі проблеми.

Під час створення захисту даної мережі були використані сучасні системи безпеки. Дані міри забезпечать роботу мережі з мінімальними ризиками для стабільності та конфіденційності присутній в ній та використовючих її користувачів. Інформацію щодо створених підмереж та їх призначення у даній мережі буде представлено в таблиці 3.1.

Таблиця 3.1 – Список підмереж

VLAN	Призначення
10	Адміністративна підмережа, для проведення віддаленого налаштування.
20	Підмережі охорони
30	Підмережа фінансового відділу
40	Підмережа загального відділу
50	Підмережа відведена під сервер лагування та збереження облікових данних працівників

Для забезпечення коректної роботи внутрішніх процесів даної мережі та забезпечення їх конфіденційного виконання було розроблено мережеву структуру, що розділяє трафік на кілька окремих підмереж. Ізоляція та фільтрація трафіку мережі була досягнена завдяки розділенню на підмережі (VLAN), списків доступу (ACL) та розділення на зони (Zone Based Policies), що в свою чергу покращило безпеку та спростило адміністрування усіх підключених пристроїв. Далі буде наведеня деталізація структури мережі.

1. VLAN 10 (підмережа адміністрації) – об’єднує обладнання адміністрації та комутатори мережі. Трафік є ізольованим від інших підмереж для забезпечення стабільної роботи. Надає безпечний доступ до налаштувань комутаторів.

2. VLAN 20 (підмережа охорони) – об’єднує робоче місце працівника охорони та камери розташовані по всьому приміщенню. Повний доступ наданий лише адміністрації. Включає маршрутизацію лише по внутрішній локальній мережі. Забезпечує спостереження по всій будівлі.

3. VLAN 30 (підмережа фінансового відділу) – об’єднує комп’ютери працівників корпорації та принтер для особистого користування відділу. Трафік

ізольований всередині підмережі для захисту даних банку і зниження ризику атак на систему. Повний доступ наданий лише адміністрації. Забезпечує доступ працівників до інтернету та локальної мережі.

4. VLAN 40 (підмережа загального відділу) – об'єднує комп'ютери працівників корпорації та принтер для особистого користування відділу. Трафік ізольований всередині підмережі для захисту даних банку і зниження ризику атак на систему. Повний доступ наданий лише адміністрації. Забезпечує доступ працівників до інтернету та локальної мережі.

5. VLAN 50 (підмережа серверу) – займається логуванням та збереження даних, та аутентифікацією особистості користувачів. Повний доступ наданий лише адміністрації. Забезпечує доступ працівників до їх облікових записів.

3.2 Налаштування матеріального обладнання

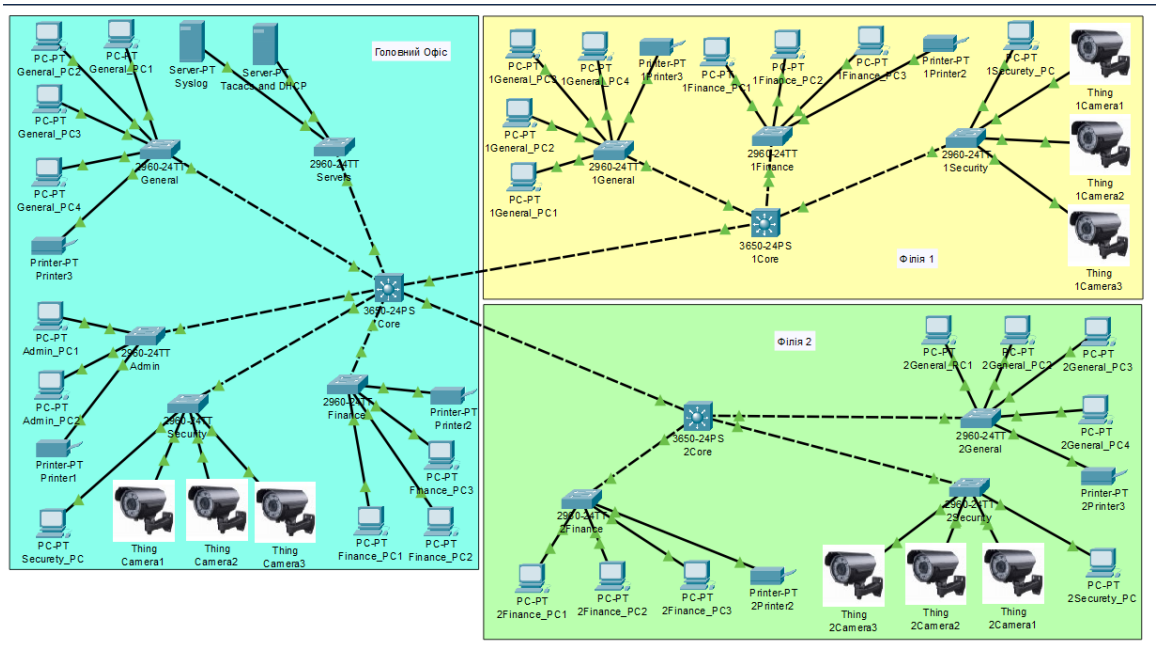


Рисунок 3.1 –Структура створюваної мережі;

Для виконання поставленого завдання для даної мережі було прийняте рішення встановити п'ять комутаторів, по комутатору другого рівня на підмережу та комутатор третього рівня як точка перевірки та фільтрації трафіку.

В цілях облегшування маніпулювання мережею було необхідно виконати органцізацію кінцевих пристроїв у відповідності з їх функцією в даній мережі. Таблицю з назвами кінцевих пристроїв, їх підмережами, IP-адресами, підключенням до комутатора та портом даного комутатора буде наведено нижче.

Таблиця 3.2 – Параметри кінцевих пристроїв;

Назва кінцевого пристрою	Сегмент мережі	IP адреса	Комутатор (до якого підключений кінцевий пристрій)	Порт на комутаторі використаний для підключення
Admin_PC1	10 (Адміністрація)	192.168.10.1	2960-24TT – Admin	FastEathernet 0/1
Admin_PC2	10 (Адміністрація)	192.168.10.2	2960-24TT – Admin	FastEathernet 0/2
Printer1	10 (Адміністрація)	192.168.10.3	2960-24TT – Admin	FastEathernet 0/3
Security_PC	20 (Охорона)	192.168.20.1	2960-24TT – Security	FastEathernet 0/1
Camera1	20 (Охорона)	192.168.20.2	2960-24TT – Security	FastEathernet 0/2
Camera2	20 (Охорона)	192.168.20.3	2960-24TT – Security	FastEathernet 0/3
Camera3	20 (Охорона)	192.168.20.4	2960-24TT – Security	FastEathernet 0/4
Finance_PC1	30 (Фінансовий відділ)	192.168.30.1	2960-24TT – Finance	FastEathernet 0/1
Finance_PC2	30 (Фінансовий відділ)	192.168.30.2	2960-24TT – Finance	FastEathernet 0/2
Finance_PC3	30 (Фінансовий відділ)	192.168.30.3	2960-24TT – Finance	FastEathernet 0/3
Printer2	30 (Фінансовий відділ)	192.168.30.4	2960-24TT – Finance	FastEathernet 0/4
General_PC1	40 (Загальний відділ)	192.168.40.1	2960-24TT – General	FastEathernet 0/1
General_PC2	40 (Загальний відділ)	192.168.40.2	2960-24TT – General	FastEathernet 0/2
General_PC3	40 (Загальний відділ)	192.168.40.3	2960-24TT – General	FastEathernet 0/3
General_PC4	40 (Загальний відділ)	192.168.40.4	2960-24TT – General	FastEathernet 0/4

Кінець таблиці 3.2

Printer3	40 (Загальний відділ)	192.168.40.5	2960-24TT – General	FastEathernet 0/5
Server-Tacacs+	50 (Сервер)	192.168.50.10	3650-24PS – Core	GigabitEthernet 1/0/24

Під час налаштування комутатора адміністрації слід налаштувати ім’я хоста на Admin та підключити пароль через команду «secret». В подальшому на локальному сховищі слід налаштувати три окремих аккаунта, а саме аккаунт для адміністрації з максимальним рівнем привілеїв, для техніків з сьомим рівнем привілоеїв, який буде налаштований далі, та гостьовий аккаунт з першим рівнем привілеїв.

Налаштування підмереж данного комутатора вимагає введення лише двох, а саме 10-ї (адміністраторської підмережі) та 50-ї (підмережа сервера) для доступу до сервісу AAA та можливістю передачі трафіку підмережі адміністрації. Для субпорту 10-ї підмережі слід дати IP-адресу 192.168.10.253 та для 50-ї 192.168.50.253.

Для налаштування доступу адміністрації до комутатора через SSH слід задати ім’я домену «admin» та згенерувати криптоключ RSA з параметром кількості виставленим на 1024. Також для коректного надання доступу до налаштування комутаторів лише адміністраторам слід налаштувати розширений список доступу «SSH_ONLY» та вписати в нього доступ до tcp на порті 22 лише для таких адрес: 192.168.10.1, 192.168.10.2. Наведені адреси є адресами комп’ютерів адміністрації. В кінці даного списку слід додати команду «deny any any», що буде виконувати функцію блокування любого іншого трафіку, що не відповідає тому, що був уже визначений як дозволений раніше. В подальшому цей список доступу слід вписати в лінії віртуального терміналу 0 – 15 та задати віддалений доступ до комутатора лише через SSH.

Правильне налаштування портів буде відбуватись наступним чином: порти FastEthernet 0/1 – 3 будуть мати режим доступу «access», з доступом лише до 10-ї підмережі, а GigabitEthernet 0/1 матиме режим доступу «trunk» з дозволеними 10-

ю та 50-ю підмережами для доступу до сервера з обліковими даними та можливістю передачі трафіку підмережі адміністрації.

Логування буде відбуватись одночасно через syslog, що буде займатись логуванням локальних подій на матеріальному забезпеченні, та через аккаунтингову частину AAA, що буде займатись логуванням використання облікових даних користувачів. Для налаштування syslog слід задати IP-адресу серверу логування як 192.168.50.10, ввімкнути trap debugging та ввімкнути сервіс timestamps з часом записаним в мілісекуднах. Також слід окремо налаштувати логівання успішних та невдалих спроб логіну в систему комутатора.

Для налаштування доступу до бази данних аккаунтів на сервері AAA слід налаштувати сервер протоколу tacacs+ на туж IP-адресу, що і syslog та задати ключ «adadad», що буде відповідним до ключа налаштованого на сервері для профілю користувача з підмережі адміністрації. Далі слід задати параметри логіну через AAA для використання бази даних серверу, а у випадку, якщо сревер недоступний використовувати локальні облікові записи та вписати дані параметри в лінії віртуального терміналу 0 – 15.

До AAA аккаунтингу слід також додати параметри запису початку та завершення сессій, запису введених команд для аккаунтів з рівнями привілеїв 15, 7 та 1 у відповідності до попередньо налаштуваних облікових записів під час налаштування комутатора.

Додатково у параметрах комутатора слід визначити IP-адресу default gateway як 192.168.10.254, для визначення необхідності перенаправлення всього трафіку за замовчуванням до центрального комутатора для подальшої фільтрації, та блокування спроб входу в обліковий запис на 60 секунд у випадку, якщо буде виконано три спроби в проміжку десяти секунд.

Даний комутатор буде визначений як один із головних елементів мережі оскільки трафік з нього буде мати доступ до всіх частин створюваної мережі та подальше налаштування мережі буде відбуватись з підмережі цього комутатора.

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	10	--	0005.5E12.5901
FastEthernet0/2	Up	10	--	0005.5E12.5902
FastEthernet0/3	Up	10	--	0005.5E12.5903
FastEthernet0/4	Down	1	--	0005.5E12.5904
FastEthernet0/5	Down	1	--	0005.5E12.5905
FastEthernet0/6	Down	1	--	0005.5E12.5906
FastEthernet0/7	Down	1	--	0005.5E12.5907
FastEthernet0/8	Down	1	--	0005.5E12.5908
FastEthernet0/9	Down	1	--	0005.5E12.5909
FastEthernet0/10	Down	1	--	0005.5E12.590A
FastEthernet0/11	Down	1	--	0005.5E12.590B
FastEthernet0/12	Down	1	--	0005.5E12.590C
FastEthernet0/13	Down	1	--	0005.5E12.590D
FastEthernet0/14	Down	1	--	0005.5E12.590E
FastEthernet0/15	Down	1	--	0005.5E12.590F
FastEthernet0/16	Down	1	--	0005.5E12.5910
FastEthernet0/17	Down	1	--	0005.5E12.5911
FastEthernet0/18	Down	1	--	0005.5E12.5912
FastEthernet0/19	Down	1	--	0005.5E12.5913
FastEthernet0/20	Down	1	--	0005.5E12.5914
FastEthernet0/21	Down	1	--	0005.5E12.5915
FastEthernet0/22	Down	1	--	0005.5E12.5916
FastEthernet0/23	Down	1	--	0005.5E12.5917
FastEthernet0/24	Down	1	--	0005.5E12.5918
GigabitEthernet0/1	Up	--	--	0005.5E12.5919
GigabitEthernet0/2	Down	1	--	0005.5E12.591A
Vlan1	Down	1	<not set>	0001.C715.7D4B
Vlan10	Up	10	192.168.10.253/24	0001.C715.7D01
Vlan50	Up	50	192.168.50.253/24	0001.C715.7D02

Рисунок 3.2 – Налаштування портів комутатора адміністрації;

Налаштування комутаторів Охорони, Загального та Фінансового відділів будуть виконуватись по приблизна тому-ж принципу за виключенням наступних вийнятків.

Під час налаштування комутатора Охорони слід налаштувати ім’я хоста на Security. Налаштування підмереж данного комутатора вимагає введення трьох, а саме 10-ї (адміністраторської), 20-ї (підмережа охорони) та 50-ї (підмережа сервера) для доступу до AAA. Для субпорту 10-ї підмережі слід дати IP-адресу 192.168.10.252 та для 50-ї 192.168.20.252.

Для налаштування доступу адміністрації до комутатора через SSH слід задати ім’я домену «security». Правильне налаштування портів буде відбуватись наступним чином: порти FastEthernet 0/1 – 4 будуть мати режим доступу «access», з доступом лише до 20-ї підмережі, а GigabitEthernet 0/1 матиме режим доступу «trunk» з дозволеними 10-ю, 20-ю та 50-ю підмережами для доступу для адміністрації та до сервера з обліковими даними.

Для налаштування доступу до бази данних аккаунтів на сервері AAA слід налаштувати сервер протоколу tacacs+ на туж IP-адресу, що і syslog та задати ключ «sesese».

У налаштуваннях комутатора слід визначити IP-адресу default gateway як 192.168.20.254. В свою чергу, налаштування логування syslog та AAA буде відбуватись таким-же чином як на комутаторі адміністрації.

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	20	--	0060.5C92.2C01
FastEthernet0/2	Up	20	--	0060.5C92.2C02
FastEthernet0/3	Up	20	--	0060.5C92.2C03
FastEthernet0/4	Up	20	--	0060.5C92.2C04
FastEthernet0/5	Down	1	--	0060.5C92.2C05
FastEthernet0/6	Down	1	--	0060.5C92.2C06
FastEthernet0/7	Down	1	--	0060.5C92.2C07
FastEthernet0/8	Down	1	--	0060.5C92.2C08
FastEthernet0/9	Down	1	--	0060.5C92.2C09
FastEthernet0/10	Down	1	--	0060.5C92.2C0A
FastEthernet0/11	Down	1	--	0060.5C92.2C0B
FastEthernet0/12	Down	1	--	0060.5C92.2C0C
FastEthernet0/13	Down	1	--	0060.5C92.2C0D
FastEthernet0/14	Down	1	--	0060.5C92.2C0E
FastEthernet0/15	Down	1	--	0060.5C92.2C0F
FastEthernet0/16	Down	1	--	0060.5C92.2C10
FastEthernet0/17	Down	1	--	0060.5C92.2C11
FastEthernet0/18	Down	1	--	0060.5C92.2C12
FastEthernet0/19	Down	1	--	0060.5C92.2C13
FastEthernet0/20	Down	1	--	0060.5C92.2C14
FastEthernet0/21	Down	1	--	0060.5C92.2C15
FastEthernet0/22	Down	1	--	0060.5C92.2C16
FastEthernet0/23	Down	1	--	0060.5C92.2C17
FastEthernet0/24	Down	1	--	0060.5C92.2C18
GigabitEthernet0/1	Up	--	--	0060.5C92.2C19
GigabitEthernet0/2	Down	1	--	0060.5C92.2C1A
Vlan1	Down	1	<not set>	0000.0C30.B5DB
Vlan10	Up	10	192.168.10.252/24	0000.0C30.B501
Vlan50	Up	50	192.168.50.252/24	0000.0C30.B502

Рисунок 3.3 – Налаштування портів комутатора охорони;

Під час налаштування комутатора фінансового відділу слід налаштувати ім’я хоста на Finance. Налаштування підмереж данного комутатора вимагає введення трьох, а саме 10-ї (адміністраторської), 30-ї (підмережа фінансового відділу) та 50-ї (підмережа сервера) для доступу до AAA. Для субпорту 10-ї підмережі слід дати IP-адресу 192.168.10.251 та для 50-ї 192.168.20.251.

Для налаштування доступу адміністрації до комутатора через SSH слід задати ім’я домену «finance». Правильне налаштування портів буде відбуватись наступним чином: порти FastEthernet 0/1 – 4 будуть мати режим доступу «access»,

з доступом лише до 30-ї підмережі, а GigabitEthernet 0/1 матиме режим доступу «trunk» з дозволеними 10-ю, 30-ю та 50-ю підмережами для доступу для адміністрації та до сервера з обліковими даними.

Для налаштування доступу до бази данних аккаунтів на сервері AAA слід налаштувати сервер протоколу tacacs+ на туж IP-адресу, що і syslog та задати ключ «fififi».

У налаштуваннях комутатора слід визначити IP-адресу default gateway як 192.168.30.254.

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	30	--	0060.7061.1C01
FastEthernet0/2	Up	30	--	0060.7061.1C02
FastEthernet0/3	Up	30	--	0060.7061.1C03
FastEthernet0/4	Up	30	--	0060.7061.1C04
FastEthernet0/5	Down	1	--	0060.7061.1C05
FastEthernet0/6	Down	1	--	0060.7061.1C06
FastEthernet0/7	Down	1	--	0060.7061.1C07
FastEthernet0/8	Down	1	--	0060.7061.1C08
FastEthernet0/9	Down	1	--	0060.7061.1C09
FastEthernet0/10	Down	1	--	0060.7061.1C0A
FastEthernet0/11	Down	1	--	0060.7061.1C0B
FastEthernet0/12	Down	1	--	0060.7061.1C0C
FastEthernet0/13	Down	1	--	0060.7061.1C0D
FastEthernet0/14	Down	1	--	0060.7061.1C0E
FastEthernet0/15	Down	1	--	0060.7061.1C0F
FastEthernet0/16	Down	1	--	0060.7061.1C10
FastEthernet0/17	Down	1	--	0060.7061.1C11
FastEthernet0/18	Down	1	--	0060.7061.1C12
FastEthernet0/19	Down	1	--	0060.7061.1C13
FastEthernet0/20	Down	1	--	0060.7061.1C14
FastEthernet0/21	Down	1	--	0060.7061.1C15
FastEthernet0/22	Down	1	--	0060.7061.1C16
FastEthernet0/23	Down	1	--	0060.7061.1C17
FastEthernet0/24	Down	1	--	0060.7061.1C18
GigabitEthernet0/1	Up	--	--	0060.7061.1C19
GigabitEthernet0/2	Down	1	--	0060.7061.1C1A
Vlan1	Down	1	<not set>	0009.7C4E.685C
Vlan10	Up	10	192.168.10.251/24	0009.7C4E.6801
Vlan50	Up	50	192.168.50.251/24	0009.7C4E.6802

Рисунок 3.4 – Налаштування портів комутатора фінансового відділу;

Під час налаштування комутатора Загального відділу слід налаштувати ім’я хоста на General. Налаштування підмереж данного комутатора вимагає введення трьох, а саме 10-ї (адміністраторської), 40-ї (підмережа загального відділу) та 50-ї (підмережа сервера) для доступу до AAA. Для субпорту 10-ї підмережі слід дати IP-адресу 192.168.10.250 та для 50-ї 192.168.20.250.

Для налаштування доступу адміністрації до комутатора через SSH слід задати ім’я домену «finance». Правильне налаштування портів буде відбуватись наступним чином: порти FastEthernet 0/1 – 5 будуть мати режим доступу «access»,

з доступом лише до 40-ї підмережі, а GigabitEthernet 0/1 матиме режим доступу «trunk» з дозволеними 10-ю, 40-ю та 50-ю підмережами для доступу для адміністрації та до сервера з обліковими даними.

Для налаштування доступу до бази данних аккаунтів на сервері AAA слід налаштувати сервер протоколу tacacs+ на туж IP-адресу, що і syslog та задати ключ «gegege».

У налаштуваннях комутатора слід визначити IP-адресу default gateway як 192.168.40.254.

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	40	--	0030.F21A.A401
FastEthernet0/2	Up	40	--	0030.F21A.A402
FastEthernet0/3	Up	40	--	0030.F21A.A403
FastEthernet0/4	Up	40	--	0030.F21A.A404
FastEthernet0/5	Up	40	--	0030.F21A.A405
FastEthernet0/6	Down	1	--	0030.F21A.A406
FastEthernet0/7	Down	1	--	0030.F21A.A407
FastEthernet0/8	Down	1	--	0030.F21A.A408
FastEthernet0/9	Down	1	--	0030.F21A.A409
FastEthernet0/10	Down	1	--	0030.F21A.A40A
FastEthernet0/11	Down	1	--	0030.F21A.A40B
FastEthernet0/12	Down	1	--	0030.F21A.A40C
FastEthernet0/13	Down	1	--	0030.F21A.A40D
FastEthernet0/14	Down	1	--	0030.F21A.A40E
FastEthernet0/15	Down	1	--	0030.F21A.A40F
FastEthernet0/16	Down	1	--	0030.F21A.A410
FastEthernet0/17	Down	1	--	0030.F21A.A411
FastEthernet0/18	Down	1	--	0030.F21A.A412
FastEthernet0/19	Down	1	--	0030.F21A.A413
FastEthernet0/20	Down	1	--	0030.F21A.A414
FastEthernet0/21	Down	1	--	0030.F21A.A415
FastEthernet0/22	Down	1	--	0030.F21A.A416
FastEthernet0/23	Down	1	--	0030.F21A.A417
FastEthernet0/24	Down	1	--	0030.F21A.A418
GigabitEthernet0/1	Up	--	--	0030.F21A.A419
GigabitEthernet0/2	Down	1	--	0030.F21A.A41A
Vlan1	Down	1	<not set>	0001.C927.971D
Vlan10	Up	10	192.168.10.250/24	0001.C927.9701
Vlan50	Up	50	192.168.50.250/24	0001.C927.9702

Рисунок 3.5 – Налаштування портів комутатора загального відділу;

Під час налаштування центрального комутатора слід налаштувати ім’я хоста на Core. Налаштування підмереж данного комутатора вимагає введення всіх раніше названих підмереж, а саме 10-ї (адміністраторської), 20-ї (пімережі охорони), 30-ї (підмережа фінансового відділу), 40-ї (підмережа загального відділу), 50-ї (підмережа сервера) та 99-ї (підмережа, що відповідає за інтернет) для доступу до AAA. Для субпорту 10-ї підмережі слід дати IP-адресу

192.168.10.254, для 20-ї 192.168.20.254, для 30-ї 192.168.30.254, для 40-ї 192.168.40.254 та для 50-ї 192.168.50.254.

Для налаштування доступу адміністрації до комутатора через SSH слід задати ім’я домену «core». Правильне налаштування портів буде відбуватись наступним чином: порти GigabitEthernet 1/0/1 – 4 матимуть режим доступу «trunk», порт під номером 1/0/1 матиме дозволеними підмережі 10-ту та 50-ту у відповідності до комутатора адміністрації, порт 1/0/2 матиме 10-ту, 20-ту та 50-ту, порт 1/0/3 матиме 10-ту, 30-ту та 50-ту, порт 1/0/4 матиме 10-ту, 40-у та 50-ту.

Для налаштування доступу до бази данних аккаунтів на сервері AAA слід налаштувати сервер протоколу tacacs+ на туж IP-адресу, що і syslog та задати ключ «сососо».

Оскільки налаштовуваний комутатор є центральним, через нього буде проходити переважна більшість трафіку мережі і через це розширені списки доступу будуть переважно використані на ньому.

Під час налаштування буде необхідним створити шість розширених списків доступу для кожної підмережі та ще один список описаній раніше для доступу адміністрації до комутатора через SSH. Серед списків доступу буде передбачено список для підмережі адміністрації в якому буде прописано лише одна умова, щоб список пропускав любий трафік з мережі адміністрації. Список доступу для підмережі охорони буде давати доступ пакетам tcp з 20-ї до 50-ї підмереж на порту 49 (tacacs+) та дозвіл на передачу пакетів всередині підмережі, заборони будуть видані на переміщення данних між підмережею охорони (20) та підмережами фінансового (30) та загального (40) відділів. В кінці окремо слід прописати заборону на передачу пакетів по ip від будь-якого до буль-якого IP оскільки в списку умови виконуються зверху вниз і дана умова просто заблокує трафік який не було визначено як дозволений раніше.

Список доступу для фінансового відділу буде давати доступ пакетам tcp з 30-ї до 50-ї підмереж на порту 49 (tacacs+) та доступ пакетам tcp з 30-ї до 99-ї підмережі на порту 80 і 443 (https). Заборони будуть видані на переміщення

данних з підмережі фінансового (30) відділу до підмережі охорони (20) та загального (40) відділу.

Список доступу для загального відділу буде давати доступ пакетам tcp з 40-ї до 50-ї підмереж на порту 49 (tacacs+) та доступ пакетам tcp з 40-ї до 99-ї підмережі на порту 80 і 443 (https). Заборони будуть видані на переміщення данних з підмережі загального (40) відділу до підмережі охорони (20) та фінансового (30) відділу.

Розширений список доступу сервера буде лише надавати доступ трафіку tcp з серверу до інших підмереж на порті 49 та надасть повний доступ адміністрації.

Розширений список доступу до інтернету дозволить доступ до трафіку інтернету на портах 80 (https) та 443 (www) для підмережі адміністрації, загального і фінансового відділів.

В рамках даного завдання, слід налаштувати видачу IP адрес за допомогою протоколу DHCP, в сервері що ми попередньо додали у мережу. Для цього спочатку необхідно оголосити використання двох наборів адрес для підмереж 30 та 40 (Pool Name, Default Gateway, DNS Server та Start IP Address).

Таблиця 3.3 – Таблиця параметрів налаштування DHCP в сервері;

Pool Name	Default Gateway	DNS Server	Start IP Address
FinancePool	192.168.30.254	0.0.0.0	192.168.30.0
GeneralPool	192.168.40.254	0.0.0.0	192.168.40.0
FinancePool1	192.168.31.254	0.0.0.0	192.168.31.0
GeneralPool1	192.168.41.254	0.0.0.0	192.168.41.0
FinancePool2	192.168.32.254	0.0.0.0	192.168.32.0
GeneralPool2	192.168.42.254	0.0.0.0	192.168.42.0

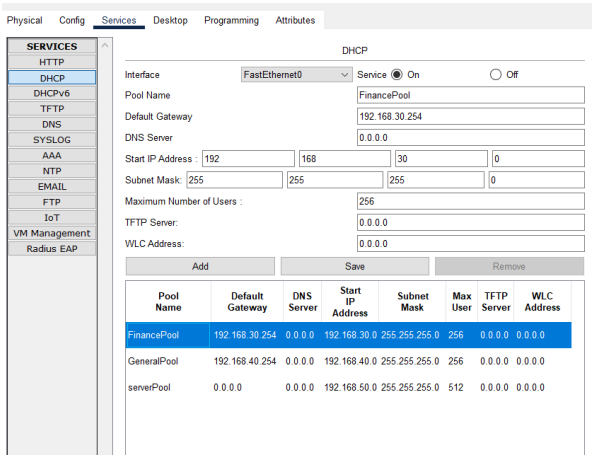


Рисунок 3.6 – Процес додавання наборів адрес до серверу;

В подальшому до налаштувань центрального комутатора на сабпорти підмереж які ми використовуєма слід додати команди, що визначають ip helper-address для портів GigabitEthernet якими вони під’єднані до центрального комутатора. У даному випадку для VLAN 30 та 40 ip helper-address буде визначено як 192.168.50.10.

Налаштування зонових політик безпеки вимагає визначення портів комутаторів мережі які будуть відповідати зовнішнім та внутрішнім з’єднанням. В даному випадку портом зовнішнього з’єднання буде виступати GigabitEthernet 1/0/24 на цетральному комутаторі. Портами внутрішнього з’єднання будуть виступати порти під’єднані доінших комутаторів та сервера, а саме: GigabitEthernet 1/0/1 – 4 та GigabitEthernet 1/0/23 на цетральному комутаторі.

Процес налаштування зонових політик безпеки також включає налаштування розширеного списку доступу в якому прописується доступ підмережі 99 (інтернет) до підмереж 30 (фінансовий відділ) та 40 (загальний відділ) лише на портах 80 (https) та 443 (www) для обмеження використовуваного трафіку інтернету в мережі лише до сайтів.

Далі слід налаштувати зонову пару та застосувати раніше створений розширений список доступу для того, щоб трафік який проходіть через цю пару проходив постійну перевірку на відповідність до умов списку.

3.3 Підбір матеріального забезпечення

Lenovo M715 SFF є надійною комп’ютерною системою, що включає в собі поєднання компактності та продуктивності, що ідеально підходить для використання в бізнес-середовищі. При покупці доступні три варіанти з різними процесорами, такими як:

– AMD Bristol Ridge PRO A12, A10, A8, A6;

– AMD Carrizo DDR4 PRO A12, A10, A6;

– AMD Summit Ridge Ryzen 7, Ryzen 5, Ryzen 3.

Що дозволить обирати операційні потужності комп’ютера залежно від вимог користувача. Наприклад, в процесорі AMD Ryzen 7 наявно 8 ядер, що дають йому здатність досягати тактової частоти до 3.6 ГГц, що забезпечує високу ефективність роботи при багатозадачності.

Дана система обладнана оперативною пам'яттю об’ємом до 64 ГБ DDR4-2400, які дозволять легко справлятися з великим об’ємом важких завдань. Серія налічує варіанти з різними SSD, є наявні, як швидкі жорсткі диски на базі M.2, так і звичайні SSD під’єднувані через порт SATA 6GB/s. Всі раніше названі властивості роблять Lenovo m715 SFF підходящим вибором для виконання інтенсивних аналітичних чи офісних завдань.

Рисунок 3.7 – Lenovo M715 SFF [17]

Щодо сервера, булор обрано Dell PowerEdge R650 – сервер, що належить до класу 1U, розроблений для покращення ефективності використання простору та полегшеної масштабованості, є орієнтованим на високу продуктивність. Цей сервер оснащений процесорами Intel Xeon Scalable, що мають до 40 ядер кожен і підтримку до 256 ГБ оперативної пам'яті DDR4. Для підвищення ефективності зберігання даних в сервері також передбачено PMEM 200.

Сховище даного сервера є налаштовуваним та має значний потенціал, беручи до уваги можливість розміщення до 12 SSD та підтримку PCIe 4.0 слотів для додаткових карт розширення та контролерів RAID. Додатково в даному сервері була передбачена можливість моніторингу усіх аспектів його роботи, перегляд продуктивності серверу, прямий доступ до BIOS через веб-консоль та віддалене керування завдяки технології iDRAC9.

Враховуючи зазначені раніше характеристики, Dell PowerEdge R650 є підходящим вибором, як для обробки великих кількостей даних, для яких є необхідними висока швидкість читання та запису, так і при використанні в середовищах, що мають вимоги до пропускної здатності значного об’єму даних. Цей сервер є найкращим варіантом для великих організацій, в яких наявна необхідність в потужних серверах з гнучкими параметрами для налаштування сервера в цілях обробки або зберігання даних.

Рисунок 3.8 – Dell PowerEdge R650 [40]

В процесі проектування даної мережі було використано три однакових комутатора другого рівня з однаковими параметрами. В зв’язку з цим в надалі буде описано лише один варіант комутатора другого рівня.

Cisco Catalyst C1000FE-24T-4G-L – високопродуктивний, керований комутатор другого рівня, що є здатним до підтримки класичних та високошвидкісних Ethernet портів для з'єднання з іншими пристроями. Обраний комутатор обладнаний 24-ма портами Fast Ethernet (10/100) з підтримкою Power over Ethernet (PoE+). Power over Ethernet дає можливість живити до 24 пристроїв використовуючи мережеві кабелі, наприклад телефони або IP-камери.

Cisco Catalyst C1000FE-24T-4G-L включає в себе використання технології Cisco EnergyWise, що забезпечує зменшене енергоспоживання комутатора при низьких навантаженнях або в неактивні години. Додатково була передбачена підтримка Jumbo Frames для ефективної роботи з великими пакетами даних, що покращує передачу даних при роботі з великими файлами.

Даний комутатор працює на програмному забезпеченні Cisco IOS і підтримує просте управління пристроями, вбудований веб-інтерфейс та мережевим управлінням за допомогою CLI.

Рисунок 3.9 – Cisco Catalyst C1000FE-24T-4G-L [33]

Обраний комутатор третього рівня належить до серії комутаторів Cisco Catalyst 9200 – це інноваційне сучасне обладнання, яке дозволяє миттєво виконувати класичні, стандартні організаційні завдання, як базові, так і складніші. Комутатори Cisco Catalyst 9200 були розроблені в цілях підтримки та доступу до системи автоматизації мережі. Особливістю лінійки є те, що всі її моделі ефективно підвищують надійність усіх мереж без винятку.

Комутатори надають безпеку та захист цілісності апаратного та програмного забезпечення, а також даних як компаній, так і користувачів, які проходять через пристрій. Відмови та перебої комутаторів мінімальні, завдяки цьому ваш бізнес працюватиме без перебоїв.

Щодо керування комутатором, Cisco Catalyst C1000FE-24T-4G-L працює на програмному забезпеченні Cisco IOS® і підтримує просте управління пристроями та мережевим управлінням за допомогою внутрішнього CLI інтерфейсу.

З PoE+, додатковим живленням і охолоджувачами, комутатори Catalyst 9200 забезпечують до 160 Гбіт/с високої пропускної здатності, модульними інтегрованими лініями, підтримкою третього класу та холодним фіксуванням – це безпрецедентне рішення в галузі з диференційованим захистом від несправностей і відмов, а також інноваційним дизайном для економічно ефективних філій.

Рисунок 3.10 – Комутатор Cisco C9200-24PB-A [31]

В процесі розробки мережевої інфраструктури було обрано обладнання, що відповідає встановленим раніше вимогам мережі. Мережа має мати здатність до забезпечення відповідного рівня надійності та безпеки. Було обране матеріальне обладнання, що включає сервери, комутатори та кінцеві пристрої (персональні комп’ютери) високої якості для можливості підтримки надійної роботи мережі.

Таблиця 3.4 – Обрахунок грошових витрат на створення мережі

Пристрій	Кількість	Вартість за одиницю (грн)	Загальна вартість (грн)
Lenovo M715 SFF	26	31 419,36	816 903,36

Кінець таблиці 3.4

Dell PowerEdge R650	2	523 557,72	1 047 115,44
Cisco Catalyst C1000FE-24T-4G-L	11	29 357,58	322 933,38
Cisco Catalyst C9200-24PB-A	3	158 827,50	476 482,50
ZOSI 1080P 4 Pack HD TVI Security Cameras	3 (ідуть в комплектах по 4)	2 943,08	8 829,24
Разом			2 672 263,92 UAH

Обрахована вартість обладнання для створеної мережі становить 1 087 594,64 UAH. Обладнання обране для даного проекту спроможне забезпечити необхідний рівень безпеки та надійності для всіх встановлених відділів та потенційних вимог до роботи компанії.

Ціна обладнання, по більшій частині, залежить від поставлених вимог до потужності кожного пристрою: Фінансовий та Загальний відділи мають запит на більш потужне та дороге обладнання оскільки кількість працівників пов’язана з ними є значно більшою ніж для комутатора адміністрації. Дана мережа буде спроможна на забезпечення необхідного рівня стабільності та безпечної роботи всіх необхідних сервісів, що входять до структури мережі та систем задіяних в ній.

3.4 Тестування мережі

Для перевірки налаштування комутаторів слід перевірити можливість під’єднання комп’ютерів в межах кожної зі створених підмереж та інших підмереж через комутатори використовуючи консольну команду ping.

А)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.3

Pinging 192.168.30.3 with 32 bytes of data:

Reply from 192.168.30.3: bytes=32 time=128ms TTL=128
Reply from 192.168.30.3: bytes=32 time=1ms TTL=128
Reply from 192.168.30.3: bytes=32 time<1ms TTL=128
Reply from 192.168.30.3: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.30.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 128ms, Average = 33ms
```

Б)

```
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=254
Reply from 192.168.20.2: bytes=32 time<1ms TTL=254
Reply from 192.168.20.2: bytes=32 time<1ms TTL=254
Reply from 192.168.20.2: bytes=32 time<1ms TTL=254

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

В)

```
C:\>ping 192.168.40.2

Pinging 192.168.40.2 with 32 bytes of data:

Reply from 192.168.40.2: bytes=32 time<1ms TTL=127
Reply from 192.168.40.2: bytes=32 time=12ms TTL=127
Reply from 192.168.40.2: bytes=32 time=12ms TTL=127
Reply from 192.168.40.2: bytes=32 time=3ms TTL=127

Ping statistics for 192.168.40.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 6ms
```

Рисунок 3.11 – Успішний результат перевірки під’днання комутатору адміністрації до інших

У даному випадку виконується перевірка під’єднання адміністративної підмережі у якій, по плану, було надано доступ до всіх інших підмереж та налаштування комутаторів відповідних підмереж і відділів пов’язаних безпосередньо з взаємодією з працініками компанії.

Перевірка під’єднання адміністрації до віртуальної консолі комутатора через SSH, що гарантує можливість віддаленого налаштування комутаторів. У загальному випадку під’єднання виконується через в консолі команду: ssh -l <ім’я користувача> <IP-адреса комутатора>.

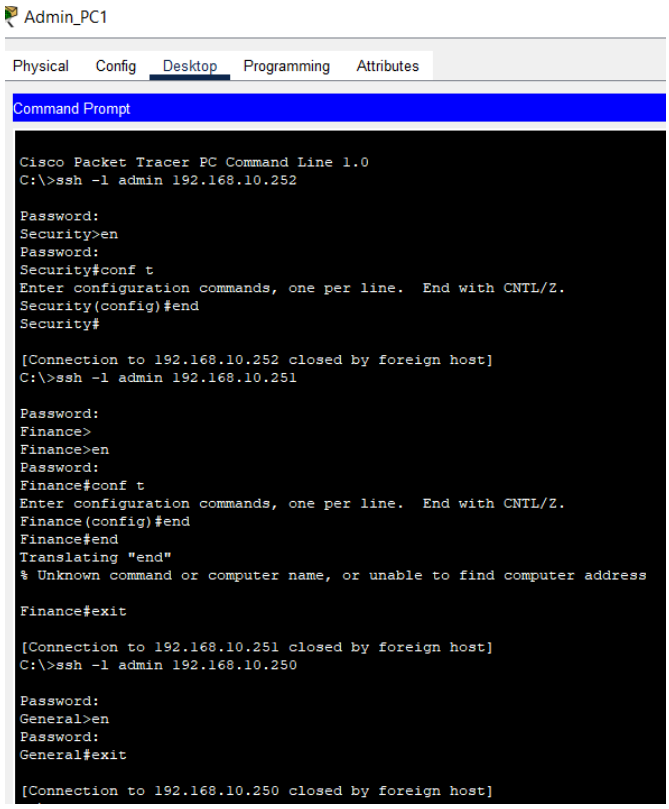


Рисунок 3.12 – Успішний результат перевірки під'єднання адміністрації до комутатора через SSH;

Під час перевірки було визначено, що вхід в обліковий запис та двофакторна аутентифікація за рахунок локального пароля виконують свої функції. Налаштування комутатора через внутрішні команди CLI працює належним чином.

Перевірка налаштування списків доступу виконується шляхом перевірки наявності можливості передачі данних між підмережами яким це заборонено.

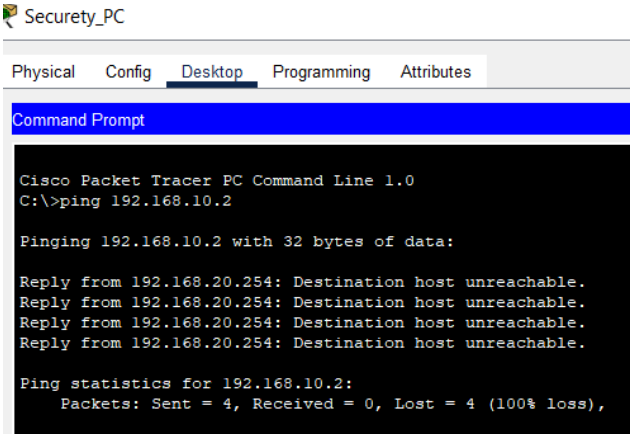


Рисунок 3.13 – Успішний результат перевірки роботи ACL

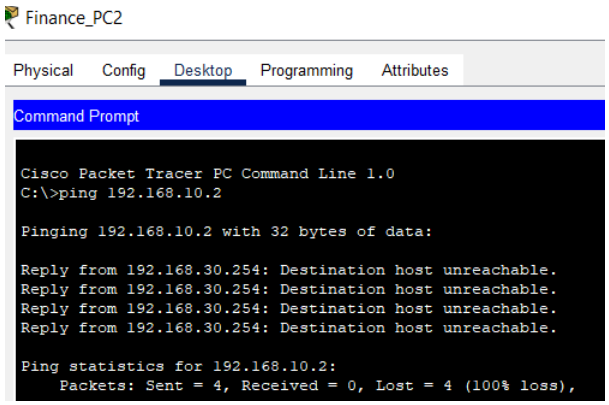


Рисунок 3.14 – Успішний результат перевірки роботи ACL відносно підмережі фінансового відділу

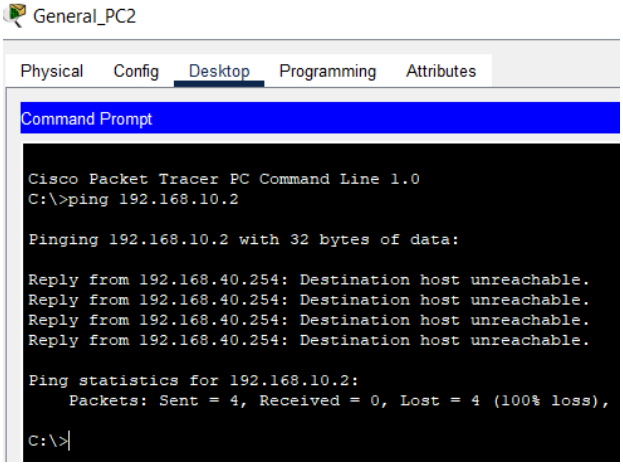


Рисунок 3.15 – Успішний результат перевірки роботи ACL відносно підмережі загального відділу

При перевірці роботи списків доступу можна побачити, що при спробі виконати перевірку підключення з іншою підмережею від IP адреси, що вказана в комутаторі як default-gateway видає повідомлення про недосяжність хоста. Дане повідомлення свідчить про те, що розширені списки доступу працюють відповідним чином та створені налаштування є корректними.

Перевірка налаштувань DHCP. Для впевненості в успішному налаштуванні сервісу DHCP на сервері слід провести первірку під’єднання одного з кінцевих пристроїв та функціонуванна автоматичної роздачи IP-адрес на кінцеві пристрої за запитом до серверів.

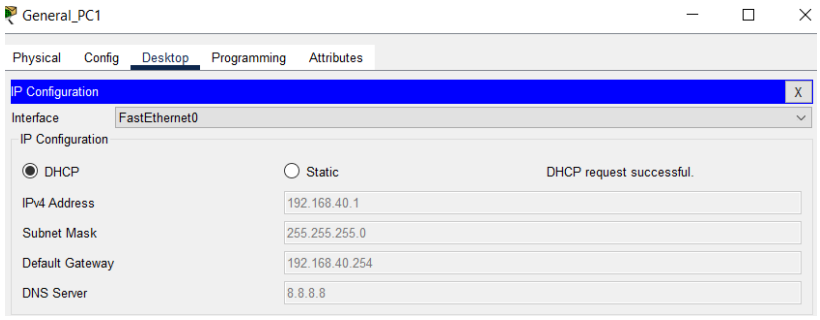


Рисунок 3.16 – Успішний поцес перевірки DHCP на підмережі загалного відділу

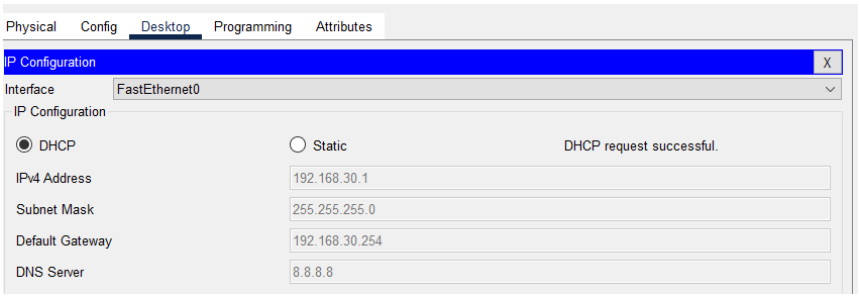


Рис.3.17 – Успішний поцес перевірки сервісу DHCP на підмережі фінансового відділу

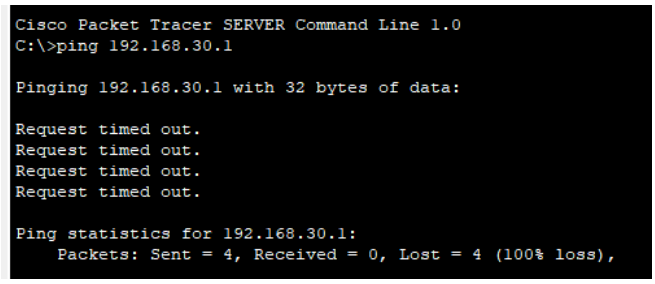


Рисунок 3.18 – Успішна перевірка зонових політик безпеки

В ході тестування кожної підсистеми даної мережі усі мережеві можливості успішно пройшли перевірки та відповідають встановленим метрикам, підтверджуючи, що пристрої та відповідні підсистеми, пов’язані з відділами компанії, мають коректну взаємодію у її межах та інфраструктура готова до розгортання у виробництві з оптимальною продуктивністю, стійкістю та безпекою.

Успішне тестування показує, що всі можливості мережі є повністю оптимізовані та відповідають поточним операційним вимогам.

3.5 Висновки до третього розділу

В ході виконання третього розділу було проведено процес розробки мережевої інфраструктури, що відповідає вимогам визначеним впродовж виконання першого розділу. Було створено мережеву інфраструктуру розділену на три віділи, серед яких головний офіс та дві окремі філії. До створюваної мережі було додано функціонал сервісу Syslog для логування внутрішніх подій матеріального обладнання мережі та мережевого трафіку через розширені списки доступу. Було додано функціонал сервісу AAA в цілях логування трафіку облікових даних користувачів та їх віддаленого збереженна на одному з серверів мережі. Додатково було використано функціонал DHCP для другорядних відділів, щоб забезпечити можливість легшого розширення створюваної мережі.

Також було проведено визначення потенційного матеріального обладнання, що відповідає встановленим раніше вимогам мережі. Мережа має мати здатність до забезпечення відповідного рівня надійності та безпеки. Було обране матеріальне обладнання, що включає сервери, комутатори та кінцеві пристрої (персональні комп’ютери) високої якості для можливості підтримки надійної роботи мережі.

ВИСНОВКИ

Впродовж розробки даного проекту було проведено основні теоретичні дослідження щодо мережевих систем засновоних на принципі безпеки «Zero Trust». Для цього було виконано аналіз предметної області, виявлено наявні проблеми та завдання, а також виконаний порівняльний аналіз переваг і неділіків існуючих рішень. Було визначено підходи придатні до використання для вирішення задачі даного дослідження та зроблено висновки. Було створено сучасну корпоративну мережеву структуру основану на принципі безпеки «Zero Trust», що є відповідною до вимог щодо стабільності, гнучкості і безпеки. Тестування мережі підтвердило, що пристрої мають коректну взаємодію у її межах.

Використані рішення є відповідними до сучасних стандартів та здатні забезпечити ефективне та комфортне обслуговування клієнтів компанії, централізоване управління мережею та стабільну роботу її систем. Створена мережева структура показує надійність і здатна до легкого масштабування.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Mark S., Nikhil K. Zero Trust Overview and Playbook Introduction. Packt Publishing Ltd. 2023. 241 p.
2. Olusegun A. Exploring the Effect of Zero-Trust Architecture on Organisations. *Iconic research and engineering journals*. Vol.8, Issue 1. 2024. P. 671 – 678. URL: https://www.irejournals.com/formatedpaper/1707145.pdf (дата звернення: 05.03.2026).
3. Ev K., Sakshyam S., Peter C. Identity-Native Infrastructure Access Management Preventing Breaches by Eliminating Secrets and Adopting Zero. O'Reilly Media, Inc. 2023. 155 p.
4. Sushama P., Shonal V., Yogita K., Manisha P. Zero Trust Architecture: A Paradigm Shift in Cybersecurity. *International Journal of Research Publication and Reviews*. Vol.5, Issue 3. 2024. P. 6455 – 6460. URL: https://ijrpr.com/uploads/V5ISSUE3/IJRPR24246.pdf (дата звернення: 05.05.2026).
5. Avinash N. In Zero Trust We Trust. Cisco Press Hoboken, New Jerswy. 2024. 528 p.
6. Abbas K. Binil P. Zero Trust Journey Across the Digital Estate. CRC Press. 2023. 237 p.
7. Ravindra D. The Zero Trust Framework and Privileged Access Management. CRC Press. 2024. 126 p.
8. Frank M. Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity. *International Journal of Advance Research, Ideas and Innovations in Technology*. 2024. Vol.10, Issue 6. P. 339 – 346. URL: https://s3.ap-southeast-1.wasabisys.com/ijmanuscripts/manuscripts/v10i6/V10I6-1452.pdf (дата звернення: 14.05.2026).
9. Kipkoech D. A survey of security in zero trust network architectures Components of zero trust network architecture. GSC Advanced Research and Reviews.

2025. P 183 – 214. DOI: https://doi.org/10.30574/gscarr.2025.22.2.0036 (дата звернення: 09.04.2026).

10. M. Nasiruzzaman, M. Ali, I. Salam and M. H. Miraz. The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation. *International Conference on Information Technology (IT).* 2025. 10 p. URL: https://arxiv.org/pdf/2504.11984 (дата звернення: 05.03.2026).

11. Manar H., Wesam S., Nabeel H. Kaghed Al-aaraji Integration of Zero Trust Architecture and Machine Learning for Improving the Security of Software Defined Networking: A Review. *Journal of Intelligent Informatics, Networking, and Cybersecurity* 2025. Vol.1 Issue 1. 21 p. URL: https://jiinc.uobabylon.edu.iq/cgi/viewcontent.cgi?article=1000&context=journal (дата звернення: 05.04.2026).

12. Sharanya V. P. Zero trust architecture: The future of enterprise security. *World Journal of Advanced Engineering Technology and Sciences.* 2025. P. 661 – 666. DOI: https://doi.org/10.30574/wjaets.2025.15.1.0247 (дата звернення: 05.04.2026).

13. Rajender P. R. Zero Trust Architectures in Modern Enterprises: Principles, Implementation Challenges, and Best Practices. *International Journal of Computer Trends and Technology.* 2025. Vol.73 Issue 6, P. 48 – 57. URL: https://www.ijcttjournal.org/2025/Volume-73/Issue-6/IJCTT-V73I6P107.pdf (дата звернення: 05.03.2026).

14. Lakshmi N. Zero Trust Architecture: A Comprehensive Framework for Modern Data Security. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT).* 2025. Vol.5 Issue 7, P. 390 – 405. URL: https://ijarsct.co.in/Paper24449.pdf (дата звернення: 05.03.2026).

15. Tilmar A. J. Zero Trust Security A Hands-on Guide. John Wiley & Sons, Inc., Hoboken, New Jersey. 2026. 225 p.

16. Комп’ютер Lenovo M715 SFF URL: https://www.lenovo.com/au/en/p/desktops/thinkcentre/m-series-sff/thinkcentre-m715s/11tc1md715s (дата звернення: 16.04.2026).

17. Josh H. Zero Trust in Resilient Cloud and Network Architectures. Cisco Press Hoboken, New Jersey. 2025. 106 p.

18. Stephen K. D. Zero Trust Architecture Implementation in Enterprise Networks: Evaluating Effectiveness Against Cyber Threats. *International Journal of Computer Applications*. 2025. Vol.187, P. 21 – 39. URL: https://www.ijcaonline.org/archives/volume187/number45/dotse-2025-ijca-925740.pdf (дата звернення: 05.04.2026).

19. Gary A., Judith K., Michat T. Cloud Native Data Security With Oauth A Scalable Zero Trust. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. 2025. 514 p.

20. Marija Z., Milan P., Dragan R. One example of implementing zero trust. *Annual conference on Challenges of Contemporary Higher Education*. 2025. P. 222 – 227. URL: https://acche.rs/ACCHE_2025/radovi/electrical/32.pdf (дата звернення: 05.03.2026).

21. Nathan H., Sanjit G., Gerard F. Seven Elements of Highly Successful Zero Trust Architecture. Zscaler, Inc.2024. 154 p.

22. Mark B., Stefaan Van d., Carsten H. Security Architecture for Hybrid Cloud. O'Reilly Media, Inc. 2024. 477 p.

23. Gopalakrishna K. Zero trust and AI: A synergistic approach to next-generation cyber threat mitigation. *World Journal of Advanced Research and Reviews*. 2024. P. 3375 – 3387. DOI: https://doi.org/10.30574/wjarr.2024.24.3.3883 (дата звернення: 11.03.2026).

24. Ravindra D. The Zero Trust Framework Threat Hunting & Quantum Mechanics. CRC Press. 2024. 157 p.

25. Razi R., Christina M., Evan G., Doug B. Zero Trust Networks, 2nd edition. O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472. 2024. 493 p.

26. Tom M. Zero-trust – An Introduction. River Publishers Alsbjergvej 10, 9260 Gistrup, Denmark. 2024. 134 p.

27. Gregory C. Zero Trust and Third-Party Risk. John Wiley & Sons, Inc., Hoboken, New Jersey. 2024. 176 p.

28. Chidiebere U. The Future of Zero-Trust Security Architecture with Ai Automation. *International journal of research and scientific innovation (IJRSI)*. Vol.13, Issue 1. 2026. P 700 – 713. DOI: https://dx.doi.org/10.51244/IJRSI.2026.13010060 (дата звернення: 07.04.2026).

29. Bashaa, Manar H., Bhaya, Wesam S., and Al-aaraji i Nabeel H. Kaghed Integration of Zero Trust Architecture and Machine Learning for Improving the Security of Software Defined Networking: A ReviewImproving the Security of Software Defined Networking: A Review. *Journal of Intelligent Informatics, Networking, and CybersecurityJournal of Intelligent Informatics, Networking, and Cybersecurity*. Vol.1, Issue 1. 2025. P. 2 – 20. URL: https://jiinc.uobabylon.edu.iq/journal/vol1/iss1/1/ (дата звернення: 05.03.2026).

30. Комутатор Cisco C9200-24PB-A URL: https://networkwarehouse.co.uk/products/cisco-c9200-24pb-a (дата звернення: 16.04.2026).

31. Shikha T. A. Zero trust architecture: A practical framework for enterprise cybersecurity. *International Journal of Computing and Artificial Intelligence*. 2024. P. 61 – 66. URL: https://www.computersciencejournals.com/ijcai/archives/2024/vol5issue1/PartA/6-2-29-559.pdf (дата звернення: 05.06.2026).

32. Oladoyin A. Using Zero Trust Security Architecture Models to Secure Artificial Intelligence Systems. *Journal of Emerging Technologies and Innovative Research*. 2024. Vol.11, Issue 4, P. 349 – 373. URL: https://www.jetir.org/papers/JETIR2404H46.pdf (дата звернення: 05.03.2026).

33. Комутатор Cisco Catalyst C1000FE-24T-4G-L URL: https://www.serversupply.com/NETWORKING/SWITCH/24%20PORT/CISCO/C1000FE-24T-4G-L_351746.htm (дата звернення: 16.03.2026).

34. Kamaludin N., Benfano S. Zero trust architecture with single sign on method on enhance security and user ctivity monitoring. *Journal of Theoretical and Applied Information Technology*. 2025. Vol.103. P. 2722 – 2733. URL: https://jatit.org/volumes/Vol103No7/8Vol103No7.pdf (дата звернення: 05.04.2026).

35. Oliver B. Implementing a Zero Trust Architecture. CRC Press. 2024. 54 p.

36. Prince K. Zero Trust Architecture For Sme Cybersecurity: Enhancing Resilience In The Digital Transformation Era. *International Journal Of Progressive Research In Engineering Management And Science (Ijprems)*. Vol.5, Issue 4. 2025. P. 2791 – 2819. URL: https://www.ijprems.com/ijprems-paper/zero-trust-architecture-for-sme-cybersecurity-enhancing-resilience-in-the-digital-transformation-era (дата звернення: 05.03.2026).

37. Pawan K. Building Up Better Microsoft Cloud Data Security with Stronger Security Methods. Metropolia University of Applied Sciences Master of Engineering Information Technology Master's Thesis. 2025. 58 p.

38. Cindy G., Brandon F. Zero Trust Architecture. Cisco Press Hoboken, New Jersey. 2024. 97 p.

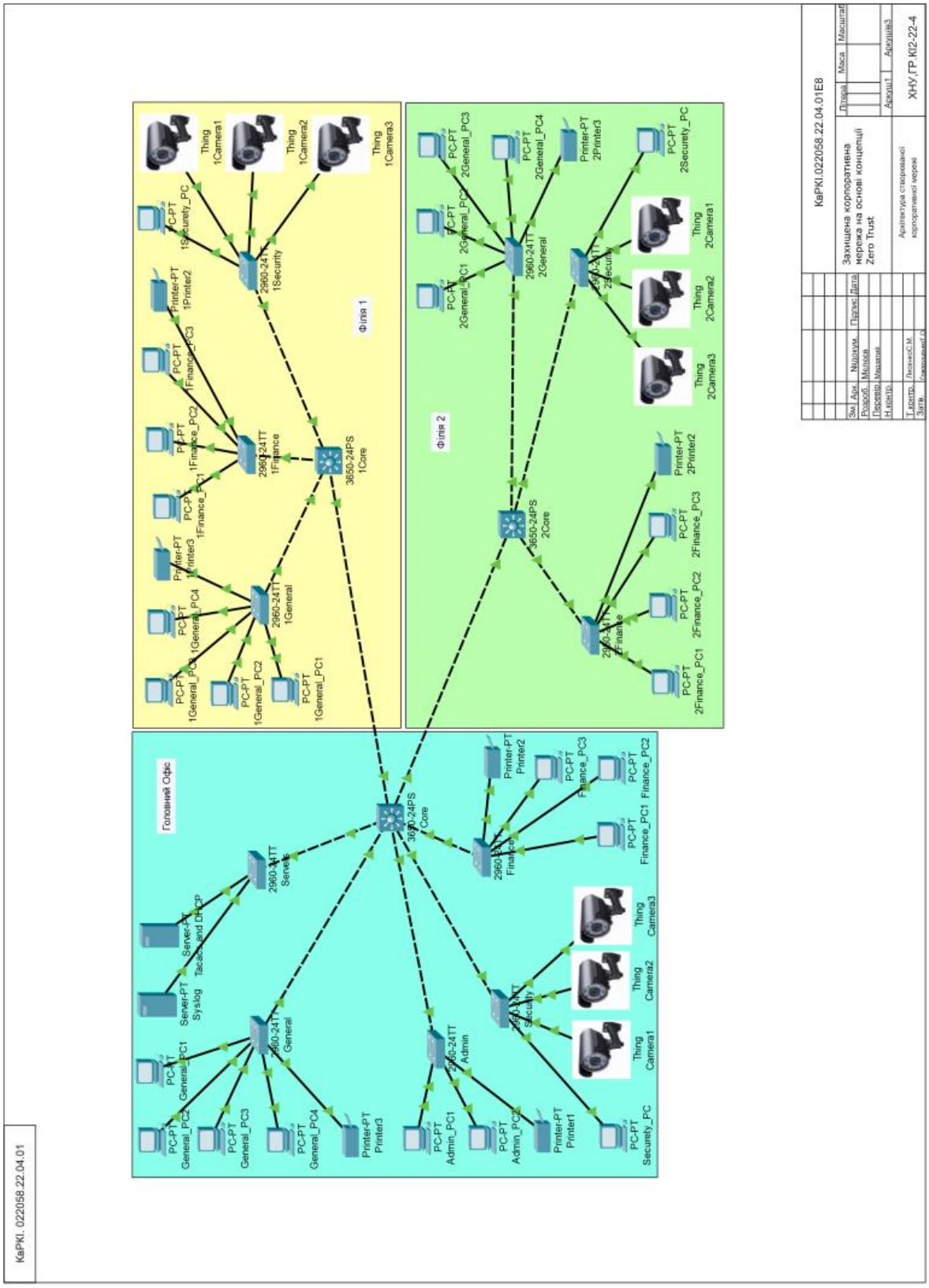
39. Vikas P. Role of Identity and Access Management in Zero Trust Architecture for Cloud Security: Challenges and Solutions. *International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)*. Vol.5 Issue 3. 2025. P. 6 – 28. URL: https://ijarsct.co.in/Paper23902.pdf (дата звернення: 05.03.2026).

40. Сервер Dell PowerEdge R650 URL: https://serversolutions.com.ua/products/server-dell-poweredge-r650-dual-xeon-silver-4314 (дата звернення: 16.04.2026).

ДОДАТОК А

(обов’язковий)

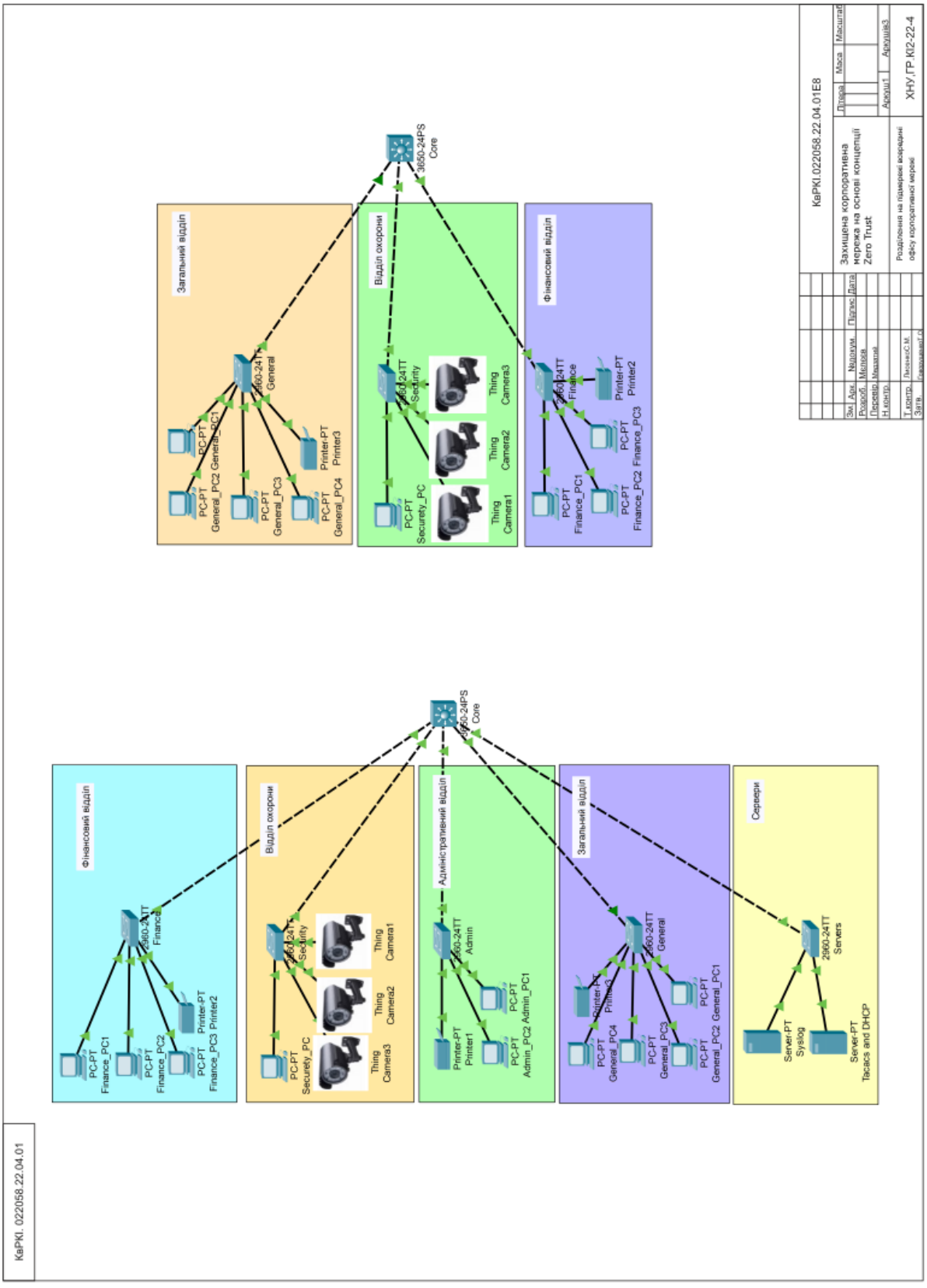
Копія плакату «Архітектура створюваної корпоративної мережі»



ДОДАТОК Б

(обов’язковий)

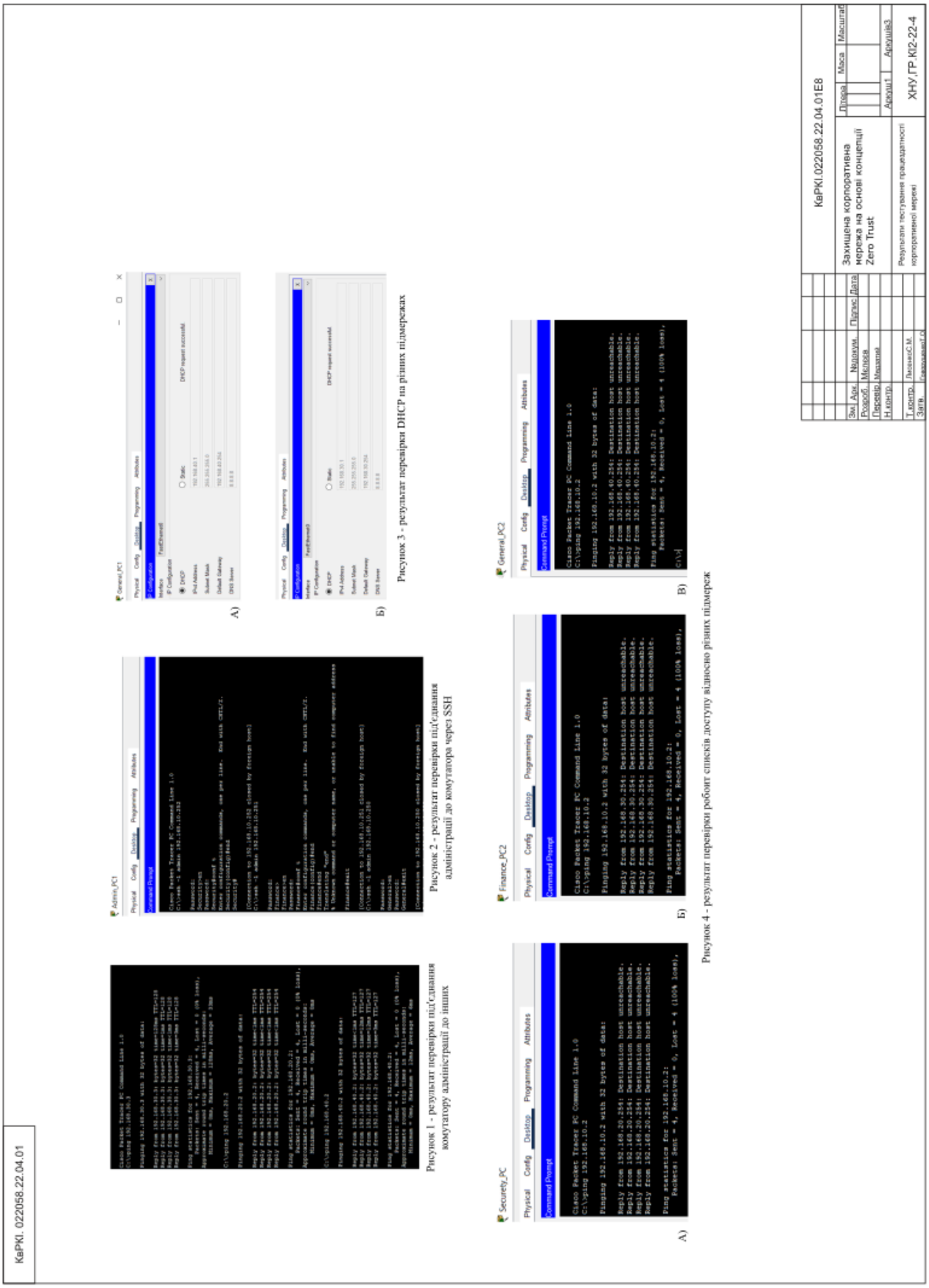
Копія плакату «Розділення на підмережі всередині офісу корпоративної мережі»



ДОДАТОК В

(обов’язковий)

Копія плакату «Результати тестування працездатності корпоративної мережі»



Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Нікіта МЄЛЄСВ

Співавтор:

Назва: Захищена корпоративна мережа на основі концепції Zero Trust

Експерт: Дмитро Медзатий

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:1.26%

Коефіцієнт подібності 2:0.28%

Мікропробіли: 25

Заміна букв: 3

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2026-05-28 16:16:50.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-05-28 Доцент Андрій Нічепорук

Дата експерт

Anti-Plagiarism (http://ap.km.ua) v-15.701

Максимальне співпадіння з одним документом 28.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 14%**

ID: 272631 Назва: БКР Захищена корпоративна мережа на основі концепції Zero Trust Додано в БД: 2026-05-28 Автора: Нікіта МЄЛЄЄВ Керівники: Дмитро Медзатий Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	88869	702	25459 (29%)	233 (33%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
269502	Назва: Звіт з ПДП завдання Захищена корпоративна мережа на основі концепції Zero Trust Додано в БД: 2026-02-25 Автора: Н. Б. Мєлєєва Керівники: Павлова О.О. Консультанти: Опоненти:	24832 (28.0%)	223 (32.0%)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Мелєєв Нікіта Борисович

Тема: Захищена корпоративна мережа на основі концепції Zero Trust

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень 3 Кількість сторінок записки 64

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є створення захищеної корпоративної мережі на основі концепції Zero Trust

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: В першому розділі кваліфікаційної роботи проведено дослідження предметної області (проаналізовано теорію архітектури мереж Zero Trust, а також розроблення і опис необхідного функціоналу для реалізації корпоративної мережі з архітектурою Zero Trust) та виконано постановку задачі дослідження. В другому розділі кваліфікаційної роботи проведено моделювання та проєктування захищеної корпоративної мережі на основі концепції Zero Trust а саме: визначено необхідний функціонал для реалізації архітектури Zero Trust; виконано проектування попередньої структури корпоративної мережі; виконано планування налаштувань сервісу DHCP у створюваній мержі; визначено необхідні налаштування списків доступу для корректної роботи мережі; виконано попереднє планування функціоналу сервісу SSH; визначено попередній розподіл на підмережі; створено схему розділення створюваної мережі на зони (підмережі); побудовано схему захищеної корпоративної мережі. В третьому розділі кваліфікаційної роботи виконано реалізацію захищеної корпоративної мережі на основі концепції Zero Trust а саме: реалізовано схему захищеної корпоративної мережі на основі концепції Zero Trust; змодельовано мережу в середовищі Cisco Packet Tracer.

4. Позитивні сторони роботи: висока практична цінність роботи.

5. Негативні сторони роботи: недостатня увага моделюванню мережі в середовищі Cisco Packet Tracer.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: задовільно

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Янчик О.М., доцент кафедри ІПЗ

"12" 06 2026 р. _____(підпис)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Нікіта МЄЛЄЄВ
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-22-4

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 академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

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

1 травня 2026 року

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Захищена корпоративна мережа на основі концепції Zero Trust

Автор Нікіта МЄЛЄЄВ
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: к.т.н., доцент Дмитро МЕДЗАТИЙ

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

№	Висновок	Позначка про відповідність
1	Ознаки академічного плагіату	
1.1	Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту.	відповідає
1.2	Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована.	
1.3	Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат.	
1.4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
2	Інші види порушень академічної доброчесності	

Підтвердження:

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

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 1,26%; та системою Anti-Plagiarism складає 0,28%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.06.2026

Завідувач кафедри _____ Підпис Ольга ПАВЛОВА Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Підпис Андрій НІЧЕПОРУК Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Підпис Дмитро МЕДЗАТИЙ Ім'я, ПРІЗВИЩЕ