Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

МОДЕРНІЗОВАНА КОРПОРАТИВНА МЕРЕЖА ПІДПРИЄМСТВА З ЛІСОЗАГОТІВЛІ «ЛІСГОСП»

MODERNISED CORPORATE NETWORK OF TIMBER ENTERPRISE «LISHOSP»

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІ-41
Шевчук Артем Юрійович

(підпис)

Керівник:
к.т.н., доцент
Багнюк Наталія Володимирівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« _____ » червня 2023 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2023 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
«_____» _____ 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Шевчуку Артему Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Модернізована корпоративна мережа підприємства з лісозаготівлі «Лісгосп»*

Керівник роботи *к.т.н., доцент Багнюк Наталія Володимирівна*

затверджені наказом закладу вищої освіти від «28» грудня 2022 року № 982/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 01.06.2023р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Теоретичні аспекти розробки корпоративної мережі
Проектування корпоративної мережі
Практична розробка мережі
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Існуючі рішення
Використані технології
Архітектура мереж
Топологія мереж

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Теоретичні аспекти розробки корпоративної мережі	*Багнюк Н.В.*		
Проектування корпоративної мережі	*Багнюк Н.В.*		
Практична розробка мережі	*Багнюк Н.В.*		
Висновки			

7. Дата видачі завдання 01.11.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Обгрунтування теми*	До 15.11.2022 р.	Виконано
2.	*Огляд літератури із досліджуваної проблеми*	До 15.12.2022 р.	Виконано
3.	*Теоретичні аспекти розробки корпоративної мережі*	До 02.02.2023 р.	Виконано
4.	*Проектування корпоративної мережі*	До 02.03.2023 р.	Виконано
5.	*Практична розробка мережі*	До 02.04.2023 р.	Виконано
6.	*Висновок*	До 02.04.2023 р.	Виконано
7.	*Формування списку використаних джерел*	До 15.04.2023 р.	Виконано
8.	*Формування додатків*	До 02.05.2023 р.	Виконано
9.	*Оформлення ілюстративного матеріалу*	До 15.05.2023 р.	Виконано
10.	*Нормоконтроль*	До 25.05.2023 р.	Виконано
11.	*Інструментальна перевірка на академічний плагіат*	До 01.06.2023 р.	Виконано
12.	*Представлення кваліфікаційної роботи бакалавра до захисту*	До 07.06.2023 р.	Виконано

Здобувач вищої освіти _____ Шевчук А.Ю.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Багнюк Н.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Шевчук А.Ю. Модернізована корпоративна мережа підприємства з лісозаготівлі «Лісгосп». Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2023.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел (згідно структури кваліфікаційної роботи, затвердженої кафедрою).

Перший розділ присвячено теоретичним аспектам розробки корпоративної мережі. Розглядаються основні поняття про корпоративну мережу, її архітектуру, які протоколи, технології та методи захисту інформації використовуються при розробці корпоративної мережі. Також в цьому розділі здійснено огляд як проводиться аудит та моніторинг корпоративної мережі.

В другому розділі здійснено аналіз потреб користувача та відповідно до нього розроблена схема мережі, її топологія, визначенні способи захисту мережі. Також здійснено підбір необхідного мережевого обладнання.

У третьому розділі на основі проведених досліджень описано практичну розробку корпоративної мережі.

Об'єкт дослідження – процес розробки корпоративної мережі.

Предмет дослідження – корпоративна мережа на підприємстві.

Метою роботи є розробка корпоративної мережі для підприємства «Лісгосп».

Ключові слова: корпоративна мережа, мережеве обладнання, топологія, протоколи, технології.

ANNOTATION

Shevchuk A.Y. Upgraded corporate network of the logging enterprise «Lisgosp». Manuscript.

Bachelor's thesis in the field of Computer Engineering, specialization 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2023.

The thesis consists of an introduction, three chapters, conclusions, and a list of references (according to the structure of the thesis approved by the department).

The first chapter is devoted to the theoretical aspects of corporate network development. It explores the basic concepts of a corporate network, its architecture, the protocols, technologies, and methods used for information security in corporate network development. This chapter also provides an overview of the auditing and monitoring of a corporate network.

The second chapter analyzes the user's needs and based on that, a network scheme, its topology, and methods of network security are developed. The selection of necessary network equipment is also performed in this chapter.

The third chapter describes the practical development of the corporate network based on the conducted research.

The research object is the process of developing a corporate network.

The research subject is the corporate network in the enterprise.

The goal of this work is to develop a corporate network for the "Forest Management" enterprise.

Keywords: corporate network, network equipment, topology, protocols, technologies.

ЗМІСТ

ВСТУП

Актуальність теми. Після проведення в Україні реформи державної лісогосподарської галузі в рамках якої усі 158 лісогосподарських підприємств країни об'єднуються в єдине державне спеціалізоване підприємство „Ліси України'', а 24 облуправління об'єднанні до 9 регіональних. Постала потреба в розробці єдиного стандарту і впровадження корпоративної мережі на усіх лісогосподарських підприємствах для коректної і стабільної роботи та взаємодії між собою.

Метою роботи є розробка корпоративної мережі підприємства з лісозаготівлі „Лісгосп".

Об'єктом дослідження є процес розробки корпоративної мережі.

Предметом дослідження є корпоративна мережа на підприємстві.

Методи проектування. Теоретичне ознайомлення з існуючими аналогами та принципами створення, використання здобутих знань для розробки корпоративної мережі.

Завдання:

- Огляд технологічних рішень для розробки корпоративної мережі.
- Аналіз потреб підприємства в інформаційних технологіях та визначення функціональних вимог до мережі.
- Розробка архітектури корпоративної мережі з використанням відповідних технологічних рішень.
- Вибір та конфігурування необхідного обладнання для мережі.
- Налагодження та тестування мережі.
- Розробка стратегії захисту інформації в мережі.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ РОЗРОБКИ КОРПОРАТИВНОЇ МЕРЕЖІ

1.1 Поняття корпоративної мережі

Корпоративна мережа – це інформаційна мережа, яка створюється в організації з метою об'єднання різних комп'ютерів та інших пристроїв в єдину систему, що забезпечує швидкий та безпечний обмін даними між співробітниками організації.

Корпоративні мережі можуть мати різну топологію, що залежить від конкретних потреб організації. Найпоширеніші топології корпоративних мереж – це зірка, кільце, дерево та змішана

Основною функцією корпоративної мережі є забезпечення ефективного обміну інформацією між співробітниками організації. Крім того, корпоративна мережа може забезпечувати доступ до спільних ресурсів, таких як бази даних, принтери, сканери та інші пристрої.

Переваги використання корпоративної мережі для організації:

– покращення комунікації та співпраці між співробітниками;
– забезпечення безпеки даних та конфіденційності інформації;
– підвищення продуктивності роботи співробітників;
– зниження витрат на обслуговування комп'ютерної інфраструктури;
– забезпечення доступу до спільних ресурсів та послуг.

Для того, щоб корпоративна мережа працювала ефективно, вона повинна мати надійну інфраструктуру та правильно сконфігуровані компоненти. Основні компоненти корпоративної мережі – це сервери, роутери, комутатори, мережеві кабелі, а також програмне забезпечення для управління та моніторингу мережі.

1.1.1Типи топологій

Топологія мережі визначає, як пристрої та вузли здійснюють підключення один до одного та які комунікаційні канали вони використовують. В корпоративному середовищі важливо вибрати оптимальний тип топології

мережі, який забезпечить ефективне та надійне функціонування, і водночас буде простий в встановленні та підтримці.

Основні типи топологій [1] мереж включають: зірка, дерево, загальна шина, кільце та змішана.

Топологія зірка (рис. 1.1) є однією з найбільш поширених у корпоративних мережах, де всі пристрої підключені до центрального комутатора або маршрутизатора. При використанні зіркоподібної топології кожний кабельний сегмент, від будь–якого комп'ютера мережі, буде підключатися до центрального комутатора або концентратора. Всі пакети будуть транспортуватися від одного комп'ютера до іншого через цей пристрій. Допускається використання як активних, так і пасивних концентраторів. Ця топологія має перевагу в простоті встановлення та підтримки, але може бути неефективною з точки зору використання пропускної здатності [1].

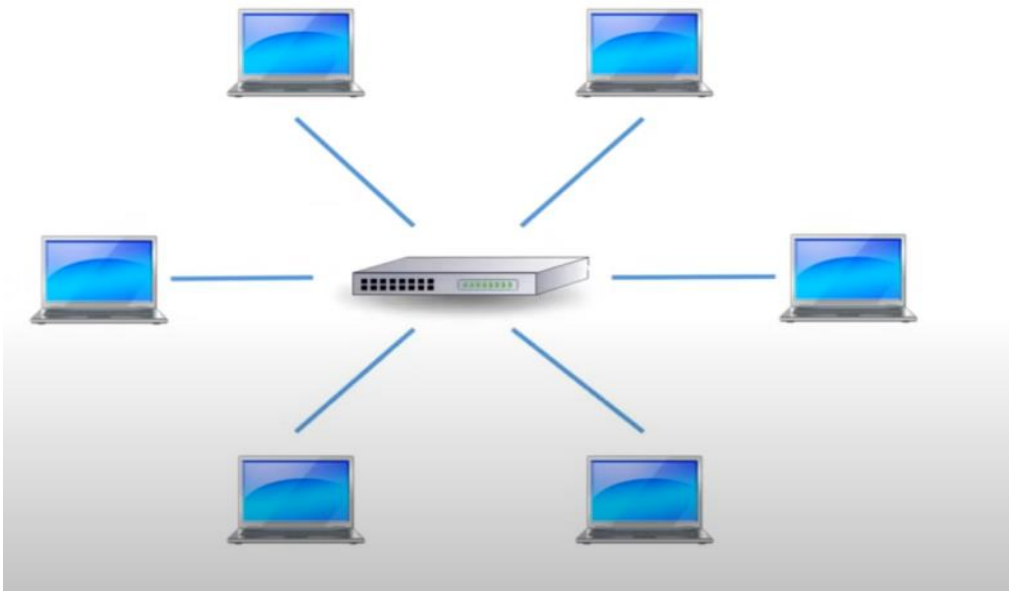

Рисунок 1.1 – Топологія зірка

Переваги «зірки»:

– простота створення і управління;
– високий рівень надійності мережі;
– висока захищеність інформації, яка передається всередині мережі

(якщо у центрі зірки розташований комутатор).

Основний недолік – поломка концентратора призводить до припинення роботи всієї мережі.

Топологія дерево (рис. 1.2) має ієрархічну структуру, де вузли групуються в піддерева та підключаються до центрального комутатора або маршрутизатора. Побудова деревоподібних мереж базується на використанні технології кабельного телебачення, що включає в себе різні засоби зв'язку, такі як кінцеві частотні ретранслятори, розщеплювачі–об'єднувачі, двонапрямлені посилювачі, відгалужувачі, радіочастотні модеми, фільтри та інші пристрої [3].

Ця топологія забезпечує високу пропускну здатність та надійність завдяки структурному резервуванню її зв'язкових пристроїв, що гарантує час роботи без відмов до 400 тис. годин. Однак, вона може вимагати складного управління та підтримки.

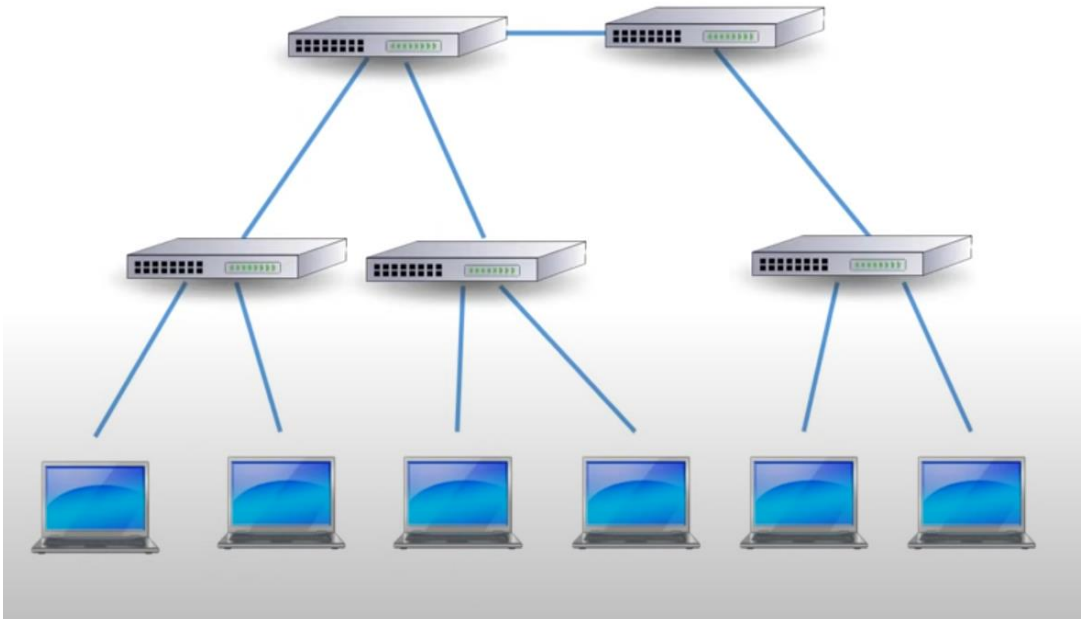

Рисунок 1.2 – Топологія дерево

Переваги використання мереж з топологією дерево є наступними:

Завдяки використанню частотного ущільнення каналів, ця топологія дозволяє передавати мову, дані та зображення одночасно на відносно великій

відстані до 50 км. Однак, основними недоліками є обмежені можливості розширення деревоподібних мереж через високу вартість їх встановлення та складність їх аналогових компонентів, що потребують постійного налагоджування.

Топологія загальна шина (рис. 1.3) передбачає підключення пристроїв у лінійний порядок. Ця топологія є простою в установленні, але не надійною та має обмежену пропускну здатність. Топологія типу шина – це загальний кабель (званий шина або магістраль), до якого приєднані всі робочі станції. Для того щоб сигнал не віддзеркалювався на кінцях кабелю знаходяться термінатор.

Повідомлення, що відправляється робочою станцією розповсюджується на всі комп'ютери мережі. Кожний комп'ютер перевіряє кому адресовано повідомлення і якщо йому, то обробляє його. При побудові великих мереж виникає проблема з обмеженням на довжину передачі даних між комп'ютерами, у такому разі мережу розбивають на сегменти. Сегменти з'єднуються різними пристроями – повторителями, концентраторами або хабами. Наприклад, технологія Ethernet дозволяє використовувати кабель завдовжки не більше 185 метрів [2].

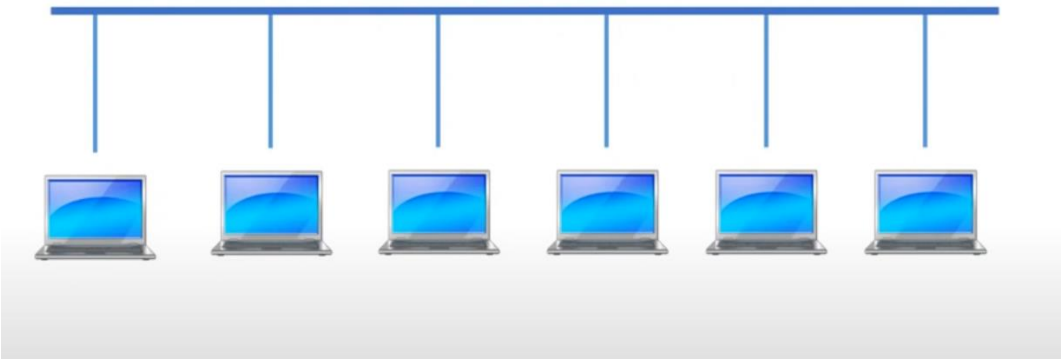

Рисунок 1.3 – Топологія загальна шина

Топологія кільце (рис. 1.4) передбачає, що кожен пристрій підключений до двох сусідніх, створюючи кільце. Ця топологія має високу надійність, але може бути складною в підтримці та відновленні мережі в разі збоїв.

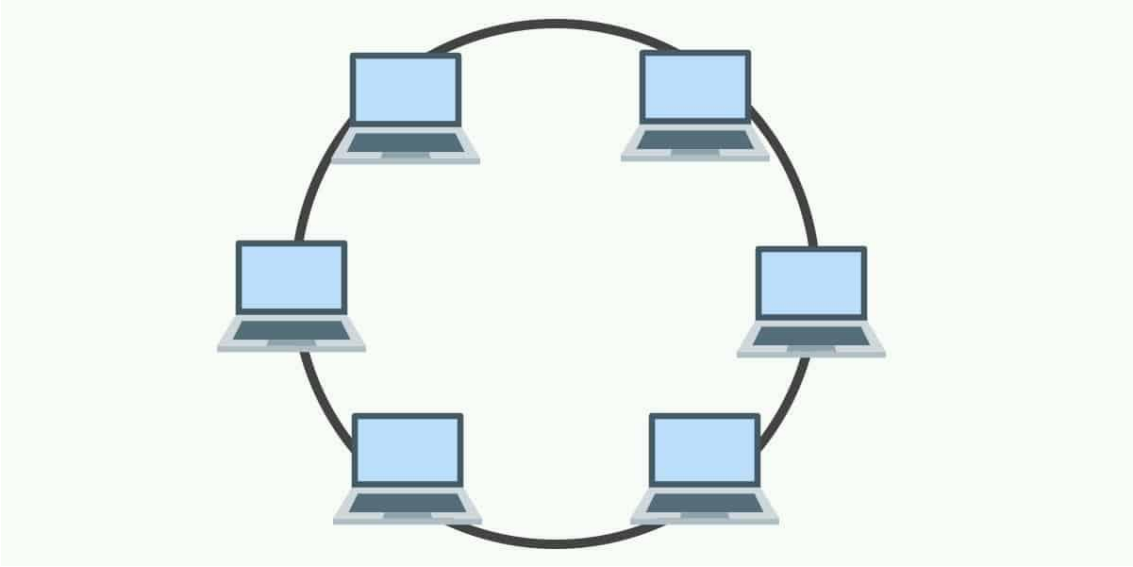

Рисунок 1.4 – Топологія кільце

Змішана топологія поєднує декілька типів топологій у загальну мережу. Наприклад, може бути застосована топологія зірка для підключення комп’ютерів у кожному офісі, а топологія загальна шина для підключення між офісами.

Кожен тип топології мережі має свої переваги та недоліки, які потрібно враховувати при виборі оптимальної топології для конкретної корпоративної мережі. Наприклад, зіркова топологія може бути більш підходящою для маленьких мереж, тоді як деревоподібна топологія підходить для більших мереж зі складною ієрархічною структурою.

Також варто зазначити, що реалізація топології мережі може залежати від конкретних вимог корпоративної мережі. Наприклад, якщо необхідна велика пропускна здатність мережі, може бути вибрана комбінована топологія, що поєднує різні типи топологій для забезпечення оптимальної швидкості передачі даних.

Отже, вибір оптимальної топології мережі є важливим етапом у розробці корпоративної мережі та потребує аналізу вимог та характеристики мережі.

Для даної корпоративної мережі будемо використовувати топологію зірка–шина, оскільки у даній топології збій на одному з комп'ютерів зовсім не

відображається на роботі інших комп’ютерів та мережі в цілому. Звичайно дана топологія має свої недоліки такі як що коли вийде з ладу центральний концентратор до якого підключенні комп’ютери окремого офісу то вони не зможуть підтримувати зв’язок з іншими офісами. Але в той самий момент це не відобразиться на роботі інших офісів.

1.2 Архітектура корпоративної мережі

Архітектура корпоративної мережі є складною системою, яка забезпечує зв’язок між комп’ютерами та іншими пристроями у межах організації. Вона включає в себе різні компоненти, такі як пристрої мережі, програмне забезпечення, протоколи, топологію мережі та безпеку.

Один з ключових компонентів архітектури корпоративної мережі – це пристрої мережі, такі як маршрутизатори, комутатори та інші. Вони забезпечують передачу даних між різними частинами мережі та регулюють доступ до мережі.

Поряд із пристроями мережі, програмне забезпечення відіграє важливу роль у роботі корпоративної мережі. Це можуть бути операційні системи, програми для моніторингу та управління мережею, програми для забезпечення безпеки та інші.

Протоколи є ще одним важливим компонентом архітектури корпоративної мережі, оскільки вони забезпечують правильну передачу даних між різними пристроями мережі. Це можуть бути такі протоколи, як TCP/IP, SNMP, DNS, DHCP та інші.

Останнім, але не менш важливим компонентом архітектури корпоративної мережі є безпека. У сучасних мережах даних, безпека є найважливішим аспектом, оскільки велика кількість конфіденційної інформації може бути передана через мережу. Забезпечення безпеки включає в себе захист від несанкціонованого доступу, вірусів, атак з мережі, перехоплення даних та інші загрози.

Організації можуть використовувати різні архітектурні моделі корпоративної мережі в залежності від їхніх потреб та бізнес–вимог. Одна з таких моделей – це модель мережі з централізованим керуванням, де всі пристрої під’єднані до центрального комутатора або маршрутизатора. Іншою популярною моделлю є розподілена модель, в якій немає центрального комутатора, а замість цього кожен вузол мережі може бути підключений до будь–якого іншого вузла в мережі [4].

При проектуванні архітектури корпоративної мережі необхідно враховувати такі чинники, як обсяг даних, які будуть передаватися, кількість користувачів та пристроїв, що підключені до мережі, розміщення пристроїв та вимоги до безпеки.

Отже, архітектура корпоративної мережі є складною системою, що містить в собі різні частини, такі як пристрої мережі, програмне забезпечення, протоколи, топологію мережі та безпеку. При розробці архітектури корпоративної мережі необхідно враховувати різні фактори, що впливають на роботу мережі, такі як обсяг даних, кількість користувачів та пристроїв, що підключені до мережі, розміщення пристроїв та вимоги до безпеки.

1.3 Протоколи та технології корпоративної мережі

Протоколи корпоративної мережі – це набір правил і процедур, що використовуються для передачі даних між комп'ютерами та іншими пристроями в мережі. Протоколи визначають формати даних, що передаються, методи комунікації та рівень безпеки.

Основні протоколи корпоративної мережі включають:

TCP/IP – це найбільш поширений протокол мережі Інтернет та корпоративних мереж. Він забезпечує забезпечення цілісності даних, аутентифікацію та шифрування. TCP/IP використовується для передачі даних в режимі реального часу та для віддаленого доступу до серверів.

DHCP – протокол, що дозволяє автоматично надавати IP–адреси та інші

параметри комп'ютерам в мережі. DHCP спрощує процес налаштування мережі та зменшує витрати на управління IP–адресами.

DNS – протокол, що забезпечує розрізнення імен хостів та їх IP–адрес. DNS дозволяє комп'ютерам знаходити інші комп'ютери в мережі за їх іменами, замість того, щоб запам'ятовувати їх IP–адреси.

SMTP – протокол, що використовується для передачі електронної пошти. SMTP дозволяє відправляти та отримувати повідомлення електронної пошти в мережі.

FTP – протокол, що використовується для передачі файлів між комп'ютерами. FTP дозволяє завантажувати та відвантажувати файли в мережі.

HTTP – протокол, що використовується для передачі веб–сторінок в мережі. HTTP дозволяє браузерам комп'ютера звертатися до веб–серверів та отримувати відповіді від них.

VPN – протокол, що використовується для забезпечення конфіденційність, цілісність і доступність даних, що передаються по мережі.

Окрім вищеописаних, у корпоративних мережах застосовуються також інші протоколи та технології, які допомагають забезпечити безпеку, надійність та ефективність роботи мережі. Деякі з цих протоколів:

Virtual Private Network (VPN) – це технологія, що дозволяє створити з'єднання між віддаленими пристроями через інтернет з застосуванням шифрування. VPN дозволяє працювати з віддаленими ресурсами, які знаходяться в іншій мережі, забезпечуючи при цьому конфіденційність інформації.

Simple Network Management Protocol (SNMP) – це протокол, що використовується для керування та моніторингу мережі. Він дозволяє збирати інформацію про стан мережевих пристроїв, таку як обсяг трафіку, статус підключення до мережі та стан апаратного забезпечення.

Spanning Tree Protocol (STP) – це протокол, що дозволяє уникнути петель в мережі. Він використовується для автоматичного виявлення та усунення петель, що можуть виникати при наявності декількох шляхів між двома

точками в мережі.

Quality of Service (QoS) – це технологія, що дозволяє контролювати трафік в мережі з метою забезпечення певного рівня якості обслуговування для різних типів трафіку. Вона забезпечує приоритетну обробку трафіку, що вимагає високої швидкості передачі, такого як голосовий чи відеотрафік.

Крім того, такі протоколи, як SSL/TLS, IPSec, SSH, використовуються для забезпечення безпеки трафіку в корпоративній мережі. SSL/TLS використовується для шифрування даних, переданих між клієнтом та сервером в Інтернеті. IPSec, з іншого боку, захищає трафік на рівні мережі, дозволяючи зашифровувати та автентифікувати пакети даних, що передаються між мережевими пристроями. SSH використовується для захисту від несанкціонованого доступу до віддалених пристроїв, забезпечуючи шифрування та автентифікацію.

Таким чином, корпоративна мережа має бути забезпечена відповідними протоколами та технологіями, що дозволяють забезпечити надійність, швидкість та безпеку передачі даних.

1.4 Методи захисту інформації в корпоративній мережі

Все більше компаній та організацій об'єднують свої ресурси в єдину корпоративну мережу. Захист інформації у таких мережах є дуже важливою задачею, оскільки вони можуть бути піддані атакам ззовні та зсередини. Тому важливо розглянути методи захисту інформації в корпоративній мережі.

Забезпечення безпеки в корпоративній мережі є одним з найбільш важливих аспектів її розробки і ефективної роботи. Зокрема, потрібно забезпечити захист від зломів, вірусів, шкідливих програм, хакерських атак та інших небезпечних загроз.

Одним з найпоширеніших методів захисту інформації в корпоративній мережі є застосування різних видів шифрування. Шифрування використовується для захисту даних, які передаються по мережі від

несанкціонованого доступу та зміни. Найбільш поширеними протоколами шифрування є SSL/TLS, IPSec, SSH, а також VPN.

Крім того, у корпоративній мережі також можуть використовуватися методи захисту на рівні програмного забезпечення, які включають шифрування файлів, застосування брандмауерів та антивірусного програмного забезпечення для захисту від вторгнень та вірусів. Для захисту від соціальної інженерії також можуть бути введені правила щодо використання паролів, обмеження доступу до конфіденційної інформації та навчання співробітників про методи захисту від фішингу та інших видів атак.

Окрім цього, важливим методом захисту є регулярне резервне копіювання даних, щоб захистити важливу інформацію від випадкового знищення або пошкодження. Це можна здійснювати як внутрішніми, так і зовнішніми засобами зберігання даних, такими як сховища даних на серверах чи на зовнішніх носіях.

Усі ці методи захисту можуть бути використані разом для створення комплексної системи захисту інформації в корпоративній мережі, яка забезпечує надійний захист від зовнішніх і внутрішніх загроз. Однак, важливо зазначити, що найбільш ефективна система захисту може бути створена тільки в результаті аналізу конкретних вимог інформаційної безпеки в конкретній організації.

Отже, як висновок можемо виділити основні методи захисту інформації в корпоративній мережі такі як:

Аутентифікація – це метод який дозволяє перевірити ідентичність користувача та перевірити, чи має він право доступу до системи. Для цього можна використовувати різні методи аутентифікації, такі як логін та пароль, біометричні методи або токени.

Авторизація – це метод, що дозволяє контролювати доступ користувача до різних ресурсів системи. Це досягається шляхом встановлення прав доступу на рівні користувача або групи користувачів.

Шифрування – це метод захисту дозволяє зашифрувати дані, які

передаються між користувачами, що знижує ризик їх перехоплення та зламу.

Firewall – це метод захисту, що дозволяє контролювати доступ до мережі ззовні, блокуючи небажаний доступ та захищаючи мережу від потенційних атак.

Антивірусне програмне забезпечення – це метод для захисту який дозволяє виявляти та блокувати шкідливе програмне забезпечення, таке як віруси, трояни, черви та інші види зловмисного програмного забезпечення.

Моніторинг – це метод захисту, що дозволяє відслідковувати дії користувачів та виявляти незвичну або небезпечну активність. Це допомагає попередити можливі атаки та злами та забезпечує більш високий рівень безпеки мережі.

Резервне копіювання даних – це метод дозволяє зберігати копії важливих даних в іншому місці, щоб забезпечити їх відновлення у випадку втрати чи пошкодження.

1.1.2 Методи тестування системи захисту. Види хакерських атак

Тестування безпеки – це важливий процес, який виконується з метою виявити недоліки в механізмах безпеки та знайти вразливості або слабкі місця комп’ютерних програм чи корпоративної мережі.

Основна мета тестування безпеки – з’ясувати, наскільки вразлива може бути корпоративна мережа чи система, та визначити, чи захищені її дані та ресурси від потенційних зловмисників(хакерів).

1. Підвищення привілеїв

Підвищення привілеїв це клас атаки, коли хакер має обліковий запис у системі і використовує його для підвищення своїх системних привілеїв на більш високий рівень, ніж йому передбачено. У разі успіху, такий тип атаки може призвести до того, що хакер отримає привілеї настільки ж високі, як root у системі UNIX. Після того, як хакер отримує привілеї суперкористувача, він може запускати код з таким рівнем, і вся система фактично порушена.

2. Інжекція SQL

Інжекція SQL це найпоширеніший вид атаки на рівні додатків, яка

використовується хакерами, в якій шкідливі оператори SQL вставляються у поле для введення, для виконання. Атаки введення SQL дуже небезпечні, оскільки зловмисник може отримати критичну інформацію з серверної бази даних. Це тип атаки, який використовує переваги лазівки, наявної у впровадженні веб–додатків, що дозволяє хакеру зламати систему. Щоб перевірити SQL, ми повинні подбати про введення полів, таких як текстові поля, коментарі тощо.

3. Несанкціонований доступ до даних

Одним з найпопулярнішим способом атак є отримання несанкціонованого доступу до даних всередині програми. Доступ до даних можна отримати на серверах або в мережі.

Несанкціонований доступ включає:

– Несанкціонований доступ до даних за допомогою операцій із отримання даних

– Несанкціонований доступ до відомостей про автентифікацію клієнтів, що використовуються повторно, шляхом контролю доступу інших.

– Несанкціонований доступ до даних, контролюючи доступ інших.

Підробка особи

Підробка ідентифікації це техніка, при якій хакер використовує облікові дані законного користувача або пристрою для запуску атак на мережеві хости, крадіжки даних або для обходу контролю доступу.

4. Взлом пароля

Взлом пароля є найважливішою частиною під час тестування системи. Щоб отримати доступ до приватних областей програми, хакери можуть скористатися інструментом злому пароля або відгадати загальне ім’я користувача/ пароль. Поширені імена користувачів та паролі легко доступні в Інтернеті разом із програмами з розкриттям пароля з відкритим кодом. Поки веб–додаток не застосовує складний пароль (наприклад, довгий пароль із комбінацією цифр, букв та спеціальних символів).

5. Тестування на проникнення

Тест на проникнення це атака на комп’ютерну систему з наміром знайти лазівки безпеки, потенційно отримати доступ до неї, її функціональності та даних.

1.5 Аудит та моніторинг корпоративної мережі

Аудит та моніторинг корпоративної мережі є важливою частиною процесу управління мережею. Це дозволяє контролювати стан мережі та виявляти можливі проблеми, що можуть виникнути в майбутньому. У цьому розділі розглянемо основні аспекти аудиту та моніторингу корпоративної мережі.

Аудит корпоративної мережі є процесом перевірки стану мережі з метою виявлення потенційних проблем. Основні завдання аудиту мережі включають:

– перевірка наявності вразливостей в мережі;
– перевірка правильності налаштування мережевих пристроїв;
– перевірка відповідності мережі вимогам безпеки;
– визначення обсягу трафіку, що проходить через мережу;
– виявлення потенційних загроз безпеці мережі.

Для проведення аудиту мережі можна використовувати спеціальні програмні засоби, які дозволяють автоматизувати цей процес та підвищують його ефективність.

Моніторинг корпоративної мережі є важливою складовою її ефективності та безпеки. Це є процесом постійного контролю за станом мережі з метою виявлення потенційних проблем та їх вчасного вирішення. Основні завдання моніторингу мережі включають:

– контроль за доступністю мережевих пристроїв та сервісів;
– контроль за використанням ресурсів мережі;
– контроль за обсягом трафіку, що проходить через мережу;
– виявлення можливих проблем та їх вчасне вирішення.

Один з найпоширеніших методів моніторингу – це використання системи керування мережею (Network Management System – NMS). NMS дозволяє зібрати та аналізувати дані про роботу мережі, такі як пропускна здатність, навантаження на мережу та інші параметри, що дозволяє забезпечити ефективне функціонування мережі та вчасно виявляти проблеми.

Ще один метод моніторингу – це використання протоколів мережевого аналізу (Network Analysis Protocol – NAP). Протокол NAP дозволяє збирати та аналізувати трафік мережі, що дозволяє виявляти та вирішувати проблеми з навантаженням та швидкістю мережі.

Також існують спеціалізовані інструменти моніторингу, які дозволяють відстежувати певні параметри мережі, наприклад, рівень безпеки, перевірку доступності мережі та інші.

Проведення моніторингу корпоративної мережі дозволяє вчасно виявляти проблеми та запобігати їх поширенню, забезпечуючи ефективну роботу мережі та збереження інформації.

РОЗДІЛ 2
ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

2.1 Аналіз потреб користувачів

Аналіз потреб користувачів є важливим етапом в процесі проектування будь–якої системи, включаючи і корпоративну мережу. Цей етап дозволяє з'ясувати, які функції мають бути реалізовані в мережі та які вимоги повинні бути враховані при її проектуванні.

При аналізі потреб користувачів необхідно визначити, які задачі вони планують виконувати в мережі, які додатки вони використовують, які обсяги даних потрібно передавати, які ресурси повинні бути доступні, які вимоги до якості обслуговування мережі, і т.д.

Для проведення аналізу потреб користувачів можна використовувати різні методи, такі як анкетування користувачів, спостереження за їх діяльністю, інтерв'ю з ключовими користувачами та інші.

Результатом аналізу потреб користувачів повинен бути список вимог, які повинна задовольняти корпоративна мережа. Цей список повинен включати вимоги щодо характеристик мережі, таких як пропускна здатність, швидкість передачі даних, надійність та інші, а також вимоги до функціональності мережі, таких як доступ до ресурсів, безпека мережі, забезпечення якості обслуговування та інші.

Першим кроком у процесі аналізу потреб є визначення груп користувачів та їх потреб. Для цього необхідно провести дослідження, зокрема, опитування та інтерв'ю з потенційними користувачами. Під час опитування важливо звернути увагу на такі аспекти, як тип діяльності, робоче місце, потреби у віддаленому доступі до мережі, рівень безпеки, обсяг даних, що передаються тощо.

Другим кроком є аналіз зібраних даних та визначення ключових потреб користувачів. Цей аналіз дозволяє зрозуміти, які саме функції та можливості має мати корпоративна мережа, щоб задовольнити потреби користувачів.

Наприклад, якщо виявлено, що більшість користувачів працюють з великими об'ємами даних, необхідно забезпечити високу швидкість передачі даних. Якщо більшість користувачів працюють з віддаленими місцями, необхідно забезпечити доступ до мережі з будь–якого місця.

Також важливо враховувати майбутні потреби користувачів, оскільки це може вплинути на вибір технологій та архітектури мережі. Наприклад, якщо очікується збільшення кількості працівників, то необхідно врахувати можливість масштабування мережі та додаткових ресурсів.

Підсумувавши можна зробити висновок, що аналіз потреб користувачів є ключовим етапом в проектуванні корпоративної мережі, який дозволяє врахувати їхні вимоги та потреби, забезпечити оптимальну роботу мережі та задовольнити потреби бізнесу.

Отже провівши аналіз потреб користувачів на підприємстві з лісозаготівлі визначено основні потреби користувачів. Усього на підприємстві знаходиться 25 користувачів, також ще 5 працюють віддалено. У своїй роботі користувачі використовують веб браузери, програму бухгалтерського обліку BAF, яка знаходиться на центральному сервері головного офісу області, програму податкової звітності серверного типу Medoc, яка знаходиться на локальному сервері підприємства. Для задовільнення потреб на підприємство було підведено основну лінію інтернету у 100 MBit/s і резервну лінію іншого інтернет провайдера зі швидкістю 100 MBit/s.

2.2 Вибір технічних засобів

При створенні корпоративної мережі, важливим етапом є вибір технічних засобів, які відповідають вимогам і потребам організації. Від вибору техніки залежить надійність, ефективність та масштабованість мережі.

Для початку проектування мережі потрібно ретельно проаналізувати потреби користувачів. Необхідно визначити кількість користувачів, які будуть працювати в мережі, їх місця роботи, види діяльності та інші характеристики,

що впливають на вибір обладнання.

Після аналізу потреб користувачів, необхідно розглянути технічні можливості та обмеження. Наприклад, якщо користувачі працюють з великими обсягами даних, потрібно вибрати високошвидкісний обладнання, що забезпечує швидкий доступ до даних.

Також необхідно враховувати вартість технічних засобів, їх підтримку та обслуговування. На цьому етапі важливо провести детальний аналіз різних пропозицій від постачальників техніки та програмного забезпечення та зробити відповідні висновки.

Отже можна виділити основні критерії вибору технічних засобів такі як:

Характеристики мережевого обладнання (потужність, швидкість передачі даних, типи портів, підтримка стандартів тощо);

Програмне забезпечення мережі (операційна система, мережеві драйвери, антивірусне програмне забезпечення, програмне забезпечення для моніторингу тощо);

Протоколи мережі (TCP/IP, HTTP, FTP, SMTP, SNMP тощо);

Безпека та захист (фаєрвол, VPN, шифрування, аутентифікація, контроль доступу до мережі тощо).

2.2.1 Вибір типу мережевих кабелів

Мережевий кабель це середовище, за допомогою якого інформація зазвичай передається від одного мережевого пристрою до іншого. Існує кілька типів кабелів, які зазвичай використовуються в корпоративних мережах. У деяких випадках мережа буде використовувати тільки один тип кабелю, інші мережі будуть використовувати різні типи кабелю. Тип кабелю, обраний для мережі, залежить від топології, протоколу та розміру мережі. Розуміння характеристик різних типів кабелю та їх зв’язку з іншими аспектами мережі необхідно для розвитку успішної мережі [5].

У таблиці 2.1 розписано специфікацію типів кабелів

Таблиця 2.1 – Специфікація типів кабелів

Специфікація	Тип кабелю
10Base2	Тонкий коаксіальний
10Base5	Товстий коаксіальний
100BaseFX	Волоконно–оптичний
100BaseBX	Волоконно–оптичний одномодовий
10BaseT	Неекранована вита пара
100BaseSX	Волоконно–оптичний багатомодовий
1000BaseT	Неекранована вита пара
1000BaseFX	Волоконно–оптичний
1000BaseBX	Волоконно–оптичний одномодовий
1000BaseSX	Волоконно–оптичний багатомодовий

Коаксіальний кабель

Коаксіальний кабель (рис. 2.1) є типом кабелю, який передає високочастотні електричні сигнали за допомогою одноядерного сердечника. Зазвичай, коаксіальний кабель використовується для підключення телевізійних антен до пристроїв. Однак, коаксіальний кабель також може бути використаний для побудови комп'ютерних мереж, підключення до Інтернету та як радіоканал.

Коаксіальний кабель має багатошарову структуру, де кожен шар виконує свою функцію у захисті основного ядра. Перший шар, відомий як ізолятор, призначений для захисту сердцевини [6].

У наступному шарі присутні заходи для запобігання втручання зовнішніх електромагнітних сигналів, які можуть вплинути на передачу даних і витік сигналу. Цей шар може мати дві різні форми: плетений обмотка або захист з фольги. Останній шар призначений для захисту кабелю від вологості та впливу навколишнього середовища.

З 1980-х до початку 1990-х років коаксіальний кабель був широко використовуваним у комп'ютерних мережах Ethernet. Коаксіальний кабель мав два основних типи: тонкий коаксіальний кабель зі стандартом 10BASE2 і товстий коаксіальний кабель зі стандартом 10BASE5. Однак, в сучасних комп'ютерних мережах коаксіальний кабель був замінений кабелями крученої пари, оскільки фізична структура коаксіального кабелю вважається жорсткою, що ускладнює процес встановлення та обслуговування кабелю.

Рисунок 2.1 – Коаксіальний кабель [5]

Вита пара

Вита пара – це тип комунікаційного кабелю, що складається з мідних проводів, що скручуються в пари (або кілька пар), і знаходяться всередині екранованої оболонки. Скручування пар проводів виконується з метою зменшення електромагнітних перешкод. Вита пара проявляє високу стійкість до впливу зовнішніх перешкод.

Стандарти категорій кабелів визначають діапазон частот, в межах якого кабель може ефективно працювати. Інші фактори, такі як клас обладнання або

якість кабельних мереж, можуть лише підтримувати задану частоту/швидкість, і в гіршому випадку можуть створювати перешкоди [7].

Категорії витих пар та їх характеристики:

- CAT1 використовується в даний час для з'єднання між розподільним щитком і квартирою, працюючи в діапазоні частот 0,1 МГц.
- CAT 2 використовується для підключення телефонних апаратів до телефонної коробки, працюючи в діапазоні частот 1 МГц (з швидкістю передачі приблизно 4 Мбіт/с).
- CAT 3 працює в діапазоні частот 16 МГц і забезпечує швидкість передачі даних до 10 Мбіт/с або 100 Мбіт/с на відстані, не перевищуючи 100 метрів.
- CAT 4 працює в діапазоні частот 20 МГц і має швидкість передачі даних до 16 Мбіт/с. Однак на сьогоднішній день цей стандарт не використовується.
- CAT 5 є категорією кабелю, який працює в діапазоні частот 100 МГц, зі швидкістю передачі даних до 100 Мбіт/с. Існує також розширений варіант CAT 5e, який підтримує частоту до 125 МГц та досягає швидкості передачі 100 Мбіт/с при використанні 2 пар або до 1000 Мбіт/с при використанні 4 пар. Кабелі цієї категорії мають найширше поширення у сучасних мережах.
- CAT 6 є категорією кабелю з діапазоном частот 250 МГц, що дозволяє досягти швидкості передачі даних 1000 Мбіт/с, що відповідає 1 Гбіт/с.
- CAT6a є категорією кабелю з діапазоном частот 500 МГц, що дозволяє досягти швидкості передачі даних 10 Гбіт/с.CAT 7 діапазон частот 600–700 МГц (10 Гбіт / с)
- Залежно від наявності захисту — електрично заземленої мідної сітки або алюмінієвої фольги навколо скручених пар, визначають різновиди цієї технології:
- неекранована вита пара (рис. 2.2)

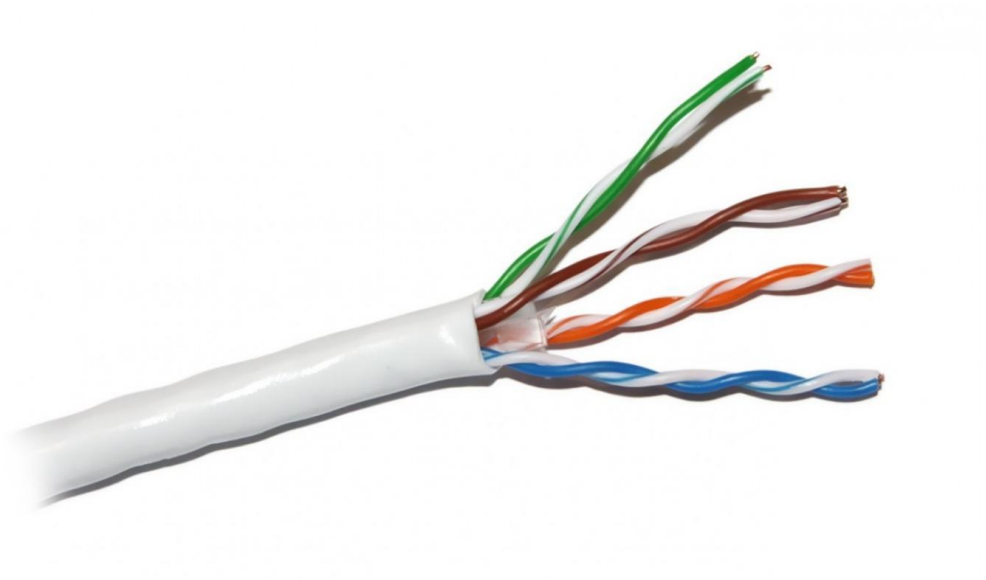

Рисунок 2.2 – Неекранована вита пара [5]

– екранована вита пара (рис. 2.3)

Рисунок 2.3 – Екранована вита пара [5]

– фольгована вита пара (рис. 2.4)

Рисунок 2.4 – Фольгована вита пара [5]

– фольгована екранована вита пара

Цей кабель відрізняється своєю простотою у встановленні. Він є найбільш доступним і поширеним типом зв'язку, який широко використовується у багатьох локальних мережах з Ethernet–архітектурою, збудованих у топології зірка. Для підключення до мережевих пристроїв використовується з'єднувач RJ45.

Цей кабель застосовується для передачі даних зі швидкістю 10 Мбіт/с і 100 Мбіт/с. Зазвичай вита пара використовується для зв'язку на відстані до кількох сотень метрів. Серед недоліків цього кабелю можна виділити можливість простого несанкціонованого підключення до мережі.

2.2.2 Аналіз мережевого обладнання

Мережне обладнання

Мережеве обладнання є необхідним для правильної роботи мережі і включає в себе такі пристрої, як маршрутизатор, комутатор, концентратор, патч–панель та інші. Зазвичай вони класифікуються на активне та пасивне обладнання. До активного мережевого обладнання належать маршрутизатори та керовані комутатори, тоді як до пасивного — некеровані комутатори, повторювачі, мережеві кабелі, шафи та інші пристрої.

Активне мережеве обладнання

Активне мережне устаткування має певні інтелектуальні можливості, такі

як маршрутизатори та комутатори. Крім того, керовані комутатори також є активним мережним обладнанням, оскільки вони можуть бути оснащені додатковими інтелектуальними функціями.

Пасивне мережеве обладнання

Обладнання, яке не має інтелектуальних функцій, називається пасивним мережевим устаткуванням. Прикладами можуть бути кабельні системи, такі як коаксіальний кабель, вита пара, роз'єми (RG58, RJ45, RJ11, GG45), патч–панелі, повторювачі , концентратори , балуни для коаксіальних кабелів (RG–58) та інше. Також до пасивного обладнання можна віднести монтажні шафи і стійки, телекомунікаційні шафи. Монтажні шафи можуть бути типовими, спеціалізованими або антивандальними та розміщуватися як на стінах, так і на підлозі або в інших місцях.

Мережеві маршрутизатори

Маршрутизатори використовують мережеві протоколи які використовуються на мережевому рівні та взаємодіють з зовнішнім світом та локальною мережею. Основний роутер в мережі може надавати IP–адреси за допомогою протоколу DHCP та контролювати допустимі адреси. Зазвичай роутер виступає як шлюз для комп'ютерів у мережі, тому зовнішня адреса буде мати адресу роутера. Зовнішню адресу можна налаштувати як статичну, так і динамічну.

Роутери також часто виконують функції мережевого екрану на вищому рівні, проводячи аналіз даних на рівні транспортних або навіть прикладних мережевих протоколів. Це означає, що можна налаштувати на роутері доступні та недоступні порти та налаштувати перенаправлення портів.

На рисунку 2.5 показаний маршрутизатор MikroTik hAP RB951Ui–2ND

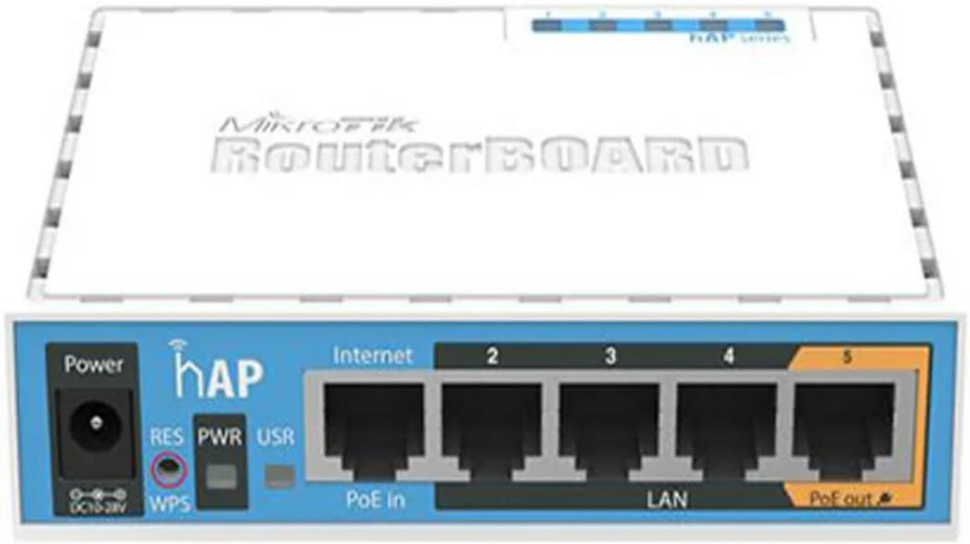

Рисунок 2.5 – Маршрутизатор MikroTik hAP RB951Ui–2ND

Мережевий концентратор

Цей пристрій працює на фізичному рівні мережевих протоколів та пересилає дані, що надходять на один порт, на всі інші порти. Використання хабів при побудові мереж стало можливим джерелом сніфінгу, тобто підслуховування передаваних даних іншими користувачами. Заснований на простому принципі, сніфінг включає в себе переведення мережевої карти в режим прослуховування всіх пакетів, що надходять на комп'ютер, а не тільки призначених для нього [9].

На рисунку 2.6 показаний мережевий концентратор TP–LINK LS1008G

Рисунок 2.6 – Мережевий концентратор(некерований світч) TP–LINK LS1008G

Мережеві комутатори

Пристрої, які функціонують на канальному рівні мережевих протоколів, широко використовуються і записують MAC–адреси підключених комп'ютерів для пересилання пакетів лише до відповідного комп'ютера, який вказаний в пакеті. Однак, це може створювати проблему зізнімання даних. Для вирішення цієї проблеми та зниження навантаження на лінію були введені комутатори. Комутатори (рис. 2.7) можуть мати окремий порт, відомий як «UpLink», для відправки пакетів, які не знайдуть адресата в локальній мережі. Найпоширеніші є керовані комутатори, оскільки вони дозволяють налаштовуватися з комп'ютера і управлятися через мережу, зберігаючи при цьому прозорість для мережевого рівня [9].

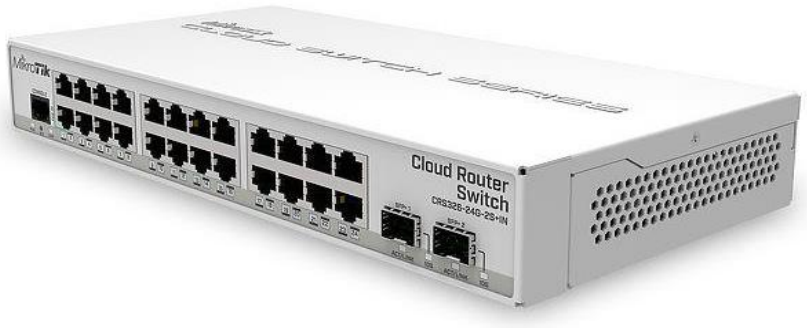

Рисунок 2.7 – Коммутатор Mikrotik CRS326–24G–2S+IN

Точка доступу

Точка доступу – це пристрій, який дозволяє підключатись до бездротової мережі (Wi–Fi) з підтримкою стандартів IEEE 802.11. Точка доступу підключається до провідної мережі за допомогою Ethernet–кабелю або іншого провідного з'єднання, а потім перетворює провідний сигнал на бездротовий, що дозволяє підключатись до мережі з будь–якої точки, яка знаходиться в зоні її дії.

Точки доступу можуть використовуватись як в приватних, так і в публічних мережах. В приватних мережах, точки доступу зазвичай розміщуються в будинках, офісах та інших закритих просторах. В публічних

мережах, таких як кав'ярні, готелі, аеропорти та інші місця з великою кількістю людей, точки доступу зазвичай розміщуються в зонах, які покривають значну площу та доступні для використання будь–яким користувачем.

Точки доступу (рис. 2.8) мають вбудовану безпеку, яка забезпечує захист від несанкціонованого доступу до мережі. Також вони можуть мати додаткові функції, такі як фільтрація трафіку та контроль пропускної здатності, які дозволяють адміністраторам мережі контролювати доступ до різних ресурсів та обмежувати швидкість інтернет–підключення [9].

Рисунок 2.8 – Точка доступа MikroTik cAP (RBCAP2ND)

2.3 Розробка схеми мережі

Відвідавши дане підприємство склали схему мережі (рис.2.9) з наступним планом приміщень:

– Кабінет головного лісника в якому знаходиться 1 ноутбук
– Кабінет головного інженера в якому знаходиться 1 комп’ютер
– Кабінет головного бухгалтера з 1 комп’ютером

Рисунок 2.9 – Схема мережі вибраного підприємства

- Кабінет де знаходяться працівники ІТ відділу, в ньому знаходиться 2 комп’ютера, спеціалізована шафа в якій розміщенно: локальний сервер підприємства, маршутизатор, 24–х портовий комутатор
- Кабінет лісового відділу у ньому розміщено 5 комп’ютерів та мережевий принтер
- Кабінет виробничого відділу у якому розміщено 4 комп’ютера
- Кабінет відділу кадрів розміщено 1 ноутбук
- Кабінет директора у якому розміщений 1 ноутбук
- Кабінет секретаря у ньому розміщено 1 комп’ютер
- Кабінет бухгалтерії в якому розміщено 6 комп’ютерів та 1 мережевий принтер

Визначившись з кількістю комп’ютерної техніки та переферії вирішили у кабінеті лісового відділу та виробнибничого відділу розмістити 8–ми портові світчі. У кабінеті бухгалтерії розмістити 12–ти портовий світч, оскільки окрім бухгалтерії до нього буде під’єднаний ще кабінет директора та секретаря. У ІТ відділі буде розміщено головний роутер, 8–ми портовий світч, медіаконвертори та локальний сервер підприємства. Кабінет головного лісничого, головного інженера та головного бухгалтера будуть напряму під’єднанні до 8–ми портового світча.

Також для того щоб покрити усю площу підприємства безпровідною мережею (Wi Fi) на стелі у коридорі розмістимо 2 точки доступу, також ще 1 точку доступу буде розміщена у кабінеті ІТ.

2.4 Вибір топології мережі

Провівши вище розгляд основних топологій мереж визначили що для даного підприємства найкраще підійде топологія загальна шина–зірка (рис. 2.10). Топологією типу зірка будуть під’єднанні комп’ютери у кожному кабінеті до комутатора, а вже самі комутатори будуть під’єднанні до головного

роутера.

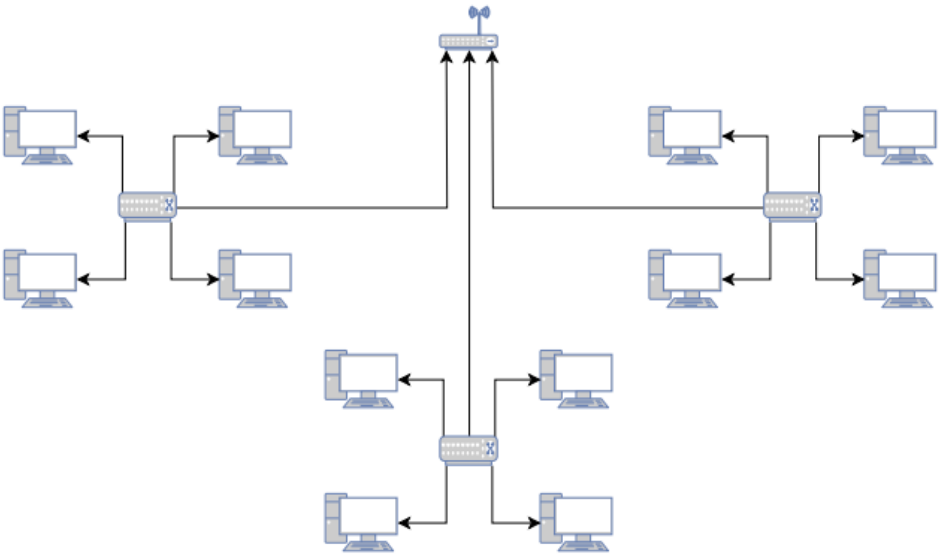

Рисунок 2.10 – Схематичне зображення вибраної топології

Даний тип топології є найбільш вдалим та простим в обслуговуванні і підтримці і буде надавати безперебійну роботу усього підприємства.

2.5 Підбір мережевого обладнання

Склавши схему мережі потрібно підібрати мережеве обладнання яке буде встановлене на підприємстві. Провівши аналіз ринку та переглянувши цінову політику на мережеве обладнання виявили що найкращим на ринку для мережевого інтелектуального обладання є 2 фірми Cisco та Microtik.

2.5.1 Cisco

Cisco – це один з найбільших світових постачальників технологій мережевого обладнання і рішень для комунікаційного обладнання. Компанія Cisco Systems була заснована у 1984 році і швидко стала лідером у сфері мережевих технологій, пропонуючи широкий спектр продуктів та рішень для побудови мережі.

Cisco пропонує широкий вибір мережевого обладнання, включаючи

маршрутизатори, комутатори, маршрутизатори з комутацією мультимедіа (Multilayer Switch Routers), мережеві пристрої для безпеки (firewalls), точки доступу Wi–Fi, відеоконференційні системи та багато іншого. Ці продукти спроектовані для побудови надійних, масштабованих та безпечних корпоративних мереж.

Основні характеристики технологій Cisco включають:

Надійність: Продукти Cisco відомі своєю високою надійністю та стабільністю. Вони побудовані з використанням передових технологій та мають механізми резервування та відновлення, що забезпечують безперебійну роботу мережі.

Масштабованість: Обладнання Cisco розроблене з урахуванням масштабуваності, що дозволяє легко розширювати мережу залежно від потреб бізнесу. Висока продуктивність комутаторів та маршрутизаторів Cisco дозволяє ефективно обробляти великий обсяг трафіку і підтримувати високу швидкість передачі даних.

Безпека: Cisco приділяє велику увагу захисту мережевих інфраструктур. Вони пропонують різні технології та продукти для забезпечення безпеки мережі, такі як брандмауери, VPN (віртуальні приватні мережі), системи виявлення вторгнень (IDS) та інші рішення для контролю доступу та захисту даних.

Управління: Cisco надає рішення для ефективного управління мережею. Це включає централізоване керування, моніторинг та управління мережевим обладнанням через спеціальне програмне забезпечення, таке як Cisco Prime Infrastructure. Завдяки цьому, адміністратори можуть легко налаштовувати, контролювати та підтримувати роботу мережі.

Інновації: Cisco постійно працює над розробкою нових технологій та рішень, щоб задовольнити зростаючі потреби бізнесу. Вони активно займаються дослідженнями і розробками, співпрацюючи зі світовими технологічними компаніями та академічними установами.

Технології Cisco використовуються в різних сферах, включаючи

корпоративний сектор, постачання послуг, урядові установи та інші галузі. Вони допомагають підприємствам забезпечити надійну і безпечну мережу, що впливає на ефективність роботи, забезпечує легкість спілкування та сприяє розвитку бізнесу.

Загалом, Cisco відома своїми передовими технологіями, надійними продуктами та високою якістю обслуговування, що робить її одним з переважних виборів для побудови сучасних корпоративних мереж.

2.5.2 MicroTik

MikroTik є латвійською компанією, яка спеціалізується на розробці мережевого обладнання та програмного забезпечення. Вони виробляють широкий спектр мережевих пристроїв, включаючи маршрутизатори, комутатори, точки доступу Wi–Fi, файрволи та інші засоби для побудови мережевої інфраструктури.

Основні характеристики MikroTik:

RouterOS: MikroTik використовує операційну систему RouterOS, яка є потужною та гнучкою платформою для управління мережевими пристроями. RouterOS надає широкий спектр функціональності, включаючи маршрутизацію, комутацію, безпеку, моніторинг та управління мережею.

Висока продуктивність: Продукти MikroTik відомі своєю високою продуктивністю, що дозволяє ефективно обробляти великий обсяг трафіку та забезпечувати швидку передачу даних. Вони підтримують різні технології, такі як багатопотокова передача даних (multi–threading), що забезпечують оптимальну продуктивність мережі.

Безпека: MikroTik надає рішення для забезпечення безпеки мережі. Вони підтримують різні функції безпеки, такі як файрвол, віртуальні приватні мережі (VPN), системи виявлення вторгнень (IDS) та інші механізми захисту даних.

Легкість використання: Продукти MikroTik відомі своєю простотою налаштування та використання. Вони надають графічний інтерфейс користувача (GUI) та командний рядок (CLI) для налаштування та управління пристроями. Крім того, MikroTik також надає детальну документацію та

ресурси.

Розширені можливості мережі: Продукти MikroTik підтримують різні технології та протоколи, що дозволяють розширити функціональні можливості мережі. Наприклад, вони підтримують VLAN (Virtual Local Area Network), що дозволяє створювати логічні сегменти мережі для кращого управління трафіком та безпеки. Також MikroTik підтримує протоколи маршрутизації, такі як OSPF (Open Shortest Path First) та BGP (Border Gateway Protocol), що забезпечують ефективний розподіл трафіку в мережі.

Гнучкість та розширюваність: Продукти MikroTik відомі своєю гнучкістю та можливістю розширення. Вони надають різноманітні опції для розширення функціональності мережі, включаючи підтримку додаткових модулів та розширювачів, що дозволяють додавати нові функції та можливості до мережевих пристроїв.

Підтримка технологій безпроводового зв'язку: MikroTik також виробляє пристрої для безпроводового зв'язку, включаючи точки доступу Wi–Fi. Вони підтримують різні стандарти безпроводового зв'язку, такі як 802.11ac, 802.11n, і мають розширені можливості для управління безпроводовою мережею.

В цілому, MikroTik є популярним виробником мережевого обладнання, який пропонує широкий спектр продуктів для побудови та управління корпоративними мережами. Їх продукти відомі своєю надійністю, продуктивністю, гнучкістю та розширюваністю, що робить їх привабливим вибором для підприємств будь–якого розміру.

2.5.3 Порівняння Cisco та Microtik

Cisco і MikroTik є двома відомими виробниками мережевого обладнання, які пропонують рішення для побудови та управління корпоративними мережами. Ось порівняння між ними за деякими ключовими характеристиками:

Репутація та досвід: Cisco є одним з найбільш відомих та впливових виробників мережевого обладнання. Вони мають довгу історію і широкий досвід у розробці інноваційних технологій для мережевої інфраструктури. MikroTik, хоч і менш відомий, також має свою власну базу клієнтів та

репутацію, особливо серед невеликих та середніх підприємств.

Широкий асортимент продуктів: Cisco пропонує широкий спектр мережевого обладнання, включаючи маршрутизатори, комутатори, точки доступу Wi–Fi, файрволи та багато іншого. Вони мають рішення для корпоративних мереж різних розмірів і потреб. MikroTik також пропонує різні типи мережевого обладнання, проте їх асортимент може бути меншим у порівнянні з Cisco.

Вартість: У багатьох випадках, MikroTik пропонує більш доступні цінові рішення порівняно з Cisco. Це робить їх привабливим вибором для невеликих та середніх підприємств з обмеженими бюджетами. Cisco, з іншого боку, часто спрямований на підприємства великого розміру, де вимагається висока продуктивність та рівень підтримки.

Надійність та стабільність: Як Cisco, так і MikroTik прагнуть забезпечити надійність своїх продуктів. Обидва виробники проводять тестування та валідацію перед випуском нових пристроїв на ринок. Однак, вважається, що Cisco має більш довгу історію надійності та стабільності своїх пристроїв.

Підтримка та екосистема: Cisco є лідером у галузі мережевих технологій і має розгалужену екосистему, яка включає в себе сертифікаційні програми, навчальні матеріали, партнерські взаємини та широку базу знань. У випадку потреби в підтримці або консультаціях, Cisco може забезпечити професійну допомогу. MikroTik також надає підтримку своїм клієнтам, але можливості підтримки можуть бути менш широкими.

Інтерфейс та управління: Cisco та MikroTik мають свої власні інтерфейси управління, які дозволяють налаштовувати та керувати мережевими пристроями. Cisco використовує свою власну операційну систему IOS (Internetwork Operating System), яка має великий набір функцій і можливостей. MikroTik використовує RouterOS, який також має багато функцій та дозволяє гнучке управління мережею.

Отже, як Cisco, так і MikroTik є відомими виробниками мережевого обладнання, кожен з яких має свої переваги та особливості. Cisco відомий

своєю репутацією, широким асортиментом продуктів та високою продуктивністю, що робить його популярним вибором для великих підприємств. Але в нашому випадку для нас найбільше підходить MikroTik оскільки провівши порівняння двох виробників виявили що саме ця фірма не поступається світовому бренду Cisco але цінова політика даного бренду набагато краще чим у Cisco. Також для неінтелектуального обладнання вибираєм TP–Link оскільки даний бренд є найкращим вибором порівнюючи ціну та якість для використання на даному підприємстві

Маршрутизатор MikroTik RB3011UiAS–RM

На рисунку 2.11 зображено маршрутизатор MikroTik RB3011UiAS–RM

Рисунок 2.11 – Маршрутизатор MikroTik RB3011UiAS–RM [10]

Характеристка:

Інтерфейси:

–10 x LAN

–1 x SFP

–1 x Серійний порт RJ45

–1 x USB 3.0

Призначення роутера: Серверний

Швидкість LAN портів: 1 Гбіт/с

WAN–порт: Ethernet

USB–порт: 1 x USB 3.0

Підтримка протоколів:

–DHCP

–IPsec

–L2TP

–NAT

–PPPoE

–PPTP

Габарити і вага: 443 x 92 x 44 мм, 0.67 кг

Точка доступу Ubiquiti UniFi AP AC Pro

На рисунку 2.12 зображено точку доступу Ubiquiti UniFi AP AC Pro

Рисунок 2.12 – Точка доступу Ubiquiti UniFi AP AC Pro [9]

Характеристика:

Стандарт зв’язку: Wi–Fi 5 (802.11ac)

Частота роботи Wi–Fi:

2.4 ГГц

5 ГГц

Особливості:

Підтримання PoE

Підтримка MIMO

Тип антен: Вбудовані

Кількість антен: 1

Швидкість Wi–Fi: 1300 Мбіт/с

Мережевий концентратор(некерований світч) TP–LINK LS1008G

На рисунку 2.13 зображено некерований світч TP–LINK LS1008G

Рисунок 2.13 – Некерований світч TP–LINK LS1008G [12]

Характеристика:

Кількість портів Ethernet: 8 (10/100/1000 Мбит/с)

Стандарти та протоколи: IEEE 802.3i/802.3u/802.3ab/802.3x

Максимальне енергоспоживання: 3.9 Вт

Тепловиділення: 13.299 БТЕ/год

Комутаційна здатність: 16 Гбіт/сек

Швидкість передавання пакетів: 11.9 мільйона пакетів у секунду

Таблиця MAC адрес: 4K

Буфер пам'яті пакетів: 1.5 МБ

Кадри Jumbo: 16 КБ

Метод передавання: Store and Forward (Зберігання та передавання)

2.6 Захист мережі. Технологія OpenVPN

Технологія OpenVPN є однією з найпопулярніших і найбільш широко використовуваних відкритих VPN (Virtual Private Network) рішень. OpenVPN є безкоштовним, відкритим програмним забезпеченням, яке забезпечує

безпечний тунелевий зв'язок між двома вузлами мережі через ненадійну мережу, таку як Інтернет.

Технологія OpenVPN базується на протоколі SSL/TLS (Secure Sockets Layer/Transport Layer Security), що гарантує високий рівень безпеки та шифрування передачі даних. Вона підтримує різні алгоритми шифрування, включаючи AES (Advanced Encryption Standard) і Blowfish, що забезпечують конфіденційність і цілісність даних під час їх передачі.

OpenVPN працює в режимі клієнт–сервер. Сервер OpenVPN встановлюється на центральній точці мережі, тоді як клієнтські програми встановлюються на кожному клієнтському пристрої, який підключається до мережі. Клієнти можуть бути встановлені на різних платформах, включаючи Windows, macOS, Linux, Android та iOS.

OpenVPN дозволяє налаштовувати різні параметри зв'язку, включаючи IP–адреси, порти, протоколи та маршрутизацію. Він також підтримує автентифікацію користувачів за допомогою сертифікатів, логінів/паролів або токенів, що забезпечує високий рівень безпеки доступу до мережі.

Однією з переваг OpenVPN є його здатність працювати за NAT–проксі або брандмауерами, що робить його універсальним і підходящим для використання в різних мережевих середовищах.

Узагальнюючи, технологія OpenVPN забезпечує надійний та безпечний механізм створення віртуальної приватної мережі через ненадійний канал зв'язку, такий як Інтернет. Вона дозволяє забезпечити захищений доступ до ресурсів мережі, незалежно від фізичного розташування користувача.

Деякі з основних переваг технології OpenVPN включають:

Безпека – OpenVPN забезпечує високий рівень безпеки шляхом застосування шифрування даних, аутентифікації та обміну сертифікатами. Це дозволяє забезпечити конфіденційність, цілісність і доступність даних під час їх передачі по мережі.

Гнучкість – OpenVPN підтримує різні типи мережевих протоколів, включаючи TCP і UDP. Вона також дозволяє налаштувати різні параметри

зв'язку, такі як розмір пакетів, шифрування і алгоритми хешування.

Кросплатформеність – OpenVPN підтримується на різних операційних системах, включаючи Windows, macOS, Linux, Android та iOS. Це дозволяє використовувати OpenVPN на різних пристроях і забезпечує сумісність з різними платформами.

Простота налаштування – OpenVPN має простий у використанні і налаштуванні інтерфейс. Існують графічні інтерфейси користувача та консольні інтерфейси командного рядка, які допомагають у налаштуванні та управлінні VPN–з'єднаннями.

Отже, для того щоб користувачі на підприємстві мали змогу працювати в центральній базі використовується технологія OpenVPN. Також щоб користувачі могли працювати віддалено викороистовуєм дану технологію.

РОЗДІЛ 3
ПРАКТИЧНА РОЗРОБКА МЕРЕЖІ

3.1 Побудова схеми мережі підприємства у Cisco Packet Tracer

Для практичної побудови мережі використовуєм програму Cisco Packet Tracer. Ця програма дозволяє віртуально розробити та налаштувати мережу, але єдиний недолік даної програми що моделювання мережі відбувається виключно на обладнані від Cisco. На рисунку 3.1 зображена практично побудована схема мережі у Cisco Packet Tracer.

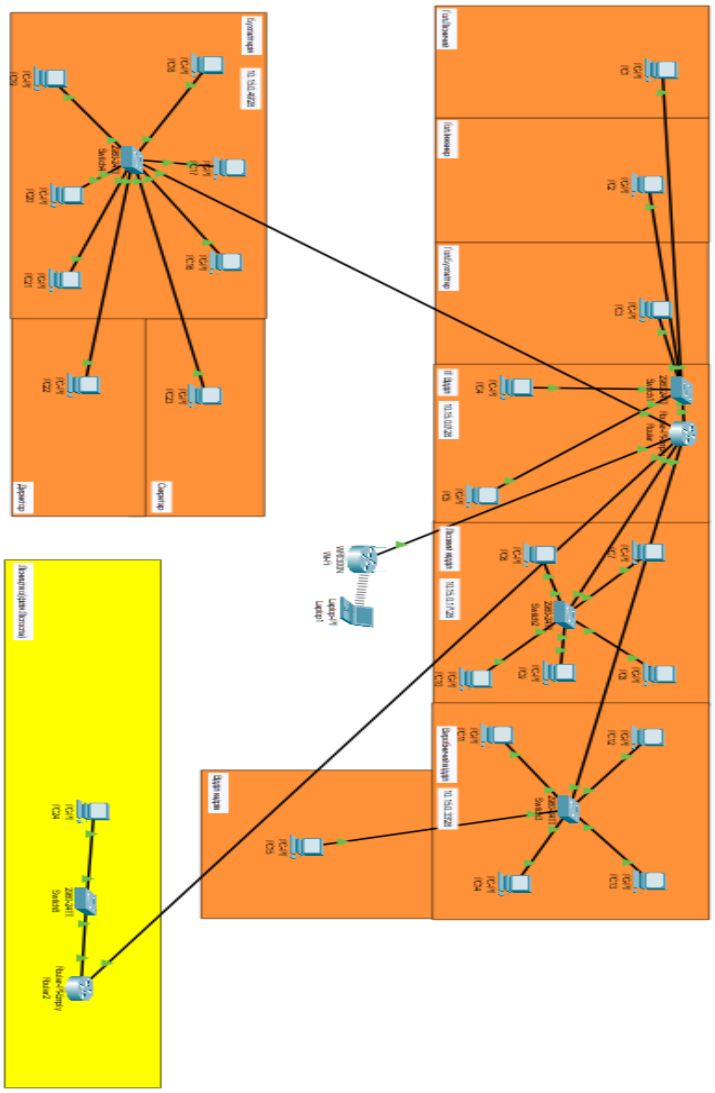

Рисунок 3.1 – Практично реалізована схема

Все наше підприємство розбите на 6 підмереж. Серед них знаходиться 4 підмережі з робочою адресацією. Одна підмережа з адресацією 192.168.0.1 це є гостьова адресація до неї будуть підключенні точки доступу(для наглядності в практичній реалізованій схемі розміщено 1 точку доступу в даній адресації). І ще одна підмережа виділенна для підключення 2 роутерів, один з яких знаходиться на лісгоспі а другий знаходиться на лісництві, що є філією даного лісгоспу. Таким чином у першій під мережі у нас знаходиться 4 кабінета: кабінет головного лісничого, головного інженера, головного бухгалтера та IT відділ, відповідно кожна кімната має свою підмережу.

Таблиця адресації даної підмережі подана нижче у таблиці 3.1

Таблиця 3.1 – Розподіл IP у 1 кімнаті

Підмережа 1	
IP–адреса мережі:	10.15.0.1
IP–адреса шлюза:	10.15.0.1
IP–адреса комутатора	10.15.0.2
IP–адреси вузлів	10.15.0.3–10.15.0.17

У другій підмережі знаходиться кабінет лісового відділу таблиця адресації подана ниже у таблиці 3.2

Таблиця 3.2 – Розподіл IP у 2 кімнаті

Підмережа 2	
IP–адреса мережі:	10.15.0.17
IP–адреса шлюза:	10.15.0.1
IP–адреса комутатора	10.15.0.18
IP–адреси вузлів	10.15.0.17–33

У третій підмережі знаходиться кабінет виробничого відділу та відділу

кадрів. Таблиця адресації подана ниже у таблиці 3.3.

Таблиця 3.3 – Розподіл IP у 3 кімнаті

Кімната 3	
IP–адреса мережі:	10.15.0.33
IP–адреса шлюза:	10.15.0.1
IP–адреса комутатора	10.15.0.34
IP–адреси вузлів	10.15.0.33–10.15.0.49

У таблиці 3.4 показано розподіл IP у 4 кімнаті.

Таблиця 3.4 – Розподіл IP у 4 кімнаті

Кімната 4	
IP–адреса мережі:	10.15.0.49
IP–адреса шлюза:	10.15.0.1
IP–адреса комутатора	10.15.0.50
IP–адреси вузлів	10.15.0.49–10.15.0.65

На точці доступу налаштовано DHCP Server. Налаштування показані нижче на рисунку 3.2. Тобто у нас на підприємстві є 2 загальні підмережі робоча та гостьова.

Рисунок 3.2 – DHCP Server

На рисунку 3.3 показано працюючий DHCP Server, для тесту було

підключенно ноутбук до точки доступу та перевіренно коректність виданої IP адреси.

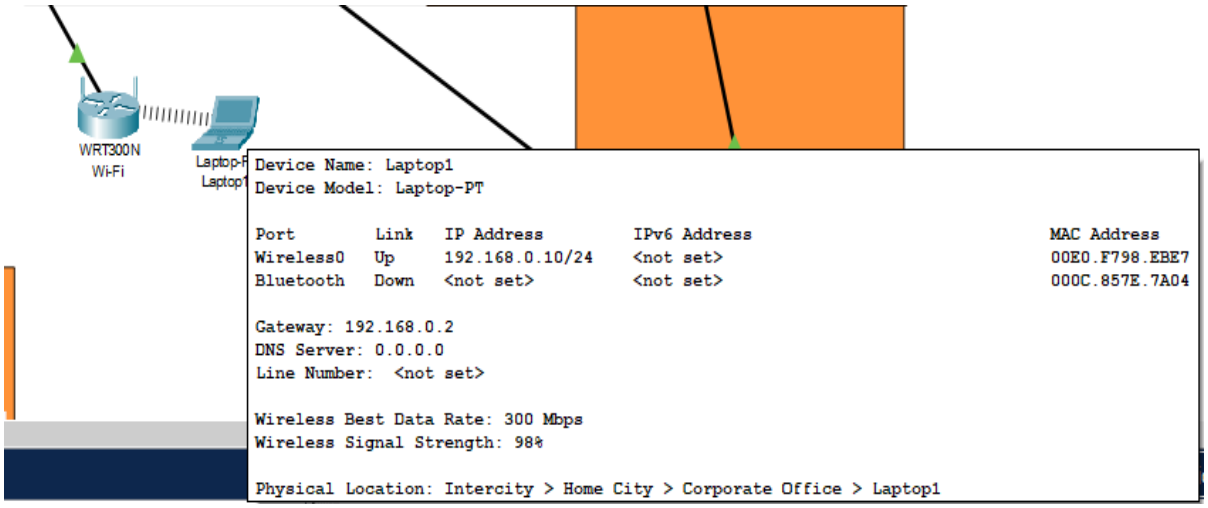

Рисунок 3.3 – Підключення ноутбука о точки доступу

На рисунку 3.4 показано що дана схема працює коректно і комп'ютери між собою у локальній мережі і комп'ютери між лісгоспом та філією можуть передавати інформацію.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC1	PC4	ICMP		0.000	N	0
	Successful	PC3	PC6	ICMP		0.000	N	1
	Successful	PC10	PC11	ICMP		0.000	N	2
	Successful	PC15	PC24	ICMP		0.000	N	3

Рисунок 3.4 – Отримання пакетів між комп'ютерами в різних підмережах

На рисунку 3.5 зображено приклад виконання команди ip ospf neighbor яка показує коректно налаштований ospf на головному роутері підприємства.

```
Router#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/DR         00:00:37    201.20.17.2     GigabitEthernet9/0
```

Рисунок 3.5 – Налаштований ospf на роутері підприємства

На рисунку 3.6 зображено приклад виконання команди ip ospf neighbor яка показує коректно налаштований ospf на роутері філії.

```
Router2#show ip ospf neighbor


Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/BDR        00:00:37    201.20.17.1     GigabitEthernet6/0
```

Рисунок 3.6 – Налаштований ospf на роутері філії

На рисунку 3.7 показано усі підмережі на які розбите підприємство.

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/28 is subnetted, 5 subnets
O       10.0.0.0 [110/2] via 201.20.17.2, 00:37:07, GigabitEthernet9/0
C       10.15.0.0 is directly connected, GigabitEthernet0/0
C       10.15.0.16 is directly connected, GigabitEthernet3/0
C       10.15.0.32 is directly connected, GigabitEthernet4/0
C       10.15.0.96 is directly connected, GigabitEthernet8/0
C    192.168.0.0/24 is directly connected, GigabitEthernet1/0
C    201.20.17.0/24 is directly connected, GigabitEthernet9/0
```

Рисунок 3.7 – show ip route

На рисунку 3.8 продемонстрована команда show flash.

```
Router#show flash

System flash directory:
File  Length   Name/status
  3   5571584  pt1000-i-mz.122-28.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[5827403 bytes used, 58188981 available, 64016384 total]
63488K bytes of processor board System flash (Read/Write)
```

Рисунок 3.8 – show flash

На рисунку 3.9 продемонстрована команда show protocols.

```
Router#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 10.15.0.1/28
GigabitEthernet1/0 is up, line protocol is up
  Internet address is 192.168.0.1/24
GigabitEthernet3/0 is up, line protocol is up
  Internet address is 10.15.0.17/28
GigabitEthernet4/0 is up, line protocol is up
  Internet address is 10.15.0.33/28
GigabitEthernet8/0 is up, line protocol is up
  Internet address is 10.15.0.97/28
GigabitEthernet9/0 is up, line protocol is up
  Internet address is 201.20.17.1/24
```

Рисунок 3.9 – show protocols

3.2 Розрахунок довжини кабелю

Підприємство складається з 1 поверха. Уся комп’ютерна техніка знаходиться на одному поверху, що значно спрощує прокладання кабелю. Вона розміщена у 10 кімнатах в 1 знаходиться 5 комп’ютерів, ще одній кімнаті розміщено 6 комп’ютерів. Та ще в 6 кімнатах по 1 комп'ютеру.При розрахунку кількості кабелю в середньому 6 метрів кабелю якщо враховувати її прокладання від комутатора до робочого місця через напольні плінтуси, але також для 1 комп'ютера потрібно 10 метрів, ще для 2 кімнат по 8 метрів та для ще 3 кімнат 8, 12, 15 метрів. Отже для прокладання по кабінетах потрібно (5*6)=30, (6*6)= 36, 30+36+10+16+35=127 метрів

Від комутатора до світчів для кожної кімнати іде різний метраж кабелю. Для 1 кімнати–2м. для 2 кімнати– 8м, для 3– 12м, для 4 кімнати– 20м. Також для підключення точок доступу потрібно 15 метрів та 20 мертрів. Отже для усього підприємства знадобиться 127+42=169 метрів кабелю.

3.3 Розрахунок електричних характеристик

Згідно плану мережі підприємства визначили які мережеві та переферійні пристрої використовуються та розраховуєм потужність мережі підприємства

Отже на підприємстві знаходиться 24 комп’ютера кожен з яких споживає 400 Вт, в сумі це дає 9 600 Вт. Також в мене в мережі є 4 комутатора TP–Link TL–SF1008D кожен споживає по 2.05 Вт. Маршутизатор MikroTik RB3011UiAS–RM споживає 30 Вт. І 3 точки доступу Ubiquiti UniFi AP AC Pro кожна з яких споживає 9 Вт. У таблиці 3.5 показана кількість споживання 1 одиницею техніки та загальне споживання кожної групи техніки.

Таблиця 3.5 – Споживання електрики пристроями

Техніка	Споживання 1 одиниці техніки, Вт	Загалом споживання,Вт
Комп'ютери		
24	400	9 600
Комутатори		
4	2.05	8.2
Маршутизатори		
1	30	30

3.4 Розрахунок затрат

Отже склавши план будівлі та схему мережі на підприємстві потрібно розрахувати собі вартість усього потрібного обладнання та матеріалів

Кабель Одескабель КПВ–ВП (100) 4х2х0.49 мм² (U/UTP–cat.5E) 305 м – 4 375 грн

Монтажний комплект(дюбеля, ізолента, стяжки і тд) 3000 грн

Ubiquiti UniFi AP AC Pro 6 269 грн(ціна за 1 шт) нам потрібно 3 шт 18 807 грн

TP–LINK LS1008G 899 грн (ціна за 1 шт) нам потрібно 4 шт 3 596 грн

Маршрутизатор MikroTik RB3011UiAS–RM 6 649 грн

Підсумувавши загалом на даний проектнам потрібно 36 427 грн

3.5 Використання OpenVPN

Оскільки головний сервер для звітності усіх лісгоспів знаходиться відаленно для підключення до серверу використовується технологія OpenVPN. Дана технологія реалізовується тим що або на роутер чи на користувацький комп’ютер встановлюється програма OpenVPN та імпортуються конфігураційний файл з розширенням .ovpn, та сертифікат з розширенням .p12. Але для зручності на лісгоспах генерується загальний сертифікат на головний роутер. Для віддаленої роботи з дому для користувачів генерується особистий сертифікат. Приклад генерування сертефікату на впн сервері

cd /etc/openvpn/_____/easy–rsa/ //переходимо в папку з easy rsa

./easyrsa build–client–full CERTIFICATE_NAME // CERTIFICATE_NAME прописуємо прізвище та ініціали користувача

./easyrsa export–p12 CERTIFICATE_NAME // після генеруємо рандомний пароль та вводимо пароль до CERTIFICATE_NAME.key потім пароль на CERTIFICATE_NAME.p12 (він буде вводитись для експорту в сховище) за стандартом такий самий пароль як на CERTIFICATE_NAME.key

cd pki/private/ // переходимо в директорію з сертифікатами

cp CERTIFICATE_NAME.p12 /home/YOUR_USER_NAME/ //копіюємо сертифікат в папку свого користувача

rm CERTIFICATE_NAME.key // видаляємо ключ

cd /etc/openvpn/_____/ccd //відкриваємо директорію з конфігурацією користувачів ovpn

echo "ifconfig–push IP_ADDRESS 255.255.255.0" > CERTIFICATE_NAME // прописуємо ip адресу

chown –R YOUR_USER_NAME /home/YOUR_USER_NAME // надаємо доступ серверному користувачу

cp /etc/openvpn/_____/clientconf/windows/*.opvn /home/YOUR_USER // копіюємо файл конфігурації для підключення.

3.6 Використання системи моніторингу Zabbix

Zabbix є відкритою системою моніторингу мережі та управління віддаленими пристроями. Вона надає широкі можливості для відстеження та аналізу стану різних компонентів мережі, таких як сервери, маршрутизатори, комутатори, додаткове обладнання та програмне забезпечення.

Zabbix працює на основі клієнт–серверної архітектури, де серверний компонент відповідає за збір, обробку та аналіз отриманих даних, а клієнтські компоненти (агенти) встановлюються на кожному моніторинговому об'єкті та надсилають інформацію про його стан до сервера. За допомогою Zabbix можна відслідковувати показники продуктивності, доступність, використання ресурсів, а також реагувати на незвичайні або критичні події.

Сервер Zabbix надає широкий спектр функцій, таких як налаштування моніторингу, автоматичне виявлення пристроїв, створення графіків та звітів, сповіщення про події через електронну пошту або SMS, управління конфігураціями та інші. Крім того, Zabbix має веб–інтерфейс, який надає зручну панель керування для налаштування та відстеження моніторингу.

За допомогою Zabbix можна стежити за різними аспектами мережі, включаючи параметри роботи серверів, баз даних, мережевих пристроїв, сервісів та додатків. Вона дозволяє виявляти проблеми, забезпечувати швидку реакцію на них, а також проводити аналіз продуктивності та планування майбутнього розвитку мережі.

Zabbix є потужним інструментом для моніторингу корпоративних мереж.

Отже на нашому підприємстві та взагалом на усіх філіях буде налаштована дана система моніторингу. У ній буде налаштовано моніторинг для наступних речей:

- доступність мережевого обладнання;
- перепідключення та наявне підключення різних інтернет провайдерів;
- доступність локальних серверів підприємств та загального серверу для усіх підприємст;

– обсяг використаної оперативної пам’яті на серверах;
– контороль роботи служб на сервері та комп’ютерах;

ВИСНОВОК

У кваліфікаційній роботі було розроблено корпоративну мережу для підприємства з лісозаготівлі «Лісгосп».

Поставлену мету роботи повністю досягнуто, у процесі розробки вирішено такі задачі:

Оглянуто технологічні рішення для розробки корпоративної мережі, виявлено широкий спектр технологічних рішень для побудови корпоративної мережі. Ці рішення включають різноманітні протоколи, технології та методи, що дозволяють забезпечити ефективну та безпечну роботу мережі.

Провели аналіз потреб підприємства в інформаційних технологіях та визначення функціональних вимог до мережі. Шляхом аналізу потреб підприємства в інформаційних технологіях встановлені конкретні функціональні вимоги до мережі. Ці вимоги послужили основою для розробки архітектури мережі, що відповідає цілям підприємства та забезпечує ефективність його діяльності.

Здійснено розробку архітектури корпоративної мережі з використанням відповідних технологічних рішень. На основі проведених досліджень та аналізу була розроблена архітектура корпоративної мережі, використовуючи відповідні технологічні рішення. Ця архітектура відповідає потребам підприємства та забезпечує оптимальну структуру мережі.

Здійснили вибір та конфігурування необхідного обладнання для мережі. Проведений вибір та конфігурування необхідного мережевого обладнання з урахуванням встановлених вимог та архітектури мережі дозволяє забезпечити належну функціональність та ефективність роботи мережі.

Налагодили та відтестували мережу для перевірки її працездатності та відповідності вимогам. Цей етап допомагає виявити та виправити можливі проблеми та забезпечує належну роботу мережі.

Розробили стратегію захисту інформації в мережі що дозволяє забезпечити конфіденційність, цілісність та доступність даних. Застосування

відповідних захисних заходів допомагає уникнути можливих загроз безпеці мережі та інформації.

Отже, виконані завдання дозволили розробити оптимальну архітектуру корпоративної мережі, вибрати відповідне обладнання, налагодити та протестувати мережу, а також розробити стратегію захисту інформації. Результати цієї роботи можуть бути використані для покращення ефективності, безпеки та стабільності роботи підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Топології та її види URL:https://studopedia.com.ua/1_4351_zagalna–shina.html (дата звернення: 15.11.2022)

2.Загальна шина URL:https://jak.koshachek.com/articles/zagalna–shina–studopedija.html. (дата зверненуя: 25.02.2023)

3.Топології дерев плюси і мінуси URL:https://4apple.org/topologija–derevo–pljusy–i–minusy/ (дата звернення: 25.02.2023)

4.Організація комп'ютерних мереж URL:https://kremenetskyy.blogspot.com/2017/10/blog–post.html (дата звернення: 15.03.2023)

5.Введення в мережеві кабелі та типи мережевих кабелів – 2022 URL:https://uk.go–travels.com/15104–introduction–to–network–cables–817868–3058944 (дата звернення: 12.12.2022)

6.Типи мережевого кабелю та його функції, які вам потрібно знати URL:https://altitudetvm.com/uk/networking/1993–jenis–jenis–kabel–jaringan–beserta–fungsinya–yang–perlu–anda–ketahui.html (дата звернення: 19.03.2023)

7.Вита пара URL:https://cabel.com.ua/articles/twister–pair/ (дата звернення: 20.03.2023)

8.Комп'ютерні мережі. Апаратне і програмне забезпечення комп'ютерних мереж URL:https://ukrreferat.com/chapters/komputerny–nauki/kompyuterni–merezhi–aparatne–i–programne–zabezpechennya–kompyuternih–merezh–referat.html (дата звернення: 17.04.2023)

9.Мережеве обладнання URL:https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B5_%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F (дата звернення: 20.04.2023)

10.Маршрутизатор MikroTik RB3011UiASRM URL:https://rozetka.com.ua/ua/mikrotik_rb3011uias_rm/p24593114/ (дата звернення: 25.04.2023)

11.Маршрутизатор інтернет WiFi4 MikroTik hAP RB951Ui–2ND URL:https://comfy.ua/ua/marshrutizator–ethernet–mikrotik–hap–rb951ui–

2nd.html (дата звернення: 27.04.2023)

12.Комутатор TL–SF1008D URL:https://www.tp–link.com/ru/business–networking/unmanaged–switch/tl–sf1008d/#overview (дата звернення: 27.04.2023)

13.Subnet Masks Reference Table URL:https://www.cloudaccess.net/cloud–control–panel–ccp/157–dns–management/322–subnet–masks–reference–table.html (дата звернення: 28.04.2023)

14.Курс комп’ютерні мережі Cisco URL:https://lms.netacad.com/course/view.php?id=1005944 (дата звернення: 29.04.2023)

15.Курс «Комп’ютерні мережі» URL:https://www.youtube.com/playlist?list=PLtPJ9lKvJ4oiNMvYbOzCmWy6cRzYAh9B1 (дата звернення: 29.04.2023)