Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Заянчуковського Владислава Володимировича

на здобуття ступеня вищої освіти Бакалавра

Система захисту інформації в локальній мережі підприємства за концепцією BYOD

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

Шифр КРБКБ.2101119.21.01.08 ПЗ

Виконав студент 4 курсу група КБ-21-1 Владислав ЗАЯНЧУКОВСЬКИЙ

Керівник к.т.н., доцент Юрій КЛЬОЦ

Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

09. 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ

Завідувач кафедри кібербезпеки

Юрій КЛЬОЦ

15 лютого 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Заянчуковському Владиславу Володимировичу

1 Тема роботи Захист локальної мережі підприємства за концепцією BYOD

Керівник роботи к.т.н., доцент Юрій КЛЬОЦ

Затверджено наказом ректора університету від 7 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру 02.06.2025

3 Вихідні дані до роботи Вибір системи, здатну виявляти різноманітні кіберзагрози на пристроях та мережевому рівні. Потрібно здійснити аналіз можливих загроз. Обрати відповідні інструменти. Спроєктувати архітектуру рішення. Реалізувати систему виявлення атак у віртуальному середовищі. Провести налаштування компонентів, оцінити ефективність виявлення і реагування системи на ці загрози.

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Аналіз предметної області. Основи мережної безпеки. Характеристика концепції BYOD. Огляд можливих рішень впровадження концепції. Вибір обладнання для локальної мережі. Впровадження концепції та конфігурація безпеки мережі. Висновки.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Схема логічної топології мережі. Схема фізичної топології мережі.

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

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

Студент _____ Владислав ЗАЯНЧУКОВСЬКИЙ

Керівник кваліфікаційної роботи _____ Юрій КЛЬОЦ

ABSTRACT

Theme of the qualification work: Information security system in the local network of the enterprise according to the BYOD concept.

Author of the work: Vladyslav Volodymyrovych Zayanchukovskyi.

Supervisor of the work: Klots Yuri Pavlovych.

Explanatory note: 62 p., 3 appendices, 13 figures, 3 tables, 28 sources.

Graphic part: 2 posters, 10 presentation slides.

PROTECTED LOCAL AREA NETWORK, LOGICAL TOPOLOGY, PHYSICAL TOPOLOGY, CONFIGURATION, BYOD.

The bachelor's thesis is devoted to the design of a secure corporate network supporting the BYOD concept. The work analyzes modern threats to information security arising from the connection of employees' personal devices to the corporate network, and also considers modern methods of protecting information in such conditions.

A network architecture modeled in Cisco Packet Tracer is proposed, using VLAN segmentation, 802.1X access control, NAC, access control lists, wireless network protection, and VPN. Particular attention is paid to network security.

04.06.2025 _____

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту інформації в локальній мережі підприємства за концепцією BYOD.

Автор роботи: Заянчуковський Владислав Володимирович.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 62 с., 3 додатки, 13 рисунків, 3 таблиці, 28 джерел.

Графічна частина: 2 плакати, 10 презентаційних слайдів.

ЗАХИЩЕНА ЛОКАЛЬНА МЕРЕЖА, ЛОГІЧНА ТОПОЛОГІЯ, ФІЗИЧНА ТОПОЛОГІЯ, КОНФІГУРАЦІЯ, BYOD.

Кваліфікаційна робота бакалавра присвячена проєктуванню безпечної корпоративної мережі з підтримкою концепції BYOD. У роботі проведено аналіз сучасних загроз інформаційній безпеці, що виникають через підключення особистих пристроїв співробітників до корпоративної мережі, а також розглянуто сучасні методи захисту інформації у таких умовах.

Запропоновано архітектуру мережі, змодельовану у Cisco Packet Tracer, із використанням сегментації за допомогою VLAN, контролю доступу 802.1X, NAC, списків контролю доступу, захисту бездротових мереж, застосування VPN. Особлива увага приділена безпеці мережі.

04 .06 .2025 _____

ЗМІСТ

ВСТУП

Розвиток технологій та мереж впродовж часу виходить на новий рівень, тому з’являються нові потреби у сфері IT, існує багато рішень для розширення мережі компанії, для цього використовують нові впровадження, які збільшать продуктивність працівників та самої компанії. Підхід BYOD, який розшифровується як принеси свій девайс вже давно набув популярності серед компаній, він включає в себе використання своїх пристроїв, таких як телефони, ноутбуки та планшети на робочому місці з можливостю підключення до корпоративної мережі, що це дає? Це можна розглядати з двох сторін, комфортності для працівників, можливість роботи дистанційно та з іншої сторони безпека для самої компанії. Сьогодні використання дистанційного формату роботи є доволі популярним, адже це дає можливість також економити, робоче місце та самий пристрій для робітника, тому за допомогою концепції BYOD можна досягти зручність та безпеку для певної корпоративної мережі.

Сама технологія зародилась доволі давно, а у 2009 році була застосована авторитетною компанією «Intel», що вже собою являє довіру та ефективне використання такого підходу, знову ж таки потрібно не забувати про правильність налаштування такої складної мережі у сфері безпеки, адже пристрої, які будуть використовуватися для доступу до конфіденційних даних, ми будемо також використовувати дома для своїх потреб, що несе собою з боку компанії створення великого рівня захисту від витоку інформації, а також контроль за користувачем під час використання девайсу при його роботі з мережею, слід добавити використання лише ліцензійного програмного забезпечення, обмеження завантажень файлів, які можуть призвести до різних інцидентів, ну і також слід використовувати довірені «VPN» під час роботи дистанційно з корпоративною мережею компанії, такі проблеми призводять до того, що потрібно правильно налаштувати мережу, створити різні рівні захисту і звичайно постійно слідкувати за користувачами та надавати рекомендації під час роботи, звісно ж що політика безпеки в такому випадку буде гнучка, та часто змінюватись до принципу зміни

програмного забезпечення та їх останніх оновлень. Щоб мінімізувати ці ризики, компаніям необхідно розробляти чіткі політики BYOD, які визначатимуть вимоги до безпеки пристроїв, правила використання корпоративних ресурсів, стандарти конфігурації та процедури реагування на інциденти. Важливо також регулярно навчати співробітників, протидії фішингу та правильній роботі з корпоративними даними. Сучасні технології захисту, такі як шифрування даних, багатофакторна аутентифікація, принцип Zero Trust, що передбачає постійну перевірку кожної дії користувача, стають невід'ємною частиною захисту корпоративної мережі. Не менш важливо здійснювати постійний контроль і моніторинг пристроїв, перевіряти встановлене програмне забезпечення, відстежувати підозрілу активність і своєчасно оновлювати системи безпеки. При звільненні працівника слід забезпечити видалення корпоративної інформації з його пристрою, щоб уникнути витоку даних у майбутньому.

Отже, BYOD - це сучасний та ефективний підхід, який дозволяє компаніям бути гнучкими, економити ресурси та підвищувати ефективність працівників. Проте для його успішного впровадження необхідно приділяти особливу увагу питанням безпеки, впроваджувати сучасні технології захисту, навчати персонал та постійно контролювати стан корпоративної мережі. Лише комплексний підхід дозволить отримати максимальні переваги від BYOD і водночас мінімізувати ризики для компанії.

1 ТЕОРИТИЧНІ ОСНОВИ ПОСТАВЛЕНОГО ЗАВДАННЯ

1.1 Локальна мережа підприємства та концепція BYOD

У сучасному світі, коли обсяг та швидкість обміну інформацією є важливим чинником ефективності бізнесу. Локальні мережі стали незамінною основою інформаційної структури будь-якої організації. Локальна мережа включає в себе технічні та програмні засоби, які забезпечують зв'язок між різними компонентами мережі, таких як комп'ютер, принтер, сервер, IP-телефон, телефон чи відеоконференції та хмарні сервіси, які вимагають стабільного та безпечного перебування всередині корпоративної інфраструктури в межах обмеженої зони, будівлі чи офіса.

Основні функції локальної мережі це забезпечення спільного доступу до ресурсів мережі, передача даних з великою швидкістю та з відповідним рівнем безпеки, централізоване адміністрування, також включаючи внутрішню безпеку мережі, розмежування доступу між користувачами та контроль дій і їх прав. [1]. Архітектура сучасної локальної мережі складається на базі моделі, яка включає три рівні. Рівень доступу, який відповідає за кінцеві пристрої, рівень розподілу задача якого об'єднувати точки доступу і рівень ядра, який забезпечує швидкий обмін даними між системами. Всі ці рівні управляються централізовано та за допомогою деяких засобів моніторингу, до прикладу SNMP, NetFlow, sFlow, систем аутентифікації та політик безпеки VLAN, ACL, 802.1X.

У стандартних локальних мережах переважно знаходяться переважно керовані пристрої, які ж належать компанії, це включає в себе персональні комп'ютери з корпоративною операційною системою, сервери, які використовують системи моніторингу, точки доступу робота яких виконується на корпоративних каналах зв'язку і керовані комутатори з встановленою політикою безпеки. Однак з підвищенням популярності мобільної роботи, віддаленого доступу та хмарних сервісів, велика кількість працівників починають використовувати для роботи свої особисті пристрої, ноутбуки, планшети, смартфони, домашні персональні комп'ютери. Це все призвело до виникнення

концепції BYOD – Bring Your Own Device. Концепція BYOD передбачає, що працівникам дозволяється підключати власні пристрої до корпоративної мережі для виконання службових обов'язків. Вона набула поширення насамперед у сферах, де важлива мобільність, швидке реагування та гнучкість графіка, таких як маркетинг, технічна підтримка, IT та освіта. Основні переваги BYOD включають зниження витрат на закупівлю техніки, оскільки компанія не мусить забезпечувати кожного співробітника обладнанням; підвищення задоволеності персоналу завдяки використанню звичних і зручних пристроїв; збільшення мобільності працівників і можливість організовувати роботу з будь-якої точки світу; а також гнучкість у виборі операційної системи та програмного забезпечення, що дозволяє адаптуватися під індивідуальні потреби користувачів.

Окрему увагу слід зосередити на підборі належної мережевої топології, на рисунку 1.1 можна розглянути типи топології.

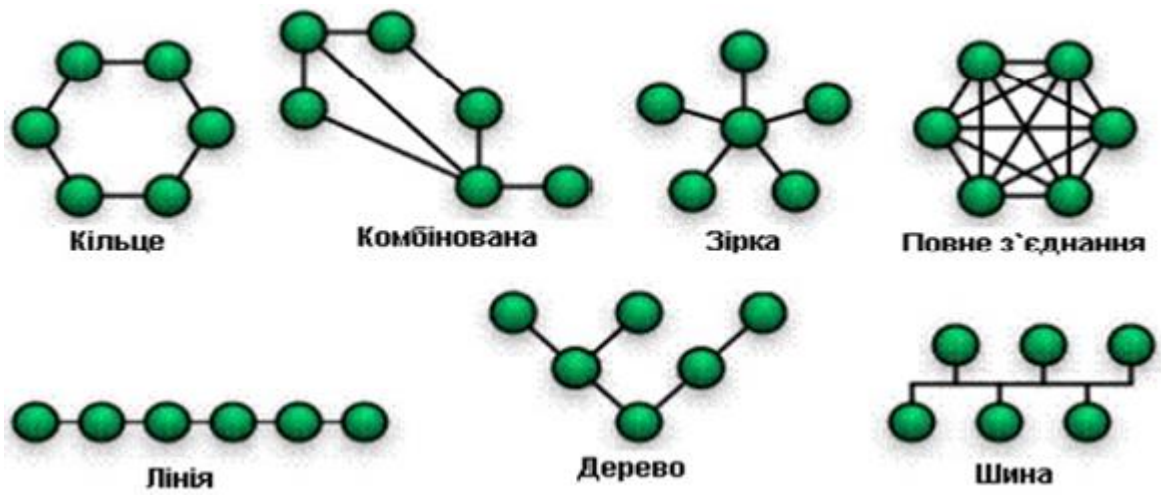


Рисунок 1.1 – Типи топології.

Топологія задає фізичний і логічний взаємозв'язок мережевих пристроїв, що безпосередньо впливає на швидкість роботи, стабільність, можливість розширення та захищеність мережі. Зважаючи на особливості BYOD, коли кількість підключених пристроїв може стрімко збільшуватися, а також підвищені вимоги до захисту корпоративних даних, вибір найліпшої топології відіграє ключову роль. Одна з найпопулярніших в корпоративних мережах, що

підтримують BYOD, є зіркоподібна структура. Вона передбачає з'єднання всіх кінцевих пристроїв до центрального комутатора. Цей метод забезпечує зручне управління мережею, легке розширення та високу стійкість до збоїв на рівні окремих пристроїв, вихід з ладу одного з них не впливає на функціонування інших. Водночас, центральний вузол у зірковій топології є єдиною точкою відмови і його несправність може спричинити повну зупинку мережі. Окрім цього, для організації такої мережі необхідна велика кількість кабелів, що підвищує вартість її впровадження.

Водночас із цими перевагами виникають і суттєві виклики. По-перше, компанія втрачає повний контроль над кінцевими пристроями, що ускладнює забезпечення їх відповідності корпоративним стандартам безпеки. По-друге, існує високий ризик витоку конфіденційної інформації через використання особистих пристроїв, які можуть не мати достатнього захисту або бути зараженими шкідливим програмним забезпеченням. Крім того, підключення зламаних або скомпрометованих пристроїв до корпоративної мережі створює загрозу проникнення та поширення кібератак. Також стає важким процес логування, моніторингу та реагування на інциденти безпеки, оскільки особисті пристрої мають різні конфігурації і рівні захисту, а контроль над ними обмежений.

Класична модель безпеки корпоративної мережі базується на підході, за якого мережа захищається насамперед на зовнішньому кордоні за допомогою між мережевих екранів, шлюзів та інших засобів, що контролюють доступ ззовні. У цій моделі все, що знаходиться всередині мережі, вважається безпечним і довіреним. Однак концепція BYOD суттєво порушує цю логіку, оскільки до внутрішньої мережі підключаються особисті пристрої співробітників, які не проходять жорсткого корпоративного контролю, сертифікації чи тестування. Це значно розширює поверхню атаки і робить традиційний захист менш ефективним [2].

У таких умовах компанії змушені переходити до принципу Zero Trust, який передбачає, що жоден пристрій, користувач чи запит не отримує автоматичної довіри незалежно від того, знаходиться він всередині корпоративної мережі чи

поза нею. Кожен елемент мережевого середовища повинен проходити сувору перевірку перед наданням доступу до ресурсів. Це означає обов'язкову аутентифікацію кожного пристрою, що підключається, а також користувача, який ним користується. Для цього застосовують сучасні механізми ідентифікації, багатофакторну аутентифікацію та постійний моніторинг активності.

Ключовим інструментом у реалізації такого підходу є використання мережевих політик доступу Network Access Protection або Network Access Control. Вони дозволяють визначати, чи відповідає пристрій корпоративним вимогам безпеки і на основі цього надавати або обмежувати доступ до мережі. NAC системи можуть автоматично ізолювати пристрої, які не відповідають політикам, направляти їх на виправлення або надавати обмежений доступ до гостьових сегментів.

Ще одним важливим елементом захисту є сегментація мережі - розподіл корпоративної інфраструктури на логічні або фізичні сегменти з різними рівнями довіри і доступу. Це дозволяє ізолювати BYOD-пристрої в окремі VLAN або підмережі, мінімізуючи ризики поширення загроз і обмежуючи доступ до критичних ресурсів лише тим користувачам і пристроям, які мають відповідні права. Використання сегментації в поєднанні з політиками контролю доступу створює багаторівневий захист, що є особливо актуальним у BYOD середовищах з великою кількістю різнорідних пристроїв.

Таким чином, у середовищі BYOD захист корпоративної мережі базується на комплексному підході, який поєднує обов'язкову аутентифікацію, застосування політик контролю доступу , а також сегментацію мережі і постійний моніторинг. Впровадження таких заходів дозволяє не лише мінімізувати ризики витоку даних і несанкціонованого доступу, а й підвищити загальну стійкість корпоративної інфраструктури до різноманітних загроз. Крім того, гнучкість і адаптивність системи безпеки сприяють підтримці продуктивності працівників, забезпечуючи їм зручний та безпечний доступ до необхідних ресурсів у будь-який час і з будь-якого місця. Цей підхід забезпечує ефективний захист інформації, враховуючи особливості використання особистих пристроїв, і відповідає

сучасним викликам кібербезпеки [3].

1.2 Основні загрози та атаки у середовищі

Під час використання концепції Bring Your Own Device в корпоративному середовищі з'являються нові можливості для працівників та підприємства, але з цим і відкриваються нові ризики для інформаційної безпеки. Особисті пристрої працівників, які будуть підключатись до мережі підприємства не завжди відповідають стандартам безпеки, чим створюються різного виду загрози. Однією з найбільших загроз в середовищі з концепцією BYOD є несанкціонований доступ до внутрішніх сервісів компанії. Потрібно, щоб пристрій мав належний захист, код, біометрична автентифікація або шифрування. Зловмисник може без проблем отримати доступ до ресурсів коли пристрій буде втрачено або перехоплено.

Особисті пристрої також часто можуть бути використані для особистих завдань чи робочих процесів, під час такого використання службові документи можуть стати синхронізованими з особистими хмарними сервісами, що створює ймовірність витоку даних. Працівники можуть також не свідомо встановити шкідливе програмне забезпечення на свій пристрій, який використовується в робочих в цілях і це дає змогу зловмисникам потрапити в корпоративну мережу та виконати різні протизаконні дії, мобільні трояни, фішингові додатки які здатні перехоплювати дані чи додавати шкідливий код в сервіси або ж спостерігати та досліджувати систему.

Одні з самих популярних атак це фішинг, до прикладу працівник використовує особистий пристрій для перевірки електронної пошти, на яку можуть потрапляти фішингові листи, які маскуються під справжні запити, ці атаки особливо небезпечні в такому середовищі де використовується концепція BYOD, оскільки особисті пристрої мають низький рівень фільтрації спаму. Вразливість операційної системи власного пристрою також може призвести до різних складних ситуацій з питань безпеки. Оновлення могло пройти не одразу за

відсутності централізованого контролю, також ноутбуки чи телефони можуть містити застарілі ОС чи програмне забезпечення, яке вже не актуальне в сфері безпеки, що призводить до експлуатації вразливості зловмисником. Підключення до публічних чи домашніх мереж, які не мають належного рівня захисту, через такі вразливі канали дані можуть бути перехоплені або також можливо попасти під атаку чоловік по середині. До цього слід додати, що пристрої можуть бути підключені до домашніх систем, які вже могли бути заражені шкідливим програмним забезпеченням, таке зараження може перейти на корпоративну мережу, особливо при використання знімних носіїв чи VPN [4].

Часто пристрої будуть знаходитись поза контролем IT відділу, тому це призводить до того, що на них можуть бути встановлені програми, які конфліктують з корпоративними ПЗ або можуть порушувати політику безпеки, також неможливо виконати примусово політику шифрування чи резервного копіювання, видалення даних. У разі інциденту інформаційної безпеки надзвичайно важливо мати можливість детально проаналізувати дії користувача, щоб встановити причини та наслідки події, проте особисті пристрої, які використовуються у рамках BYOD, часто не підключені до централізованих систем моніторингу подій, що значно ускладнює розслідування та виявлення джерела проблеми. Крім того, різноманітність пристроїв, які підключаються до корпоративної мережі, призводить до нерівномірного рівня захисту: деякі смартфони можуть підтримувати повне шифрування диску, тоді як інші ні. Відсутність єдиної централізованої політики безпеки, яка б гарантувала стандартизовані налаштування, залишає певні пристрої вразливими до атак і витоку даних.

Таким чином, BYOD створює значні виклики для безпеки, і його переваги зручність для працівників та економія для підприємства можуть бути реалізовані лише за умови впровадження ефективних стратегій захисту. Це включає розробку чітких політик безпеки, застосування технічних засобів контролю, таких як моніторинг активності та стандартизація захисних механізмів, а також постійне навчання персоналу для підвищення обізнаності щодо кіберзагроз і правильного

поводження з корпоративними даними. Важливо також враховувати, що технологічний розвиток вимагає регулярного оновлення політик та інструментів безпеки, щоб ефективно протистояти новим загрозам. Лише комплексний підхід забезпечить надійний захист інформації в умовах BYOD.

1.3 Вимоги до захисту інформації при використанні концепції BYOD

Сьогодні в сучасних корпоративних мережах з цією концепцією вимоги до безпеки інформації набуває високої уваги через специфіку використання своїх пристроїв робітниками на робочому місці. Вона дозволяє працівникам підключати власні планшети, ноутбуки та смартфони до мережі компанії для виконання своїх робочих завдань, що підвищує мобільність та гнучкість роботи, але з іншої сторони це створює багато викликів в сфері інформаційної безпеки, які вимагають різних підходів до захисту корпоративної мережі.

Відмінність мережі з концепцією BYOD від традиційної моделі полягає в тому, що пристрої, які підключаються в мережу не є власністю підприємства і не завжди потрапляють під централізований контроль IT відділу, вони можуть мати різний рівень захисту, різні операційні системи, що ускладнює управління безпекою, ці пристрої також і використовуються в приватних цілях, що збільшує ризик виникнення різних ситуацій з питань безпеки. У зв’язку з такою ситуацією захист в мережі повинен враховувати такі ключові аспекти. Ідентифікація пристроїв та аутентифікація робітників. Пристрій який підключається до мережі, повинен проходити обов’язкову перевірку, щоб підтвердити свою легітимність. Також слід додати, якщо використовувати багатофакторну аутентифікацію, то це одразу збільшить рівень безпеки та зменшить ймовірність несанкціонованого доступу таких пристроїв для використання в корпоративній мережі [5].

Сегментація мережі для зниження ризиків поширення загроз і витоку інформації в більш важливі ділянки компанії. Особисті пристроїв рекомендовано розміщувати в окремих сегментах VLAN, відокремлених від основної

корпоративної мережі, це дозволить контролювати трафік та обмежувати доступ до критичних ресурсів, не пропускаючи трафік далі чим потрібно.

Якщо ж перейти до більш структурованих правил то це є створення чіткої політики BYOD, яка повинна вказувати на типи дозволених пристроїв, умови доступу до корпоративної мережі, вимоги до захисту пристроїв та дії при втраті або крадіжці пристрою і також санкції за порушення цією політики. Якщо ж повернутись до аутентифікації, яка є важливо критична в такій концепції, потрібно використовувати нові технології 802.1X для контролю доступу на рівні комутатора. IEEE 802.1X це стандартний протокол контролю доступу до мережі, який забезпечує аутентифікацію пристроїв перед наданням їм доступу до локальної або бездротової мережі. Він реалізує модель взаємодії трьох сторін: клієнта , який є пристроєм, що підключається наприклад, ноутбук або смартфон, аутентифікатора мережевого пристрою, такого як комутатор або точка доступу, який контролює доступ до мережі; та сервера аутентифікації зазвичай реалізованого через RADIUS-сервер, що перевіряє облікові дані клієнта [6].

Застосування SSH ключів або сертифікатів користувачів для безпечного підключення до мережі. SSH-ключі та сертифікати користувачів є основними механізмами автентифікації в протоколі, який забезпечує безпечний віддалений доступ до серверів і захищений обмін даними [7].

Як і в будь якому безпечному сегменті, потрібне шифрування даних з метою запобіганню витоку інформації, для цього потрібно організувати VPN з’єднання, шифрування збереженої інформації на пристрої, також використання протоколів TLS для хмарних та внутрішніх веб додатків чи сервісів. TLS – це протокол, який захищає онлайн-комунікацію шляхом шифрування інформації та перевірки особи для забезпечення цілісності. Від перегляду веб сторінок до електронної пошти та VoIP, TLS є фундаментальною технологією, яка оберігає цифрову взаємодію та підтримує конфіденційність даних у сучасному інтернет-середовищі[8].

Також слід добавити, що всі дані які передаються чи зберігаються в мережі, повинні бути захищені такими способами, як застосування шифрування під час передачі за допомогою IPsec. IPsec це комплекс протоколів, призначений для

гарантування захисту даних, які передаються через IP-мережі. Він функціонує на мережевому рівні 3 моделі OSI, що дає змогу захищати будь-який трафік, який ґрунтується на протоколах TCP, UDP та інших. Головна мета IPsec є забезпечення конфіденційність, цілісність і справжність переданої інформації між двома кінцевими точками, якими можуть бути окремі пристрої чи мережеві шлюзи [9].

Використання протоколів, які не підтримують шифрування, таких як FTP і HTTP, створює серйозні ризики для безпеки корпоративної мережі та передачі даних. FTP передає інформацію у відкритому вигляді, включно з логінами, паролями та файлами, що робить її вразливою до перехоплення зловмисниками. Аналогічно, що HTTP не забезпечує захищеного каналу передачі даних, тому будь-яка інформація, що надсилається через цей протокол, може бути легко прочитана або змінена під час передачі. У сучасних умовах, коли захист конфіденційної інформації є пріоритетом, використання таких протоколів вважається неприпустимим.

Для забезпечення безпеки передачі файлів і даних рекомендується переходити на захищені альтернативи, такі як SFTP або FTPS, які шифрують трафік і гарантують цілісність та конфіденційність інформації. Так само для веб-трафіку слід використовувати HTTPS замість HTTP, оскільки HTTPS застосовує шифрування на транспортному рівні, що захищає дані від перехоплення і підробки. Використання цих протоколів дозволяє створити безпечний канал зв’язку, який є критично важливим для захисту облікових даних, фінансової інформації та інших конфіденційних даних.

Крім того, відкриті порти, які використовують незашифровані протоколи, часто стають мішенню для атак, тому їх слід блокувати на рівні брандмауерів і мережевого обладнання. Впровадження політик, що забороняють використання FTP і HTTP, а також перехід на безпечні протоколи, значно знижує ризики компрометації мережі. Це особливо важливо для корпоративних середовищ, де обробляється велика кількість чутливої інформації.

Постійне відстеження дій користувачів та пристроїв – потрібний для ефективного захисту корпоративної мережі, оскільки дає змогу завчасно виявляти

й ліквідовувати потенційні небезпеки. Збирання журналів автентифікації, VPN з'єднань та відвіданих ресурсів надає уявлення про активність у мережі, допомагаючи виявити аномалії або несанкціоновані дії. Обробка цих даних у режимі реального часу дозволяє IT-спеціалістам швидко реагувати на підозрілі події, мінімізуючи ризики втрати даних або порушення працездатності мережі. Сучасне програмне забезпечення для моніторингу мережі автоматично сповіщає про інциденти безпеки, значно пришвидшуючи процес реагування.

Впровадження систем управління мобільними пристроями є критично важливим для захисту корпоративних даних, особливо в умовах популярності концепції. Незважаючи на численні переваги, MDM-системи супроводжуються певними ризиками та викликами, які потребують уваги для їх ефективної та безпечної інтеграції. Одним з основних ризиків є загроза конфіденційності користувачів, оскільки можливості MDM-систем включають відстеження місцезнаходження пристроїв, контроль додатків та активності. Це може викликати у співробітників занепокоєння щодо їхньої приватності, особливо коли йдеться про використання особистих пристроїв для роботи. Надмірний контроль може зменшити мотивацію та підірвати довіру до роботодавця.

Безпека платформи MDM є ще одним критично важливим аспектом. Недоліки у системі або слабка автентифікація можуть стати воротами для зловмисників, що загрожує витоком конфіденційної інформації та компрометацією мережі. Невчасне оновлення програмного забезпечення через неправильні налаштування підвищує ризик вразливості пристроїв до атак. Крім того, суворі політики безпеки можуть обмежувати функціональність пристроїв, ускладнювати користування деякими додатками чи сервісами, знижуючи продуктивність співробітників. Існує також ризик випадкового чи навмисного блокування пристроїв, що може призвести до втрати цінної інформації і простоїв.

Інтеграція у наявну інфраструктуру супроводжується технічними та організаційними викликами, такими як налаштування політик і навчання персоналу, що може стати перешкодою для успішного впровадження. Важливим є розуміння того, що навіть при використанні MDM захист від соціальної

інженерії та фішингових атак залишається на рівні користувача.

Окрім того, моніторинг сприяє оптимізації продуктивності мережі, виявляючи вузькі місця та перевантаження, що дає змогу своєчасно коригувати налаштування та розподіл ресурсів. Безперервний контроль за діями користувачів та пристроїв також сприяє дотриманню корпоративних політик безпеки та відповідності стандартам. У разі інцидентів ведення журналів подій є незамінним для розслідування та визначення першопричин порушень. Запровадження комплексної системи моніторингу мережі є критично важливим для забезпечення цілісності, конфіденційності та доступності інформації в сучасних організаціях [10].

Освітній компонент та навчання персоналу — це ключова частина ефективної кібербезпеки в кожній організації, особливо в епоху BYOD. Жоден технічний захист не є бездоганним без відповідного рівня обізнаності співробітників, оскільки людський фактор часто є вразливою ланкою в системі безпеки. Відтак, регулярні тренінги з кібербезпеки, включаючи навчання методикам соціальної інженерії, є критично важливими.

Важливо, щоб навчання відбувалося періодично та містило не лише теоретичні знання, а й практичні елементи, наприклад, внутрішні тести і симуляції реальних атак. Такий підхід дає змогу працівникам опанувати навички швидкого реагування та формує культуру безпеки в організації, крім того, працівники повинні мати постійний доступ до корпоративної бази знань, де містяться політика безпеки, правила та інструкції щодо безпечного використання інформаційних ресурсів і пристроїв.

Окрему увагу слід приділяти роз’ясненню прав та обов’язків користувачів, які працюють. Це допомагає уникнути непорозумінь і забезпечує відповідальне ставлення до безпеки як з боку співробітників, так і керівництва. Важливо створити чітку систему відповідальності, яка засвідчує їх обізнаність та готовність дотримуватися встановлених правил.

Підсумовуючи, освітній компонент є фундаментом для створення ефективної системи захисту інформації, адже навіть найсучасніше технічне

обладнання не зможе повністю захистити організацію без свідомого та відповідального ставлення персоналу до кібербезпеки. Відтак, інвестиції в навчання персоналу є одним із найбільш ефективних способів захисту корпоративних мереж і даних у сучасних реаліях.

1.4 Постановка задачі

Мета даної роботи розробити та реалізувати систему захисту інформації в локальній мережі підприємства з концепцією BYOD, використовуючи інформацію про можливі атаки та з урахуванням, як потрібно виконувати захист. У ході роботи буде проведено аналіз основних загроз інформаційній безпеці, які можуть виникнути при роботі власних девайсів з корпоративною мережею. Увага буде зосереджена на моделюванні локальної мережі з урахуванням бездротового доступу для власних пристроїв, які будуть мати доступ в мережу. Потрібно виконати сегментацію мережі за допомогою VLAN, використовувати пристрої з сучасними протоколами безпеки WPA2 і також налаштування списків контролю доступу для виконання фільтрації трафіку між різними сегментами мережі.

Очікуваним результатом є створення готової моделі корпоративної мережі з реалізованими механізмами захисту для BYOD.

2 ОЦІНКА ТА ВИБІР ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ BYOD У КОРПОРАТИВНИХ МЕРЕЖАХ

2.1 Огляд сучасних рішень для захисту мережі

Існує декілька видів використання власних пристроїв на робочому місці з доступом в корпоративну мережу, які відрізняються між собою за рівнем контролю та власності над самим пристроєм. Найпоширеніший це BYOD, який вже був описаний, але є ще два популярних варіанти COPE, яка означає, що пристрій належить компанії, але працівники можуть його використовувати в різних місцях і в будь-який час, але це створює виклик безпеки через відсутність централізованого контролю над пристроєм з боку компанії.

Ще одна модель CYOD, коли пристрій обирається з затвердженого переліку від підприємства, він належить суто організації і постійно контролюються, цим забезпечуючи великий рівень безпеки та баланс між вибором та мінімум небезпеки. Кожен з цих видів має свої недоліки і також переваги в категоріях безпеки, контролю та зручності для працівників. Усі ці підходи передбачають використання сучасних технологій управління мобільними пристроями, шифрування, аутентифікації та мережевих політик для мінімізації загроз і забезпечення безпечного доступу до корпоративних ресурсів [11].

Системи виявлення та запобігання вторгненням є актуальною та ключовою складовою у сучасній мережевій безпеці, особливо при використані концепції, коли кількість різноманітних пристроїв підключених до мережі є доволі багато, вони створюють умови для моніторингу трафіку в мережі з цілю виявлення шкідливої активності, аномалій чи потенційних атак, що в майбутньому дозволить захистити корпоративні мережі від загроз. Система виявлення вторгнень – це інструмент, який працює у пасивному режимі, проводячи аналіз мережевого трафіку. Його головна ціль розпізнавати потенційно небезпечні дії, мережеві атаки та різного роду аномалії. Він реєструє виявлені інциденти та інформує відповідального адміністратора безпеки, не перериваючи та не змінюючи трафік у мережі. Система запобігання вторгненням, на відміну від простого виявлення,

діє активно. Вона негайно блокує спроби атак, реагуючи на них в реальному часі. Це дозволяє зупинити розповсюдження шкідливої активності, зводячи до мінімуму можливу шкоду. Вони функціонують у вигляді апаратно-програмних комплексів або програмних рішень, які гарантують всебічний аналіз мережевого трафіку, ідентифікацію відомих сигнатур атак, а також аномалій, які можуть вказувати на нові, невідомі загрози [12]. Найбільш використовуваними інструментами у цій галузі є Snort, Suricata.

Snort - це вільний софт, що застосовує сигнатурний аналіз мережевого трафіку для виявлення спроб проникнення. Розроблений у 1998 році, він стрімко завоював популярність як загальновизнаний стандарт завдяки легкості написання правил та активній підтримці спільноти. Він вдало поєднує сильні сторони сигнатурного підходу з можливістю виявляти аномалії в режимі реального часу, що робить його багатофункціональним інструментом для різних організацій. Але через архітектуру не повністю використовує переваги багатоядерних процесорів, що обмежує його продуктивність на сучасних апаратних платформах [13].

Suricata, зі свого боку, постає високопродуктивною системою IDS/IPS, сконструйованою на базі Snort, поширюючи складну обробку, що дозволяє оптимально використовувати ресурси сучасних багатоядерних процесорів та, навіть, графічних процесорів. Це надає можливість суттєво збільшити швидкість опрацювання трафіку на звичайному устаткуванні. Вона сумісна з тими самими модулями виявлення, що й Snort, але володіє більшими функціями IPS, які дозволяють не тільки виявляти загрози, але й активно їх блокувати. Система спроможна розпізнавати атаки як за сигнатурами, так і за аномаліями, що підвищує її результативність у протидії новим видам загроз. Поміж недоліків велика кількість налаштувань і відсутність достатньо чіткої документації, проте при правильній конфігурації вона демонструє високу надійність та швидкість роботи [14].

Застосування IDS/IPS в корпоративних мережах надає багато суттєвих переваг. Перш за все, це сприяє підвищенню загального рівня захищеності, шляхом своєчасного виявлення та припинення спроб атак, що суттєво знижує

імовірність злому систем та втрати інформації. По-друге, системи демонструють високу гнучкість, механізми оновлення правил та сигнатур забезпечує можливість швидкого реагування на виникнення нових загроз.

Найкращим рішенням для захисту мережі при використання концепції є впровадження MDM, який надає можливість керування мобільними пристроями. Являє собою програмно апаратне рішення, яке дозволяє використовувати централізоване управління, моніторинг і захист пристроїв смартфонів, планшетів чи ноутбуків в корпоративній мережі. Головним завданням є зниження ризиків для витоку конфіденційної інформації, перешкоджанням несанкціонованому доступу в мережу та строго слідувати політиці безпеки, яка була встановлена для відповідної мережі чи компанією. Вона дозволяє контролювати налаштувань безпеки для пристрою, вимога пароля, контролювати оновлення ОС на пристрої та шифрувати пам'ять. Забезпечує встановлення або видалення програмних застосунків компанії. Виконує контроль мереж до яких підключається пристрій та відслідковувати місце знаходження пристрою, також легко можна інтегрувати з різними системами автентифікації. Завдяки цій системі використання власних пристроїв стає більш безпечним для підприємства, зберігаючи контроль над корпоративною інформацією, що знижує можливість витоку інформації через програмне забезпечення чи не правильне зберігання інформації.

На ринку доступний різноманітний вибір систем, кожна з яких вирізняється унікальними рисами, перевагами та недоліками. Щоб зробити обдуманий вибір найбільш кращого рішення, варто провести ретельний аналіз кількох провідних продуктів, при цьому слід враховувати такі ключові аспекти, як продуктивність, рівень захисту, можливості взаємодії з наявною інфраструктурою, простота налаштування та підтримки, а також вартість впровадження та подальшого використання. Застосування такого підходу дозволить не тільки визначити оптимальний варіант з урахуванням технічних характеристик, а й забезпечить максимальну відповідність потребам конкретної компанії. Це є особливо важливим, враховуючи постійну еволюцію кіберзагроз та необхідність оперативного реагування на них.Серед великої кількості рішень, найбільш

поширеніші в корпоративному сегменті це Microsoft Intune, VMware WorkSpace ONE та IBM MaaS360 [15][16]. Вони всі забезпечують мінімальний функціонал керування та розширенні можливості будь яких інтеграцій для безпеки під час концепції BYOD. В таблиці 2.1 описано більш обширне порівняння.

Таблиця 2.1 – Порівняння систем MDM

Характеристика	Microsoft Intune	VMware WorkSpace ONE	IBM MaaS360
Платформа	Хмара	Хмара, Локально	Хмара, Локально
Інтеграція з ОС	Windows, iOS, Android, macOS	Windows, iOS, Android, macOS, Linux	Windows, iOS, Android, macOS
Контейнеризація	Часткова	Повноцінна	Повноцінна
Інтеграція з MFA	Microsoft Entra ID	VMware Verify	IBM Cloud Identity
Переваги	Глибока інтеграція з Windows365, просте управління	Висока персоналізація, розширена аналітика	Швидкий доступ, низький поріг входу

Щодо висновків, то можна добавити ще недоліки, для першої це те що вона працює в екосистемі Microsoft, для наступної це велика складність налаштування та доволі висока ціна і для останньої це обмежена підтримка з боку Linux[17].

Впровадження систем управління мобільними пристроями не лише знижує ризики витоку інформації, а й закладає початок для побудови архітектури Zero Trust. Ця концепція передбачає гнучке формування довіри до пристрою, користувача та запиту на основі різноманітних факторів, що суттєво покращує загальний рівень безпеки організації. Відтак, вибір відповідного рішення повинен брати до уваги наявну інфраструктуру, масштаб компанії та специфіку бізнес-процесів, що дасть змогу максимально ефективно захистити корпоративні дані в умовах BYOD.

Zero Trust модель нульової довіри – це сучасна концепція у сфері кібербезпеки, яка відходить від звичної практики захищати лише кордони мережі, де внутрішній простір сприймається як безпечний, а зовнішній, як потенційно небезпечний. Згідно з такою концепцією, жоден пристрій, користувач чи запит не отримують автоматичного доступу, незалежно від їхнього місцезнаходження усередині корпоративної мережі чи за її межами. Кожен запит на доступ до ресурсів підлягає ретельній перевірці, що включає аутентифікацію, авторизацію та оцінку контексту, враховуючи стан пристрою, роль користувача, місцезнаходження та інші показники. Цей підхід спирається на засади нікому не довіряй за замовчуванням, надання мінімально необхідних прав, в мережі та безперервний контроль активності та ризиків[18].

Система контролю доступу до мережі (NAC) – це важливий засіб для забезпечення безпеки, який перевіряє пристрої перед тим, як вони отримають доступ до мережі. Вона аналізує основні характеристики кінцевих точок, зокрема MAC-адресу, тип операційної системи, стан антивірусного захисту, наявність оновлень безпеки та інші важливі параметри. Тільки пристрої, які відповідають встановленим політикам безпеки, допускаються до мережі, тоді як ті, що не відповідають вимогам або можуть становити небезпеку, блокуються або ізолюються. Такий підхід суттєво зменшує вірогідність проникнення шкідливого програмного забезпечення та інших кіберзагроз у корпоративну мережу.

Розширені можливості NAC дозволяють не тільки перевіряти відповідність пристроїв політикам безпеки, але й автоматично реагувати на виявлені порушення. Система може ізолювати інфіковані або вразливі пристрої в карантинні сегменти мережі, де їм надається обмежений доступ для оновлення або лікування. Також підтримує інтеграцію з різноманітними антивірусними рішеннями та системами управління оновленнями, що дає змогу централізовано контролювати стан безпеки кінцевих точок. NAC здійснює інвентаризацію мережі, виявляє неконтрольовані або підозрілі пристрої, а також захищає від атак типу MAC Spoofing.

Крім того, сучасні рішення інтегруються з платформами управління мобільними пристроями та сервісами відповідності, наприклад, Microsoft Intune, що дозволяє приймати рішення про доступ на основі поточного стану пристрою, його реєстрації та відповідності корпоративним політикам. NAC реалізує умовний доступ, дозволяючи або обмежуючи доступ залежно від результатів перевірок, що збільшує гнучкість та безпеку мережі.

Щодо архітектури, може працювати в різних режимах In-band, коли весь трафік проходить через сервер контролю доступу, або Out-band, коли трафік перенаправляється на сервер лише у випадку необхідності перевірки. Це дозволяє оптимізувати продуктивність мережі та забезпечити ефективне управління доступом.

Отже, це комплексний інструмент, який не тільки контролює доступ до мережі, а й забезпечує автоматизоване виявлення, ізоляцію та лікування потенційно небезпечних пристроїв, інтегрується з іншими системами безпеки та підтримує гнучкі політики доступу. Це робить його незамінним елементом сучасних корпоративних мереж, особливо в умовах широкого впровадження BYOD та збільшення кількості мобільних та IoT-пристроїв. Наступне важливе сучасне рішення це використання антивірусних програмних забезпечень на пристроях, які будуть підключені до корпоративної мережі. Антивірусне забезпечення є критично важливим елементом у стратегії BYOD та загальному захисті корпоративної інфраструктури. Оскільки персональні пристрої працівників часто мають підвищену вразливість перед різноманітними онлайн-загрозами, такими як віруси, шкідливі програми, фішингові атаки, антивірусне програмне забезпечення на них відіграє ключову роль. Воно забезпечує виявлення, блокування та видалення шкідливих файлів, суттєво зменшуючи ризик поширення зараження в корпоративну мережу через особисті гаджети.

Не менш важливо, що антивірусне програмне забезпечення працює в реальному часі, постійно оновлюючись для ефективного протистояння новим загрозам. Це лише частина комплексного підходу до безпеки, який включає брандмауери, системи контролю доступу та моніторинг активності. Якщо на

особистому пристрої відсутній антивірус або він застарілий, це створює потенційні ризики в системі безпеки, через які зловмисники можуть проникнути в корпоративну мережу та викрасти важливу інформацію.

Серед популярних антивірусних продуктів, що активно використовуються в корпоративному секторі України та ідеально підходять, особливої уваги заслуговують Bitdefender GravityZone, ESET Endpoint Security, Sophos Intercept X та Avast Business Antivirus. Зазначені рішення гарантують всебічний захист від поточних кібернетичних загроз, демонструють підтримку різних операційних систем Windows, macOS, Android, iOS та надають можливість централізованого адміністрування безпекою значної кількості пристроїв, що надзвичайно важливо для надійного захисту корпоративних даних. В контексті, де співробітники підключаються до корпоративних ресурсів з різних місць та через різні мережі, антивірусний захист стає незамінним компонентом. Він допомагає мінімізувати ризики, пов'язані з використанням незахищених пристроїв або підключенням до ненадійних безпровідних мереж. Крім того, антивірусні рішення легко інтегруються з іншими системами безпеки.

2.2 Вибір обладнання для формування мережі з урахуванням концепції

Для того, щоб сформувати мережу з концепцією BYOD, потрібно підібрати та використати обладнання, яке буде підтримувати налаштування відповідного рівня безпеки мережі, також воно має буде розраховане на майбутнє розширення чи будь які зміни під час експлуатації. На цьому етапі слід відповідно віднестись до завдання та обрати оптимальні складові, для правильного формування та налаштувань корпоративної мережі підприємства. Отже насамперед потрібно обрати основні компоненти, які будуть керувати великим трафіком та піддаватись гнучким налаштуванням. Перший компонент який слід обрати маршрутизатор — це мережеве обладнання, що відіграє центральну роль у направленні трафіку між різними частинами мережі, зокрема, офісними підмережами, та забезпечує доступ

до Інтернету. Вони функціонують на мережевому рівні 3 моделі OSI, визначаючи шлях для пересилання пакетів даних, використовуючи таблиці маршрутизації та протоколи маршрутизації. Він повинен забезпечувати зв’язок між різними сегментами мережі та виконувати оптимізацію мережевого трафіку, знаходячи найкращі маршрути для передачі пакетів. Відповідає за забезпечення мінімального рівня безпеки через фільтрацію трафіку та контроль доступу ACL. Вимоги в зв’язку з концепцію це підтримка сучасних протоколів маршрутизації, можливості налаштування NAT,PAT, IPSec, VPN. В цьому випадку найбільш стабільним та хорошим варіантом буде Cisco ISR4331/K9 з двома портами, які дозволять отримати продуктивність від 50 Мбіт/с до 2 Гбіт/с, сам пристрій та його характеристики зображені на рисунку 2.1 [19].

Рисунок 2.1 – Маршутизатор Cisco ISR4331/K9

Для корпоративних мереж традиційно застосовуються маршрутизатори Cisco серій ISR4331/K9, які враховують потреби актуальних мереж та надають необхідні можливості маршрутизації, захисту та перетворення адрес. Ці прилади мають потрібну продуктивність для обробки значного обсягу трафіку та забезпечують гнучкість в конфігуруванні мережевих сервісів.

Для розбудови системи захисту інформації в локальній мережі підприємства, за концепцією BYOD, оптимальним варіантом буде комутатор Cisco Catalyst 3560. Цей корпоративний комутатор рівня доступу гарантує стабільну комутацію в локальних сегментах мережі та можливість підключення

різних пристроїв, таких як ПК, принтери, сервери, IP-камери та бездротові точки доступу. Його роль особливо важлива в BYOD-середовищі, де одночасно використовуються багато різних пристроїв з різними рівнями довіри. Cisco Catalyst 3560 підтримує VLAN, що дає змогу розділити мережу на окремі логічні підмережі, скажімо, для адміністраторів, співробітників, гостьових пристроїв та IoT, що значно покращує безпеку, ізолюючи трафік різних груп пристроїв.

Якість обслуговування забезпечує пріоритизацію трафіку для критичних додатків, як-от відеоконференції або голосовий зв'язок, що гарантує стабільність функціонування мережі навіть за великого навантаження. Порт-безпека дає змогу обмежувати доступ до портів комутатора за MAC-адресами, контролюючи, які саме пристрої можуть підключатися до мережі, що відчутно зменшує ризики несанкціонованого доступу.

Підтримка протоколу 802.1x забезпечує автентифікацію пристроїв при підключенні, що є важливим компонентом захисту BYOD, оскільки дає можливість перевіряти користувачів і пристрої перед наданням доступу до мережі. Окрім цього, комутатор підтримує списки контролю доступу (ACL) для фільтрації трафіку на рівнях 2-4, що забезпечує гнучке налаштування політик безпеки та блокування небажаного трафіку. Безпечне адміністрування досягається завдяки підтримці SSH, SNMPv3.

З технічного боку Cisco Catalyst 3560 має 8 портів Fast Ethernet з підтримкою PoE, один порт Gigabit Ethernet, Керування Cisco Catalyst 3560 реалізується за допомогою інтуїтивно зрозумілого веб-інтерфейсу, командного рядка, або віддалено через Telnet, що суттєво спрощує процес управління мережею. Комутатор забезпечує централізоване керування, надаючи можливість швидкої конфігурації та моніторингу мережевих параметрів, а також оперативного реагування на виниклі проблеми. Для підвищення загальної надійності мережі, пристрій використовує технології швидкого відновлення зв'язку, а також механізми резервування каналів і автоматичного виявлення помилок, інтеграцію з маршрутизаторами через протоколи маршрутизації OSPF, EIGRP і RIP. Завдяки своїм можливостям сегментації, контролю доступу, пріоритезації трафіку та

безпечного адміністрування Cisco Catalyst 3560 є надійним і функціональним рішенням для побудови захищеної локальної мережі підприємства з підтримкою BYOD, його можна розглянути на рисунку 2.2[20].

Рисунок 2.2 – Комутатор Cisco Catalyst 3560

Між мережевий екран Cisco ASA 5506-X – це сучасний брандмауер нового покоління, розроблений для забезпечення безпеки мережі вашого підприємства. Він протистоїть зовнішнім загрозам, контролює доступ між різними ділянками мережі, фільтрує трафік та дозволяє створювати безпечні VPN-з'єднання., гарантуючи комплексний захист від шкідливого програмного забезпечення та атак на всіх етапах, до атаки, під час неї та після її завершення. Фізичний дизайн Cisco ASA 5506-X представляє собою компактний вигляд, призначений для установки на стіл, з можливістю монтажу у типову стійку. Пристрій також має USB-порти, що дозволяють розширити функціональність та зручний інтерфейс для керування. Підсумовуючи, цей між мережевий екран є поєднанням надійності, високої продуктивності й передових функцій безпеки, що робить його ідеальним рішенням для захисту корпоративних мереж у контексті актуальних кіберзагроз та широкого використання концепції BYOD. Cisco ASA 5506-X легко інтегрується з іншими компонентами мережевої інфраструктури Cisco, підтримуючи централізоване управління. Це дозволяє адміністраторам повністю контролювати безпеку мережі, відслідковувати загрози та оперативно реагувати на інциденти. Поєднання високої продуктивності, масштабованості та розширених функцій

безпеки робить його ідеальним рішенням для захисту локальних мереж підприємств малого та середнього бізнесу, забезпечуючи надійний захист від зовнішніх атак та контроль доступу між внутрішніми сегментами мережі, який зображений на рисунку 2.3.

Рисунок 2.3 – Між мережевий екран ASA 5506-X

Для налагодження бездротового доступу в локальній мережі підприємства з урахуванням концепції BYOD, найкращим варіантом є маршрутизатор TP-Link Archer A64, що підтримує актуальні стандарти Wi-Fi 802.11ac/n і працює у двох діапазонах частот: 2,4 ГГц і 5 ГГц. Цей пристрій забезпечує швидкість до 867 Мбіт/с на частоті 5 ГГц і до 400 Мбіт/с на 2,4 ГГц, що дозволяє під'єднувати велику кількість пристроїв одночасно, серед яких ноутбуки, смартфони та інші BYOD-пристрої, зберігаючи високу продуктивність і стабільність з'єднання.

Він підтримує сучасні протоколи захисту WPA2 і WPA3, що гарантує надійний захист бездротової мережі. Також він має функцію створення гостьових мереж з ізоляцією пристроїв, що дає змогу розмежувати доступ гостей і корпоративної мережі, тим самим покращуючи безпеку інформації.

Окрім того, пристрій підтримує інтелектуальне підключення Smart Connect, яке автоматично розподіляє клієнтів між діапазонами для досягнення оптимальної продуктивності, а також забезпечує пріоритезацію трафіку для важливих додатків. Обладнаний чотирма гігабітними LAN-портами та одним гігабітним WAN-портом, що гарантує високу швидкість дротового підключення. Цей

маршрутизатор може інтегруватися в масштабовану мережу з плавним роумінгом, що особливо корисно для великих офісних просторів.

Управління пристроєм здійснюється через зручний веб-інтерфейс або мобільний додаток, що полегшує налаштування та моніторинг мережі. Отже, він забезпечує ефективне та безпечне рішення для організації бездротового доступу в мережі, яке відповідає вимогам сучасних стандартів, безпеки та сегментації мережі і зображений на рисунку 2.4[21].

Рисунок 2.4 – Маршутизатор Archer A64

Сервери у локальній мережі підприємства виконують критично важливі задачі, забезпечуючи стабільну роботу та безпеку мережі. Internet Server може виступати шлюзом або працювати з сервісами компанії, гарантуючи доступ до зовнішніх ресурсів та розміщення корпоративних веб-сайтів та інших сервісів. DHCP Server відповідає за автоматичне розподілення IP-адрес пристроям у мережі, що полегшує адміністрування та уникнення конфліктів. IOT GO Server призначено для управління IoT-пристроями, збереження даних та їх аналізу, що є необхідним для систем, інтегрованих у корпоративній інфраструктурі.

Для реалізації цих функцій, сервери повинні бути надійними, захищеними та підтримувати резервне копіювання, що є гарантією збереження даних та безперервності функціонування. Централізоване управління серверами дозволяє

ефективно контролювати процеси, оновлення та систему безпеки. У контексті IoT-систем ключовою є роль шлюзів, які забезпечують комунікацію між локальними пристроями та централізованими серверами, що дозволяє розвантажити канали зв'язку пристроїв та забезпечити надійне зберігання та обробку інформації.

Важливо пам'ятати, що централізація серверів створює єдину точку відмови та потенційну вразливість для атак, тому вкрай важливо впроваджувати надійні заходи безпеки, шифрування та контроль доступу. Отже, сервери DHCP та IOT у локальній мережі підприємства забезпечують комплексне управління мережевими ресурсами, автоматизують адресацію, а також збирають та аналізують дані, що є основою для створення надійної, захищеної та масштабованої системи інформаційної безпеки з урахуванням концепції BYOD.

Клієнтське обладнання, зокрема стаціонарні комп'ютери, ноутбуки та смартфони, відіграють роль робочих інструментів для співробітників, персональних пристроїв та адміністративних точок доступу в корпоративній мережі. Їхня конфігурація має повністю відповідати нормам політики безпеки, що включає встановлення антивірусного ПЗ, забезпечення підтримки VPN-клієнтів для безпечного дистанційного доступу, а також налаштування підключення як через дротові з’єднання, так і бездротові. Для гарантування безпеки користувачі зобов’язані проходити навчання з IT-безпеки уникати встановлення програмного забезпечення, не передбаченого офіційним білим списком дозволених програм, що зменшує загрозу зараження шкідливим програмним забезпеченням та несанкціонованого доступу. Додатково, робочі місця мають відповідати вимогам безпеки праці та охорони здоров'я, забезпечуючи оптимальні ергономічні умови, а технічне обладнання повинно бути в робочому стані, не наражаючи співробітників на небезпеку для життя та здоров'я. Отже, клієнтські пристрої у мережі підприємства мають бути правильно налаштовані та використовуватися з урахуванням вимог безпеки, сумісності з корпоративною інфраструктурою та підтримки сучасних методів захисту інформації, що є критичним аспектом впровадження концепції.

Веб-камери в мережі використовуються для відеоспостереження та контролю доступу. Вони мають підтримувати з'єднання до мережі з можливістю ізоляції їх трафіку в окремому VLAN, що дозволяє забезпечити безпеку передачі відеоданих і уникнути несанкціонованого доступу з інших сегментів мережі. Така сегментація надзвичайно важлива для захисту конфіденційної інформації, яка передається через камери і для мінімізації ризиків атак на мережеві пристрої відеоспостереження. Таким чином веб-камери повинні бути інтегровані в локальну мережу з урахуванням вимог безпеки, підтримуючи мережеві підключення та VLAN-сегментацію задля захисту інформації та ефективного керування мережевими ресурсами.

Обравши ці всі компоненти було б доцільно розрахувати скільки це все коштує, придбання мережевого устаткування та точний прорахунок його ціни надзвичайно важливий етап під час розгортання корпоративної мережі. Від них безпосередньо залежить ефективність, стабільність і здатність до масштабування всієї інфраструктури. Коректний вибір обладнання гарантує необхідну швидкість обміну даними, підтримку сучасних протоколів та технологій, а також відповідний рівень захисту, що надзвичайно важливо в умовах активного використання BYOD. До того ж, ретельне планування бюджету дає змогу уникнути непередбачуваних витрат, пов’язаних з додатковими матеріалами, монтажем, ліцензійними продуктами та послугами провайдерів, які часто виникають під час встановлення мережевих складових., яке буде закуплене, також розрахунки можуть не точні, через те що не буде розрахована коштовність це все встановити, витрати для матеріалів, які можуть з’явитись в ході встановлення різних компонентів і також оплата для використання різних програмних забезпечень, оплата послуг інтернет провайдера та встановлення відповідних з’єднань між пристроями, отже якщо це все не враховувати, то можна приблизно розрахувати витрати на ведення концепції, враховуючи лише мережеві компоненти, які були вказані вище. Додатково, беручи до уваги ці фактори, вдасться гарантувати безперебійне функціонування мережі та оптимізувати

вартість і ефективність придбаного обладнання та сервісів. В таблиці 2.2 приблизні витрати для корпоративної мережі.

Таблиці 2.2 – Розрахунок вартості

Обладнання	Кількість	Ціна
Cisco ISR4331/K9	1	62 840 грн
Cisco Catalyst 3560	3	89 997 грн
Archer A64	1	1599 грн
IP відеокамера DS-2CD1321-I	3	8139 грн
Cisco ASA 5506-X	1	39 800 грн
Сервер Supermicro 6038R-C1R16	2	31 665 грн

Отже, згідно з таблицею 2.2, загальна вартість необхідного обладнання для побудови захищеної корпоративної мережі за концепцією становить 225 901 гривню. Така інвестиція є виправданою з огляду на високий рівень безпеки, масштабованість та довготривалу експлуатацію обладнання в умовах політики BYOD.

2.3 Вибір рішень для побудови надійної системи захисту інформації

Маршрутизатори, комутатори, точки доступу, сервери та інші мережеві складові у мережі з концепцією BYOD виконують ключову функцію у гарантуванні безпеки та результативності роботи. Власні пристрої користувачів, а також інші елементи мережі, розподілятимуться на окремі VLAN (Virtual Local Area Network) – віртуальні локальні мережі, які логічно розділяють фізичну інфраструктуру. Це дає можливість ізолювати різні групи пристроїв, такі як, співробітників, гостьові пристрої, IoT-пристрої, адміністратори, власні пристрої,

що суттєво збільшує рівень безпеки, обмежуючи доступ до конфіденційних ресурсів та знижуючи ймовірність поширення загроз у мережі.

Комутатори, які підтримують VLAN, нададуть можливість конфігурувати порти належності до конкретної групи користувачів, а маршрутизатори забезпечують маршрутизацію між ними, застосовуючи при цьому списки контролю доступу для фільтрації трафіку за IP-адресами, портами та протоколами. Це дасть змогу гнучко регламентувати взаємодію між сегментами мережі та запобігати несанкціонованому доступу.

Для бездротових пристроїв у мережі налаштовані будуть точки доступу з підтримкою сучасних протоколів безпеки WPA2, що гарантує шифрування трафіку й автентифікацію користувачів. Гостьові мережі організовуються в окремому сегменті, ізольовані від основної корпоративної мережі, що дозволяє безпечно надавати доступ до інтернету особистим пристроям співробітників і гостей. Крім того, для захищеного віддаленого доступу співробітників з власних пристроїв будуть використовувати VPN, що забезпечить конфіденційність і цілісність переданих даних. Усі ці компоненти та функції підтримуються вибраним обладнанням і реалізуються у Cisco Packet Tracer, що дозволяє змоделювати та протестувати політики безпеки та контролю доступу в мережі.

Таким чином, поділ власних пристроїв і мережевих компонентів на VLAN, у поєднанні з налаштуванням ACL, сучасними протоколами Wi-Fi та VPN, створює надійну, керовану та безпечну мережеву інфраструктуру, яка відповідає вимогам та забезпечує ефективний захист корпоративних ресурсів.

У системі захисту інформації в мережах, де підтримується BYOD, протоколи IPSec, SSH та SSL відіграють ключову роль, гарантуючи безпечний обмін даними та автентифікацію користувачів. IPSec – це набір протоколів, що забезпечують захист IP-пакетів за допомогою шифрування та аутентифікації. Він функціонує у двох режимах: транспортному, де шифрується лише корисне навантаження пакету, та тунельному, в якому весь IP-пакет шифрується. Тунельний режим часто використовується для організації VPN-з’єднань між

віддаленими користувачами та корпоративною мережею, що особливо актуально для BYOD.

SSH – цей протокол забезпечить віддалений доступу до мережевих пристроїв та серверів. Він забезпечить шифрування команд та даних, що передаються між клієнтом та сервером, захищаючи інформацію від перехоплення.

SSL, точніше його сучасна версія TLS, буде використовуватися для захисту даних у мережі на рівні додатків. Вони забезпечуть шифрування трафіку між веб-браузерами та серверами, що особливо важливо для захисту веб-додатків та корпоративних сервісів, доступних співробітникам з власних пристроїв.

Отже, впровадження IPSec для організації VPN-з'єднань, використання SSH для безпечного адміністрування мережі та застосування SSL/TLS для захисту додатків і веб-трафіку формують багаторівневу систему безпеки. Ці протоколи забезпечують конфіденційність, цілісність та доступність даних, що критично важливо для захисту корпоративних ресурсів у сучасних гібридних мережах.

Протокол IEEE 802.1X – це стандарт аутентифікації на основі портів мережі, який забезпечує управління доступом до локальних мереж шляхом перевірки даних пристроїв, що намагаються підключитися до мережі. Його значення у контексті концепції є надзвичайно важливим, адже 802.1X дозволяє застосувати первинну фільтрацію доступу, унеможливлюючи під'єднання незатверджених чи скомпрометованих пристроїв до корпоративного середовища. У середовищі Cisco Packet Tracer є базова реалізація функціональності 802.1X, яка, хоча й не охоплює всіх аспектів протоколу, дає змогу змоделювати його основні принципи. Зокрема, у симуляції відтворюється процес аутентифікації за участю трьох основних складових: клієнтського пристрою, комутатора та сервера аутентифікації. Комутатор діє як посередник, який отримує запити на підключення та пересилає їх на сервер, котрий проводить перевірку облікових даних. Моделювання в Cisco Packet Tracer дозволить наочно показати, як блокуються порти для невідомих клієнтів, як активується доступ після успішної аутентифікації, а також динамічне призначення VLAN на основі результатів перевірки. Хоча симулятор не підтримує

повний набір функцій, що є у справжньому мережевому обладнанні Cisco, але він є ефективним інструментом для демонстрування основ управління доступом.

У контексті безпеки 802.1X виступає важливим елементом загальної архітектури Zero Trust, забезпечуючи ізоляцію неавторизованих пристроїв, зменшення області атаки та сприяючи сегментації мережі, таким чином, використання протоколу 802.1X є цінним навчальним засобом, який дає можливість дослідити базові аспекти мережевої безпеки в умовах сучасного цифрового середовища.

Регулярне оновлення прошивок мережевого устаткування, антивірусних баз та політик безпеки – це фундамент надійного захисту даних у корпоративних мережах, особливо з огляду на BYOD. Оновлення прошивок маршрутизаторів, комутаторів та точок доступу дозволяє ліквідовувати виявлені слабкі місця, покращувати стійкість роботи обладнання та збільшувати швидкість мережі. Виробники постійно випускають оновлення, які закривають вразливості у безпеці, які можуть бути використані зловмисниками для несанкціонованого доступу або атак. Відмова від цих оновлень створює суттєві ризики для цілісності мережі. Оновлення антивірусних баз забезпечує захист від нових видів шкідливого програмного забезпечення, що постійно удосконалюється.

Своєчасне оновлення дозволяє виявляти і блокувати актуальні загрози, мінімізуючи ймовірність зараження пристроїв та розповсюдження шкідливого коду в мережі. Не менш важливо регулярно переглядати та оновлювати політики безпеки, які визначають доступ користувачів і пристроїв, правила фільтрації трафіку. Це дає можливість адаптувати систему захисту до нових викликів та змін у структурі мережі.

Проведення аудиту і тестування системи безпеки є критично важливим для оцінки ефективності впроваджених заходів. Регулярний моніторинг мережевого трафіку, перевірка на вразливості та імітація атак допомагають виявити слабкі місця і швидко їх виправити, що суттєво збільшує загальний рівень захищеності. Отже, комплексний підхід до оновлення і підтримки системи безпеки – це

ключовий чинник забезпечення стабільної, безпечної та продуктивної роботи корпоративної мережі в умовах концепції.

Оцінка ризиків та план реагування на інциденти є ключовим елементом ефективної системи захисту інформації, особливо з огляду на впровадження BYOD, де різноманіття пристроїв і відсутність централізованого управління значно збільшують потенційні загрози. Обрані технічні рішення, як-от сегментування мережі за допомогою VLAN, впровадження контролю доступу через 802.1X, використання списків контролю доступу ACL, захищені протоколи VPN, а також сучасні методи шифрування Wi-Fi WPA2, суттєво зменшують ймовірність несанкціонованого доступу, розповсюдження шкідливого програмного забезпечення та витоку конфіденційної інформації.

Умови BYOD потребують посиленої уваги до безпеки мережі, особливо щодо управління доступом. У Cisco Packet Tracer налаштування AAA становить важливий компонент для забезпечення такого контролю. Це дає можливість централізовано управляти автентифікацією користувачів, санкціонуванням їх дій і обліком подій доступу, що критично важливо у ситуаціях, коли до мережі під'єднуються різноманітні персональні пристрої співробітників. У середовищі для впровадження AAA зазвичай використовують модель, де автентифікація відбувається через локальну базу користувачів. Конфігурація починається з увімкнення служби командою aaa new-model, після чого формуються списки методів автентифікації, які використовуються для різних типів доступу консоль чи VTY. Для середовищ з концепцією де є власні девайсе це дозволяє гнучко налаштовувати правила доступу.

Проте навіть за наявності комплексного захисту ризики інцидентів не можуть бути повністю виключені, тому вкрай важливо мати чітко окреслений план дій у разі їх виникнення. Такий план передбачає негайне виявлення інцидентів за допомогою систем моніторингу та ведення журналів, швидку ізоляцію уражених сегментів мережі, аналіз причин інциденту та оцінку масштабів його впливу. Наступним кроком є усунення вразливостей, відновлення

нормальної роботи системи та інформування відповідальних осіб і, за потреби, зовнішніх організацій.

Окрім технічних заходів, план реагування включає розробку процедур управління інцидентами, навчання персоналу діям у разі загроз, а також регулярне тестування готовності системи до надзвичайних ситуацій. Такий підхід дозволяє мінімізувати негативні наслідки інцидентів, зменшити час простою та забезпечити безперебійність бізнес-процесів.

2.4 Постановка задачі

В мережі, де буде активно функціонувати концепція BYOD особлива увага буде до питань безпеки. Ізоляція трафіку та управління доступом в мережі буде на першому кроці. Насамперед потрібно спроектувати та побудувати мережу підприємства з використанням маршрутизаторів, комутаторів, точок доступу, серверів, між мережевого екрану та кінцевих пристроїв. Потрібно реалізувати ізольовані сегменти для різних груп користувачів співробітники, адміністратор, IoT пристрої, власні девайси на основі VLAN. Щодо цього, потрібно його одразу й налаштувати для логічного розподілу, обмежити доступ до критичних ресурсів деяких груп користувачів мережі. Впровадження між мережевої маршрутизації з використанням списків контролю доступу, що дасть змогу керувати взаємодією між сегментами та блокувати несанкціонований доступ до корпоративних ресурсів. Забезпечення безпечного бездротового зв'язку через налаштування точок доступу з підтримкою WPA2. Впровадження VPN для безпечного віддаленого доступу, який гарантує конфіденційність та цілісність інформації, якою обмінюються співробітники, працюючи за межами офісного приміщення. Застосування актуальних протоколів безпеки SSH, SSL/TLS, 802.1X для гарантування захищеного адміністративного доступу, шифрування мережевого трафіку та автентифікації обладнання, що приєднується до мережі. Впровадження системи AAA Автентифікація, Авторизація, Облік для централізованого

керування, перевіркою ідентифікації, наданням дозволів та веденням обліку доступу користувачів та пристроїв. Це набуває особливої актуальності у контексті BYOD середовища. Політика оновлень та підтримки безпеки, створення моделей періодичного оновлення прошивок, антивірусних баз даних та правил доступу з метою забезпечення актуального рівня захисту. Важливо взяти до уваги використання IP-камер відеоспостереження, які працюють разом з IoT сервером для централізованого збирання, опрацювання та збереження відеоінформації. Камери під'єднані до мережі через комутатори з підтримкою PoE, завдяки чому вони отримують живлення і передають дані одним кабелем. Сервер відіграє роль платформи для управління пристроями, надаючи можливість спостерігати за станом камер, управляти ними.

Для автоматичного розподілу IP-адрес усім пристроям мережі, включно з камерами, персональними пристроями користувачів BYOD та сервером IoT, налаштовуються DHCP сервери. Вони спрощують адміністрування мережі, забезпечують динамічне і унікальне присвоєння адрес, що допомагає уникнути конфліктів і забезпечує безперебійну роботу мережі. У середовищі Cisco Packet Tracer DHCP сервери можуть бути розташовані як на маршрутизаторах, так і на окремих серверах, що дозволяє організувати мережеву інфраструктуру та забезпечити масштабованість.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ З ПІДТРИМКОЮ BYOD

3.1 Формування архітектури мережі

В межах цього проекту імітується корпоративна мережа, що враховує концепцію BYOD, яка надає безпечний доступ працівникам до інформаційних ресурсів підприємства. Мережа створена у середовищі Cisco Packet Tracer та складається з кількох логічно та фізично розділених частин, що дає змогу ефективно управляти доступом, збільшити рівень безпеки та забезпечити масштабованість інфраструктури. Перша зона в мережі, це доступ до мережі Інтернет, цей сегмент містить сервер, який імітує зовнішній інтернет ресурс і маршрутизатор, який забезпечує підключення між корпоративною та глобальною мережею. Таке моделювання дозволяє створювати реальні сценарії взаємодії з Інтернетом, виконувати тестування політики безпеки та виконувати фільтрацію трафіку зображено на рисунку 3.1.

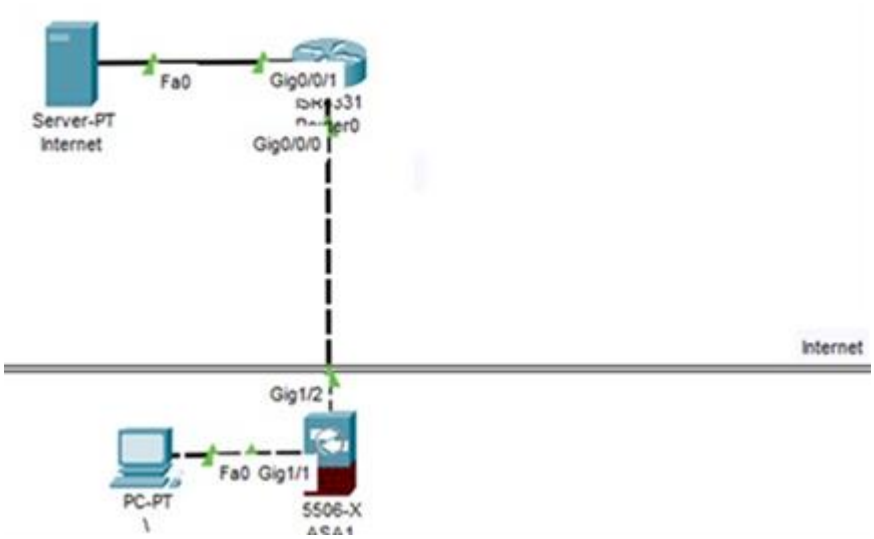


Рисунок 3.1 – Сегмент мережі Інтернет

Наступна зона це головний офіс, який містить між мережевий екран Cisco ASA 5506-X, функція якого контролювати між сегментний трафік, можливо організувати VPN з’єднання та захищає мережі від зовнішніх загроз. Також тут

розміщено сервер IoT для прямого доступу до нього в випадку збою і також для керування IP камерами, які знаходяться в іншому місці, а також окремий комп'ютер для адміністратора, що забезпечує централізоване керування мережею цей сегмент зображено на рисунку 3.2.

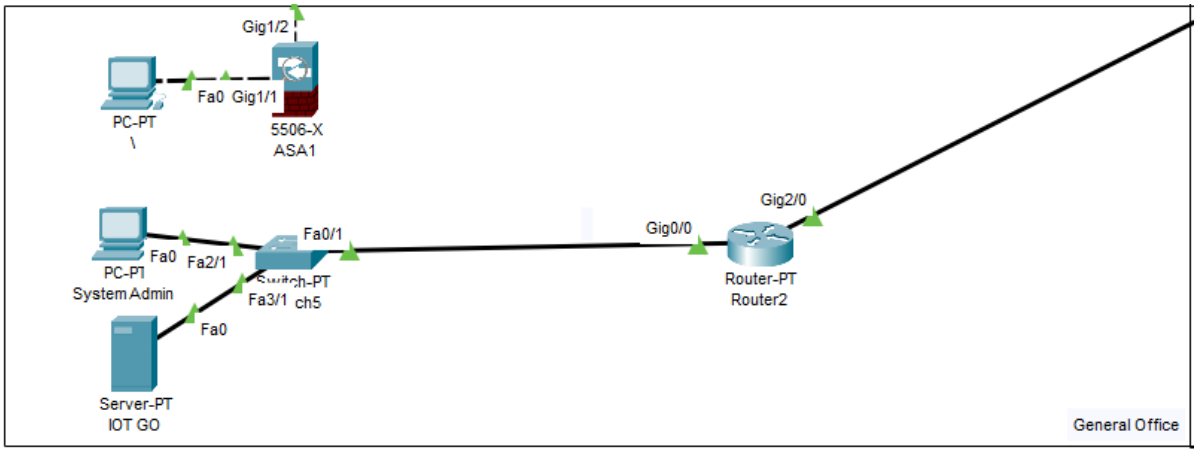


Рисунок 3.2 – Сегмент мережі головного офісу

Наступна і найбільш складна зона це сама офісна частина, вона містить основну частину корпоративної мережі, де знаходяться робочі станції співробітників, власні пристрої, які використовуються для роботи смартфони та ноутбуки, також знаходиться два комутатори, один для організування з'єднання з головним офісом та роботою з BYOD, а інший поміщає в себе робочі станції робітників, які належать суто підприємству. Також тут знаходяться IP камери, доступ до яких дозволено лише з головного офісу. Наявність DHCP серверу дозволяє динамічно розподіляти IP адреси для користувачів в середині сегменту, але також і маршрутизатор для власних пристроїв має власні налаштування типу DHCP і також видає IP адреси власним пристроям, які відносяться до цього сегменту мережі і не конфліктує з основним DHCP сервером. Це дає змогу змоделювати сучасне офісне середовище, включаючи підтримку корпоративних мереж Wi-Fi. Всі пристрої підключені через керований комутатор, який дозволяє сегментувати мережу за допомогою VLAN. Також слід добавити, що в цьому сегменті знаходиться персональний комп'ютер адміністратора, який має права доступу лише в цьому сегменті мережі, та не може звернутись в головний офіс для

керування пристроями там чи змінити налаштування головного маршрутизатора, сегмент мережі зображено на рисунку 3.3.

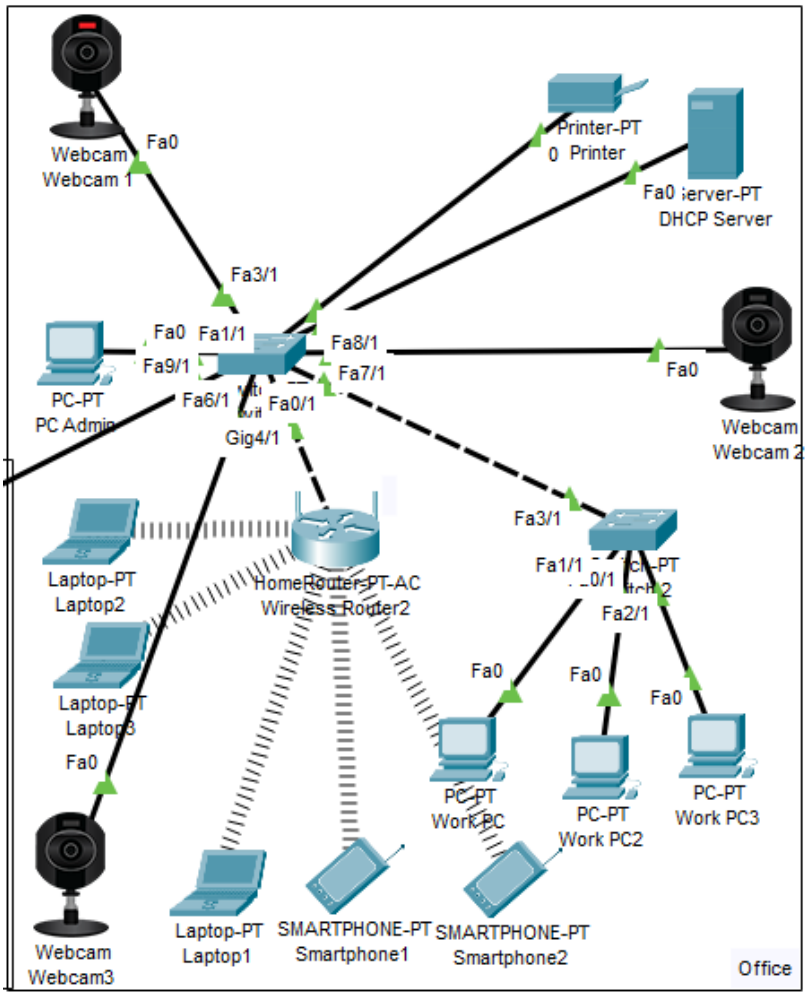


Рисунок 3.3 – Сегмент мережі основного офісу

Завдання цього кроку – створення адаптивної, розширюваної та захищеної мережі, що відповідає поточним потребам корпоративної інфраструктури, гарантує безпечний доступ для різноманітних категорій користувачів та пристроїв, а також надає можливість ефективного керування всіма складовими мережі.

Також слід добавити, що це лише логічне формування мережі, а для повноцінного зображення, потрібно відобразити фізичне розташування та виконати розрахунок розмірів розташування, правильне підключення та розмежування. Середовище Cisco Packet Tracer надає деякі функції для виконання

цього завдання. Як зрозуміло то головний офіс та фактичний знаходяться в різних місцях, що було відображено в середовищі, добавляючи, що Інтернет теж знаходиться в іншому місці, для більш правдивого оформлення ситуацій з реального життя. Це дозволяє створити більш правдоподібну модель, яка враховує географічні та інфраструктурні особливості, а також спрощує планування і подальше масштабування мережі. Виконана сегментація у фізичному вигляді зображена на рисунку 3.4.

Рисунок 3.4 – Фізичне відображення мережі

На рисунку видно структуру розташування окремих просторів або зон, з'єднаних мережевими лініями. Це не тільки візуалізує логіку мережі, але й дає змогу оцінити фактичні відстані між складовими, що важливо при плануванні кабельних трас, встановленні обладнання та забезпеченні належного рівня сигналу, особливо для бездротових мереж. Кожен сегмент мережі має чітко окреслені межі, розмір та функціональне призначення.

Детальне фізичне планування мережі враховує не тільки поточні потреби, але й можливість подальшого розширення, оновлення або зміни фізичної структури мережі без значних додаткових витрат. За допомогою середовища Cisco Packet Tracer було збудовано мережу, що складається з кількох частин, відокремлених як логічно, так і фізично. Доступ до Інтернету, головний офіс з між мережевим екраном та сервером IoT, а також офісна зона з робочими станціями, власними пристроями, IP камерами та DHCP серверами. Ця архітектура мережі сприяє ефективному контролю доступу, збільшує рівень захисту та підтримує можливість розширення інфраструктури.

3.2 Конфігурація мережі

Насамперед конфігурація мережі розпочнеться з налаштування маршрутизатора, який розділяє мережу на два сегменти, потрібно підключити два комутатори з двох різних сегментів та розпочати конфігурацію на самому пристрої. Для початку підняти порти для того, щоб вони перейшли в режим роботи, після цього встановити IP адреси підмереж з маскою, яка буде вказувати на кількість можливих підключених пристроїв в підмережі. Саме ці налаштування виконуються на інтерфейсах в які підключені комутатори. В середовищі виконання завдання це можна виконати за допомогою застосунка, або ж команд[22]. Встановлення IP адрес зображено на рисунку 3.4.

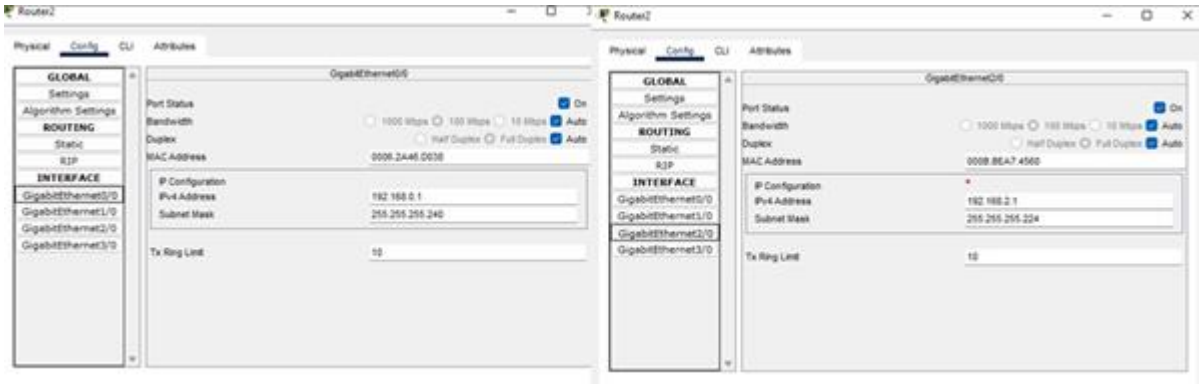


Рисунок 3.4 – Налаштування IP на маршрутизаторі

Наступним чином це налаштування комутаторів, а саме VLAN. Кожна віртуальна локальна мережа VLAN отримує свій унікальний ідентифікатор та розподіляється конкретній групі користувачів. Порти комутаторів, до яких під'єднані кінцеві пристрої, налаштовуються для належності до певної VLAN, що дозволяє ізолювати їхній трафік від інших частин мережі. Для взаємодії між комутаторами використовуються типи портів, які можуть передавати трафік відразу кількох VLAN одночасно. Ці порти функціонують в режимі trunk, що дозволяє об’єднати різні VLAN в один фізичний канал зв’язку, зберігаючи при

цьому поділ трафіку на логічному рівні. Це забезпечує правильне направлення даних між різними частинами мережі, а також спрощує розширення інфраструктури. Підсумовуючи, впровадження VLAN та trunk-ліній у мережі дає можливість ефективно контролювати доступ та оптимізує використання мережевих ресурсів. Створені VLAN отримують свій унікальний ідентифікатор[23]. Назви груп користувачів та ідентифікатори знаходяться в таблиці 3.1.

Таблиця 3.1 – Створені VLAN

VLAN 10	Робочі підстанції підприємства
VLAN 20	BYOD пристрої
VLAN 30	IoT пристрої
VLAN 40	Адміністративний доступ

Для автоматичного розподілу IP-адрес обладнанням, приєднаним до офісної ділянки, задіяно DHCP-сервер. Це суттєво полегшує управління мережею, усуває потребу ручного вводу IP-адрес на кожному пристрої та мінімізує можливість адресних конфліктів, що критично важливо в BYOD середовищі, де кількість підключених пристроїв може змінюватися. У вкладці DHCP сервера зазначено, що служба DHCP активна для інтерфейсу FastEthernet0. Створено пул адрес під назвою serverPool, призначений для видачі IP-адрес у підмережі 192.168.2.0/27. Початкова IP-адреса для розподілу 192.168.2.5, декілька адрес збережено для статичного ведення деяким пристроям, які цього потребують, а максимальна кількість клієнтів, які можуть отримати IP-адресу з цього пулу, дорівнює 27. Як стандартний шлюз використано адресу 192.168.2.1, що дозволяє всім клієнтам автоматично налаштовувати параметри для доступу за межі локальної мережі. Завдяки такому налаштуванню, всі пристрої, підключені до відповідного VLAN або мережевого сегмента, у тому числі робочі станції, портативні комп'ютери, смартфони та IoT-пристрої, автоматично отримують унікальні IP-адреси, маску підмережі та адресу шлюзу[24]. Це забезпечує стабільну роботу мережі, спрощує

підключення нових пристроїв та дозволяє ефективно управляти адресним простором навіть при динамічному підключенні BYOD-пристроїв, налаштування зображено на рисунку 3.5.

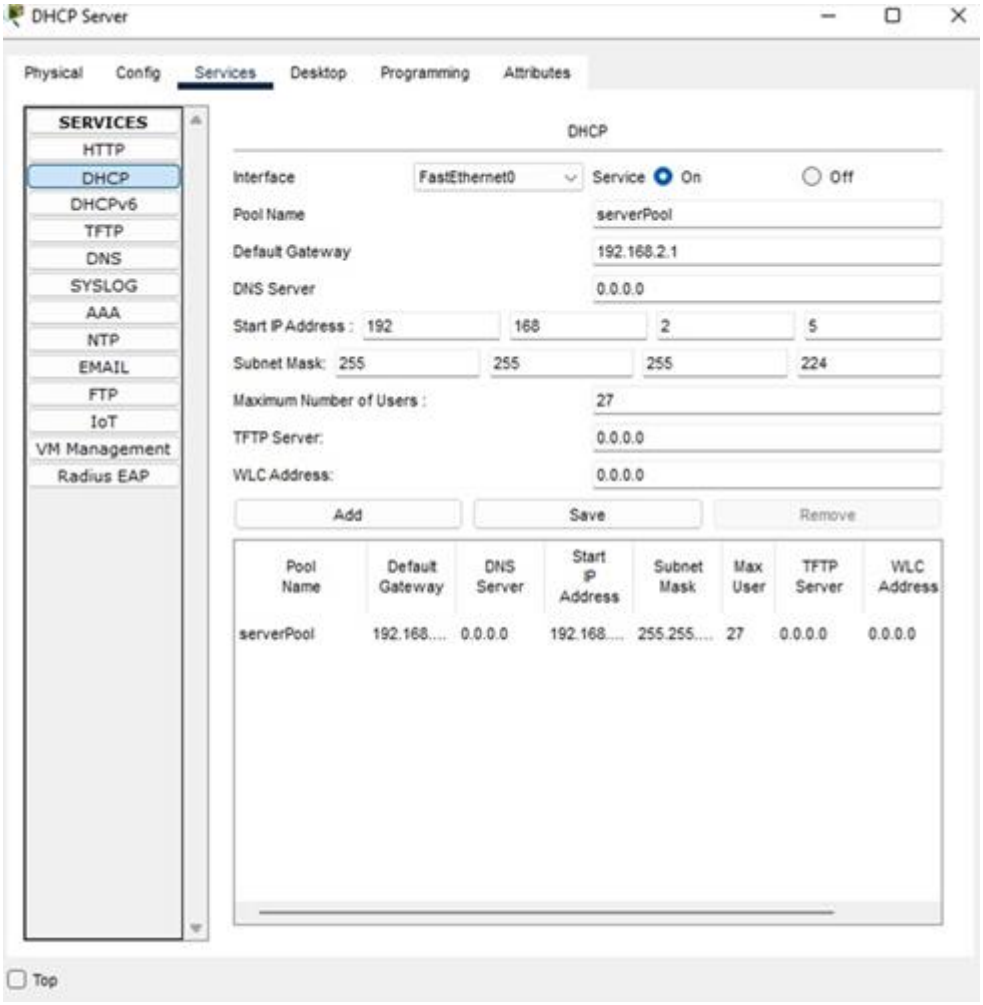


Рисунок 3.5 – Налаштування DHCP сервера

Впровадження DHCP у мережі збільшує масштабованість інфраструктури, зменшує обсяг роботи адміністратора та забезпечує безперервність функціонування офісної частини мережі, незалежно від кількості та типу підключених пристроїв.

Конфігурація бездротового доступу у мережі реалізовано бездротову точку доступу, необхідну для забезпечення сучасного офісу та концепції BYOD. Вона дає змогу мобільним пристроям працівників підключатись до корпоративної Wi-Fi мережі. Згідно з налаштуваннями, бездротовий маршрутизатор працює на

частоті 2,4 ГГц і має покриття 250 метрів, що дає змогу охопити всю офісну територію. Для забезпечення високого рівня безпеки використовується протокол аутентифікації WPA2 з шифруванням AES. Це сучасний стандарт для захисту бездротових мереж, який гарантує захист даних від несанкціонованого доступу та перехоплення[25]. Налаштовано використання спільного секретного ключа. Такий підхід забезпечує централізоване управління доступом до мереж, налаштування зображено на рисунку 3.6.

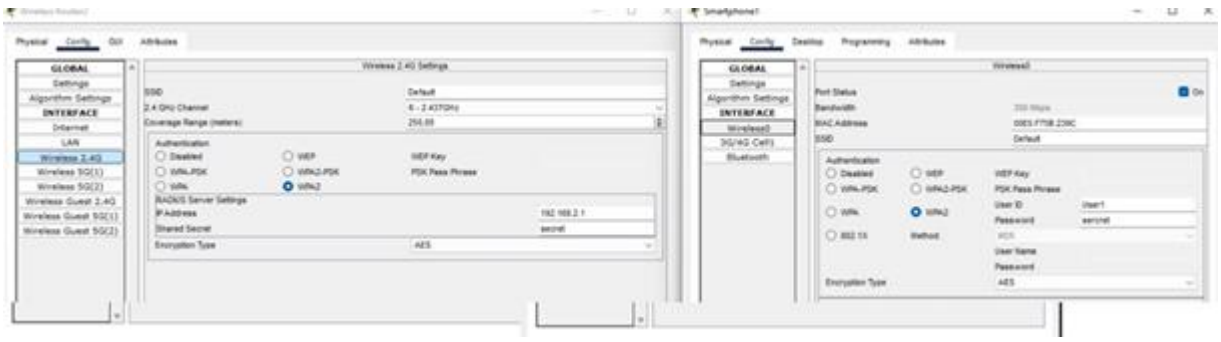


Рисунок 3.6 – Налаштування аутентифікації власних пристроїв в мережі

На прикладі підключення смартфона, що для доступу до Wi-Fi використовується автентифікація WPA2 з введенням логіна та пароля. Після успішної аутентифікації пристрій автоматично отримує IP-адресу за допомогою DHCP, спрощуючи процес підключення та адміністрування мережі. Завдяки такому налаштуванню бездротова мережа не лише зручна, але й добре захищена від зовнішніх загроз. Це дає можливість безпечно підключати BYOD-пристрої.

Мережа включає впровадження AAA, яка гарантує контроль доступу до мережевих ресурсів, підсилюючи рівень безпеки, особливо з огляду на BYOD. На маршрутизаторі CentralRouter та комутаторі OfficeSwitch втілено базові механізми автентифікації користувачів і пристроїв, авторизації операцій та обліку активності. На маршрутизаторі активовано локальну базу користувачів, де створено обліковий запис адміністратора з розширеними привілеями, що дає можливість контролювати доступ до пристрою. Вхід через консольний порт та віддалені сесії (VTY) захищено паролями, а для віддаленого доступу використовується протокол SSH, що забезпечує шифрування трафіку та захист від

перехоплення даних. Для підвищення безпеки виконано шифрування паролів у конфігурації. Комутатор OfficeSwitch також налаштовано на захищений доступ з використанням паролів для консолі та віддалених сесій, а також містить секретний пароль для посилення захисту. Завдяки цьому, адміністрування комутатора доступне тільки авторизованим користувачам [26].

Незважаючи на використання локальної автентифікації у конфігурації, це створює надійний базовий рівень контролю доступу. Для подальшого підвищення безпеки можлива інтеграція зовнішніх серверів RADIUS, що дозволить централізовано керувати обліковими записами, авторизацією та аудитом дій користувачів у мережі. Отже, запровадження AAA у мережі гарантує, що доступ до мережевого обладнання мають тільки авторизовані користувачі, що критично важливо для захисту корпоративної мережі в умовах активного використання різних пристроїв.

У межах проекту впровадження списків контролю доступу є важливим елементом підвищення безпеки мережі та контролю трафіку між різними сегментами. Зокрема, налаштований розширений ACL з номером 102 дозволяє доступ IP-камер до сервера з IP-адресою 192.168.0.3, що забезпечує безпечний канал передачі відеоданих. Також у ACL передбачено дозвіл для ПК системного адміністратора з мережі головного офісу до сегменту робочої зони, що гарантує адміністративний контроль. Всі інші спроби доступу, які не відповідають цим правилам, блокуються за допомогою директиви "deny ip any any", що запобігає несанкціонованому трафіку та знижує ризики проникнення або поширення загроз у мережі. Цей ACL застосовано на інтерфейсі GigabitEthernet2/0 вхідним напрямком, що дозволяє контролювати трафік, який надходить у мережу офісної зони, і ефективно фільтрувати пакети ще до їх обробки внутрішніми пристроями. Впровадження таких правил є актуальним і необхідним, особливо в умовах активного використання BYOD, коли кількість пристроїв з різними рівнями довіри постійно зростає. ACL дозволяє чітко регламентувати доступ до критичних ресурсів, мінімізуючи ризики несанкціонованого проникнення та забезпечуючи виконання політик безпеки. Таким чином, налаштування ACL у мережі сприяє

підвищенню рівня захисту, контролю доступу та стабільності роботи інфраструктури, відповідаючи сучасним вимогам кібербезпеки та корпоративної політики.

Налаштування Cisco ASA 5506-X служить як між мережевий екран, що гарантує захист корпоративної мережі, контроль трафіку та маршрутизацію між внутрішньою та зовнішньою мережами. Інтерфейс GigabitEthernet1/1 визначено як внутрішній з найвищим рівнем безпеки та отримав IP-адресу 192.168.0.1 з маскою 255.255.255.240, яка відповідає локальній мережі підприємства. Інтерфейс GigabitEthernet1/2 налаштовано як зовнішній з найнижчим рівнем безпеки та має IP-адресу 210.210.0.2, що з'єднує ASA із зовнішньою мережею або Інтернетом. Об'єктна конфігурація obj_any визначає правило NAT, яке забезпечує динамічну трансляцію внутрішніх IP-адрес у зовнішній інтерфейс ASA, дозволяючи внутрішнім користувачам мати доступ до Інтернету через одну публічну адресу. Маршрути за замовчуванням прописані для обох інтерфейсів: внутрішній інтерфейс має маршрут на всі мережі через 0.0.0.0, а зовнішній інтерфейс скеровує трафік на шлюз провайдера 210.210.0.1. Це забезпечує коректну маршрутизацію трафіку між внутрішньою мережею та Інтернетом. Політика доступу на зовнішньому інтерфейсі реалізована через access-list outside_access_in, яка дозволяє весь IP-трафік та ICMP-повідомлення, що відкриває базовий зовнішній доступ. Цей список доступу застосовано до зовнішнього інтерфейсу для контролю вхідного трафіку. Для забезпечення захисту мережі використовується класова карта inspection_default, яка застосовує інспекцію трафіку за замовчуванням. Глобальна політика global_policy включає інспекцію різних протоколів, таких як DNS, FTP, H323, HTTP, ICMP та TFTP, що дозволяє ретельно аналізувати та контролювати мережевий трафік, запобігаючи можливим загрозам [27].

У цілому, конфігурація ASA 5506-X забезпечує надійний захист внутрішньої мережі, контроль доступу та безпечний вихід до зовнішньої мережі, задовольняючи сучасні вимоги корпоративної безпеки та ефективного управління трафіком.

У роботі реалізовано механізм забезпечення якості обслуговування з метою контролю різноманітних видів трафіку. Це гарантує ефективне використання мережевих ресурсів та підтримує стабільну роботу критичних програм, зокрема в умовах BYOD середовища. Конфігурування стартує зі створення класів трафіку class-map, які розподіляють пакети за протоколами: HTTP, HTTPS, та відео трафік. Це дозволяє ідентифікувати ключові типи даних, які потребують першочергової обробки.

Наступним кроком є створення політики QoS, де кожному класу трафіку визначається певний відсоток пріоритетного каналу 15% для HTTP та HTTPS, а 30% для відео трафіку. Решту трафіку обробляють за допомогою механізму справедливої черги fair-queue, забезпечуючи рівномірний розподіл пропускної здатності для менш важливих даних. Політика QoS застосовується на вихідних інтерфейсах GigabitEthernet2/0 та GigabitEthernet0/0, що дозволяє розподілити трафік на фізичному рівні, забезпечуючи якісне обслуговування як для користувачів офісної мережі, так і для зовнішніх ресурсів [28]. Впровадження такої системи особливо важливе для корпоративних мереж з BYOD, адже дозволяє забезпечити якісний зв'язок для важливих сервісів, таких як відеоконференції та веб-застосунки, навіть при значному навантаженні на мережу. Це підвищує продуктивність та зручність користувачів, а також знижує ризик втрати даних або затримок у роботі критичних додатків. Підсумовуючи, налаштований QoS сприяє раціональному використанню мережевих ресурсів, гарантує пріоритетність важливого трафіку та відповідає сучасним вимогам до якості обслуговування в умовах динамічних корпоративних середовищ.

В межах змодельованої мережі, побудованої на Cisco ASA 5506-X, запровадження VPN гарантує захищений віддалений доступ для персоналу до корпоративних ресурсів, що критично важливо в умовах BYOD. Технологія VPN дозволить працівникам приєднуватись до офісної мережі з будь-якої точки, забезпечуючи безпечний канал для передачі даних та збереження приватності інформації. Для досягнення цієї мети на ASA 5506-X налаштовується Remote Access VPN, який оперує за протоколом IPsec з шифруванням трафіку. Мережа

клієнта має два головні інтерфейси: внутрішній з IP-адресою 192.168.0.1 та зовнішній з адресою 210.210.0.2, підключений до Інтернету. VPN-клієнти будуть здійснювати підключення через зовнішній інтерфейс, отримуючи IP-адреси з виділеного пулу, наприклад, 192.168.100.10–192.168.100.50, що логічно ізолює їх від основної внутрішньої мережі. Автентифікацію користувачів можна організувати з використанням локальної бази ASA, де створюються облікові записи співробітників з відповідними ідентифікаторами та паролями. Таким чином, реалізація VPN на Cisco ASA 5506-X у мережі забезпечує надійний захист даних, зручність віддаленого доступу та ефективне управління мережею, що сприяє підвищенню продуктивності працівників і збереженню корпоративної інформації.

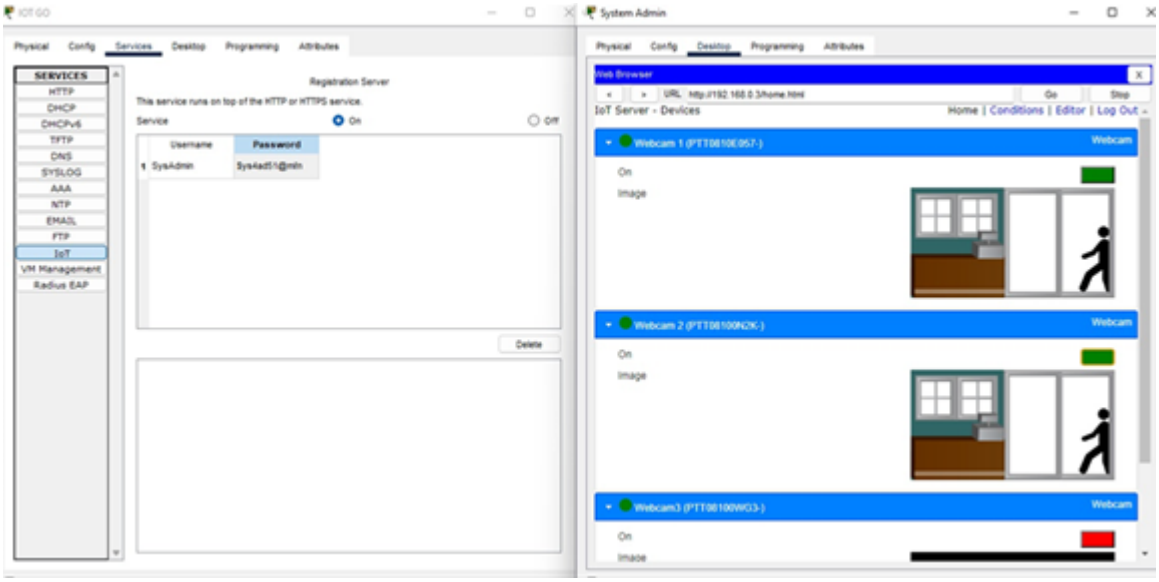


Рисунок 3.7 – Принцип роботи IoT сервера

Також реалізований контроль за відеокамерами, за допомогою підключення до серверу IoT, доступ до якого є лише у системного адміністратора, для підключення потрібно на ПК підключитись в мережу та ввести дані для входу, логін та пароль, який був створений для користувача, після цього буде доступне керування, яке зображено на рисунку 3.7.

Для підключення до IoT-сервера адміністратору необхідно з робочого комп’ютера приєднатися до корпоративної мережі та ввести облікові дані - логін

і пароль, які були попередньо створені для цього користувача. Після успішної аутентифікації відкривається інтерфейс керування, через який можна здійснювати моніторинг та керування підключеними IP-камерами. Завдяки впровадженню цієї системи, доступ до відеоінформації суворо регламентований, що відповідає сучасним вимогам корпоративної безпеки та захисту даних.

3.3 Політика безпеки мережі

В рамках мережевої інфраструктури компанії, розроблено всеосяжну політику безпеки для користувачів, спрямовану на захист інформаційних активів, керування доступом та мінімізацію вірогідності несанкціонованого доступу або витоку даних. Враховуючи особливості реалізації концепції BYOD та сучасні виклики інформаційній безпеці, ця політика відповідає поточним вимогам корпоративних мереж. Кожному користувачеві надається персональний обліковий запис з унікальним логіном та надійним паролем, які підлягають періодичній заміні. Права доступу суворо визначені відповідно до посадових обов'язків, що дозволяє обмежити адміністративні привілеї лише необхідному колу користувачів. Особливий контроль передбачено для доступу до критичних ресурсів, таких як сервери, системи відеоспостереження та IoT-пристрої.

Впроваджено механізми AAA (Аутентифікація, Авторизація, Облік), що забезпечують надійну ідентифікацію користувачів, моніторинг їхніх дій та ведення журналу активності. Для віддалених підключень використовується VPN з аутентифікацією, що суттєво покращує рівень захисту від несанкціонованого доступу. Застосування технології VLAN дозволяє логічно відокремити різні групи пристроїв та користувачів, що зменшує ризики розповсюдження кіберзагроз та забезпечує контрольований доступ до мережевих ресурсів. Організовано безперервний автоматизований моніторинг мережевого трафіку та подій безпеки, що дає змогу оперативно виявляти підозрілу активність та реагувати на можливі загрози. Особлива увага приділяється моніторингу активності віддалених

користувачів, що підвищує загальний рівень безпеки мережі. Користувачі повинні дотримуватися встановлених правил безпечної роботи з корпоративними обліковими записами: не розголошувати паролі, використовувати лише дозволені пристрої та програмне забезпечення, уникати відкриття сумнівних листів та файлів, а також негайно інформувати адміністраторів про будь-які підозрілі інциденти. На пристроях користувачів встановлено антивірусне програмне забезпечення, забезпечено регулярне оновлення операційних систем та застосування політик безпеки, що сприяє захисту від шкідливого програмного забезпечення та кіберзагроз. Між мережеві екрани та системи фільтрації трафіку контролюють вхідний та вихідний потік даних, запобігаючи проникненню шкідливих пакетів та обмежуючи доступ користувачів до небажаних ресурсів.

В рамках політики безпеки корпоративної мережі, першочергову увагу приділити плановому оновленню програмного забезпечення та операційних систем на всіх пристроях, що належать мережі, включно з робочими станціями, серверами, мобільними телефонам. Своєчасне оновлення має критичне значення для підтримки високого рівня безпеки, бо воно усуває відомі уразливості, збільшує сумісність з актуальними платформами та забезпечує безперебійну роботу мережі. Щодо мобільних телефонів, які використовуються працівниками в корпоративному середовищі, встановлення останніх версій операційних систем і програмних оновлень слугує гарантією захисту від новітніх загроз та шкідливого програмного забезпечення. До того ж, на мобільних пристроях реалізується політики безпеки, що регулює використання паролів, шифрування даних та контроль доступу до корпоративних ресурсів.

Розроблена політика безпеки користувачів гарантує конфіденційність, цілісність та доступність корпоративних даних, знижує ризики внутрішніх та зовнішніх загроз, а також підтримує гнучкість та мобільність співробітників в сучасних умовах BYOD та віддаленої роботи. Постійне удосконалення та виконання цієї політики є ключовими факторами надійного захисту мережі підприємства.

3.4 Висновки до розробленої мережі

Розбудова корпоративної мережі надає низку вагомих переваг, гарантуючи її стабільність, захищеність та продуктивність. Впроваджено сегментування мережі на базі VLAN, що дозволяє розмежувати різні категорії пристроїв та користувачів, посилюючи контроль доступу та зменшуючи ризики розповсюдження загроз. Механізми AAA забезпечують надійну автентифікацію, авторизацію та аудит дій користувачів, що сприяє зростанню рівня безпеки. Використання між мережевого екрану Cisco ASA 5506-X забезпечує захист внутрішньої мережі від зовнішніх атак та дозволяє організувати безпечний вихід у глобальну мережу. Налаштований VPN-сервіс надає захищений віддалений доступ для співробітників, що особливо актуально в умовах BYOD та мобільності персоналу. Автоматизація розподілу IP-адрес через DHCP полегшує адміністрування мережі та забезпечує динамічне підключення пристроїв. Впровадження механізмів якості обслуговування дозволяє розподіляти важливі сервіси, такі як відеоконференції та веб-додатки, що покращує загальну продуктивність та зручність користувачів. Окрім того, регулярне оновлення операційних систем, програмного забезпечення та політик безпеки на всіх пристроях, включаючи мобільні телефони, забезпечує захист від сучасних загроз та підтримує стабільну роботу мережі.

Разом з тим, у поточній конфігурації мережі відсутні деякі важливі елементи, які могли б суттєво покращити рівень безпеки та управління. Зокрема, не впроваджено систему управління мобільними пристроями, що ускладнює централізований контроль над BYOD-пристроями, їхньою безпекою та оновленнями, а також обмежує ефективне застосування політик використання. Відсутність Network Access Control обмежує можливості автоматичного контролю доступу пристроїв до мережі на основі їхньої відповідності корпоративним стандартам безпеки, що може призвести до підключення небезпечних або несанкціонованих пристроїв. Крім того, відсутність інтеграції з RADIUS-

сервером або Cisco ISE ускладнює централізовану автентифікацію та авторизацію користувачів та пристроїв, що обмежує впровадження розширених політик безпеки та профілювання пристроїв.

ВИСНОВКИ

У результаті проведених робіт було розроблено та змонтовано корпоративну мережу, що відповідає актуальним потребам безпеки, масштабованості та ефективності функціонування бізнесу. Впроваджена мережа гарантує стабільний та безпечний доступ користувачів до інформаційних ресурсів, підтримує концепцію BYOD, а також дозволяє централізовано керувати усіма компонентами інфраструктури.

Створена мережа має чітку структуру – як логічну, так і фізичну. Це дозволяє ефективно сегментувати трафік за допомогою VLAN, ізолювати різноманітні категорії пристроїв та користувачів, а також контролювати доступ до критичних ресурсів. Застосування між мережевого екрану Cisco ASA 5506-X забезпечує надійний захист від зовнішніх загроз, а налаштування VPN дозволяє організувати безпечний віддалений доступ для співробітників.

Впровадження механізмів DHCP, AAA, а також списків контролю доступу сприяє автоматизації управління мережею, підвищує безпеку та гнучкість інфраструктури. Налаштування якості обслуговування забезпечує пріоритет критичних сервісів, таких як відеоконференції та веб-додатки, що позитивно впливає на продуктивність та зручність користувачів.

Окрему увагу було приділено оновленню програмного забезпечення та операційних систем на всіх пристроях, включно з мобільними телефонами та BYOD-пристроями, що дає змогу підтримувати високий рівень захисту від актуальних загроз. Централізоване управління оновленнями мінімізує ризики вразливостей і забезпечує стабільність роботи мережі.

Загалом, створена мережа відповідає вимогам сучасного підприємства, забезпечує єдиний інформаційний простір, підвищує швидкість обробки даних і сприяє зменшенню витрат на зв’язок та адміністрування. Одночасно з цим реалізовані заходи безпеки гарантують захист корпоративної інформації, що є вкрай важливим в умовах сучасних ризиків та активного використання мобільних пристроїв. Отже, розроблена мережа є надійною, масштабованою та безпечною

платформою для підтримки бізнес процесів підприємства, що забезпечує ефективну роботу співробітників і сприяє досягненню стратегічних цілей організації.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Вивчення мереж URL: https://www.globalyo.com/uk/blog/understanding-the-basics-what-is-a-network-and-how-does-it-work/ (дата звернення 04.03.2025)
2. Концепція BYOD URL: https://netwave.ua/blog/tehnologiya-byod-sho-ce-plyusi-ta-riziki/ (дата звернення: 04.03.2025).
3. Definition of Bring Your Own Device URL: https://www.gartner.com/en/information-technology/glossary/bring-your-own-device-byod (дата звернення: 05.03.2025)
4. Тренд BYOD: як зменшити ризики використання особистих девайсів в корпоративних мережах URL: https://www.pcweek.ua/themes/detail.php?ID=168468&THEME_ID=13875 (дата звернення 09.03.2025)
5. Bring Your Own Device (BYOD) Security Configuration URL: https://www.cisco.com/c/en/us/td/docs/wireless/technology/5760_deploy/Bring_Your_Own_Device_-BYOD-_Security_Configuration.html (дата звернення 09.03.2025)
6. Інтеграція стандарту кібер-безпеки 802.1X в IP протокол CIAS URL: https://www.fortisec.com.ua/news/integratsiya-standartu-kiber-bezpeky-802-1x-v-ip-protokol-cias (дата звернення 11.03.2025)
7. Що таке автентифікація на основі сертифіката SSH? URL: https://oberig-it.com/statti/shcho-take-avtentifikatsiya-na-osnovi-sert/#:~:text=Сертифікат SSH-це відкритий ключ (дата звернення 13.03.2025)
8. Що таке протокол безпеки TLS URL: https://alexhost.com/uk/faq/shho-take-protokol-bezpeky-tls/#:~:text=TLS – це важливий протокол, який,даних у сучасному інтернет-середовищі. (дата звернення 15.03.2025)
9. IPsec URL: https://www.vpnunlimited.com/ua/help/cybersecurity/ipsec?srsltid=AfmBOorEpAAqaRC5WsELKURdvCK7axy04Xt7_MnfOWRGOZwYCBrFOdst
10. Моніторинг мережі: контроль за стабільністю та безпекою інфраструктури URL: https://avolutech.com/blog/моніторинг-мережі/

11. BYOD, CYOD, COPE, COBO: What do they really mean? URL: https://www.samsungknox.com/en/blog/byod-cyod-cope-cobo-what-do-they-really-mean

12. Що таке IPS/IDS і де застосовується URL: https://www.hostzealot.com.ua/blog/about-solutions/shho-take-ipsids-i-de-zastosovujetsya

13. Snort URL: https://www.vpnunlimited.com/ua/help/cybersecurity/snort?srsltid=AfmBOooiim6PaR4sIuaIx84ZdokF6zSQXN7Fxkv5VDPH_YCjboWKB-vl

14. Suricata 4.0 виявляє зловмисників та контролює мережевий трафік URL: https://uk.ubunlog.com/meerkat-4-0-відстежує-мережевий-трафік/

15. Microsoft Intune URL: https://www.microsoft.com/uk-ua/security/business/microsoft-intune

16. VMware Workspace ONE URL: https://softprom.com/ua/vendor/vmware/product/vmware-workspace-one

17. IBM MaaS360 vs Microsoft Intune vs Workspace ONE UEM comparison URL: https://www.peerspot.com/products/comparisons/ibm-maas360_vs_microsoft-intune_vs_workspace-one-uem

18. Модель Zero Trust: принципи та переваги URL: https://techexpert.ua/zero-trust-model/

19. Маршрутизатор Cisco ISR4331/K9 URL: https://stack-systems.com.ua/marshrutizator-cisco-isr4331-k9?srsltid=AfmBOoorEJZ5K9RF_gtuMKlAlPiwcbKjOGGtXRXgMvLVFbkQ_yVd9av-

20. Комутатор Cisco WS-C3560-8PC-S URL: https://stack-systems.com.ua/kommutator-cisco-ws-c3560-8pc-s

21. AC1200 Wi-Fi маршрутизатор з MU-MIMO URL: https://www.tp-link.com/uk-ua/home-networking/wifi-router/archer-a64/

22. Налаштування маршрутизаторів Cisco URL: https://daad.org.ua/13641-nalashtuvannya-marshrutizatora-cisco.html#_2

23. VLAN це: Як працює та навіщо потрібен URL: https://cyberset.com.ua/network/vlan-how-it-works-and-why-you-need-it/

24. DHCP сервер на маршрутизаторі Cisco URL: https://sysadmin-god.at.ua/publ/cisco/ccna4_accessing_the_wan/dhcp_server_na_marshrutizatori_cisco/7-1-0-5

25. Налаштування маршрутизатора Cisco URL: https://lucky.net/cisco/

26. Configure Basic AAA on an Access Server URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/10384-security.html

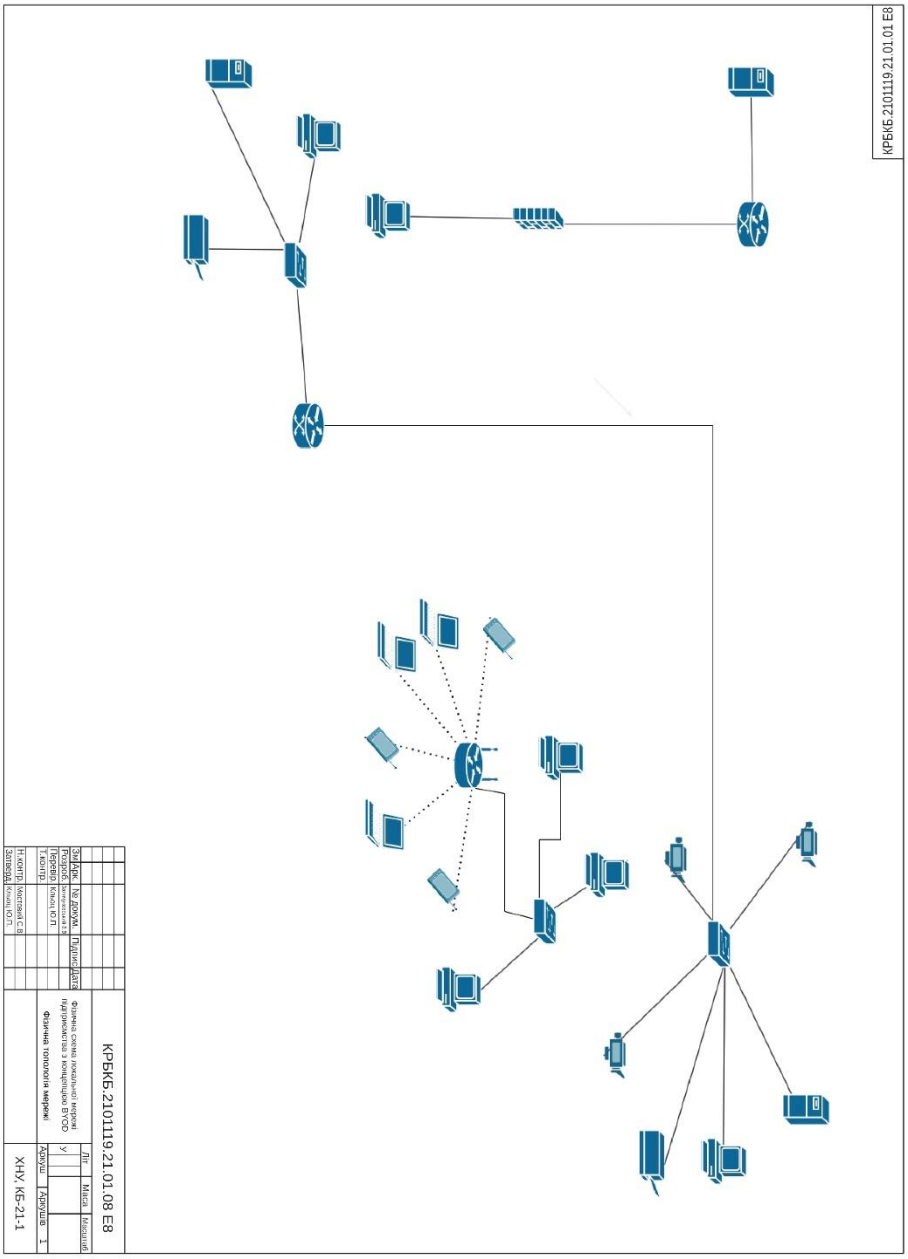
27. Packet Tracer – Configure ASA Basic Settings and Firewall Using the CLI Answers URL: https://itexamanswers.net/21-7-5-packet-tracer-configure-asa-basic-settings-and-firewall-using-the-cli-answers.html

28. Cisco 800M Series ISR Software Configuration Guide URL: https://www.cisco.com/c/en/us/td/docs/routers/access/800M/software/800MSCG/QoS.html

ДОДАТОК А

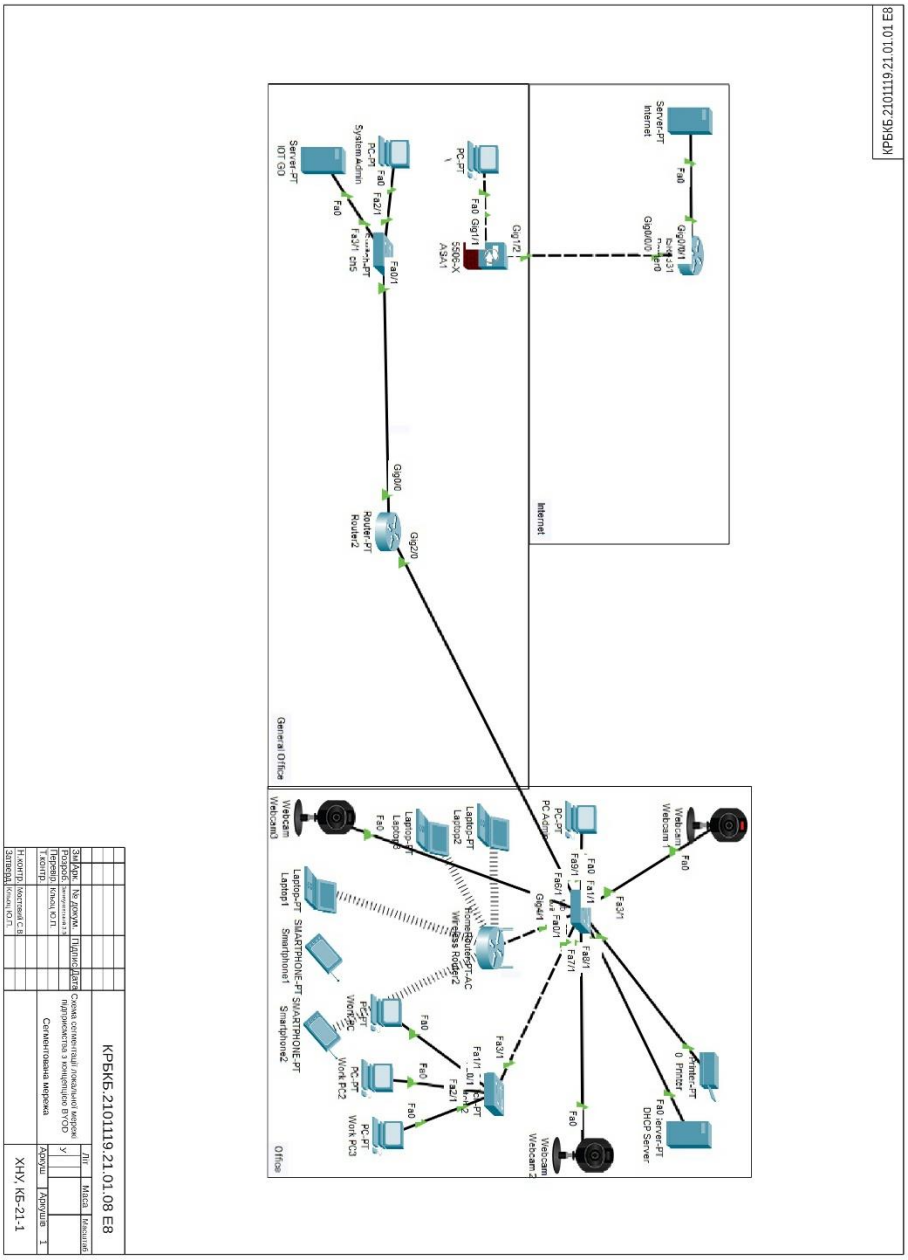
Копія графічної частини

Логічна топологія



Фізична топологія

Схема сегментації мережі



ДОДАТОК Б

Конфігурація мережі

// General Office

```
enable
configure terminal
hostname CentralRouter
banner motd $Authorized access only!$
enable secret Adm1n$
service password-encryption
no ip domain-lookup
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.240
no shutdown
interface GigabitEthernet2/0
ip address 192.168.2.1 255.255.255.224
no shutdown
line console 0
password 0neS
login
logging synchronous
exec-timeout 60 0
ip domain-name central
crypto key generate rsa
2048
ip ssh version 2
username admin privilege 15 secret admin
line vty 0 4
```

```
transport input ssh
login local
logging synchronous
exec-timeout 60 0
exit
exit
copy running-config startup-config

// Office swtich

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

//QoS Пріоритизація

enable
```

```
configure terminal
class-map match-all TCP
 match protocol http
class-map match-all UDP
 match protocol https
class-map match-any VIDEO-TRAFFIC
 match protocol rtp
 match protocol h323
exit
policy-map QOS-POLICY
 class TCP
  priority percent 15
 class UDP
   priority percent 15
 class VIDEO-TRAFFIC
   priority percent 30
 class class-default
  fair-queue
exit
exit
interface GigabitEthernet2/0
service-policy output QOS-POLICY
interface GigabitEthernet0/0
service-policy output QOS-POLICY
end

// Вхідний канал

interface GigabitEthernet0/0
```

```
 fair-queue

// ASA 5506-x

interface GigabitEthernet1/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.240
interface GigabitEthernet1/2
 nameif outside
 security-level 0
 ip address 210.210.0.2 255.255.255.240
object network obj_any
 subnet 0.0.0.0 0.0.0.0
 nat (inside,outside) dynamic interface
route inside 0.0.0.0 0.0.0.0 0.0.0.0
route outside 0.0.0.0 0.0.0.0 210.210.0.1
access-list outside_access_in extended permit ip any any
access-list outside_access_in extended permit icmp any any
access-group outside_access_in in interface outside
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
```

```
  inspect h323
  inspect http
  inspect icmp
  inspect tftp
service-policy global_policy global
```

// ACL

```
g2/0
access-list 102 permit ip host 192.168.2.12 host 192.168.0.3
access-list 102 permit ip host 192.168.2.13 host 192.168.0.3
access-list 102 permit ip host 192.168.2.14 host 192.168.0.3
access-list 102 permit ip 192.168.2.0 0.0.0.31 host 192.168.0.4
access-list 102 deny ip any any
interface GigabitEthernet2/0
ip access-group 102 in
```

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Заянчуковського Владислава Володимировича
ПІБ здобувача вищої освіти

Студента ФІТ, 4 курсу, групи КБ-21-1

ЗАЯВА

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

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

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

04.06.2025
дата

підпис

Протокол аналізу звіту подібності науковим керівником

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

Автор: Заянчуковський Владислав Володимирович

Співавтор:

Назва: Система захисту інформації в локальній мережі підприємства за концепцією BYOD

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1%

Коефіцієнт подібності 2:0.2%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-06 11:23:16.0

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:

06.06.2025р.

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 1.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

ID: 243865 Title: Система захисту інформації в локальній мережі підприємства за концепцією BYOD Added in a DB: 2025-06-06 Authors: Заянчуковський Владислав Володимирович Heads: Кльоц Ю.П. Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	90606	549	508 (1%)	5 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Система захисту інформації в локальній мережі підприємства за концепцією BYOD

Автор: Заянчуковський Владислав Володимирович

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Юрій КЛЬОЦ, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 99%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 99%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Юрій КЛЬОЦ

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Заянчуковський Владислав Володимирович

Тема Система захисту інформації в локальній мережі підприемства за концепцією BYOD

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 3; кількість сторінок записки 62.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі створено локальну мережу підприемства з використанням концепції BYOD, із використанням сучасного обладнання, що забезпечує захист, використано різні технології безпеки в мережі, створення відповідних правил безпеки, налаштування конфігурацій, використання між мережевого екрану захисту та розподіл під мережі на різні сегменти.

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

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі виконано аналіз теоретичних використання концепції в мережі, де розглянуто сучасні приклади використання такої концепції. Другий розділ присвячено порівнянню різних аспектів безпеки при використанні концепції, виконано підбор мережевого обладнання. У третьому розділі реалізовано практичне завдання та налаштування конфігурації для безпеки мережі при використанні такої концепції

4. Позитивні сторони роботи Робота має практичну цінність, оскільки пропонує сучасне рішення впровадження концепції в локальну мережу підприемства, реалізує моніторинг та високий рівень безпеки, використано загальні рішення безпеки, використання VPN, 802.1x, zero trust моделі.

5. Негативні сторони роботи Залежність від своєчасного оновлення політик доступу та правил аутентифікації в BYOD середовищі, несвоєчасні оновлення можуть призвести до зниження ефективності контролю пристроїв і пропуску нових загроз у локальній мережі підприемства..

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

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки весь матеріал роботи є структурованим, чітким та послідовним. Усі розділи роботи мають логічну послідовність, що сприяє зрозумінню викладеного матеріалу в рамках теми роботи. Графічний матеріал допомагає наочно продемонструвати доцільність та ефективність прийнятих рішень у проєктуванні та супроводі розробленої комплексної системи захисту інформації.

8. Інші зауваження

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є добре

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи)
Підченко Сергій Костянтинович, завідувач кафедри телекомунікацій, медійних та інтелектуальних технологій, д.т.н., професор

« 08 » 06 2025 _____ (підпис)