Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Розробка локальної комп’ютерної мережі та організація кіберзахисту для ТзОВ “Прометей”

Виконав: студент IV курсу, групи СНс-42
спеціальності 122 Комп’ютерні науки
(шифр і назва спеціальності)

_____ Олійник В.М.
(підпис) (прізвище та ініціали)

Керівник _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Боднарчук І.О.
(підпис) (прізвище та ініціали)

Рецензент _____ _____
(підпис) (прізвище та ініціали)

Тернопіль
2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
Боднарчук І.О.
(підпис) (прізвище та ініціали)
«__» _____ 2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 122 Комп'ютерні науки
(шифр і назва спеціальності)

студенту Олійнику Владиславу Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка локальної комп'ютерної мережі та організація кіберзахисту для ТзОВ "Прометей"

Керівник роботи Матійчук Любомир Павлович, д.е.н., доц., професор кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «29» квітня 2024 року № 4/7-470

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Технічне завдання на розробку мережі та організацію кіберзахисту для ТзОВ "Прометей"

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1.Аналіз предметної області. 2. Проектування локальної комп'ютерної мережі для ТзОВ "Прометей" 3. Моделювання роботи локальної комп'ютерної мережі ТзОВ "Прометей" з організацією кіберзахисту 4. Безпека життєдіяльності, основи охорони праці. Висновки. Список літературних джерел

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Мета та актуальність роботи. 2. Практичне значення результатів. 3. Фізична топологія 4. Розрахунок IP адрес 5. Вибір обладнання 6. Модель мережі компанії "Прометей" 7. Налаштування статичних параметрів на ПК 8. Налаштування комутатора 9. Налаштування WiFi 10. Налаштування DHCP сервера 11. Налаштування маршрутизатора 12. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Сенчишин В.С. заступник завідувача кафедри інжинірингу машинобудівних технологій		

7. Дата видачі завдання 29 січня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	30.01.2025	*Виконано*
2.	Підбір наукових джерел щодо розробки проекту	31.01.2025-03.02.2025	*Виконано*
	мережі ТзОВ “Прометей”		
3.	Переклад та опрацювання джерел щодо розробки	04.02.2025-06.02.2025	*Виконано*
	мережі ТзОВ “Прометей”		
4.	Виконання дослідження щодо розробки проекту	07.02.2025-11.02.2025	*Виконано*
	мережі ТзОВ “Прометей”		
5.	Оформлення розділу «Аналіз предметної області»	03.06.2025-05.06.2025	*Виконано*
6.	Оформлення розділу «Проектування локальної комп’ютерної мережі для ТзОВ “Прометей”	06.06.2025-08.06.2025	*Виконано*
7.	Оформлення розділу «Моделювання роботи локальної комп’ютерної мережі ТзОВ “Прометей” з організацією кіберзахисту	09.06.2025-11.06.2025	*Виконано*
8.	Виконання завдання до підрозділу «Безпека життєдіяльності»	12.06.2025-13.06.2025	*Виконано*
9.	Виконання завдання до підрозділу «Основи охорони	14.06.2025-15.06.2025	*Виконано*
	праці»		
10.	Оформлення кваліфікаційної роботи	16.06.2025-17.06.2025	*Виконано*
11.	Нормоконтроль	18.06.2025-19.06.2025	*Виконано*
12.	Перевірка на плагіат	20.06.2025	*Виконано*
13.	Попередній захист кваліфікаційної роботи	21.06.2025	*Виконано*
14.	Захист кваліфікаційної роботи	23.06.2025	

Студент _____ Олійник В.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка локальної комп’ютерної мережі та організація кіберзахисту для ТзОВ “Прометей”// Кваліфікаційна робота освітнього рівня «Бакалавр» // Олійник Владислав Миколайович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНс–42 // Тернопіль, 2025 // С. 66, рис. – 21, табл. – 1, кресл. – 13 , додат. – , бібліогр. – 35.

Ключові слова: локальна комп’ютерна мережа, логічна топографія, комутатор, маршрутизатор, топологія.

У роботі проведено розроблення проекту локальної комп’ютерної мережі для ТзОВ “Прометей”.

Метою роботи є розроблення проекту локальної комп’ютерної мережі для ТзОВ “Прометей” з забезпеченням кіберзахисту мережевих ресурсів.

В першому розділі кваліфікаційної роботи виконано дослідження аспектів аналізу мережевого трафіку для обгрунтування його впровадження у локальній комп’ютерній мережі ТзОВ “Прометей”.

В результаті виконання другого розділу розроблено етапи проектування локальної комп’ютерної мережі ТзОВ “Прометей”. Виконано проектування фізичної топографії мережі. Проведено планування обладнання для мережі ТзОВ “Прометей”, що дало змогу обгрунтувати вибір активної та пасивної частини. Проведено створення логічної топографії мережі.

У третьому розділі кваліфікаційної роботи розроблено та побудова проект моделі локальної комп’ютерної мережі ТзОВ “Прометей” у середовищі моделювання Cisco Packet Tracer.

ANNOTATION

Development of a Local Computer Network and Deployment of Cyber Protection for Prometheus LLC // Diploma thesis Bachelor degree // Oliinyk Vladyslav M. // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2025 // P. 66, Tables – 1, Fig. – 21, Diagrams – 13, Annexes. – , References – 35.

Keywords: local computer network, logical topography, switch, router, topology.

The paper deals with the development of a project of a local computer network for Prometheus LLC.

The aim of the work is to develop a project of a local computer network for Prometheus LLC with the provision of cyber security of network resources.

In the first chapter of the qualification work, the aspects of network traffic analysis were studied to justify its implementation in the local computer network of Prometheus LLC.

As a result of the second chapter, the stages of designing the local computer network of Prometheus LLC were developed. The physical topography of the network was designed. Equipment planning for the network of Prometheus LLC was carried out, which made it possible to justify the choice of active and passive parts. The logical topography of the network was created.

In the third section of the qualification work, a project model of the local computer network of Prometheus LLC was developed and built in the Cisco Packet Tracer modeling environment.

ЗМІСТ

ВСТУП

Розробка локальної комп’ютерної мережі для підприємства, такого як ТзОВ “Прометей”, може забезпечити численні переваги, зокрема підвищення ефективності роботи, покращення комунікації, а також забезпечення надійного зберігання та доступу до даних.

Мережі дають змогу миттєво обмінюватися файлами, електронною поштою, повідомленнями та іншими видами даних і забезпечують можливість проведення відеоконференцій та голосових дзвінків через Інтернет, що знижує витрати на телефонний зв’язок. Використання комп’ютерних мереж дає змогу компаніям значно покращити свою операційну діяльність, підвищити рівень обслуговування клієнтів та ефективніше використовувати наявні ресурси.

Актуальність теми. Локальна комп’ютерна мережа для ТзОВ “Прометей” допоможе оптимізувати робочі процеси, підвищити продуктивність праці та забезпечити надійний доступ до важливих даних, що є ключовими чинниками успіху в сучасному бізнес-середовищі.

Мета і завдання кваліфікаційної роботи. Метою роботи є провести:

– аналіз мережевого трафіку для забезпечення кібербезпеки;

– аналіз умов для розробки проекту локальної комп’ютерної мережі для ТзОВ “Прометей”;

– етапи проектування локальної комп’ютерної мережі;

– проектування фізичної топографії мережі;

– планування обладнання;

– створення логічної топографії;

– моделювання роботи мережі та організацію безпеки.

Практичне значення одержаних результатів. Виконано дослідження аспектів аналізу мережевого трафіку для обгрунтування його впровадження у локальній комп’ютерній мережі ТзОВ “Прометей”. Виявлено, що

реалізація такого підходу підвищує видимість мережі для адміністраторів, допомагає виявленню загроз і усуненню несправностей, впровадженню політик і гарантує відповідність нормативним вимогам. Наведено методи та інструменти аналізу мережевого трафіку. Здійснено аналіз умов для розробки локальної комп'ютерної мережі для ТзОВ "Прометей". Розроблено етапи проектування локальної комп'ютерної мережі ТзОВ "Прометей". Планування мережі охоплює цілий ряд факторів, від розуміння комунікаційних потреб організації та передумов безпеки до оцінки існуючої інфраструктури та вимог до масштабованості. Виконано проектування фізичної топографії мережі, що дало змогу використовуючи інженерію трафіку розробити визначення місця розміщення активного мережевого обладнання, а також можливості підключення дротових користувачів. Показано прокладання кабелів, що в даному випадку буде здійснено у підвісній стелі використовуючи спеціальні короби та кріплення. Усі кабеля будуть промарковані з використанням схеми кодування, яка задокументована і може використовуватись при пошуку несправностей. Проведено планування обладнання для мережі ТзОВ "Прометей", що дало змогу обгрунтувати вибір активної та пасивної частини. Для забезпечення функцій маршрутизації прийнято рішення використати Cisco CBS350-16P-2G-EU як один з елементів екосистеми Cisco, що прийнято для побудови локальної комп'ютерної мережі у ТзОВ "Прометей". Дане обладнання має збалансовані характеристики продуктивності при відносно невисокій ціні продукту, що збалансовує його потенціал у цій мережі. Проведено створення логічної топографії мережі, яка буде передбачати, що централізований маршрутизатор буде підключений до Інтернету, з міжмережевим екраном (брандмауером). Кілька керованих комутаторів буде додано для кожного відділу з підтримкою VLAN. DHCP-сервери будуть використовуватись для видачі динамічних IP-адрес в межах кожної підмережі. Внутрішній DNS-сервер впроваджується для розв'язуваня імен в мережі. Загальні сервери

будуть використані для кожного відділу (файлові сервери, бази даних). Розроблено та побудова проект моделі локальної комп’ютерної мережі ТзОВ “Прометей” у середовищі моделювання Cisco Packet Tracer. Здійснено налаштування основних компонентів та подано рекомендації для покращення роботи мережі у реальних умовах. Забезпечено захист від несанкціонованого підключення недозволених пристроїв через використання безпеки на портах комутаторів. Налаштовано та протестовано бездротовий зв’язок. Створено та перевірено роботу віртуальних мереж. Впроваджено отримання адрес через DHCP сервер, що розміщено у серверній фермі за периметром користувачів. Перевірено автоматичне отримання адрес для користувачів мережі. Налаштовано маршрутизацію та запропоновано модель кіберзахисту у мережі.

РОЗДІЛ 1. АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз мережевого трафіку для забезпечення кібербезпеки

Аналіз мережевого трафіку (АМТ) або Network Traffic Analisys (NTA) – це спосіб моніторингу доступності та активності мережі для виявлення аномалій, таких як проблеми з безпекою та експлуатацією. Аналіз мережевого трафіку в кібербезпеці означає моніторинг даних, які проходять через комп'ютерну мережу. Він допомагає виявити та запобігти поганим подіям у мережі, таким як, спроба хакерів проникнути в мережу або розповсюдженню вірусів [1-5].

Аналіз мережевого трафіку – це процес моніторингу даних, які рухаються через комп'ютерну мережу. Це допомагає нам зрозуміти, як мережа поводиться, працює і залишається безпечною. Перевіряючи шаблони, протоколи та обсяг даних, можна побачити, як пристрої в мережі взаємодіють один з одним. АМТ дає змогу мережевим адміністраторам і фахівцям з безпеки стежити за продуктивністю мережі, знаходити ризики для безпеки, вирішувати мережеві проблеми, розуміти, як використовується мережа, і збирати дані для перевірки відповідності та аудиту.

АМТ відстежує трафік, що проходить через мережу. Деякі з основних типів мережевих даних, які може збирати і обробляти рішення АМТ, включають наступні:

– Дані про потік: Записи потоку надають високорівневий підсумок мережевих з'єднань, що робить його більш масштабованим варіантом. Дані про потік можуть допомогти виявити несанкціоновані з'єднання, наприклад, несанкціонований пристрій, підключений до корпоративної мережі Wide Area Network (WAN), або мережевий трафік, що перетинає сегменти мережі без перевірки, або аномальні обсяги трафіку, наприклад, масштабну витік корпоративних даних.

– Пакетні дані: Захоплення пакетів містять весь вміст мережевого трафіку, надаючи більше даних ціною більших вимог до зберігання. Рішення NTA та аналітики безпеки можуть використовувати пакетні дані для розслідування кібератаки або діагностики проблеми.

Після збору даних мережевого трафіку рішення NTA аналізує їх для отримання корисної інформації. Часто рішення NTA використовують машинне навчання та поведінкову аналітику для виявлення аномалій у мережевому трафіку. Ці аномалії можуть вказувати на кібератаку або іншу проблему, яка потребує вирішення.

AMT надає організаціям можливість більш ефективно аналізувати мережевий трафік і виявляти аномалії, які можуть вказувати на кібератаки або інші потенційні проблеми. Ці можливості надають організації численні переваги, серед яких наступні:

– Видимість мережі: Корпоративні мережі стають більшими і складнішими, що ускладнює підтримку їхньої видимості. Рішення AMT можуть допомогти підвищити рівень безпеки, надаючи компаніям кращу видимість своїх мереж і аномальної мережевої активності, яка може свідчити про потенційну атаку.

– Виявлення загроз: Багато етапів кібератаки, включаючи початковий доступ, бічне переміщення і командно-контрольну комунікацію, відбуваються через мережу. AMT може допомогти організації виявити ці дії, сприяючи виявленню та усуненню кібератак.

– Усунення несправностей: Корпоративні IT-системи можуть вийти з ладу або погіршити свою продуктивність через кібератаки або природні явища. Рішення AMT можуть допомогти визначити, чи не працює система, і надати контекст, який може бути цінним для діагностики та усунення проблеми.

– Підтримка розслідувань: Рішення AMT збирають дані мережевого трафіку для аналізу і можуть зберігати ці дані для подальшого використання.

Якщо операційний центр безпеки (Seurity operation Center, SOC) виявив потенційний інцидент, рішення АМТ можна використовувати для виявлення пов’язаного з ним мережевого трафіку та його аналізу, забезпечуючи додаткову видимість зловмисних дій, що виконуються в системі.

– Розвідка загроз: Після виявлення загрози рішення АМТ може витягувати унікальні характеристики, такі як IP-адреси, які можна використовувати для побудови індикаторів компрометації (IoC). Ця інформація може бути використана для виявлення додаткових загроз і запобігання майбутнім спробам атак.

– Впровадження політики: Правила брандмауера, політики безпеки з нульовою довірою та подібні засоби контролю безпеки призначені для обмеження використання корпоративних IT-систем лише дозволеними діями. АМТ можна використовувати для виявлення порушень політики та прогалин у безпеці.

– Відповідність нормативним вимогам: Правила захисту даних зазвичай вимагають, щоб організація демонструвала, що вона захищає регульовані дані від несанкціонованого доступу. Журнали трафіку АМТ можуть допомогти продемонструвати, що лише авторизовані користувачі мають доступ до даних і систем з обмеженим доступом.

Аналіз мережевого трафіку є одним із ключових компонентів забезпечення кібербезпеки.

1.2 Методи та інструменти аналізу мережевого трафіку

Аналіз мережевого трафіку є критично важливим для забезпечення кібербезпеки. Він дає змогу своєчасно виявляти та запобігати атакам, забезпечувати відповідність нормативним вимогам і захищати інформаційні ресурси організацій. Використання сучасних інструментів та методів

аналізу мережевого трафіку допомагає ефективно реагувати на загрози та підтримувати високий рівень безпеки [6-11].

Розглянемо наступні найкращі практики, щоб максимізувати вплив аналізу мережевого трафіку:

– Встановлення динамічної базові лінії: У сучасних мережах структура мережевого трафіку може змінюватися під час нормальної роботи. З цієї причини встановлення статичної базової лінії може бути неможливим. Замість цього команди повинні виконати динамічне базове визначення, яке передбачає визначення того, як мережевий трафік змінюється в залежності від різних умов, таких як час доби або день тижня.

– Контекстуалізація даних: Самі по собі дані про мережевий трафік мають обмежену цінність. Потрібно контекстуалізувати їх, порівнюючи з іншими джерелами даних, такими як журнали кінцевих точок і метрики, щоб визначити, як незвичайні патерни трафіку корелюють з іншими подіями. Наприклад, сплеск втрачених пакетів можна пояснити збоєм програми, який зафіксовано в журналі сервера.

– Знання мережевої архітектури: Тип архітектури мережі, яку використовують, може відігравати значну роль у формуванні мережевого трафіку. Сучасні мережі, які широко використовують програмно-визначені мережеві абстракції, можуть мати складніші та менш послідовні потоки пакетів, наприклад, ніж прості мережі. З цієї причини важливо враховувати архітектуру мережі при визначенні того, чи є певний шаблон трафіку аномальним.

– Визначення пріоритетності сповіщень про трафік: Як і будь-який інший тип моніторингу та аналізу, аналіз мережевого трафіку може видавати попередження різного рівня серйозності. Наприклад, раптовий потік даних, пов’язаний з підозрою на DoS-атаку, є більш серйозним ризиком, ніж помірне збільшення затримки для некритичних додатків. Важливо знати, які типи

проблем, пов’язаних з трафіком, становлять найбільший ризик, щоб ваша команда могла відреагувати на них першою.

Ці практики допомагають гарантувати, що аналіз мережевого трафіку відіграє максимально ефективну роль, поряд з іншими методами моніторингу та управління мережею, допомагаючи вашій організації виявляти і реагувати на проблеми з продуктивністю і безпекою, які ставлять мережу під загрозу.

Інструменти для збору даних можна класифікувати наступним чином:

– Wireshark: Популярний аналізатор мережевого трафіку з можливістю захоплення і детального аналізу пакетів.

– tcpdump: Командний інструмент для захоплення і аналізу трафіку в режимі реального часу.

– NetFlow: Технологія збору інформації про мережеві потоки для подальшого аналізу.

Система для виявлення втручань (Intrusion Detection System, IDS) – це інструмент безпеки, який відстежує комп’ютерну мережу або системи на предмет зловмисних дій або порушень політик. Вона допомагає виявити несанкціонований доступ, потенційні загрози та аномальні дії, аналізуючи трафік і сповіщаючи адміністраторів про необхідність вжити заходів. IDS має вирішальне значення для підтримки безпеки мережі та захисту конфіденційних даних від кібератак.

Система для виявлення втручань (IDS) відстежує мережевий трафік, шукає незвичну активність і надсилає сповіщення, коли вона виникає. Основними обов'язками системи виявлення втручань (IDS) є виявлення аномалій і повідомлення про них, однак деякі системи виявлення втручань можуть вживати заходів при виявленні зловмисної активності або незвичайного трафіку. У цій статті ми обговоримо кожен пункт про систему виявлення втручань.

Система виявлення мережевих втручань (Network IDS, NIDS): системи виявлення мережевих втручань (NIDS) встановлюються в запланованій точці мережі для перевірки трафіку з усіх пристроїв в мережі. Вона виконує спостереження за трафіком, що проходить по всій підмережі, і порівнює трафік, який передається по підмережах, з колекцією відомих атак. Після виявлення атаки або ненормальної поведінки, сповіщення може бути надіслано адміністратору. Прикладом NIDS є встановлення її в підмережі, де розташовані брандмауери, щоб побачити, чи не намагається хтось зламати брандмауер.

Система для виявлення втручань на хост-комп'ютері (Host IDS, HIDS): системи виявлення втручань на хост-комп'ютері (HIDS) працюють на незалежних хостах або пристроях у мережі. HIDS відстежує вхідні та вихідні пакети лише з пристрою і сповіщає адміністратора, якщо виявлено підозрілу або зловмисну активність. Він робить знімок існуючих системних файлів і порівнює його з попереднім знімком. Якщо аналітичні системні файли були відредаговані або видалені, адміністратору надсилається сповіщення для розслідування. Приклад використання HIDS можна побачити на критично важливих машинах, на яких не передбачається зміна їхньої конфігурації.

Система для виявлення втручань на основі протоколу (Protocol IDS, PIDS): Система для виявлення втручань на основі протоколу (PIDS) складається з системи або агента, який постійно перебуває на передньому кінці сервера, контролюючи та інтерпретуючи протокол між користувачем/пристроєм і сервером. Він намагається захистити веб-сервер, регулярно відстежуючи потік протоколу HTTPS і приймаючи відповідний протокол HTTP. Оскільки HTTPS є незашифрованим і перед тим, як миттєво потрапити на рівень веб-презентації, ця система повинна перебувати в цьому інтерфейсі, щоб використовувати HTTPS.

Система для виявлення втручань на основі прикладних протоколів (Application IDS, APIDS): Система для виявлення втручань на основі

прикладних протоколів (APIDS) – це система або агент, який зазвичай знаходиться в групі серверів. Вона ідентифікує втручання, відстежуючи та інтерпретуючи зв'язок за протоколами, специфічними для конкретної програми. Наприклад, це може бути моніторинг протоколу SQL безпосередньо до проміжного програмного забезпечення, коли воно взаємодіє з базою даних на веб-сервері.

Гібридна система для виявлення втручань: Гібридна система для виявлення втручань створюється шляхом поєднання двох або більше підходів до системи виявлення вторгнень. У гібридній системі виявлення втручань дані хост-агента або системи об'єднуються з мережевою інформацією для отримання повного уявлення про мережеву систему. Гібридна система для виявлення вторгнень є більш ефективною в порівнянні з іншими системами виявлення вторгнень. Prelude є прикладом гібридної IDS.

До популярних IDS можна віднести:

– Snort: Відкрите програмне забезпечення для виявлення вторгнень, яке аналізує мережевий трафік та виявляє підозрілу активність.

– Suricata: Високопродуктивна система для виявлення вторгнень, яка підтримує багатопотоковість і має розширені можливості аналізу трафіку.

– Системи управління інформаційною безпекою та подіями (SIEM) відіграють важливу роль і тут можна виділити наступні:

– Splunk: Платформа для аналізу машинних даних, включаючи мережевий трафік, з можливістю виявлення аномалій і кореляції подій.

– ArcSight: Потужна SIEM-система, що забезпечує моніторинг, кореляцію подій і аналіз мережевого трафіку.

Процес аналізу мережевого трафіку відбувається в наступній послідовності:

– Збір даних: Захоплення мережевого трафіку за допомогою відповідних інструментів.

– Фільтрація та агрегація: Видалення зайвої інформації та агрегація даних для подальшого аналізу.

– Аналіз пакетів: Детальне дослідження окремих пакетів для виявлення підозрілої активності.

– Аналіз потоків: Аналіз мережевих потоків для виявлення аномалій у поведінці користувачів і систем.

– Кореляція подій: Встановлення зв’язків між різними подіями для виявлення комплексних атак.

– Виявлення аномалій: Використання методів машинного навчання та евристичного аналізу для виявлення відхилень від нормальної поведінки.

– Реагування та повідомлення: Розробка і впровадження заходів реагування на виявлені загрози, а також інформування відповідних служб і користувачів.

Аналіз мережевого трафіку допомагає командам безпеки швидко виявляти аномальну активність і зловмисну поведінку, коли така активність переміщується по мережі.

1.3 Аналіз умов для розробки локальної комп’ютерної мережі для ТзОВ “Прометей”

Проектування локальної мережі – це складний процес, що включає в себе безліч факторів, які необхідно враховувати. Добре спроектована локальна мережа забезпечить стабільне та якісне обслуговування кожного пристрою, підключеного до мережі, незалежно від його розміру. Крім того, мережа повинна забезпечувати безперервний доступ до таких функцій, як друк і спільний доступ до файлів. Щоб мережа була швидкою, ефективною та безпечною, всі ці аспекти повинні бути сплановані заздалегідь.

Створення абсолютно нової локальної мережі потребує вибору фізичних носіїв, а також концептуальної карти мережі, яка називається

топографією мережі. Концептуальний рівень мережі формується рішеннями, прийнятими щодо програмного забезпечення, яке керує мережею; фізичні кабелі, роз'єми та пристрої повинні узгоджуватися з цією структурою. Таким чином, для того, щоб всі елементи мережі об'єдналися в єдине ціле, яке працює за призначенням, кожен аспект повинен бути сумісним [12-19].

Локальна мережа забезпечує зв'язок для відносно невеликої групи користувачів в одній будівлі, офісі або кампусі. Вона також зазвичай підключається до глобальної мережі Інтернет через сервер-шлюз, який виступає основним захистом від несанкціонованого доступу до мережевих ресурсів. Враховуючи все це, на ранніх стадіях планування локальної мережі головним питанням є те, якого розміру вона буде і які послуги буде надавати.

Для кожної спеціальної послуги, яку пропонує локальна мережа, наприклад, друк, складне програмне забезпечення або електронна пошта – потрібен сервер. Один сервер може надавати кілька типів послуг, хоча для важких додатків часто потрібен виділений сервер. Сервери можуть потребувати спеціалізованого охолодження та прокладання кабелів, але наявність резервних серверів дозволяє підтримувати роботу сервісів, якщо в мережі виникнуть проблеми. Крім того, використання декількох серверів може дозволити вам легше розширювати вашу мережу.

Перевіряється швидкість передачі даних, затримки та загальна швидкість реагування мережі. Будь-які проблеми, виявлені під час тестування, розглядаються та вирішуються, щоб мережа працювала належним чином.

Програмні рішення, такі як операційні системи, програмне забезпечення для забезпечення безпеки та інструменти управління мережею, обираються для доповнення апаратного забезпечення. Топологія мережі – шина, кільце, зірка або гібрид – визначається на основі вимог організації до масштабованості та надійності. Детальна схема мережі часто створюється для візуального зображення запропонованої архітектури. Програмне

забезпечення для моніторингу мережі часто включає в себе карту топології в реальному часі з детальною інформацією про пристрої, маршрути та бокси.

Кращі практики налаштування мережі передбачають добре розуміння призначення мережі, що дає змогу з більшою впевненістю оцінити кількість користувачів та послуги, які їм потрібні. З цього моменту можна починати розробляти стратегію фізичної побудови мережі. Взагалі кажучи, чим ближче інші елементи локальної мережі до серверів, тим легше буде їх налаштувати і тим стабільнішою буде якість з'єднання кожного користувача. У найпростішій мережі кожен елемент мережі підключений безпосередньо до центрального сервера.

Прогнозування має вирішальне значення для планування мережі, надаючи необхідні дані та інформацію про майбутній попит і тенденції. Це дає змогу організаціям приймати обґрунтовані рішення щодо планування потужностей, розподілу ресурсів та розширення інфраструктури. Наведемо конкретні ролі прогнозування в мережевому плануванні:

– Прогнозування майбутнього попиту. Використовуючи аналіз даних, адміністратори можуть визначити майбутній попит на послуги. На основі цієї інформації компанія може спланувати пропускну здатність і ресурси, необхідні для задоволення цього попиту. Зазвичай це робиться шляхом аналізу історичних даних і поточних показників використання мережі, а також за допомогою моделей прогнозної аналітики.

– Планування пропускної здатності. На основі прогнозованого попиту організації можуть забезпечити достатню пропускну здатність мережі, щоб впоратися з майбутнім збільшенням трафіку без шкоди для продуктивності. Для цього необхідно оцінити поточну пропускну здатність і порівняти її з прогнозованими темпами зростання, щоб визначити необхідну модернізацію.

– Інвестиції в інфраструктуру. Прогнозуючи майбутні тенденції, організації можуть вирішити, коли і де інвестувати в розширення

інфраструктури. Це також допомагає визначити, в які технології варто інвестувати. Інвестиційні рішення часто ґрунтуються на поєднанні техніко-економічного обґрунтування, розрахунків рентабельності інвестицій та очікуваних змін на ринку.

– Розподіл ресурсів. Прогнозування також може допомогти у стратегічному розподілі ресурсів у мережі для задоволення майбутнього попиту. Рішення про розподіл зазвичай приймаються з використанням інструментів і моделей оптимізації, що гарантує, що ресурси будуть розгорнуті там, де вони принесуть найбільший ефект.

– Зниження ризиків. Прогнозуючи потенційні проблеми або виклики, організації можуть підготувати плани на випадок непередбачуваних ситуацій, які допоможуть забезпечити безперебійну роботу мережі та надійність послуг. Цей процес часто включає планування сценаріїв, де передбачаються численні потенційні проблеми, а рішення розробляються заздалегідь.

– Стратегічне планування. Точне прогнозування також може допомогти у довгостроковому стратегічному плануванні, включаючи дослідження нових ринків, планування нових послуг або заміну застарілих систем. Це передбачає всебічне дослідження ринку, участь зацікавлених сторін і бачення того, де компанія хоче бути в майбутньому.

У сучасному технологічному ландшафті дуже поширеною є комбінація мережевих елементів, що використовують як бездротові, так і дротові з’єднання. Деякі будівлі несприйнятливі до бездротових сигналів через свою конструкцію або наявну проводку. Бездротові сигнали також можуть погіршуватися через локальні перешкоди від електронних пристроїв, таких як промислове обладнання. Якщо необхідно прокласти велику кількість кабелів, необхідно нанести на карту будівлю і передбачуване місце розташування кожного елемента мережі, щоб зрозуміти, як можна оптимізувати прокладку кабелів.

Очікувані витрати передбачають розрахунок вартості складної мережі, що складається з кількох етапів. Доведеться врахувати не лише вартість кожного елемента мережі, але й вартість прокладання кабелів та трудовитрати. Запуск мережі вимагає значних інвестицій, але розширювати технологічні можливості стає легше після того, як мережа запрацює. Для зменшення витрат доцільно стандартизувати апаратну та програмну конфігурацію мережевих терміналів. Можна спробувати використовувати недороге програмне забезпечення з відкритим вихідним кодом замість комерційних додатків.

Бізнес стикається з особливими проблемами при розширенні мережі, оскільки це може призвести до перебоїв в обслуговуванні, які впливають на продуктивність під час процесу. Щоб мінімізувати цей ефект, необхідно запланувати всі основні роботи на вихідні дні. Іншим варіантом є впровадження нових мережевих можливостей у кілька змін, щоб зменшити ймовірність перебоїв у роботі. Коли ви наймаєте компанію, яка надає послуги з обслуговування мережі, вона зможе надати вам рекомендації, щоб мінімізувати будь-які перебої, які можуть виникнути в іншому випадку.

1.4 Висновки до першого розділу

В першому розділі кваліфікаційної роботи виконано дослідження аспектів аналізу мережевого трафіку для обгрунтування його впровадження у локальній комп’ютерній мережі ТзОВ “Прометей”. Виявлено, що реалізація такого підходу підвищує видимість мережі для адміністраторів, допомагає виявленню загроз і усуненню несправностей, впровадженню політик і гарантує відповідність нормативним вимогам. Наведено методи та інструменти аналізу мережевого трафіку. Здійснено аналіз умов для розробки локальної комп’ютерної мережі для ТзОВ “Прометей”.

РОЗДІЛ 2. ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ТЗОВ "ПРОМЕТЕЙ"

2.1 Етапи проектування локальної комп'ютерної мережі для ТзОВ "Прометей"

Ефективне планування мережі є основою будь-якої надійної та гнучкої IT-інфраструктури. Нижче наведені кроки, необхідні для того, щоб ваша мережа відповідала поточним і майбутнім вимогам [21-25].

1. Оцінка потреб. На цьому початковому етапі фахівці з мережевого планування проводять інтерв'ю та опитування, щоб досконально зрозуміти потреби організації в комунікаційних технологіях. Вони оцінюють такі фактори, як кількість користувачів, їхні ролі, потреби в підключенні, типи використовуваних додатків і вимоги до безпеки даних, беручи до уваги міркування відповідності. Крім того, вони оцінюють будь-яку існуючу мережеву інфраструктуру, визначаючи сфери, які потребують покращення або вдосконалення.

2. Проектування мережевої архітектури. На основі оцінки потреб фахівці з мережевого планування розробляють комплексну мережеву архітектуру, яка відповідає цілям і потребам організації. Це передбачає вибір відповідного мережевого обладнання, включаючи комутатори, маршрутизатори та точки доступу, з урахуванням таких факторів, як масштабованість, резервування та продуктивність.

3. План впровадження – це детальна дорожня карта, яка описує кожен крок розгортання мережі. Він містить інструкції щодо встановлення апаратних компонентів, таких як комутатори, маршрутизатори, точки доступу та кабелі.

Деталі конфігурації мережевих пристроїв, такі як IP-адресація, VLAN і правила брандмауера, також задокументовані. У разі переходу з існуючої

мережі описуються стратегії міграції даних. План також визначає, як всі компоненти мережі будуть з'єднані між собою і протестовані для забезпечення безперебійної роботи.

4. Тестування та валідація передбачає, що після впровадження проводиться ретельне тестування, щоб переконатися, що мережа відповідає очікуваним рівням продуктивності. Це включає підтвердження належного функціонування всіх апаратних компонентів, таких як комутатори і маршрутизатори, а також ретельне тестування систем безпеки, включаючи брандмауери і системи виявлення/запобігання вторгненням.

5. Документування мережі – це важливий крок, який передбачає ретельне документування всього процесу проектування та реалізації мережі. Сюди входить створення детальних мережевих схем, які ілюструють фізичну та логічну структуру мережі. Готуються посібники та інструкції для користувачів, які містять чіткі інструкції щодо використання мережі та усунення несправностей. Для довідки складається інвентаризація всього мережевого обладнання, ліцензій на програмне забезпечення та гарантійної інформації.

6. Належне навчання проводиться як для кінцевих користувачів, так і для IT-персоналу. Кінцеві користувачі отримують всебічну підготовку щодо ефективного використання мережі для задоволення своїх потреб. IT-персонал навчається управлінню мережею, усуненню несправностей та процедурам технічного обслуговування. Крім того, користувачів та IT-персонал навчають найкращим практикам безпеки, щоб гарантувати, що мережа залишається захищеною.

7. Обслуговування та модернізація виконуються після того, як мережа повністю введена в експлуатацію і регулярне технічне обслуговування стає критично важливим компонентом для забезпечення оптимальної функціональності. Планувальники мережі зазвичай встановлюють графік постійного моніторингу, обслуговування та оптимізації мережі.

Це включає регулярне оновлення програмного забезпечення, в тому числі патчі безпеки та оновлення мікропрограми. Періодичні оцінки продуктивності та планування пропускної здатності проводяться для того, щоб передбачити майбутні потреби і забезпечити відповідність мережі вимогам, що постійно змінюються. Оновлення та заміна обладнання планується для підтримки надійності та масштабованості мережі.

Планування мережі охоплює цілий ряд факторів, від розуміння комунікаційних потреб організації та передумов безпеки до оцінки існуючої інфраструктури та вимог до масштабованості. Цей початковий етап закладає основу для проектування мережі, яка відповідає нагальним потребам і бездоганно узгоджується з довгостроковими цілями організації, що робить його критично важливим і стратегічним завданням у сфері інформаційних технологій.

Першочерговим кроком є визначення необхідної інфраструктури. Це включає в себе рішення про те, чи буде мережа дротовою або бездротовою, а також вибір відповідної проводки та обладнання. Такі рішення зазвичай приймаються на основі обстеження об’єкта, оцінки фізичних обмежень та потреб користувачів.

Важливо, щоб мережа могла вмістити всіх користувачів. Вона повинна бути масштабованою, щоб обробляти зростаючу кількість користувачів і обсяги даних. При плануванні пропускної здатності часто використовується моделювання трафіку і прогнозування історичних даних для передбачення майбутніх потреб.

Показники продуктивності, включаючи швидкість, надійність і якість обслуговування, є фундаментальними. Дизайн мережі повинен мінімізувати затримки та простої. Зазвичай це передбачає проведення еталонних тестів, моделювання та вибір високоякісного обладнання.

Забезпечення безпеки мережі має першорядне значення. Повинні бути впроваджені засоби захисту від таких загроз, як віруси, хакерські атаки та

зломи. Це часто означає розгортання брандмауерів, систем виявлення вторгнень і регулярну оцінку вразливостей.

На кожному етапі планування слід враховувати бюджет проекту, який охоплює закупівлі, встановлення, обслуговування та інші потенційні витрати. Складання бюджету часто вимагає балансу між бажаними функціями та наявними ресурсами, що іноді вимагає поетапного розгортання.

Проект мережі повинен відповідати IT-політиці, регіональним нормам і галузевим стандартам. Перевірки відповідності та аудити, а також ретельне документування забезпечують таку відповідність.

Надійна стратегія резервного копіювання має важливе значення на випадок виходу з ладу компонентів. Стратегії включають розгортання дублікатів обладнання або створення альтернативних маршрутів зв’язку. Регулярні тести на відмовостійкість допомагають перевірити ці стратегії.

Проектування мережі з урахуванням можливості масштабування гарантує, що вона зможе пристосуватися до розширення організації. Таке передбачення може означати модульну інфраструктуру або хмарні рішення, які масштабуються відповідно до попиту.

Забезпечення безперебійного зв’язку між усіма компонентами має вирішальне значення. Досягнення цього може передбачати стандартизацію продуктів одного постачальника або забезпечення відповідності обраних продуктів універсальним стандартам.

Ефективне обслуговування та управління мережею є життєво важливим для стабільної продуктивності та надійності. Стан мережі можна відстежувати та керувати за допомогою спеціального програмного забезпечення з проактивними сповіщеннями для виявлення потенційних проблем.

2.2 Проектування фізичної топографії мережі

Визначення розмірів у мережевому плануванні – це процес визначення вимог до пропускної здатності мережі. Сюди входить визначення кількості та розміру мережевих елементів (наприклад, маршрутизаторів, комутаторів або каналів зв'язку), необхідних для обробки очікуваного навантаження трафіку.

Адміністратори повинні оцінити трафік у години пік на мережевому каналі, що з'єднує офіси з головним сервером, обсяг пам'яті, необхідний у центрі обробки даних, де зберігаються дані, або скільки одночасних з'єднань повинен витримати сервер. Ці рішення враховують такі фактори, як кількість працівників, клієнтів, додатки, які вони використовують (наприклад, платформи електронної комерції), та їхні моделі використання.

Визначення розмірів є життєво важливим при плануванні мережі. Недостатньо розгалужена мережа компанії може призвести до низької швидкості інтернету в критичні моменти, що негативно позначиться на роботі працівників та клієнтів. І навпаки, надмірно розгалужена мережа може призвести до завищених витрат без відчутних переваг. Таким чином, визначення розмірів мережі має на меті досягти балансу між задоволенням операційних потреб і дотриманням бюджетних міркувань.

Інженерія трафіку – це метод оптимізації продуктивності телекомунікаційної мережі шляхом динамічного аналізу, прогнозування та регулювання поведінки даних, що передаються цією мережею. Мета полягає в тому, щоб уникнути перевантажених маршрутів у мережі та забезпечити максимально безперебійну передачу даних.

Інженерія трафіку охоплює концепції, методи та інструменти, що використовуються на етапі проектування, до того, як мережа буде побудована, і на етапі експлуатації існуючої мережі. На етапі проектування

інженерія трафіку займається визначенням розмірів мережевих ресурсів відповідно до потреб трафіку і певних вимог до якості обслуговування (QoS).

На етапі експлуатації інженерія трафіку реагує в більш короткостроковій перспективі на непередбачувані зміни матриці трафіку або мережевих ресурсів. Вона спрямована на оптимізацію продуктивності мережі за допомогою процедур управління трафіком, таких як маршрутизація і розподіл пропускної здатності. У мережах на основі Інтернет-протоколу (IP) процеси інженерії трафіку охоплюють методи і процеси, які змушують IP-трафік проходити через мережу по шляху, відмінному від того, який був би обраний при використанні стандартних методів маршрутизації.

В інженерії трафіку використовується декілька технічних стратегій та інструментів, включаючи тактику на рівні мережі, таку як управління трафіком, надійна та ефективна маршрутизація, виділення ресурсів та схеми пріоритетів.

На рисунку 2.1 подано план будівлі одного з офісів ТзОВ “Прометей”. На його прикладі можна показати планування фізичної топографії локальної комп’ютерної мережі для цієї компанії.

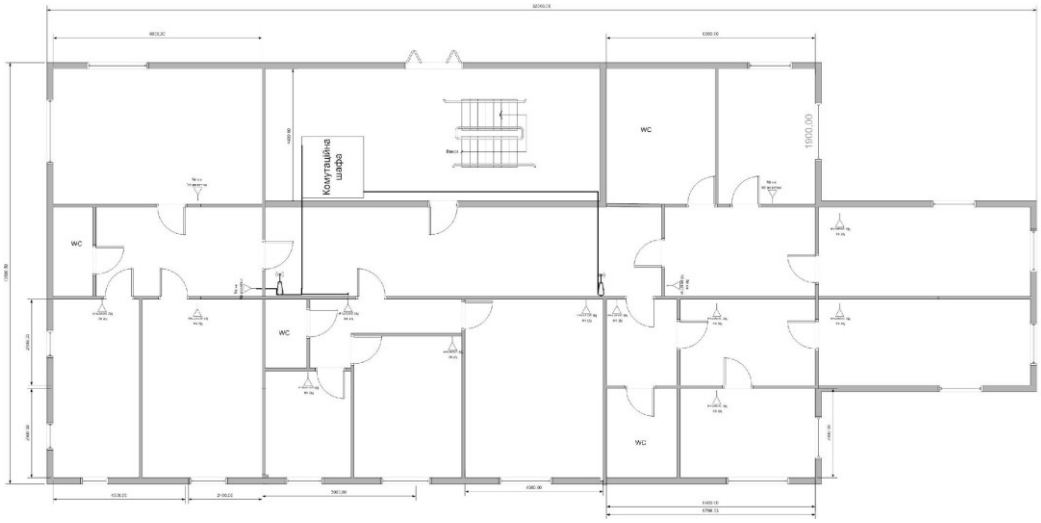

Рисунок 2.1 – Планування фізичної топографії мережі для ТзОВ “Прометей”

Під час планування визначено місце розміщення активного мережевого обладнання, а також можливості підключення дротових користувачів. Показано прокладання кабелів, що в даному випадку буде здійснено у підвісній стелі використовуючи спеціальні короби та кріплення. Усі кабеля будуть промарковані з використанням схеми кодування, яка задокументована і може використовуватись при пошуку несправностей.

Термін “живучість” в контексті мережевого планування означає здатність мережі продовжувати функціонувати навіть у випадку часткових пошкоджень, таких як вихід з ладу вузлів або з’єднань. Це важливий аспект мережевого планування, оскільки системи повинні бути спроектовані таким чином, щоб забезпечити безперервну роботу, потік даних і надання послуг, навіть якщо компоненти мережі вийшли з ладу або були скомпрометовані.

Відмовостійкі мережі призначені для автоматичного перенаправлення даних по іншому шляху при виявленні збою. Це досягається за допомогою різних стратегій, таких як резервування, коли встановлюються додаткові або дублюючі мережеві пристрої, або використовується кілька з’єднань для передачі одних і тих же даних.

Інші стратегії включають автоматичні системи обходу відмов, схеми виявлення та виправлення помилок при передачі даних, а також різні інші мережеві протоколи та алгоритми, розроблені спеціально для забезпечення відмовостійкості.

На етапі планування оцінюються різні типи збоїв, з якими може зіткнутися мережа, ймовірність їх виникнення та потенційний вплив на продуктивність системи. На основі цієї оцінки в проект мережі включаються відповідні механізми забезпечення живучості для забезпечення стійкої та безперебійної роботи.

2.3 Планування обладнання для комп’ютерної мережі ТзОВ “Прометей”

Пристрої мережевої інфраструктури, які забезпечують передачу та маршрутизацію даних у комп'ютерній мережі, є елементами активного мережевого обладнання. Це обладнання здатне виконувати функції управління та обробки інформації, завдяки наявності власного процесора та оперативної пам’яті. Така техніка оптимізує потік даних в мережі, що прискорює передачу даних, а також спрощує управління нею. Таким чином, активне мережеве обладнання обробляє, пересилає, управляє даними по мережі [26-31].

Головною відмінною рисою активного обладнання є наявність інтелектуальної складової. Організація автоматизованої, безперебійної, безпечної та якісної роботи можлива завдяки наявності додаткових функцій. Цей процес також потребуватиме мінімальної фізичної роботи людини.

Комутатор, до якого підключаються всі пристрої, пов’язані з мережею, є найпоширенішим прикладом активного мережевого обладнання. Комутатори, що розробляються в даний час, мають велику кількість портів, що усуває можливі проблеми з організацією єдиної мережі.

Пасивне обладнання виконує функцію передачі даних, але не забезпечує їх обробку. Власного джерела живлення воно також не має. Крім того, воно не здатне керувати трафіком. До пасивного мережевого обладнання належать такі компоненти:

– Розгалужувачі або сплайс-бокси (вони необхідні для розділення або об'єднання оптоволоконних ліній зв’язку).

– Патч-панелі, коннектори, кросові поля (основна функція – з’єднання кабелів і пристроїв).

– Кабелі, що використовуються для з’єднання пристроїв і передачі даних між ними.

Пасивне мережеве обладнання дає змогу забезпечити більш надійну та ефективну роботу мережі, не вимагаючи при цьому додаткових конфігурацій або спеціальних налаштувань.

Це обладнання відповідає за створення єдиної мережі за допомогою інформаційних розеток, повторювачів та інших подібних елементів, що по суті є більш простим процесом. Додаткових функцій та інтелектуальних завдань таке обладнання не виконує.

Порівняння комутаторів Cisco та Mikrotik допоможе вибрати оптимальне рішення для конкретних потреб мережі. Наведемо ключові аспекти для порівняння цих двох брендів.

Продуктивність та функціональність Cisco:

– Комутатори Cisco відомі своєю високою продуктивністю і надійністю.

– Підтримка передових функцій, таких як Layer 3 routing, QoS, MPLS, VPN, і багато іншого.

– Підходить для великих корпоративних мереж з високими вимогами до масштабованості та продуктивності.

– Забезпечення високого рівня відмовостійкості та резервування.

– Глибока інтеграція з іншими мережевими рішеннями Cisco.

Продуктивність та функціональність Mikrotik:

– Високий рівень налаштувань і гнучкість, що дозволяє адаптувати комутатори під конкретні потреби.

– Відповідає потребам малих і середніх бізнесів, включаючи базові функції маршрутизації та управління трафіком.

– Хороше співвідношення ціни та якості, з нижчою вартістю в порівнянні з Cisco.

– Власна операційна система, що надає велику кількість функцій і можливостей для налаштувань.

Управління та налаштування Cisco:

– Cisco IOS – потужна та зріла операційна система з широким набором команд і можливостей.

– Графічний інтерфейс управління (GUI) та командний рядок (CLI) для гнучкого управління.

– Cisco DNA Center – платформа для централізованого управління та автоматизації мереж.

Управління та налаштування Mikrotik:

– RouterOS – власна операційна система, яка дозволяє гнучко налаштовувати мережеві параметри.

– Winbox – зручний інструмент для управління та налаштування комутаторів через графічний інтерфейс.

– CLI – командний рядок для просунутих налаштувань та скриптів.

Ціна та вартість володіння Cisco:

– Вища ціна обладнання та ліцензій, що відображає високу якість і розширені можливості.

– Підтримка та сервіс включає в себе якісну підтримку та сервіси, але вони також можуть бути дорогими.

Ціна та вартість володіння Mikrotik:

– Бюджетний варіант, який надає набагато дешевші рішення, що робить їх привабливими для малого бізнесу та домашніх користувачів.

– Операційна система RouterOS пропонує безкоштовні оновлення та підтримку.

Великі корпорації в основному вибирають обладнання Cisco, оскільки воно підходить для великих підприємств, дата-центрів, провайдерів послуг. Також воно ідеально підходить для великих мереж з високими вимогами до безпеки та продуктивності.

Малі та середні бізнеси успішно працюють з Mikrotik, який ідеально підходить для малих та середніх підприємств, SOHO (малий офіс/домашній офіс). Використовується для домашніх мереж і невеликих офісів.

На рисунку 2.2 показано графічний інтерфейс налаштування комутатора Cisco.

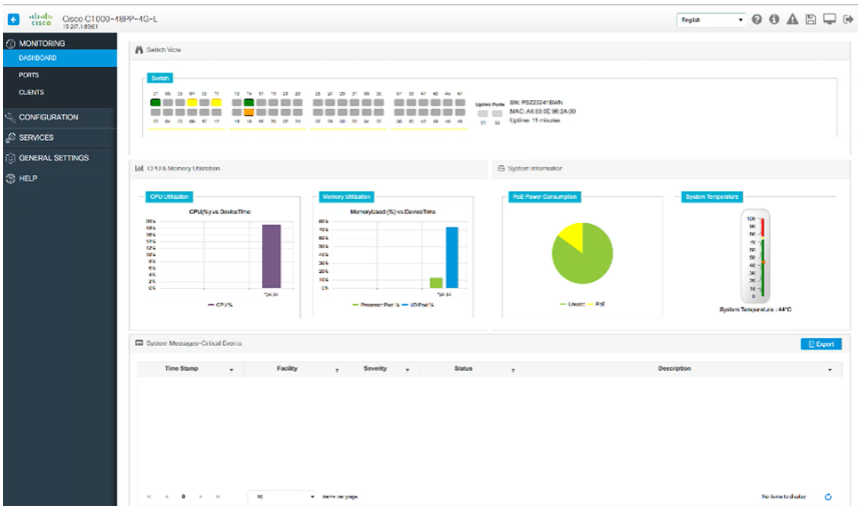

Рисунок 2.2 – Графічний інтерфейс керування комутатора Cisco C1000-24P-4G-L

Окремо можна виділи можливість налаштування використовуючи інтерфейс Bluetooth як альтернативу для підключення приклад якого показано на риснку 2.3.

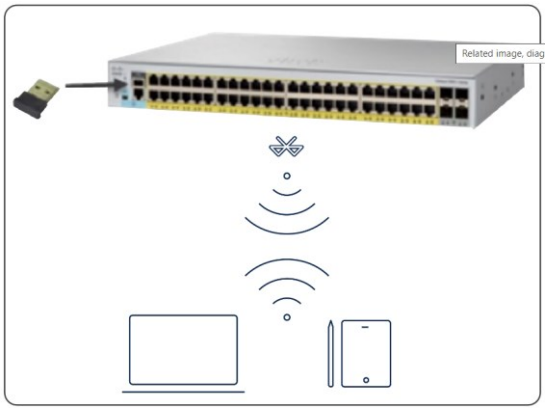

Рисунок 2.3 – Опція налаштування через Bluetooth

Для забезпечення функцій маршрутизації прийнято рішення використати Cisco CBS350-16P-2G-EU як один з елементів екосистеми Cisco, що прийнято для побудови локальної комп’ютерної мережі у ТзОВ

“Прометей”. Дане обладнання має збалансовані характеристики продуктивності при відносно невисокій ціні продукту, що збалансовує його потенціал у цій мережі.

Вибір між пристроями Cisco та Mikrotik залежить від конкретних потреб мережі, бюджету та вимог до функціональності та масштабованості. Cisco пропонує високоякісні рішення для великих корпоративних мереж з високими вимогами до надійності та продуктивності, тоді як Mikrotik забезпечує економічно ефективні рішення для малого та середнього бізнесу з достатньою функціональністю та гнучкістю налаштувань. Враховуючи проведене обгрунтування вирішено вибрати обладнання від компанії Cisco, як таке, що надає високу гнучкість, довготривалу підтримку та велику надійність роботи.

2.4 Створення логічної топографії для локальної комп’ютерної мережі ТзОВ “Прометей”

Створення логічної топографії для локальної комп’ютерної мережі ТзОВ “Прометей” включає визначення розташування та взаємодії мережевих пристроїв і сегментів мережі. Це допомагає зрозуміти структуру мережі та оптимізувати її роботу. Розробимо поетапний план створення логічної топографії:

1. Визначення вимог та обсягів передбачає:

– Визначення кількості пристроїв, які будуть підключені до мережі (комп’ютери, сервери, принтери, точки доступу Wi-Fi).

– Визначення типів пристроїв і їхніх вимог до мережі.

– Оцінка необхідної пропускної здатності для кожного сегмента мережі.

– Визначення вимог до безпеки мережі.

2. Визначення сегментів мережі надасть змогу здійснити:

– Розподіл мережі на сегменти відповідно до організаційної структури компанії (наприклад, відділ продажів, бухгалтерія, IT-відділ).

– Провести створення віртуальних локальних мереж (VLAN) для сегментації трафіку та підвищення безпеки.

3. Планування IP-адресного простору повинне опиратись на:

– Використання діапазонів приватних IP-адрес для кожного сегмента.

– Визначення діапазонів статичних та динамічних IP-адрес.

4. Вибір та розташування мережевих пристроїв доцільно проводити наступним чином:

– Розташування комутаторів для підключення пристроїв у кожному сегменті.

– Розташування маршрутизаторів для з’єднання сегментів мережі та забезпечення доступу до Інтернету.

– Розташування точок доступу для забезпечення бездротового покриття.

Для розрахунку логічної топології локальної комп’ютерної мережі ТзОВ “Прометей” пропонується використати приватний адресний простір мережі 10.0.0.0/8 і технологію Network Address Translation (NAT) для підключення до мережі Інтернет.

Логічна топологія визначає, як пристрої в мережі взаємодіють один з одним, включаючи IP-адреси, маршрутизацію, і розподіл трафіку. Для ТзОВ “Прометей” передбачається, що мережа складається з кількох відділів з різними потребами в підключенні та безпеці.

Визначення вимог та аналіз потреб кожного відділу, а також загальний підрахунок необхідних адрес дадуть змогу правильно створити відповідну топологію.

У ТзОВ “Прометей” існують наступні відділи: Адміністрація, Відділ продажів, Бухгалтерія, Відділ IT, Виробництво.

Кожен з відділів має робочі станції, принтери, сервери, комутатори, маршрутизатори, точки доступу Wi-Fi.

Необхідно забезпечити визначення типів трафіку між відділами щоб грамотно організувати доступ до Інтернету, внутрішні сервіси, бази даних.

Використовуючи технологію Variable Length Subnet Mask (VLSM) проведемо розрахунок адресних просторів для кожного з відділів. Також доцільно помістити кожен з відділів в окрему віртуальну мережу Virtual LAN (VLAN). Результат розрахунку подано в таблиці 2.1.

Таблиця 2.1 – Розрахунок IP адрес

Ім’я	К-сть адрес	Загальна к-сть адрес	Адреси без використання	Адреса мережі	Діапазон	Бродкаст
Production	100	126	26	10.0.0.0/25	10.0.0.1 - 10.0.0.126	10.0.0.127
Guest	60	62	2	10.0.0.128/26	10.0.0.129 - 10.0.0.190	10.0.0.191
Administration	30	30	0	10.0.0.192/27	10.0.0.193 - 10.0.0.222	10.0.0.223
Sales	20	30	10	10.0.0.224/27	10.0.0.225 - 10.0.0.254	10.0.0.255

Продовження таблиці 2.1

Financial	10	14	4	10.0.1.0/28	10.0.1.1 - 10.0.1.14	10.0.1.15
IT	10	14	4	10.0.1.16/28	10.0.1.17 - 10.0.1.30	10.0.1.31

Приклад логічної топографії мережі буде передбачати, що централізований маршрутизатор буде підключений до Інтернету, з міжмережевим екраном (брандмауером). Кілька керованих комутаторів буде додано для кожного відділу з підтримкою VLAN. DHCP-сервери будуть використовуватись для видачі динамічних IP-адрес в межах кожної підмережі. Внутрішній DNS-сервер впроваджується для розв’язуваня імен в мережі. Загальні сервери будуть використані для кожного відділу (файлові сервери, бази даних).

2.5 Висновки до другого розділу

В результаті виконання другого розділу розроблено етапи проектування локальної комп’ютерної мережі ТзОВ “Прометей”. Планування мережі охоплює цілий ряд факторів, від розуміння комунікаційних потреб організації та передумов безпеки до оцінки існуючої інфраструктури та вимог до масштабованості. Виконано проектування фізичної топографії мережі, що дало змогу використовуючи інженерію трафіку розробити визначення місця розміщення активного мережевого обладнання, а також можливості підключення дротових користувачів. Показано прокладання кабелів, що в даному випадку буде здійснено у підвісній стелі використовуючи спеціальні короби та кріплення. Усі кабеля будуть промарковані з використанням схеми кодування, яка задокументована і може використовуватись при пошуку несправностей.

Проведено планування обладнання для мережі ТзОВ “Прометей”, що дало змогу обгрунтувати вибір активної та пасивної частини. Для забезпечення функцій маршрутизації прийнято рішення використати Cisco CBS350-16P-2G-EU як один з елементів екосистеми Cisco, що прийнято для побудови локальної комп’ютерної мережі у ТзОВ “Прометей”. Дане обладнання має збалансовані характеристики продуктивності при відносно невисокій ціні продукту, що збалансовує його потенціал у цій мережі. Проведено створення логічної топографії мережі, яка буде передбачати, що централізований маршрутизатор буде підключений до Інтернету, з міжмережевим екраном (брандмауером). Кілька керованих комутаторів буде додано для кожного відділу з підтримкою VLAN. DHCP-сервери будуть використовуватись для видачі динамічних IP-адрес в межах кожної підмережі. Внутрішній DNS-сервер впроваджується для розв’язуваня імен в мережі. Загальні сервери будуть використані для кожного відділу (файлові сервери, бази даних).

РОЗДІЛ 3. МОДЕЛЮВАННЯ РОБОТИ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТЗОВ "ПРОМЕТЕЙ" З ОРГАНІЗАЦІЄЮ КІБЕРЗАХИСТУ

3.1 Створення та налаштування моделі мережі для ТзОВ "Прометей"

Cisco Packet Tracer є потужним інструментом для моделювання локальних комп'ютерних мереж. За допомогою цього інструменту можна створювати та тестувати мережі перед їх фактичною реалізацією. Cisco Packet Tracer надає безліч можливостей для моделювання та тестування мереж, дозволяючи випробувати різні конфігурації та сценарії без необхідності використання фізичного обладнання.

На рисунку 3.1 подано модель локальної комп'ютерної мережі ТзОВ "Прометей".

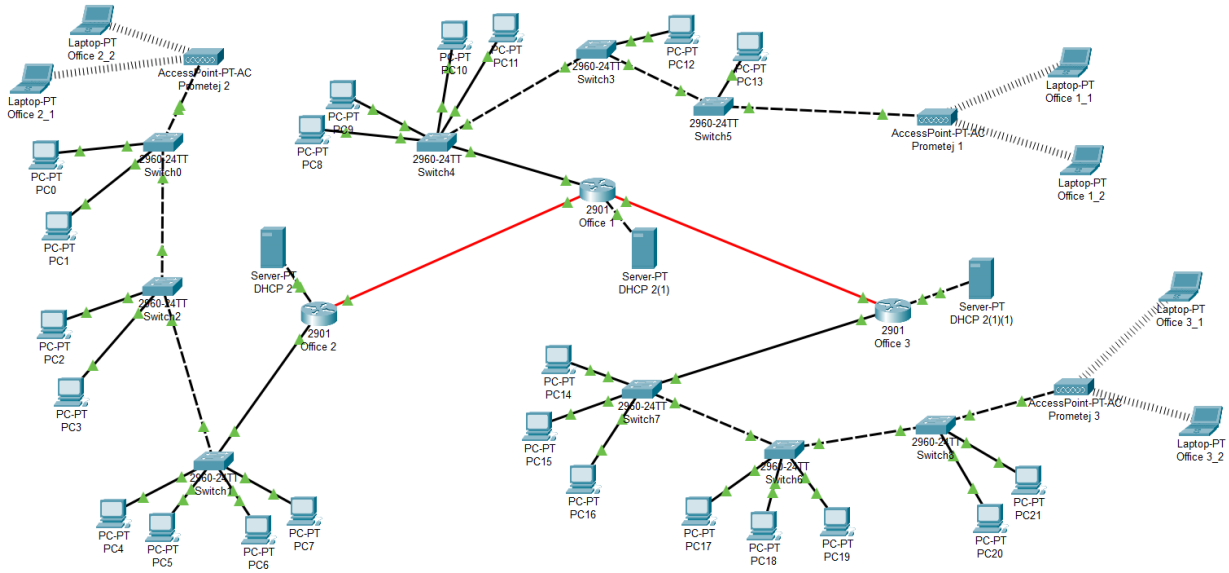

Рисунок 3.1 – Модель мережі ТзОВ "Прометей"

Як видно з поданого рисунку в компанії є три офіси, що з'єднані через маршрутизатори. В кожному офісі комутована мережа складається з трьох

комутаторів, які підключають користувачів з використанням технології VLAN. Таким чином базова безпека організована, оскільки для обміну між різними VLAN потрібно передавати дані через маршрутизатор, де будуть організовані списки контролю доступу Access Control Lists (ACL). Також на комутаторах пропонується впровадити безпеку другого рівня з фільтрацією за MAC адресами і повідомленням до адміністратора у випадку спроби несанкціонованого підключення іншого пристрою.

Налаштування функціоналу мережі покажемо на прикладі виробництва, що має назву віртуальної мережі Production.

На рисунку 3.2 показано налаштування шлюза при використанні статичних адрес. .

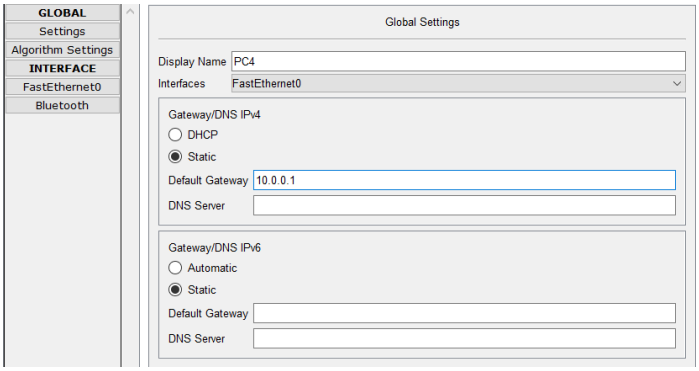

Рисунок 3.2 – Налаштування шлюза

На рисунку 3.3 зображено встановлення статичних IP адрес на комп’ютер.

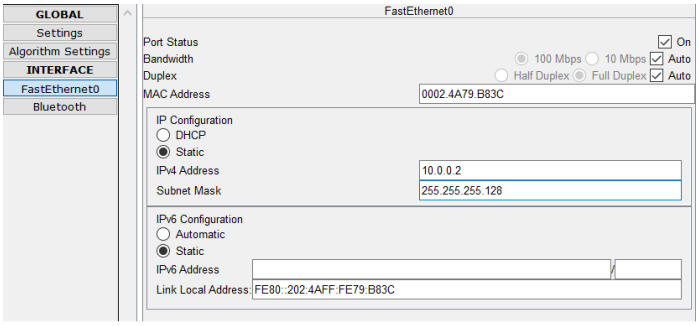

Рисунок 3.3 – Встановлення статичного IP адресу

Для захисту від несанкціонованого доступу до налаштувань комутатора та його ідентифікації серед інших пристроїв у мережі компанії проведемо налаштування показані на рисунку 3.4.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Office_2
Office_2(config)#enable secret Prometej2
Office_2(config)#line vty 0 4
Office_2(config-line)#password Prometej2
Office_2(config-line)#login
```

Рисунок 3.4 – Базові налаштування комутатора для офісу №2

Далі проведемо налаштування приналежності комп'ютерів до відповідної віртуальної мережі. На рисунку 3.5 подано створення VLAN та присвоєння інтерфейсу до неї.

```
Office_2(config)#vlan 100
Office_2(config-vlan)#name Production
Office_2(config-vlan)#exit
Office_2(config)#interface range fastethernet 0/2 - 5
Office_2(config-if-range)#switchport mode access
Office_2(config-if-range)#switchport access vlan 100
```

Рисунко 3.5 – Створення та налаштування віртуальної мережі Production

Як видно з поданого налаштування, після створення відповідної VLAN проведено присвоєння діапазону портів від другого до п'ятого для приналежності до неї. На рисунку 3.6 показано перевірку роботи цієї VLAN.

```
Office_2#show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
100  Production                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Рисунок 3.6 – Перевірка віртуальної мережі Production

Налаштування безпеки портів для обмеження недозволеного підключення інших пристроїв виконано на комутаторі, що показано на рисунку 3.7.

```
Office_2>en
Password:
Office_2#conf t
Office_2(config)#interface range fastEthernet 0/2 - 5
Office_2(config-if-range)#switchport port-security
Office_2(config-if-range)#switchport port-security mac-address sticky
Office_2(config-if-range)#switchport port-security maximum 1
Office_2(config-if-range)#switchport port-security violation shutdown
Office_2(config-if-range)#
```

Рисунок 3.7 – Налаштування безпеки портів на комутаторі

Для забезпечення користувачів бездротовим доступом проведено налаштування точки доступу (див. рисунок 3.8).

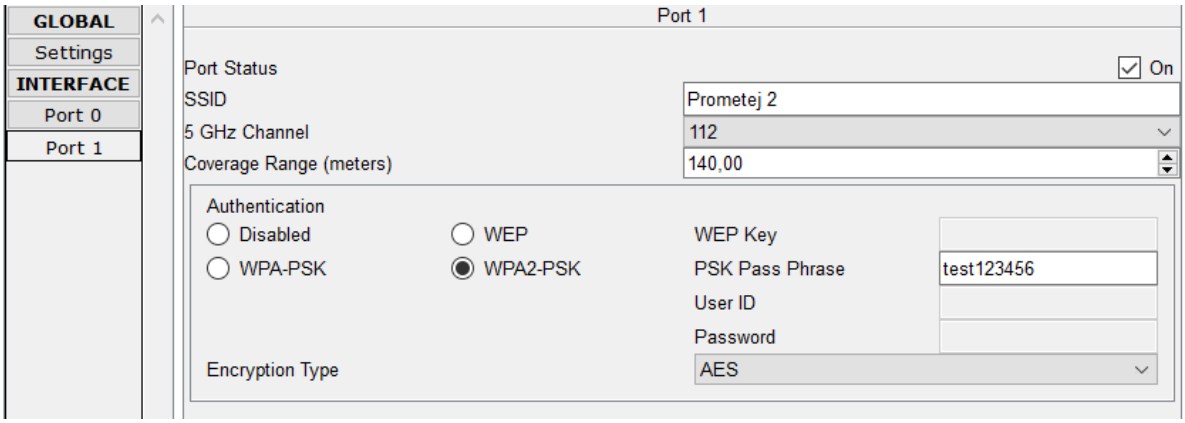

Рисунок 3.8 – Налаштування точки доступу

При цьому встановлено ім’я мережі як Prometej 2 і використано захищене з’єднання через шифрування протоколом AES з застосуванням паролю, що для цієї мережі в цілях демонстрації вставнолений як test123456.

Формування політики створення паролів має бути задокументовано для забезпечення сильних та зихищених паролів, що дасть змогу підвищити надійність передавання даних.

Приклад налаштування бездротових користувачів для цієї мережі показано на рисунку 3.9.

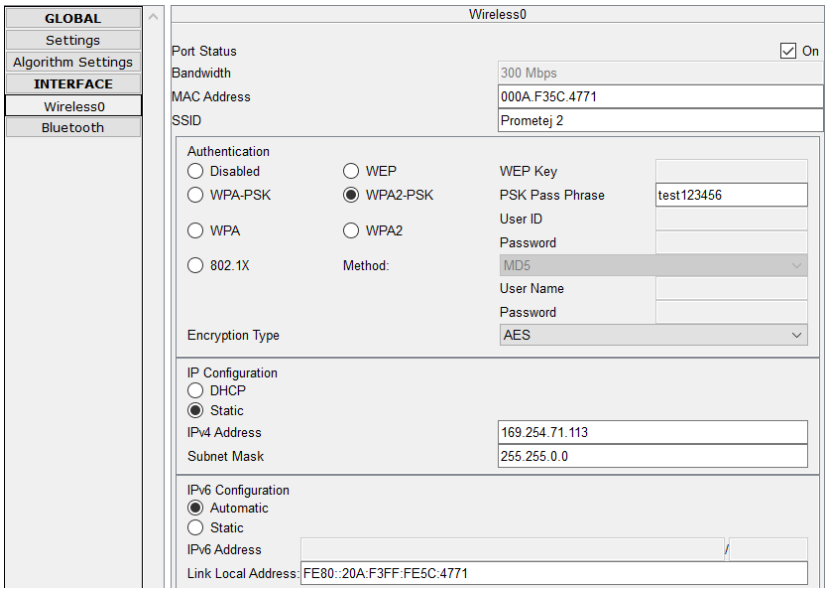

Рисунок 3.9 – Налаштування бездротового користувача

Для частини користувачів пропонується забезпечити отримання адрес автоматично через використання DHCP сервера, що буде розміщено окремо від інших пристроїв. Таким чином можна буде забезпечити керування доступу до нього та його захист. На рисунку 3.10 показано налаштування DHCP сервера.

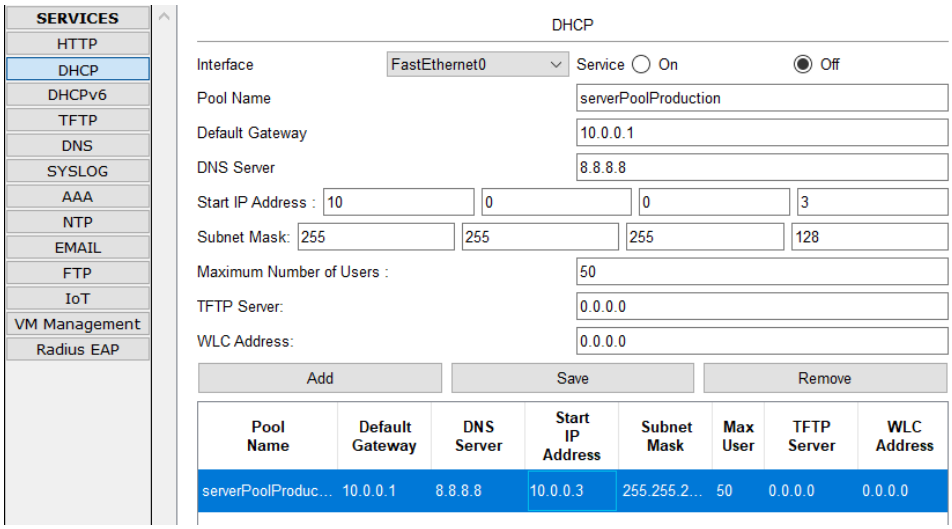

Рисунок 3.10 – Налаштування DHCP сервера

Для успішного функціонування міжмережевого з'єднання потрібно налаштувати IP адреси на маршрутизаторі. При цьому для обміну даними між віртуальними мережами буде використано протокол 802.1Q, який підтримується маршрутизаторами Cisco. На рисунку 3.11 показано налаштування підінтерфейсів для усіх відділів компанії.

```
Router(config)#int gi 0/0.100
%LINK-5-CHANGED: Interface GigabitEthernet0/0.100, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.100, changed state to up
Router(config-subif)#encapsulation dot1Q 100
Router(config-subif)#ip addr 10.0.0.1 255.255.255.128
Router(config-subif)#int gi 0/0.200
%LINK-5-CHANGED: Interface GigabitEthernet0/0.200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.200, changed state to up
Router(config-subif)#enc dot 200
Router(config-subif)#ip addr 10.0.0.129 255.255.255.192
Router(config-subif)#int gi 0/0.300
%LINK-5-CHANGED: Interface GigabitEthernet0/0.300, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.300, changed state to up
Router(config-subif)#enc dot 300
Router(config-subif)#ip addr 10.0.0.193 255.255.255.224
Router(config-subif)#int gi 0/0.400
%LINK-5-CHANGED: Interface GigabitEthernet0/0.400, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.400, changed state to up
Router(config-subif)#enc dot 400
Router(config-subif)#ip addr 10.0.0.225 255.255.255.224
Router(config-subif)#int gi 0/0.500
%LINK-5-CHANGED: Interface GigabitEthernet0/0.500, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0.500, changed state to up
Router(config-subif)#enc dot 500
Router(config-subif)#ip addr 10.0.1.1 255.255.255.240
Router(config)#int gi 0/0
Router(config-if)#no sh
```

Рисунок 3.11 – Налаштування підінтерфейсів для віртуальних мереж

Робота DHCP сервера, який знаходиться за межами мережі клієнтів потребує додаткового налаштування маршрутизатора для передавання бродкаст запитів. На рисунку 3.12 подано відповідне налаштування.

```
Router(config)#int gi 0/0
Router(config-if)#ip help
Router(config-if)#ip helper-address 10.0.1.18
```

Рисунок 3.12 – Налаштування доступу до DHCP сервера

Щоб уникнути втрат пакетів при роботі DHCP сервера та інших чутливих до затримок протоколів, потрібно включити швидку версію протоколу Spanning Tree, яка буде активовувати порти моментально. Захист від випадкового підключення до таких портів комутаторів, що може створити петлю буде реалізовано черзе BPDU Guard налаштування. Приклад такого налаштування подано на рисунку 3.13.

```
Office_2(config)#spanning-tree portfast default
Office_2(config)#interface range fastEthernet 0/2 - 24
Office_2(config-if-range)#spanning-tree portfast
Office_2(config-if-range)#spanning-tree bpduguard enable
```

Рисунок 3.13 – Налаштування RSTP з BPDU Guard

Перевірка функціонування DHCP отримання адреси проводиться на комп’ютері де включено автоматичне отримання параметрів і показано на рисунку 3.14.

```
C:\>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address.................: 0001.C9CD.1C99
   Link-local IPv6 Address.........: FE80::201:C9FF:FECD:1C99
   IPv6 Address....................: ::
   IPv4 Address....................: 10.0.0.3
   Subnet Mask.....................: 255.255.255.128
   Default Gateway.................: ::
                                     10.0.0.1
   DHCP Servers....................: 10.0.1.18
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-13-6E-01-91-00-01-C9-CD-1C-99
   DNS Servers.....................: ::
                                     8.8.8.8

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Physical Address.................: 00E0.F766.2D07
   Link-local IPv6 Address.........: ::
   IPv6 Address....................: ::
   IPv4 Address....................: 0.0.0.0
   Subnet Mask.....................: 0.0.0.0
   Default Gateway.................: ::
                                     0.0.0.0
   DHCP Servers....................: 0.0.0.0
   DHCPv6 IAID.....................:
   DHCPv6 Client DUID..............: 00-01-00-01-13-6E-01-91-00-01-C9-CD-1C-99
   DNS Servers.....................: ::
                                     8.8.8.8
```

Рисунок 3.14 – Перевірка роботи автоматичного отримання параметрів налаштування

З поданого матеріалу видно, що впровадження та налаштування DHCP сервера та клієнт виконані вірно і отримані параметри відповідають очікуваним результатам.

Оскільки дана мережа є невеликою за розміром під час моделювання її роботи для забезпечення маршрутизації вирішено використати протокол RIP, а в реальній мережі це буде виконано через статичну маршрутизацію. Налаштування маршрутизації показано на рисунку 3.15.

```
Router>en
Router#conf t
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#version 2
```

Рисунок 3.15 – Налаштування маршрутизації при моделюванні

Друга версія протоколу маршрутизації має бути включена, оскільки використовується безкласова IP адресна схема.

3.2 Організація мережевої безпеки у локальній комп'ютерній мережі ТзОВ "Прометей"

Безпека у мережі ТзОВ "Прометей" буде організовано використовуючи трирівневу модель безпеки, де на першому рівні буде реалізовано мінімальний захист для користувачів, що не володіють критичними даними (див. Рисунок 3.16).

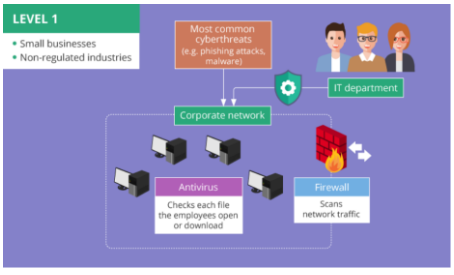

Рисунок 3.16 – Перший рівень захисту від кіберзагроз

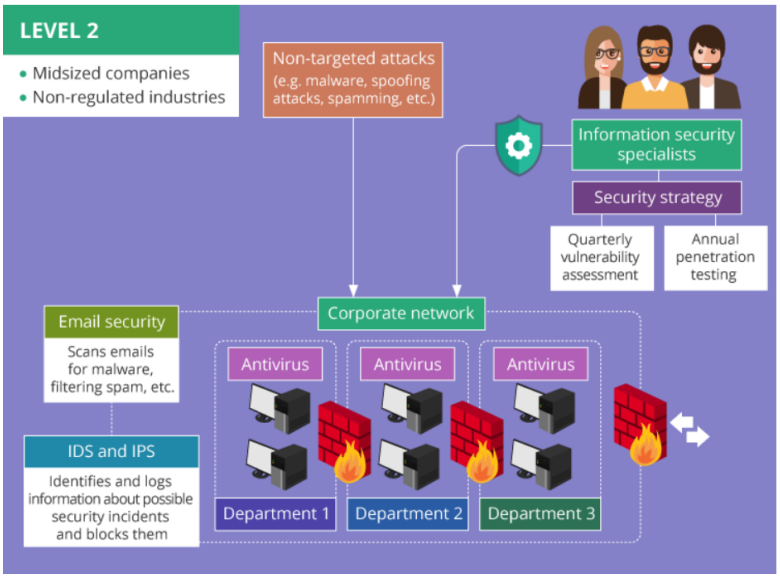

Рисунок 3.17 – Кіберзахист другого рівня

На другому рівні кіберзахисту будуть реалізовані методи та засоби, що повинні убезпечити можливість викрадення інформації та мінізувати недоліки інформаційної безпеки. Організацію другого рівня показано на рисунку 3.17.

На третьому рівні кіберзахисту будуть реалізовано технології покликані захистити від цілеспрямованих атак (див. рисунок 3.18).

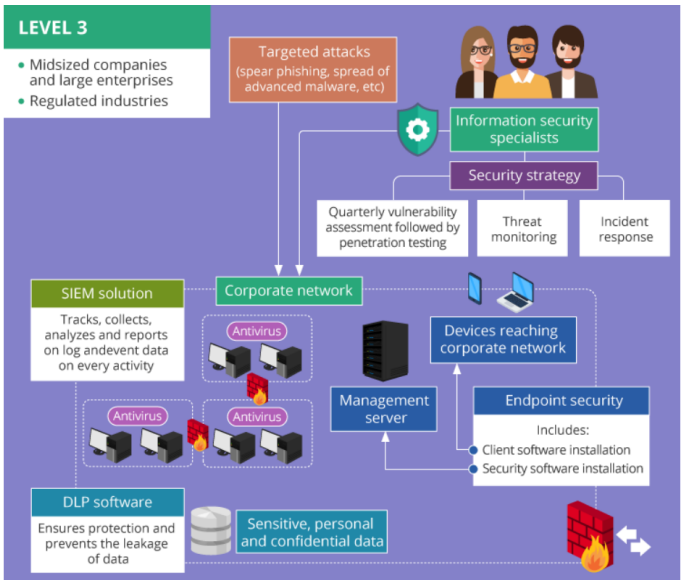

Рисунок 3.18 – Кіберзахист третього рівня

Для захисту інформації у мережі ТзОВ “Прометей” дотримуючись правил і стандартів (HIPAA, PCI DSS та ін.).

3.3 Висновок до третього розділу

У третьому розділі кваліфікаційної роботи розроблено та побудова проект моделі локальної комп’ютерної мережі ТзОВ “Прометей” у середовищі моделювання Cisco Packet Tracer. Здійснено налаштування основних компонентів та подано рекомендації для покращення роботи мережі у реальних умовах. Забезпечено захист від несанкціонованого підключення недозволених пристроїв через використання безпеки на портах комутаторів. Налаштовано та протестовано бездротовий зв’язок. Створено та перевірено роботу віртуальних мереж. Впроваджено отримання адрес через DHCP сервер, що розміщено у серверній фермі за периметром користувачів. Перевірено автоматичне отримання адрес для користувачів мережі. Налаштовано маршрутизацію та запропоновано модель кіберзахисту у мережі.

РОЗДІЛ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Безпечні умови праці при монтажі комп'ютерної мережі

Законодавчими актами, що визначають основні положення про охорону праці є загальні закони України, а також спеціальні законодавчі акти. До загальних законів належать: Конституція України, Закони України: "Про охорону праці", "Про охорону здоров'я", "Про пожежну безпеку" [32-35].

Приміщення, в яких встановлені персональні комп'ютери, повинні мати природне та штучне освітлення відповідно до ДБН В.2.5-28-2006.

Згідно з ДСанПіН 3.3.2-007-98 та з Правилами охорони праці під час експлуатації ЕОМ НПАОП 0.00-1.28-10 площа на одне робоче місце має становити не менше ніж 6,0 кв. м, а об'єм – не менше ніж 20,0 куб. м

До початку робіт у комплексній бригаді проводиться первинний інструктаж з безпечного виконання робіт з основної та суміжних професій та ознайомлення з правилами надання першої допомоги.

Особи з простудними і хронічними захворюваннями верхніх дихальних шляхів до роботи з монтажу комп'ютерних мережі та заготовки і монтажу пластмасових труб не допускаються.

Згідно ДНАОП 0.00-1.15-07. Правила охорони праці під час виконання робіт на висоті (при підйомі над поверхнею вище, ніж 1,3 м) виконуються тільки з риштувань або помостів. До виконання робіт на висоті допускаються особи, не молодше 18 років, та які пройшли:

– професійний добір відповідно до Переліку робіт, де є потреба у професійному доборі, затвердженого спільним наказом Міністерства охорони здоров'я України та Державного комітету України з нагляду за охороною праці від 23.09.94 N 263/121, зареєстрованого в Міністерстві юстиції України 25.01.95 за N 18/554;

– медичний огляд відповідно до вимог Положення про медичний огляд працівників певних категорій, затвердженого наказом Міністерства охорони здоров'я України від 31.03.94 N 45, зареєстрованого в Міністерстві юстиції України 21.06.94 за N 136/345;

– спеціальне навчання та перевірку знань з охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Державного комітету України з нагляду за охороною праці від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 (далі - НПАОП 0.00-4.36-05).

Вимоги безпеки перед початком роботи передбачають, що до початку робіт з монтажу комп’ютерної мережі керівник зобов’язаний:

– перевірити ступінь готовності будівельних робіт;

– оцінити виробничі обставини, можливість взаємодії з іншими будівельно-монтажними організаціями у відповідності з проектом виконання робіт (ПВР); можливість безпечного застосування машин, механізмів, пристосувань, місця їх установки та порядок проїзду; можливість безпечного застосування піротехнічного інструменту, безпечної подачі електричних конструкцій, електротехнічних апаратів та інших блоків;

– узгодити з відповідними службами та, при необхідності, внести уточнення в ПВР.

– ознайомити працюючих з ПВР та технологічними картами на всі види робіт.

– Керівник робіт повинен здійснити первинний інструктаж, який стосується:

– характеру та безпечних методів виконання робіт (у т.ч. за складних погодних умов); порядку проходів до кожного робочого місця;

– наявності небезпечних зон та відкритих каналів і траншей, відкритих прорізів, отворів у перекриттях та стінах;

– порядку розвантаження та складування матеріалів, устаткування та конструкцій;

– місць та порядку трансформаторів безпеки, електрифікованого інструменту, засобів електроосвітлення, випробувальних апаратів;

– порядку і місця установки вантажних лебідок та інших механізмів у монтажній зоні; порядку роботи з гідропідйомників, риштувань, підмостків, драбин; наявності діючих електроустановок та заборонених зон;

– надання першої допомоги, виклику швидкої медичної допомоги, пожежної охорони, керівника робіт чи роботодавця, представника служби охорони праці.

Перевірити наявність та термін дії посвідчень з охорони праці, електро-пожежобезпеки, посвідчень на право виконання спеціальних видів робіт (зварювання, монтаж кабельної арматури).

Видати наряд-допуск операторам на виконання робіт підвищеної небезпеки з проведенням цільового інструктажу та записом до журналу реєстрації інструктажів з питань охорони праці. Підписи інструкторів та інструктованих у журналі обов’язкові.

Попередити працюючих, що з’єднання та від’єднання від мережі обладнання, механізмів, інструменту, інвентарних шаф тощо (крім оперативного вмикання і вимикання) в умовах будівельного майданчика виконуються тільки службою експлуатації власника мережі, якщо не існує іншої письмової домовленості з власником.

Вимоги безпеки під час виконання роботи:

– прокладання кабелів слід виконувати тільки в рукавицях.

– працювати ручними ударними інструментами слід із застосуванням захисних щитків або окулярів з непробивним склом.

– переносити чи перевозити інструмент з гострими кутами треба лише в чохлах.

– не дозволяється розміщувати кабель, барабан з кабелем та без нього, механізми, пристрої та інструменти безпосередньо біля бровки траншеї.

– перекочувати барабан з кабелем слід у напрямку стрілки, нанесеної фарбою на щоці барабана.

– переміщувати барабан з кабелем вручну дозволяється тільки по твердому ґрунту або надійному настилу по горизонтальній поверхні на відстань не більше .

Не дозволяється працюючим чи стороннім особам перебувати на шляху барабана, що переміщується. Під час піднімання барабана необхідно слідкувати за тим, щоб не пошкодити щоки барабана та втулку. Перед розмотуванням барабан встановити на домкрати (чи інший підіймальний пристрій). Барабан встановити так, щоб кабель розмотувався з його верхньої частини. Розмотувати кабель з барабана слід тільки за наявності гальмівного пристрою.

Прокладання кабелів і монтаж мережевого обладнання слід виконувати у захисному одязі з можливістю використання електростатичних браслетів.

Згідно ДБН В.2.5-23:2010. Проектування електрообладнання об'єктів цивільного призначення установлена потужність робочого місця локальної обчислювальної мережі (ЛОМ) (без врахування периферійних пристроїв) приймається 250...300 Вт, сервера – 750... 1000 Вт або згідно з технічною документацією на ці електронні пристрої ЛОМ.

Граничні значення Х електронних пристроїв різної потужності для закордонних виробників обмежується стандартом EN 61000-3-2, для більшості випадків значення можливо приймати 0,72.

Усі об’єкти ЛОМ мають як активну, так і реактивну складові навантаження, тобто повна потужність у вольт-амперах (ВА, англ. «VA») і активна потужність у ватах (Вт, англ. «W») зв’язані між собою коефіцієнтом cos П. На приладах (блоці живлення комп’ютера) вказують їхню активну споживану потужність у ватах. Щоб підрахувати повну потужність у ВА,

потрібно активну потужність у Вт розділити на cos ∏. Наприклад, якщо на блоці живлення комп'ютера написано «850 Вт» (cos ∏ зазвичай не вказаний), це означає, що для грубого розрахунку повної потужності, яка споживається насправді, можна активну потужність розділити на 0,7. Споживана повна потужність дорівнюватиме 850 Вт/0,7 Н 1200 ВА = 1,2 кВА. Необхідно визначити суму потужностей усіх споживачів, що мають потребу в одночасному постачанні електроенергії.

При проектуванні електрообладнання будинків та споруд слід також керуватись вимогами відповідних розділів правила улаштування електроустановок (ПУЕ), розділів 2, 3, 4.1, 4.2, 9, та нормативно-правових актів охорони праці (НПАОП) 40.1-1.32 та вимогами інших чинних нормативних документів.

Не можна застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, які містять сірку. У всіх приміщеннях із серверами та робочими місцями, обладнаними ЕОМ, повинні бути встановлені переносні вуглекислотні вогнегасники. Використання води для гасіння пожежі в приміщеннях, де встановлено електро- і радіоелектронне обладнання, недопустиме, не можна також користуватись і кислотно-лужними вогнегасниками. У громадських будинках та приміщеннях з наявністю ПЕОМ, приміщеннях обчислювальних центрів рекомендується використовувати вуглекислотні вогнегасники типу ОУ-5, ОУ-8, ОУ-25, ОУ-80, вуглекислотні бром-етилові вогнегасники типу ОУБ-3 і ОУБ-7, вуглекислотні вогнегасники від ВВК-1 до ВВК-5, які придатні до експлуатації при температурі повітря від мінус 20 до плюс 50°С.

Кількість вогнегасників для захисту приміщень визначають згідно з п. 3.8 норм належності, затверджених МНС України, та з урахуванням сумарної площі цих приміщень. Тобто слід передбачати по одному вуглекислотному вогнегаснику з величиною заряду вогнегасної речовини 3 кг і більше на кожні

20 кв. м площі підлоги в офісних приміщеннях із ПЕОМ та електрощитових і на 50 кв. м площі підлоги приміщень машзалів.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог НАПБ Б.06.004-2005, ДБН В.2.5-56:2010. Установки порошкового пожежогасіння не застосовують для захисту приміщень із ЕОМ, апаратних залів АТС та інших приміщень із великою кількістю відкритих контактних пристроїв.

У приміщенні, де одночасно експлуатуються понад п’ять ЕОМ з ВДТ і ПП, на доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Електромережі штепсельних з’єднань та електророзеток для живлення ЕОМ з ВДТ і ПП потрібно будувати за магістральною схемою, по 3 – 6 з’єднань або електророзеток в одному колі.

4.2 Ультразвук та інфразвук, його вплив на організм людини

Ультразвук являє собою механічні коливання пружного середовища, що мають однакову зі звуком фізичну природу, але відрізняються більш високою частотою, що перевищує прийняту верхню межу чутності - понад 20 кГц, хоча при великих інтенсивностях (120 ... 145 дБ) чутними можуть бути і звуки більш високої частоти.

Ультразвук, як і звук, характеризується ультразвуковим тиском (Па), інтенсивністю (Вт/м2) і частотою коливань (Гц).

При поширенні в різних середовищах ультразвукові хвилі поглинаються, причому тим більше, чим вище їх частота. Низькочастотний ультразвук досить добре розповсюджується в повітрі, а високочастотний - практично не поширюється. У пружних середовищах (воді, металі та ін) ультразвук мало поглинається і здатний поширюватися на великі відстані,

практично не втрачаючи енергії. Поглинання ультразвуку супроводжується нагріванням середовища.

Специфічною особливістю ультразвуку, обумовлене великою частотою і малою довжиною хвилі, є можливість поширення ультразвукових коливань спрямованими пучками, які отримали назву ультразвукових променів. Вони створюють на відносно невеликій площі дуже велике ультразвукове тиск. Це властивість ультразвуку зумовило широке його застосування: для очищення деталей, механічної обробки твердих матеріалів, зварювання, пайки, прискорення хімічних реакцій, дефектоскопії, перевірки розмірів виробів, що випускаються, структурного аналізу речовин, гідролокації та ін Знайшов застосування ультразвук і в медицині для лікування захворювань хребта, суглобів, периферичної нервової системи.

При тривалій роботі з низькочастотними ультразвуковими установками, що генерують шум і ультразвук, що перевищують встановлені, можуть відбутися функціональні зміни центральної і периферичної нервової системи, серцево-судинної системи, слухового і вестибулярного апарату і т. п. У порівнянні з високочастотним шумом ультразвук значно слабше впливає на слухову функцію, але викликає більш виражені відхилення від норми вестибулярної функції, больової чутливості і терморегуляції. Те, що ультразвук впливає на різні органи і системи людини не тільки через слуховий апарат, підтверджується несприятливим його дією на глухонімих.

Для колективного захисту від дії підвищених рівнів ультразвуку можна використовувати такі напрями: зменшення шкідливого випромінювання ультразвукової енергії в джерелі її виникнення; локалізацію дії ультразвуку конструктивними і планувальними рішеннями, проведення організаційно-профілактичних заходів.

Для зменшення шкідливого випромінювання звукової енергії в джерелі рекомендується підвищувати робочі частоти джерел ультразвуку, що

забезпечує зменшення інтенсивності ультразвуку, а також виключати паразитні випромінювання звукової енергії.

Для локалізації ультразвуку обов'язковим є застосування звукоізолюючих кожухів, екранів. Якщо ці заходи не дають позитивного ефекту, то ультразвукові установки потрібно розміщувати в окремих приміщеннях і кабінах, облицьованих звукопоглинальними матеріалами.

Контактний вплив ультразвуку виключається автоматизацією виробничих процесів і застосуванням дистанційного управління. При особливої необхідності використовують спеціальний інструмент з віброізолюючий рукояткою і захисні рукавички.

Організаційно-профілактичні заходи полягають у проведенні інструктажу працюючих та встановлення раціональних режимів праці та відпочинку.

Інфразвук являє собою механічні коливання пружного середовища, що мають однакову з шумом фізичну природу, але поширюються з частотами менше 20 Гц. У повітрі інфразвук мало поглинається і тому здатний поширюватися на великі відстані. Інфразвук характеризується інфразвукових тиском (Па), інтенсивністю (Вт/м2), частотою коливань (Гц). Рівні інтенсивності інфразвуку і інфразвукового тиску виражаються в децибелах (дБ). Багато явищ природи (землетруси, виверження вулканів, морські бурі) супроводжуються випромінюванням інфразвукових коливань. У виробничих умовах інфразвук утворюється, головним чином, при роботі тихохідних великогабаритних машин і механізмів (компресорів, дизельних двигунів, електровозів, вентиляторів, турбін, реактивних двигунів і ін), які роблять обертальний або зворотно-поступальний рух з повторенням циклу менше ніж 20 разів на секунду (інфразвук механічного походження). Інфразвук аеродинамічного походження виникає при турбулентних процесах у потоках газів чи рідин.

Інфразвук справляє негативний вплив на весь організм людини, в тому числі і на орган слуху, знижуючи слухову чутливість на всіх частотах. Інфразвукові коливання сприймаються як фізичне навантаження: виникають стомлення, головний біль, запаморочення, вестибулярні порушення, знижується гострота зору і слуху, порушується периферичний кровообіг, з'являється відчуття страху і т. п. Тяжкість впливу залежить від діапазону частот, рівня звукового тиску і тривалості.

Низькочастотні коливання з рівнем інфразвукового тиску понад 150 дБ зовсім не переносяться людиною. Особливо несприятливі наслідки викликають інфразвукові коливання з частотою 2 ... 15 Гц у зв'язку з виникненням резонансних явищ в організмі людини, причому найбільш небезпечна частота 7 Гц, так як можливо його збіг з альфа-ритмом біострумів мозку.

Згідно з СН 22-74 - 80 рівні інфразвукового тиску в октавних смугах з середньогеометричними частотами 2, 4, 8 і 16 Гц не повинні перевищувати 105 дБ, а в смузі з частотою 32 Гц-102 дБ. Боротьба з несприятливим впливом інфразвуку повинна вестися в тих же напрямках, що і боротьба з шумом. Найбільш доцільно зменшувати інтенсивність інфразвукових коливань на стадії проектування машин або агрегатів.

4.3 Висновки до четвертого розділу

В даному розділі кваліфікаційної роботи розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі та висвітлено питання ультразвуку та інфразвуку і їх вплив на організм людини.

ВИСНОВКИ

За результатами виконання кваліфікаційної роботи проведено розроблення та моделювання проекту локальної комп’ютерної мережі ТзОВ “Прометей” і отримано наступні результати:

– Виконано дослідження аспектів аналізу мережевого трафіку для обгрунтування його впровадження у локальній комп’ютерній мережі ТзОВ “Прометей”. Виявлено, що реалізація такого підходу підвищує видимість мережі для адміністраторів, допомагає виявленню загроз і усуненню несправностей, впровадженню політик і гарантує відповідність нормативним вимогам.

– Наведено методи та інструменти аналізу мережевого трафіку. Здійснено аналіз умов для розробки локальної комп’ютерної мережі для ТзОВ “Прометей”.

– Розроблено етапи проектування локальної комп’ютерної мережі ТзОВ “Прометей”. Планування мережі охоплює цілий ряд факторів, від розуміння комунікаційних потреб організації та передумов безпеки до оцінки існуючої інфраструктури та вимог до масштабованості.

– Виконано проектування фізичної топографії мережі, що дало змогу використовуючи інженерію трафіку розробити визначення місця розміщення активного мережевого обладнання, а також можливості підключення дротових користувачів. Показано прокладання кабелів, що в даному випадку буде здійснено у підвісній стелі використовуючи спеціальні короби та кріплення. Усі кабеля будуть промарковані з використанням схеми кодування, яка задокументована і може використовуватись при пошуку несправностей.

– Проведено планування обладнання для мережі ТзОВ “Прометей”, що дало змогу обгрунтувати вибір активної та пасивної частини. Для забезпечення функцій маршрутизації прийнято рішення використати Cisco

CBS350-16P-2G-EU як один з елементів екосистеми Cisco, що прийнято для побудови локальної комп’ютерної мережі у ТзОВ “Прометей”. Дане обладнання має збалансовані характеристики продуктивності при відносно невисокій ціні продукту, що збалансовує його потенціал у цій мережі.

– Проведено створення логічної топографії мережі, яка буде передбачати, що централізований маршрутизатор буде підключений до Інтернету, з міжмережевим екраном (брандмауером). Кілька керованих комутаторів буде додано для кожного відділу з підтримкою VLAN. DHCP-сервери будуть використовуватись для видачі динамічних IP-адрес в межах кожної підмережі. Внутрішній DNS-сервер впроваджується для розв’язуваня імен в мережі. Загальні сервери будуть використані для кожного відділу (файлові сервери, бази даних).

– Розроблено та побудова проект моделі локальної комп’ютерної мережі ТзОВ “Прометей” у середовищі моделювання Cisco Packet Tracer. Здійснено налаштування основних компонентів та подано рекомендації для покращення роботи мережі у реальних умовах. Забезпечено захист від несанкціонованого підключення недозволених пристроїв через використання безпеки на портах комутаторів. Налаштовано та протестовано бездротовий зв’язок. Створено та перевірено роботу віртуальних мереж. Впроваджено отримання адрес через DHCP сервер, що розміщено у серверній фермі за периметром користувачів. Перевірено автоматичне отримання адрес для користувачів мережі. Налаштовано маршрутизацію та запропоновано модель кіберзахисту у мережі.

В розділі «Безпека життєдіяльності, основи охорони праці» розглянуто питання безпечних умов праці при монтажі комп’ютерної мережі та висвітлено питання ультразвуку та інфразвуку і їх вплив на організм людини.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. What is Network Traffic Analysis in Cybersecurity? [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/what-is-network-traffic-analysis/. – Назва з екрану. – Дата звернення: 5. 04.2025

2. What is Network Traffic Analysis [Електронний ресурс] – Режим доступу: https://www.checkpoint.com/cyber-hub/network-security/what-is-network-traffic-analysis-nta/. – Назва з екрану. – Дата звернення: 5. 04.2025

3. Flow-based network traffic monitoring for in-depth traffic analysis. [Електронний ресурс]. – Режим доступу: https://www.manageengine.com/products/netflow/. – Назва з екрану. – Дата звернення: 5.04.2025.

4. The-top-5-predictions-for-networking-technology-trends-in-2020 [Електронний ресурс]. – Режим доступу: https://www.techtarget.com/searchnetworking/opinion/The-top-5-predictions-for-networking-technology-trends-in-2020. – Назва з екрану. – Дата звернення: 6.04.2025.

5. What is Network Traffic Analysis [Електронний ресурс] – Режим доступу: https://www.vmware.com/topics/glossary/content/network-traffic-analysis.html. – Назва з екрану. – Дата звернення: 6. 04.2025

6. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/. – Назва з екрану. – Дата звернення: 6. 04.2025

7. Planning a New Local Area Network: From Start to Finish [Електронний ресурс] – Режим доступу: https://www.networkcablinglosangeles.com/computer-network-cabling/. – Назва з екрану. – Дата звернення: 6. 04.2025

8. NETWORK EQUIPMENT: CONCEPT AND TYPES [Електронний ресурс] – Режим доступу: https://newserverlife.com/articles/network-equipment-concept-and-types/. – Назва з екрану. – Дата звернення: 6. 04.2025

9. Top-5-network-technology-trends-for-2023 [Електронний ресурс]. – Режим доступу: https://info.pivitglobal.com/blog/top-5-network-technology-trends-for-2023. – Назва з екрану. – Дата звернення: 14. 04.2025

10. Комутатор мережевий Cisco C1000-24T-4G-L [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/288249428/p288249428/. – Назва з екрану. – Дата звернення: 15. 04.2025

11. Local area networks (LAN) design [Електронний ресурс]. – Режим доступу: https://www.dekom.com/en/media-technology/services/design-of-engineering-systems/local-area-networks-lan-design/. – Назва з екрану. – Дата звернення: 15. 04.2025

12. What Is Network Planning, And How Can You Plan For New Networks? [Електронний ресурс]. – Режим доступу: https://nilesecure.com/network-design/what-is-network-planning-and-how-can-you-plan-for-new-networks. – Назва з екрану. – Дата звернення: 15. 04.2025

13. Комутатор D-LINK DGS-1100-24PV2. [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/342410224/p342410224/. – Назва з екрану. – Дата звернення: 15. 04.2025

14. Zyxel GS1915-24EP [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/zyxel-gs1915-24ep-eu0101f/p357602781/. – Назва з екрану. – Дата звернення: 15. 04.2025

15. Business-350-series-managed-switches [Електронний ресурс]. – Режим доступу: https://www.cisco.com /c/en/us/products /collateral/switches/business-350-series-managed-switches/datasheet-c78-744156.html?dtid=osscdc000283. – Назва з екрану. – Дата звернення: 15. 04.2025

16. Комутатор Cisco CBS350-16P-2G-EU [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/zyxel-gs1915-24ep-eu0101f/p357602781/. – Назва з екрану. – Дата звернення: 15. 04.2025

17. “Cisco Network Admission Control (NAC) Solution Data Sheet - Cisco.” [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/collateral/security/nacappliance-cleanaccess/product_data_sheet0900aecd802da1b5.html. – Назва з екрану. – Дата звернення: 14. 04.2025

18. Private-wireless-networking-logistics-industry [Електронний ресурс]. – Режим доступу: https://www.nokia.com/blog/private-wireless-networking-logistics-industry/. – Назва з екрану. – Дата звернення: 15. 04.2025

19. Software modelling complex of network operating parameters with variable input data / S. Martsenko et al. *2019 IEEE 14th international scientific and technical conference on computer sciences and information technologies (CSIT)*, Lviv, Ukraine, 17–20 September 2019. 2019. URL: https://doi.org/10.1109/stc-csit.2019.8929829 (date of access: 15.05.2025).

20. The information system for planning the parameters of telecommunication operator networks / S. Martsenko et al. *2019 IEEE 14th international scientific and technical conference on computer sciences and information technologies (CSIT)*, Lviv, Ukraine, 17–20 September 2019. 2019. URL: https://doi.org/10.1109/stc-csit.2019.8929747 (date of access: 15.05.2025).

21. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 22. 04.2023.

22. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 23. 04.2023.

23. Smart city: a review of model architecture and technology / N. Martsenko et al. *2021 IEEE 16th international conference on computer sciences*

and information technologies (CSIT), LVIV, Ukraine, 22–25 September 2021. 2021. URL: https://doi.org/10.1109/csit52700.2021.9648606 (date of access: 15.06.2025).

24. Wieclaw L.; Pasichnyk V.; Kunanets N.; Duda O.; Matsiuk O.; Falat P. Cloud computing technologies in “smart city” projects. In Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). Bucharest: Romania, 21–23 September 2017. pp. 339–342.

25. Марценко С. В., Круглик Ю. Методи та засоби оптимізації роботи мереж різного призначення. *Актуальні задачі сучасних технологій* : Матеріали IX міжнар. науково-техн. конф. молодих уч. та студентів «Акт. задачі сучас. технологій» Терноп. нац. техн. ун-ту ім. Ів. Пулюя,, м. Тернопіль, 25–26 листоп. 2020 р. Тернопіль, 2020. С. 48.

26. Марценко С. В., Федина В., Шоцький М. Дослідження процесів автоматизації керування мережевими пристроями. *Актуальні задачі сучасних технологій* : Матеріали X міжнар. науково-практ. конф. молодих уч. та студентів «Акт. задачі сучас. технологій», м. Тернопіль, 24–25 листоп. 2021 р. Тернопіль, 2021. С. 140.

27. Information technology platform for the selection and analytical processing of information on COVID-19 / S. Martsenko et al. *2021 IEEE 16th international conference on computer sciences and information technologies (CSIT)*, LVIV, Ukraine, 22–25 September 2021. 2021. URL: https://doi.org/10.1109/csit52700.2021.9648839 (date of access: 26.06.2025).

28. Yevseiev S., Ponomarenko V., Laptiev O., Milov O., Korol O., Milevskyi S. et. al.. Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 2021. 188 p. DOI: https://doi.org/10.15587/978-617-7319-31-2

29. Wlan security [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-

security/115951-web-auth-wlc-guide-00.html – Назва з екрану. – Дата звернення: 24. 04.2025.

30. Network functionality [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/topics/computer-science/network-functionality – Назва з екрану. – Дата звернення: 03. 05.2025.

31. Functionality of computer networks [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/functionality-of-computer-network/ – Назва з екрану. – Дата звернення: 03. 05.2025.

32. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0007282-98#Text – Назва з екрану. – Дата звернення: 06.05.2025.

33. Про затвердження правил охорони праці під час експлуатації електронно-обчислювальних машин [Електронний ресурс]. – Режим доступу: https://dnaop.com/html/31562/doc-%D0%9D%D0%9F%D0%90%D0%9E%D0%9F_0.00-1.28-10 – Назва з екрану. – Дата звернення: 06.05.2025.

34. Проектування електрообладнання об’єктів цивільного призначення [Електронний ресурс]. – Режим доступу: http://kbu.org.ua/assets/app/documents/dbn2/92.1.%20%D0%94%D0%91%D0%9D%20%D0%92.2.5-23~2010.%20%D0%86%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D0%BD%D0%B5%20%D0%BE%D0%B1%D0%BB.pdf – Назва з екрану. – Дата звернення: 06.05.2025.

35. Про затвердження "Правил будови електроустановок. Електрообладнання спеціальних установок" [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/rada/show/v0272203-01#Text – Назва з екрану. – Дата звернення: 06.05.2025.