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 для ЗОШ с.Катеринівка Кременецького району Тернопільської області**

Виконав: студентка IV курсу, групи СНз-41
спеціальності 122 Комп'ютерні науки
(шифр і назва спеціальності)

_____ Вербицька В.О.
(підпис) (прізвище та ініціали)

Керівник _____ Марценко С.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ _____
(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)
«12» травня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

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

Студенту Вербицькій Валерії Олегівні
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка локальної комп'ютерної мережі для ЗОШ с.Катеринівка Кременецького району Тернопільської області

Керівник роботи Марценко Сергій Володимирович, к.т.н., доц., доцент кафедри КН
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «07» 05 2025 року № 4/7-449

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Технічне завдання на розробку мережі для ЗОШ с.Катеринівка Кременецького району Тернопільської області

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1.Аналіз предметної області. 2. Створення проекту локальної комп'ютерної мережі для школи с.Катеринівка 3. Налаштування та тестування змодельованої мережі школи с. Катеринівка 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. Організація LAN школи 4. Управління мережею школи 5. Фізична топологія мережі 6. Схема мережі школи 7. Вибір комутатора 8. Вибір маршрутизатора 9. Логічна топологія 10. Модель мережі школи 11. Налаштування статичних параметрів на ПК 12. Налаштування комутатора 13. Налаштування DHCP. 14. Налаштування маршрутизатора Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці			

7. Дата видачі завдання 07 травня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	07.05.2025	*Виконано*
2.	Підбір наукових джерел щодо розробки проекту	08.05.2025-15.05.2025	*Виконано*
	мережі школи с.Катеринівка		
3.	Переклад та опрацювання джерел щодо розробки	16.05.2025-18.05.2025	*Виконано*
	мережі школи с.Катеринівка		
4.	Виконання дослідження щодо розробки проекту	19.05.2025-22.05.2025	*Виконано*
	мережі школи с.Катеринівка		
5.	Оформлення розділу «Аналіз предметної області»	23.05.2025-01.06.2025	*Виконано*
6.	Оформлення розділу «Створення проекту локальної комп'ютерної мережі для школи с.Катеринівка»	23.05.2025-01.06.2025	*Виконано*
7.	Оформлення розділу «Налаштування та тестування змодельованої мережі школи с.Катеринівка»	23.05.2025-01.06.2025	*Виконано*
8.	Виконання завдання до підрозділу «Безпека життєдіяльності»	02.06.2025-05.06.2025	*Виконано*
9.	Виконання завдання до підрозділу «Основи охорони	02.06.2025-05.06.2025	*Виконано*
	праці»		
10.	Оформлення кваліфікаційної роботи	06.06.2025-10.06.2025	*Виконано*
11.	Нормоконтроль	11.06.2025-13.06.2025	*Виконано*
12.	Перевірка на плагіат	15.06.2025	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.06.2025	*Виконано*
14.	Захист кваліфікаційної роботи	19.06.2025	

Студент _____ Вербицька В.О.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценко С.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка локальної комп’ютерної мережі для ЗОШ с.Катеринівка Кременецького району Тернопільської області// Кваліфікаційна робота освітнього рівня «Бакалавр» // Вербицька Валерія Олегівна // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно–інформаційних систем і програмної інженерії, кафедра комп’ютерних наук, група СНз–41 // Тернопіль, 2025 // С. 66, рис. – 22, табл. – 2, кресл. – , додат. – , бібліогр. – 38.

Ключові слова: локальна комп’ютерна мережа школи, логічна топологія мережі, комутатор, маршрутизатор, точка доступу.

У роботі здійснено проектування локальної комп’ютерної мережі для ЗОШ с.Катеринівка Кременецького району Тернопільської області.

Метою роботи є розроблення проекту локальної комп’ютерної мережі для ЗОШ с.Катеринівка Кременецького району Тернопільської області.

В першому розділі кваліфікаційної роботи проведено аналіз призначення та основних компонентів локальної комп’ютерної мережі школи с.Катеринівка.

У другому розділі кваліфікаційної роботи проведено формування етапів проектування локальної комп’ютерної мережі школи с.Катеринівка, що дало змогу визначити її потреби та розробити архітектуру для успішного функціонування.

Третій розділ кваліфікаційної роботи описує основні етапи моделювання роботи мережі школи с.Катеринівка у середовищі Cisco Packet Tracer. У моделі реалізовано функціонування технології VLAN, здійснено захист основних компонентів мережі від несанкціонованого доступу та описано повний процес налаштування кінцевого обладнання.

ANNOTATION

Development of a Local Computer Network for Katerynivka School, Kremenets District, Ternopil Region // Diploma thesis Bachelor degree // Verbytska Valeriia O. // Ternopil' Ivan Pul'uj National Technical University, Faculty of Computer Information System and Software Engineering, Department of Computer Science // Ternopil', 2025 // P. 66, Tables – 2, Fig. – 22, Diagrams – , Annexes. – , References – 38.

Keywords: local computer network for school, logical network topology, switch, router, access point.

The work involves the design of a local computer network for the secondary school in the village of Katerynivka, Kremenets district, Ternopil region.

The aim of the work is to develop a project for a local computer network for the secondary school in the village of Katerynivka, Kremenets district, Ternopil region.

The first section of the thesis analyzes the purpose and main components of the local computer network of the school in Katerynivka.

The second section of the thesis outlines the stages of designing a local computer network for the school in Katerynivka, which made it possible to determine its needs and develop an architecture for its successful operation.

The third section of the thesis describes the main stages of modeling the operation of the network of the school in the village of Katerynivka in the Cisco Packet Tracer environment. The model implements the functioning of VLAN technology, protects the main components of the network from unauthorized access, and describes the complete process of configuring the end equipment.

ЗМІСТ

ВСТУП

У сучасних навчальних закладах якісна локальна мережа є важливим компонентом ефективної освітньої діяльності. Вона забезпечує доступ до навчальних матеріалів, підтримує адміністративні процеси та дає змогу впроваджувати сучасні цифрові технології в освітній процес.

Проектування локальної мережі школи с.Катеринівка має на меті створення стабільної, безпечної та масштабованої інфраструктури, яка відповідатиме потребам вчителів, учнів та адміністрації. Враховуючи вимоги до продуктивності та безперебійності роботи, мережа буде побудована з використанням сучасного комунікаційного обладнання, відповідно до стандартів безпеки та оптимізації мережевих ресурсів.

Актуальність теми. У цій кваліфікаційній роботі розглядаються ключові аспекти створення локальної мережі школи, зокрема вибір фізичної та логічної топології, налаштування обладнання, забезпечення безпеки та управління трафіком. Основною метою є розробка ефективної мережевої інфраструктури, що сприятиме покращенню навчального процесу та загальної цифрової взаємодії в закладі.

Мета і завдання кваліфікаційної роботи. Метою роботи є здійснити:

– аналіз призначення та основних компонентів локальної комп’ютерної мережі школи с.Катеринівка;

– проаналізувати типи локальних мереж для школи;

– оцінити кращі практики побудови та впровадження LAN у школі;

– здійснити етапи проектування мережі школи;

– провести вибір та проектування фізичної топології мережі школи;

– підібрати обладнання для мережі;

– змоделювати роботу мережі школи.

Практичне значення одержаних результатів. Проведено аналіз призначення та основних компонентів локальної комп'ютерної мережі школи с.Катеринівка. Як наслідок, визначено типи серверів, що можуть обслуговувати потреби школи. Одним з варіантів здешевлення проекту запропоновано використання тонких клієнтів у якості користувацього обладнання. Економію ліцензій можна здійснити через використання серверних версій програмного забезпечення і віддаленого доступу до нього. Проаналізовано типи локальних мереж для школи та наведено кращі практики організації управління мережею. У другому розділі кваліфікаційної роботи проведено формування етапів проектування локальної комп'ютерної мережі школи с.Катеринівка, що дало змогу визначити її потреби та розробити архітектуру для успішного функціонування. Сформовано план впровадження, що допоможе уникнути неочікуваних ситуацій. Запропоновано оцінювати продуктивність мережі за визначеними показниками і враховувати фінансове планування для розвитку та модернізації мережі. Наведено перелік документів, що повинні зберігатись для ефективного та швидкого виявлення та виправлення несправностей у разі їх виникнення. На етапі вибору та проектування фізичної топології запропоновано використовувати з'єднання типу "точка-точка" для підключення провайдера послуг Інтернет і використати розширену зірку для забезпечення з'єднанням користувачів. У процесі планування вибрано місце розташування активних мережевих пристроїв, а також кабелювання і розміщення розеток. Кабельна інфраструктура прокладається у підвісній стелі, використовуючи спеціальні короби та кріплення для забезпечення надійності. Усі кабелі маркуються відповідно до задокументованої схеми кодування, що полегшує пошук і усунення несправностей. В процесі вибору активного мережевого обладнання порівняно комутатори Cisco 1000 серії та Mikrotik CRS326 серії, проаналізувавши їхні ключові характеристики та можливості. Для реалізації

функцій маршрутизації прийнято рішення використовувати Cisco CBS350-16P-2G-EU як частину екосистеми Cisco. На основі аналізу прийнято рішення на користь обладнання Cisco, яке гарантує високу гнучкість, тривалу підтримку та стабільність роботи мережі. Спроектовано логічну схему мережі де запропоновано використати дворівневу модель організації зв'язків. На першому рівні, який буде відігравати роль кореневого буде використано маршрутизатор або комутатор L3 для забезпечення функцій доступу до Інтернету, маршрутизації між VLAN, організації функцій безпеки у якості фаєрволу та виконання NAT трансляції, базової фільтрації трафіку користувачів. На другому будуть комутатори доступу рівня L2. Створення мережі школи с.Катеринівка передбачає розроблення політики поділу на сегменти через використання віртуальних мереж VLAN. Для адміністрації та дирекції буде використано VLAN з номером 100, вчителі будуть у VLAN 200, для учнів VLAN 300, гостьовий доступ організується у VLAN 400, інші ресурси такі як принтери, системи дистанційного навчання та інші сервіси будуть у VLAN 500. Проведено розрахунок відповідних адрес та їх розподіл для відповідних підрозділів. Третій розділ кваліфікаційної роботи описує основні етапи моделювання роботи мережі школи с.Катеринівка у середовищі Cisco Packet Tracer. У моделі реалізовано функціонування технології VLAN, здійснено захист основних компонентів мережі від несанкціонованого доступу та описано повний процес налаштування кінцевого обладнання. При налаштуванні DHCP сервера також виконано додаткове налаштування обладнання для уможливлення роботи єдиного сервісу з різних мереж.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Аналіз призначення та основних компонентів локальної комп'ютерної мережі ЗОШ с. Катеринівка

Локальна мережа школи (Local Area Network (LAN)) з'єднує персональні комп'ютери, принтери та інші комп'ютерні ресурси в межах будівлі або кампусу. Зараз багато шкіл, офісів і будинків мають локальні мережі. Ці мережі дозволяють спільно використовувати принтери, а також документи та проекти. Локальні мережі дозволяють комп'ютерам спілкуватися між собою і використовуються для спільного доступу до Інтернету всіх комп'ютерів у будівлі або школі [1-5].

Більшість локальних мереж використовують дроти або кабелі для підключення комп'ютерів та інших периферійних пристроїв. У більшості мереж мережевий кабель (який зазвичай виглядає як великий телефонний шнур) з'єднує комп'ютер із мережевою розеткою в стіні. Іноді в класах або офісах багато комп'ютерів підключаються до проміжного концентратора або комутатора, а не безпосередньо до мережевої розетки. Концентратор або комутатор, до якого підключені всі комп'ютери, є пристроєм, що підключається до мережевої розетки. В обох випадках мережева розетка підключається до невеликого маршрутизатора за допомогою іншого кабелю. Принтери також часто використовуються спільно за допомогою цього методу концентраторів і комутаторів.

Деякі локальні мережі зараз є бездротовими. Бездротові локальні мережі в основному такі самі, як і дротові, але кабелі замінені невеликими "радіоприймачами", які містяться всередині комп'ютерів. Бездротові локальні мережі зазвичай дещо повільніші за дротові, але їх набагато простіше налаштувати, і вони дозволяють користувачам переміщати свої машини без необхідності перепідключення мережевих кабелів.

Протягом останніх кількох років бездротові локальні мережі стали основним стандартом у школах і класах; проте важливо зазначити, що безпека є набагато складнішою при використанні бездротової мережі. Крім того, впровадження конкуруючих протоколів створює певну плутанину на ринку. Керівництву школи необхідно ретельно підбирати бездротовий протокол, враховуючи можливості модернізації мережі та її сумісність з існуючими бездротовими протоколами.

Якщо локальна мережа може з'єднувати всі комп'ютери в будівлі або на території кампусу, то глобальна мережа (Wide Area Network (WAN)) з'єднує кілька локальних мереж. Зараз багато районів мають глобальні мережі, що з'єднують усі школи в районі для спільного використання доступу до Інтернету, вибраних файлів або інших ресурсів.

Локальні мережі часто включають в себе безліч різних компонентів, наприклад, величезну кількість серверів, комутаторів, маршрутизаторів, брандмауерів тощо. Наведемо опис частини з цих компонентів.

Хоча про сервери часто говорять майже містичним тоном, насправді це просто потужні комп'ютери, на яких працює спеціалізоване програмне забезпечення, призначене для обміну файлами, управління принтерами або виконання будь-яких інших спеціалізованих завдань. Більшість цих комп'ютерів достатньо потужні, щоб виконувати кілька завдань одночасно; наприклад, один мережевий сервер може бути одночасно файловим сервером, сервером друку та поштовим сервером.

Файловий сервер – це, по суті, комп'ютерний еквівалент картотеки. Документи, електронні таблиці та інші (комп'ютерні) файли зберігаються на файловому сервері, так само як паперові документи зберігаються в картотеці. Завдання файлового сервера – зробити ці файли доступними для користувачів комп'ютерів у локальній мережі та, за необхідності, дозволити користувачам оновлювати файли.

Принтерний сервер – це програмне або апаратне забезпечення, яке управляє завданнями на друк, поданими користувачами. Коли документ надсилається на мережевий принтер, сервер друку отримує завдання і ставить його в чергу (ставить у чергу за раніше відправленими завданнями). Коли завдання доходить до початку черги, сервер друку надсилає його на принтер. Не обов'язково купувати окремий принтер для кожного персонального комп'ютера. Користувачі в класах або офісах часто спільно використовують принтери, оскільки зазвичай не всі друкують одночасно. Цей варіант може заощадити школі значну суму грошей.

Третій поширений тип сервера – поштовий сервер. Поштовий сервер виступає в ролі каналу зв;'язку із зовнішнім світом під час надсилання та отримання повідомлень. Деякі сервери налаштовані таким чином, що вся пошта залишається на поштовому сервері, доки користувач її активно не видалить. В інших конфігураціях користувач може переміщати пошту з сервера на настільний комп'ютер. Цей процес називається "завантаженням" і використовує менше місця на поштовому сервері.

Маршрутизатор – це обладнання, яке виконує функцію інтерфейсу між локальною мережею та Інтернетом, маршрутизуючи трафік з однієї мережі в іншу. Маршрутизатор може бути комп'ютером, призначеним для управління трафіком WAN, або програмним забезпеченням, що працює на комп'ютері, який також налаштований для виконання інших завдань. Маршрутизатори також можуть використовуватися в локальних мережах для маршрутизації внутрішнього трафіку.

Важливим компонентом будь-якої мережі є брандмауер. Брандмауер, простими словами, це стіна, яка діє як протипожежний бар'єр – вона запобігає поширенню вогню. У цьому сенсі комп'ютерний брандмауер захищає мережу від хакерів шляхом блокування доступу до всієї мережі або її частини. Управління брандмауерами вимагає значних знань і досвіду. Хоча адміністратор мережі повинен забезпечити, щоб у мережу не

потрапляв небажаний трафік іззовні, необхідно створити такий рівень доступу до Інтернету та з Інтернету, який дозволить авторизованим користувачам безпечно та ефективно виконувати свою роботу.

Надійний, добре розроблений брандмауер є критично важливим для забезпечення доступу до обмеженої мережі тільки авторизованим користувачам. Як і маршрутизатори та сервери, брандмауери доступні у вигляді апаратного або програмного забезпечення. Вибір брандмауера для конкретної мережі – це питання, яке найкраще вирішувати на місцевому рівні після огляду доступних варіантів.

Прогрес у сфері технологій призвів до зникнення різниці між настільним комп'ютером і мережевим сервером. Обчислювальна потужність продовжує зростати в геометричній прогресії – насправді більшість користувачів не потребують усієї доступної їм обчислювальної потужності (принаймні на даний момент). Те саме стосується мережевих серверів, які стали настільки потужними, що деякі адміністратори мереж запускають додатки, окрім серверного програмного забезпечення, з мережевого сервера, а не встановлюють додатки безпосередньо на кожен комп’ютер, підключений до мережі. Сьогодні сервери здатні обробляти набагато більший обсяг роботи, ніж у минулі роки.

Запуск програм з сервера має ряд переваг. Однією з ключових переваг є ліцензування, оскільки набагато простіше відстежувати використання. Інша перевага полягає в тому, що місцеві користувачі не можуть змінювати конфігурацію програм, що може призвести до збою програмного забезпечення та створити проблеми для інших користувачів. Крім того, набагато простіше оновлювати програмне забезпечення, оскільки потрібно оновлювати лише одну копію, а не кожну копію на кожному персональному комп’ютері. Однак програми, що запускаються з мережевого сервера, часто працюють порівняно повільніше, ніж програми, що запускаються безпосередньо на настільному комп’ютері.

Ще однією перевагою додатків, що працюють на сервері, є економія коштів завдяки використанню тонких клієнтів. Тонкі клієнти – це прості, недорогі комп'ютери, які не мають достатньої потужності для запуску складних програмних додатків, але мають достатню потужність для доступу до додатків, встановлених на сервері. Придбавши одну копію додатка, який може працювати в мережі, з ліцензіями для декількох користувачів, організація може заощадити на вартості декількох копій програмного забезпечення і придбати менш потужні комп'ютери за значно нижчою ціною. Приклад організації LAN школи подано на рисунку 1.1.

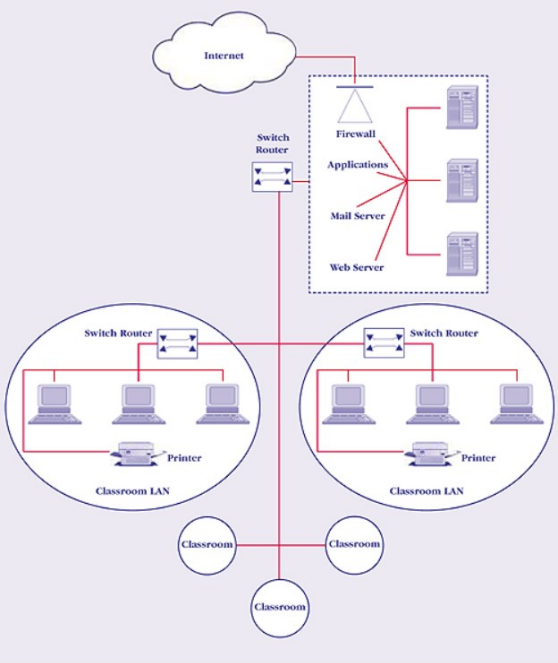

Рисунок 1.1 – Організація LAN школи

Крім того, завдяки впровадженню середовища тонких клієнтів старі комп'ютери в школах мають довший термін експлуатації. В останні роки все більше локальних мереж використовують тонкі клієнти для різних цілей. Крім того, все більше комп'ютерних програм пишуться з урахуванням можливостей веб-мережі для віддаленого запуску. Настільний комп'ютер користувача по суті діє як "нерозумний" термінал, просто відображаючи веб-сторінки, що транслюються сервером. Обчислення

фактично відбуваються на інтернет-сервері, а користувачі передають свої команди через веб-сторінку. Ця веб-модель працює найкраще, коли користувачі мають високошвидкісні інтернет-з'єднання.

Сьогодні обчислення відбуваються як на настільних комп'ютерах, так і на мережевих серверах та інтернет-серверах. У багатьох випадках відмінності між різними типами комп'ютерів і серверів стають все менш важливими. Зі збільшенням швидкості комп'ютерів і мережевої передачі даних ці відмінності стануть ще важче зрозуміти. Зростаюча складність обчислень і мереж підсилює необхідність для шкіл використовувати послуги кваліфікованого адміністратора мережі.

1.2 Типи локальних мереж, що можуть використовуватись у школі

Локальні мережі можна класифікувати за типом підключених пристроїв, архітектурою та використовуваним носієм. Існує також новий ринок LAN, який виник у епоху хмарних технологій. На рисунку 1.2 показано типи локальних мереж.

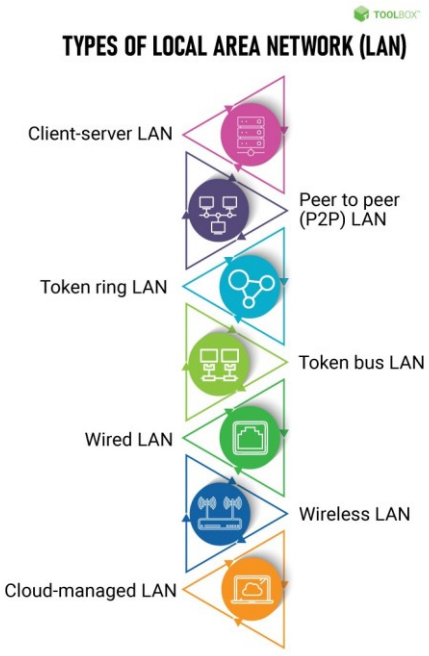

Рисунок 1.2 – Типи локальних мереж

У клієнт-серверному середовищі локальної мережі один сервер підключається до декількох пристроїв, які називаються клієнтами. Клієнтські пристрої не можуть взаємодіяти між собою, а централізована машина обробляє такі дії, як управління мережевим трафіком, контроль доступу до мережі тощо. Цей тип локальної мережі може бути швидшим у невеликих периметрах, але у великих периметрах він створює занадто велике навантаження на центральний сервер.

У P2P-LAN немає централізованого сервера, і всі підключені пристрої мають доступ один до одного, незалежно від того, чи є вони серверами чи клієнтами. Перевага P2P-LAN полягає в тому, що пристрої можуть вільно обмінюватися даними між собою, що спрощує потокову передачу медіа, надсилання файлів та виконання подібних операцій з обміну даними. Недоліком є те, що вони, як правило, менш потужні, ніж клієнт-серверні LAN.

Залежно від архітектури, локальні мережі можна класифікувати на мережі типу “токен-ринг” або “токен-шину”. У першому випадку всі пристрої підключаються до мережі у вигляді кільця. Кожному підключеному пристрою присвоюється токен відповідно до його вимог. Ця технологія була впроваджена компанією IBM у 1984 році для використання в корпоративних середовищах, коли технологія Ethernet ще перебувала на початковій стадії розвитку.

У токен-шині LAN підключені вузли розташовані у вигляді деревоподібної топології, а токени передаються вліво або вправо. Зазвичай вона забезпечує кращу пропускну здатність, ніж середовище токен-кільця LAN.

Провідна локальна мережа, ймовірно, є найпоширенішим типом локальної мережі, що використовується сьогодні. Вона використовує електронні хвилі для передачі даних по оптичному волокну (або кабельних варіантах) замість токенів. Провідна локальна мережа є надзвичайно

надійною і може бути дуже швидкою, залежно від продуктивності центрального сервера. Однак вона може перешкоджати мобільності та гнучкості, особливо в середовищах, де немає фіксованої кількості пристроїв.

Бездротова локальна мережа зазвичай використовується в домашніх умовах для підключення комп'ютерних пристроїв, носимих пристроїв, розумних побутових приладів тощо, але існує також величезний корпоративний ринок бездротових локальних мереж, який, за даними IDC, щорічно зростає на 10,3%. Цей тип локальної мережі використовує радіочастоти для передачі даних, що може зробити її вразливою до ризиків безпеки. Вона також споживає багато енергії і може демонструвати нестабільну продуктивність залежно від місця розташування бездротового пристрою.

Хмарна локальна мережа – це особливий тип бездротової локальної мережі, в якій централізована хмарна платформа використовується для управління мережевим забезпеченням, впровадженням політик, контролем доступу та іншими аспектами продуктивності та безпеки мережі. У гетерогенному мережевому середовищі хмарна локальна мережа оптимізує управління, що робить її ідеальною для використання в підприємствах. За даними дослідження Market Research Future, до 2025 року глобальний обсяг ринку хмарних локальних мереж перевищить 1,18 млрд доларів.

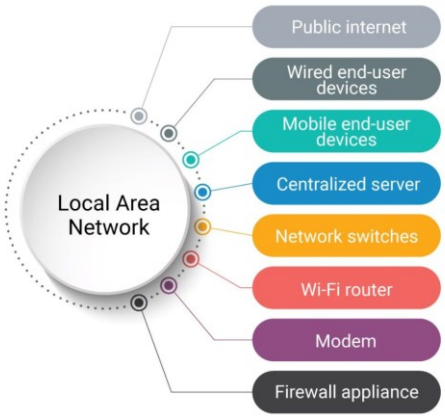

Рисунок 1.3 – Ключові компоненти мережі школи

Публічний Інтернет – це те, до чого здійснюється доступ через локальну мережу. Зазвичай централізований сервер отримує пакети даних з публічного Інтернету та запити на доступ від клієнтських пристроїв. Потім він обробляє ці запити, забезпечуючи передачу даних до різних підключених вузлів через дротовий або бездротовий канал. Технічно локальна мережа може існувати без доступу до публічного Інтернету – наприклад, для обміну приватними даними або використання приватного інтранету. Однак доступ до Інтернету є однією з головних причин впровадження локальних мереж.

У середньому середовищі локальної мережі будуть використовуватися як дротові, так і бездротові пристрої. Пристрої кінцевих користувачів є ноутбуки, настільні комп'ютери, смарт-телевізори, смарт-монітори, обладнання для спільної роботи, системи для конференц-залів тощо. Ці пристрої мають порт Ethernet, через який можна підключити локальну мережу безпосередньо до самого пристрою. Провідні пристрої кінцевих користувачів зазвичай мають високошвидкісний доступ до Інтернету, високоякісну передачу медіа та швидку обробку даних.

Мобільні пристрої кінцевих користувачів – це пристрої, які підключаються за допомогою Wi-Fi, а не кабелю Ethernet. Один і той самий пристрій може виконувати функції як дротового, так і мобільного пристрою. Наприклад, можна підключити ноутбук до локальної мережі за допомогою порту Ethernet на пристрої або через Wi-Fi, залежно від того, де знаходиться пристрій і яка продуктивність вам потрібна. До цієї категорії належать носимі пристрої, розумні побутові прилади, компоненти розумних будівель, ноутбуки, смартфони та захищені портативні пристрої.

Централізований сервер є, мабуть, найважливішим компонентом у середовищі локальної мережі, особливо для корпоративних рішень. Компанії можуть придбати або орендувати сервери у таких постачальників, як IBM, Cisco, HPE тощо. Можна отримати сервери для локальної мережі у

місцевого оператора телекомунікаційних послуг. Або можна підключити всі свої пристрої до одного або декількох модемів, які, в свою чергу, підключені до сервера, розташованого в іншому місці. Зазвичай це стосується споживчих додатків, оскільки в цьому випадку не виникає витрат на розміщення та обслуговування сервера. З іншого боку, підприємства, що мають локальні сервери, розташовані на своїй території, користуються більш високою швидкістю та більшою пропускною здатністю.

Мережевий комутатор є важливим компонентом локальної мережі. Він регулює розподіл пакетів даних і мережевих ресурсів між пристроями, підключеними до централізованого сервера. До багатопортового мережевого комутатора можна підключити кілька кабелів Ethernet. Комутатор забезпечує дотримання мережевих політик, оптимізуючи продуктивність для кожного підключеного кінцевого пристрою. Для локальної мережі можна розглянути два типи комутаторів: керовані та некеровані. Керовані комутатори надають більше можливостей для управління, але некеровані комутатори можуть бути дешевшими та простішими в обслуговуванні.

Wi-Fi-маршрутизатор зараз є основним компонентом локальних мереж, оскільки без нього неможливо реалізувати бездротову локальну мережу. Маршрутизатор підключається до модему, щоб отримувати мережеві сигнали, і перетворює їх на бездротові сигнали, які можуть обробляти мобільні пристрої кінцевих користувачів. В останні роки поширеною практикою є об’єднання Wi-Fi-маршрутизаторів і модемів в одному корпусі, оскільки мережі, що працюють тільки по дротовому з’єднанню, зараз стають все рідшими. Разом із маршрутизатором можна використовувати супутні компоненти, такі як Wi-Fi-посилювачі, точки доступу, Wi-Fi-підсилювачі та аналізатори, щоб підвищити продуктивність.

Усі ці компоненти доступні як у споживчому, так і в корпоративному варіантах.

1.3 Кращі практики побудови та впровадження LAN у школі

Впровадження локальної мережі (LAN) є важливим кроком у розвитку школи. Воно дозволяє скористатися перевагами новітніх цифрових технологій, таких як онлайн-сервіси, інформація, що зберігається в хмарі, та хмарні платформи управління процесами. Наведемо кілька найкращих практик, рисунок 1.4, які допоможуть у впровадженні та управлінні локальною мережею для досягнення успіху в освітньому процесі.

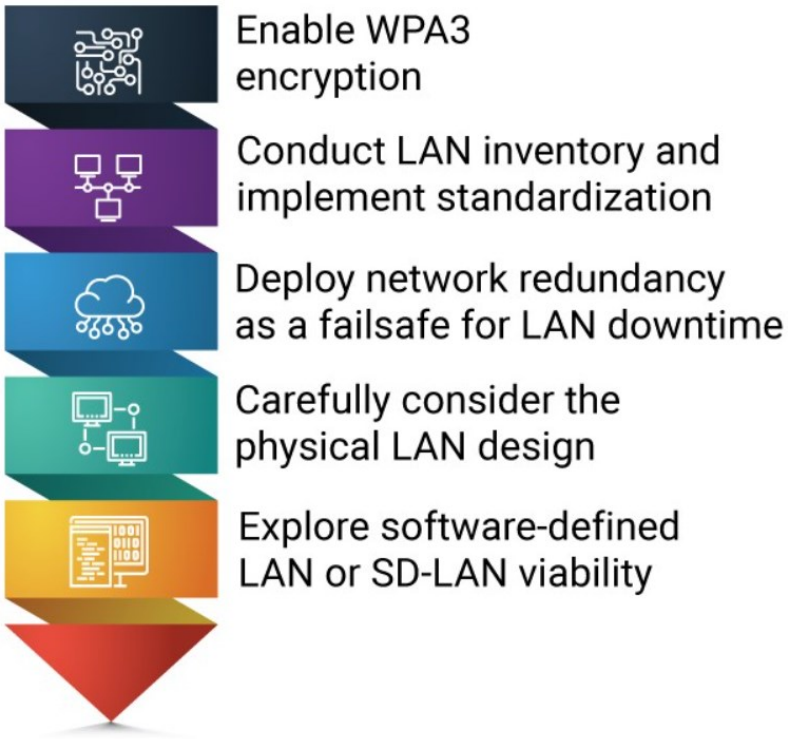

Рисунок 1.4 – Кращі практики управління мережею школи

Шифрування WPA2 було світовим стандартом безпеки Wi-Fi, що є надзвичайно важливим, враховуючи ризикований характер такого

з’єднання. З 2006 року все сертифіковане для підприємств обладнання Wi-Fi використовує WPA2, а в 2018 році з’явився новий стандарт WPA3. WPA3 покращує WPA2, усуваючи вразливості, пов’язані з паролями, захищаючи публічний Wi-Fi та спрощуючи налаштування безпечної мережі Wi-Fi. Школам рекомендується перейти на WPA3 протягом найближчого часу, оскільки він підтримує зворотну сумісність із WPA2.

Як уже зазначалося, середня локальна мережа складається з восьми основних компонентів, і з часом їх кількість може збільшуватися. Від IP-телефонів, IP-камер, IP-динаміків тощо до настільних комп’ютерів, принтерів, точок доступу та брандмауерів, розкиданих по всьому офісному комплексу, існує ризик зростання безладу в міру розвитку мережевого середовища. Безлад не тільки ускладнює та здорожує обслуговування локальної мережі, але й створює вразливі місця в системі безпеки. Ось чому потрібно провести детальну інвентаризацію, проаналізувати мережеві політики та версії обладнання, а також запровадити стандартизацію для спрощення управління.

Резервування (або резервний мережевий ресурс, який вмикається в разі надзвичайної ситуації) є необхідним для надійної роботи локальної мережі. Зв’язок у локальній мережі може бути порушений через несприятливі погодні умови, проблеми з конфігурацією центрального сервера, загрози безпеці, зношення обладнання, надмірний попит на пропускну здатність та безліч інших причин. Школа повинна залишатися підключеним протягом усього цього періоду за допомогою механізму відмовостійкості. Можна налаштувати проміжні маршрутизатори, які забезпечують автоматичне переключення на іншу лінію в разі порушення зв’язку. Ви також можете інвестувати в резервну локальну мережу від іншого оператора, щоб уникнути проблем, пов’язаних з простоєм оператора.

Деякі постачальники зараз обіцяють готові до використання LAN-рішення, але вони можуть не підходити для всіх випадків. Особливо для використання в школі, кожна організація потребує локальної мережі, адаптованої до її унікальних вимог. Фізична конструкція LAN-архітектури, включає точне розташування маршрутизаторів, кількість і конфігурацію мережевих комутаторів, а також якість використовуваних кабелів.

Існує два типи мереж, що використовуються для підключення пристроїв IoT: мережі з низьким енергоспоживанням і великим радіусом дії (LPWAN) та бездротові локальні мережі в межах однієї будівлі або на відстані до 100 метрів. Можна підключити пристрій IoT за допомогою дротової локальної мережі, якщо він має порт Ethernet, що часто буває у випадку побутової техніки, такої як смарт-телевізори або корпоративні системи для проведення нарад. Все це вимагає чітко сформульованого плану, в якому оцінені існуючі пристрої IoT і прогнозу майбутніх потреб. Можна виділити спеціальні мережеві ресурси через LAN, а також LPWAN, залежно від радіусу дії мережі.

SD-LAN відокремлює фізичні компоненти мережі від платформи, з якої вони управляються. Замість налаштування кожного окремого пристрою для оптимізованого підключення до локальної мережі, SD-LAN використовує централізовану платформу (зазвичай розміщену в хмарі та живиться даними бездротовим способом). SD-LAN має ряд переваг над традиційним управлінням локальною мережею. Існує можливість спостереження за всією мережею через єдине вікно. Також можна скористатися програмними засобами, такими як код автоматизації мережі або оновлення, що надаються через хмару. Послуги SD-LAN нового покоління, такі як Macquarie Telecom SD-LAN, використовують штучний інтелект (AI) для забезпечення швидкості, що в 5 разів перевищує навіть Wi-Fi 5.

Послуги з управління локальною мережею дозволяють передати функції обслуговування, управління та забезпечення безпеки локальної мережі зовнішньому постачальнику. Майже всі великі телекомунікаційні оператори у світі, включаючи Orange, Verizon та Vodacom, пропонують керовані локальні мережі своїм корпоративним клієнтам. Можна співпрацювати з технологічними компаніями, які мають досвід в управлінні та модернізації мережевих пристроїв. Зазвичай керовані локальні мережі використовують хмарну платформу, щоб забезпечити прозорість та регулярний доступ до інформації про роботу локальної мережі без необхідності вкладати будь-які зусилля на місці.

Сегментація дозволяє розгалужувати локальну мережу для підвищення продуктивності та забезпечення безпеки. Різні сегменти LAN не мають доступу один до одного і отримують вигоду від виділених ресурсів, призначених їм через мережевий маршрутизатор і комутатор. Є два способи зробити це. Можна розмістити фізичний LAN-міст між центральним сервером і підключеними пристроями, щоб створити кілька гілок. Або використовувати віртуальну LAN або технологію VLAN, щоб за допомогою програмно-визначених мережевих політик розділити вашу мережу на групи.

Через повсюдну поширеність програмного забезпечення для брандмауерів споживачі та малі підприємства часто роблять помилку, не інвестуючи в додаткове обладнання для брандмауерів. Однак програмне забезпечення само по собі не може на 100% захистити вас від ризиків і вразливостей, пов’язаних з мережею. Програмне забезпечення брандмауера знаходиться в тій самій системі, що й усі інші програми на кінцевому пристрої. Це означає, що якщо пристрій заражений або скомпрометований будь-яким чином, програмне забезпечення брандмауера також може перестати функціонувати. Додатковий брандмауер регулює трафік даних і

застосовує обмеження з зовнішнього вузла, який майже неможливо зламати.

LAN є ключовим інфраструктурним елементом школи і не повинен бути об’єднаний з іншими IT-послугами або завданнями з адміністрування мережі. Потрібен спеціальний проектний менеджер, який буде відповідати за впровадження LAN, і він може бути як членом внутрішньої IT-команди, так і співробітником постачальника керованих послуг. Після встановлення LAN повинна бути команда фахівців з управління мережею, яка буде оптимізувати її конфігурації. Також потрібен централізований орган, який буде приймати рішення та контролювати проект.

1.4 Висновки до першого розділу

В першому розділі кваліфікаційної роботи проведено аналіз призначення та основних компонентів локальної комп’ютерної мережі школи с.Катеринівка. Як наслідок, визначено типи серверів, що можуть обслуговувати потреби школи. Одним з варіантів здешевлення проекту запропоновано використання тонких клієнтів у якості користувацього обладнання. Економію ліцензій можна здійснити через використання серверних версій програмного забезпечення і віддаленого доступу до нього. Проаналізовано типи локальних мереж для школи та наведено кращі практики організації управління мережею.

2 СТВОРЕННЯ ПРОЕКТУ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ШКОЛИ С.КАТЕРИНІВКА

2.1 Етапи проектування локальної комп'ютерної мережі для школи с.Катеринівка

Грамотне планування мережі є ключовим фактором у створенні надійної та гнучкої IT-інфраструктури у школі. Нижче наведено основні етапи, що забезпечують відповідність мережі поточним і майбутнім вимогам [1-9].

Визначення потреб проводиться на самому початку етапу планування. Спеціалісти аналізують комунікаційні вимоги організації, проводячи опитування та інтерв'ю. Враховуються кількість користувачів, їхні ролі, типи додатків, параметри безпеки та відповідність стандартам. Також оцінюється існуюча інфраструктура для визначення зон, що потребують удосконалення.

Розробка архітектури є основою подальшого успішного функціонування мережі. На основі отриманих даних створюється загальна схема мережі. Визначаються оптимальні комутатори, маршрутизатори та точки доступу, а також береться до уваги резервування та можливість масштабування.

План впровадження допоможе уникнути несподіваних ситуацій. Розробляється детальна дорожня карта встановлення обладнання та налаштування мережевих параметрів IP-адресації, VLAN, правил брандмауера. Документується міграція даних у разі переходу з попередньої мережі та передбачаються тести працездатності.

Перевірка та тестування має проводитись не тільки на етапі прийому мережі, а також має бути план системного аналізу змін у продуктивності. Виконується контрольна перевірка всіх апаратних компонентів та

налаштувань комутаторів, маршрутизаторів, систем захисту, щоб забезпечити відповідність заявленим рівням продуктивності.

Документування має за мету створення різних журналів для подальшого обслуговування мережі. Створюються структуровані схеми мережі, посібники з використання та усунення несправностей, а також перелік обладнання, ліцензій та гарантій.

Навчання персоналу є основою правильної експлуатації мережі. Проводиться підготовка користувачів щодо ефективного застосування мережі. ІТ-фахівці отримують знання з адміністрування, обслуговування та усунення несправностей, включаючи аспекти безпеки.

Обслуговування та модернізація є безперервним процесом і має мати чіткі інструкції щодо проведення. Після запуску мережі забезпечується її регулярний моніторинг та оптимізація. Оновлюється програмне забезпечення, тестується продуктивність, проводиться модернізація обладнання, що підтримує надійність і масштабованість.

Планування мережі включає аналіз потреб користувачів, оцінку безпеки та довгострокових перспектив. Визначається дротовий або бездротовий формат, підбирається необхідне обладнання. Важливо врахувати можливість масштабування та відповідність мережевим стандартам.

Продуктивність мережі оцінюється за показниками швидкості, надійності та мінімізації затримок. Враховуються заходи безпеки, включаючи брандмауери та системи захисту від вторгнень.

Фінансове планування охоплює витрати на закупівлю, монтаж, підтримку та модернізацію. Документуються відповідність стандартам, резервування ресурсів та забезпечення стабільного зв’язку між компонентами.

Ретельне адміністрування та управління мережею забезпечують стабільність її роботи. Спеціалізоване програмне забезпечення допомагає автоматично визначати потенційні проблеми та швидко їх вирішувати.

Оцінка продуктивності мережі передбачає аналіз різних показників для визначення ефективності та надійності мережі. Деякі ключові фактори включають:

– затримку – час, необхідний для передачі даних від джерела до пункту призначення, що визначає швидкість передавання;

– коливаня – мінливість затримки пакетів, яка може впливати на роботу додатків, що працюють у режимі реального часу, таких як VoIP і може показувати про потенційні проблеми у мережі;

– втрата пакетів – відсоток пакетів даних, які не досягли пункту призначення, що у свою чергу потребує визначення причини втрат;

– пропускна здатність – фактичний об’єм передачі даних у мережі, що має наближатись до теоретичного значення заявленого відповідною технологією;

– ширина каналу здатність – максимальна здатність мережі передавати дані;

– частота помилок – частота пошкодження або втрати пакетів даних, що може бути зумовлена несправністю компонентів мережі, неправильними налаштуваннями чи зловмисними діями;

– перевантаження мережі – рівень трафіку, що впливає на продуктивність і є дуже важливим показником, оскільки визначає необхідність дослідження змін у мережі.

Наведемо перелік документів, які слід створити під час проектування мережі.

– технічний журнал, що буде містити увесь мерелік необхідних даних згідно політики мережі;

– логічна топологія, призначена для відображення організації передавання даних у мережі та опесу взаємозв’язків елементів та структур;

– фізична топологія буде відображати прокладення дротів, з’єднання пристроїв та елементів у комутаційній шафі;

– технічні специфікації опису обладнання та його додаткових фізичних конфігурацій;

– матриці вирішення проблем, що допоможуть в подальшому швидко відновлюватись від поломок не затрачаючи час на пошук типових рішень;

– маркування розеток для швикого розуміння підключення пристроїв;

– маркування кабельних трас використовується при пошуку пошкоджень чи плановій заміні елементів;

– зведення даних про розетки та кабельні траси, може влючати резервні та не задіяні канали;

– зведення даних про пристрої, MAC-адреси та IP-адреси допоможе у контролі цілісності мережі.

Слідування основним етапам планування та впровадження мережі дасть змогу організувати надійну та високопродуктивну мережу у школі с. Катеринівка.

2.2 Вибір та проектування фізичної топології мережі школи с.Катеринівка

Вибір та проектування фізичної топології мережі школи залежить від кількох ключових факторів, таких як кількість пристроїв, необхідна пропускна здатність, безпека та можливість масштабування.

Топологія “точка-точка” – це тип топології, що працює на основі функціональності відправника та одержувача. Це найпростіший вид зв’язку

між двома вузлами, де один є відправником, а інший – одержувачем. Топологія “точка-точка” забезпечує високу пропускну здатність і у випадку школи має бути розглянута для високошвидкісного приєднання до провайдера послуг Інтернет.

У зірковій топології всі пристрої підключені до єдиного комутатора за допомогою кабелю. Цей комутатор є центральним вузлом, до якого підключені всі інші вузли і може забезпечувати також функції логічного поділу мережі на сегменти з використанням технології VLAN, надавати базову безпеку через використання захисту портів, запобігати петлям комутації, надавати сервіси якості зв’язку.

Перевагами зіркової топології є її розповсюдженість та легкість монтажу і використання, що можна об’єднати як:

– якщо N пристроїв з’єднані між собою в зірковій топології, то кількість кабелів, необхідних для їх з’єднання, дорівнює N. Отже, її легко налаштувати;

– кожен пристрій потребує лише 1 порт, тобто для підключення до комутатора, тому загальна кількість необхідних портів дорівнює N;

– вона є надійною. Якщо одне з’єднання виходить з ладу, це вплине лише на це з’єднання, а не на інші;

– легко виявляти та ізолювати несправності;

– зіркова топологія є економічно вигідною, оскільки використовує відносно недорогі пристрої та кабелі.

Підсумовуючи, можна сказати, що топології мереж відіграють вирішальну роль у визначенні ефективності та надійності комп’ютерної мережі. Кожна топологія має свої унікальні переваги та потенційні недоліки. Розуміючи ці різні схеми, при розробці мережі можна вибрати найбільш підходящу топологію для задоволення конкретних потреб школи, забезпечуючи оптимальну продуктивність і зв’язність.

На основі цього можна навести рекомендації щодо процесу вибору топології, що показано на рисунку 2.1.

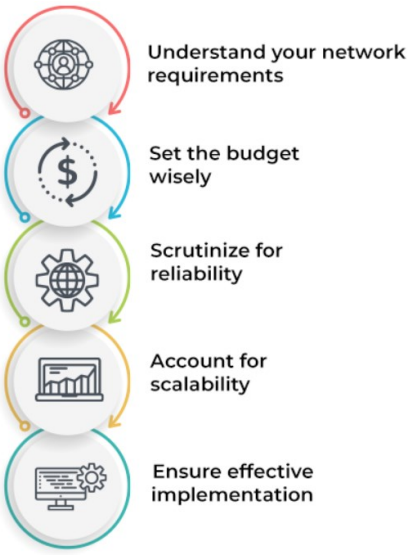

Рисунок 2.1 – Порядок вибору фізичної топології мережі

Перш ніж вибрати топологію мережі, необхідно врахувати кінцеву мету її роботи. Різні мережеві додатки вимагають різного обладнання, і вибір правильного обладнання перед побудовою мережі допоможе уникнути багатьох непотрібних операційних проблем у майбутньому.

Набір програм, які будуть запускатись, відстань передачі даних та очікувані рівні продуктивності повинні бути розглянуті на цьому етапі. Різне обладнання підходить для різних топологій мережі і навпаки. Необхідно оцінити наявне обладнання та врахувати можливість додавання нового, яке планується придбати у майбутньому. Іноді існуюче обладнання можна перепрофілювати для нової топології мережі без будь-яких істотних недоліків, що дозволить зменшити витрати та час на закупівлю.

Фізичний простір – ще один фактор, який потрібно врахувати. Якщо всі системи, які потрібно з’єднати, знаходяться близько одна до одної, то необхідно розглянути можливість використання конфігурації, яка мінімізує використання кабелів.

Потрібно оцінити тип кабелю, який повинні використовувати. Різні за вартістю варіанти крученої пари можуть мати відмінні характеристики. Це може впливати на легкість монтажу через твердість дроту або погіршення при передаванні на відстань через брак якості. Якщо низькі вимоги до пропускної здатності, виберіть економічні кручені пари. І навпаки, більш якісні кабеля потрібні, коли вимоги до пропускної здатності вищі. Волоконно-оптичні кабелі ще ефективніші в передачі даних, однак вони дорожчі і вимагають додаткових компонентів, таких як оптичні приймачі.

Структура мережі впливає на її вразливість до загроз безпеки та легкість впровадження заходів безпеки. Централізовані топології, такі як зіркові топології, можуть спростити впровадження протоколів безпеки та контролю доступу, тоді як децентралізовані структури, такі як сітчасті, забезпечують вбудовані переваги безпеки завдяки різноманітності шляхів передачі даних.

Брандмауери часто використовуються в топологіях мереж для захисту від зовнішніх загроз. Безпечна топологія мережі не тільки запобігає несанкціонованому доступу, але й допомагає організаціям дотримуватися галузевих нормативних вимог, таких як GDPR та HIPAA. Розуміння цих наслідків є надзвичайно важливим для проектування мереж, які захищають конфіденційну інформацію та відповідають вимогам безпеки.

Вибір топології значно впливає на ефективність управління мережею та швидкість вирішення проблем, що є важливим для забезпечення безперебійної роботи. Автоматизовані інструменти моніторингу можуть ще більше покращити управління мережею, прискорюючи та оптимізуючи процеси виявлення та вирішення проблем. Адміністратори також можуть використовувати інструменти для відображення топології мережі, щоб надати візуальні зображення, які допоможуть мережевим командам виявити потенційні проблеми.

На рисунку 2.2 показано плану будівлі школи с.Катеринівка, що має бути використаний для аналізу та розробки фізичної топології. У процесі планування потрібно буде вибрати місце розташування активних мережевих пристроїв, а також провести кабелювання і розміщення розеток.

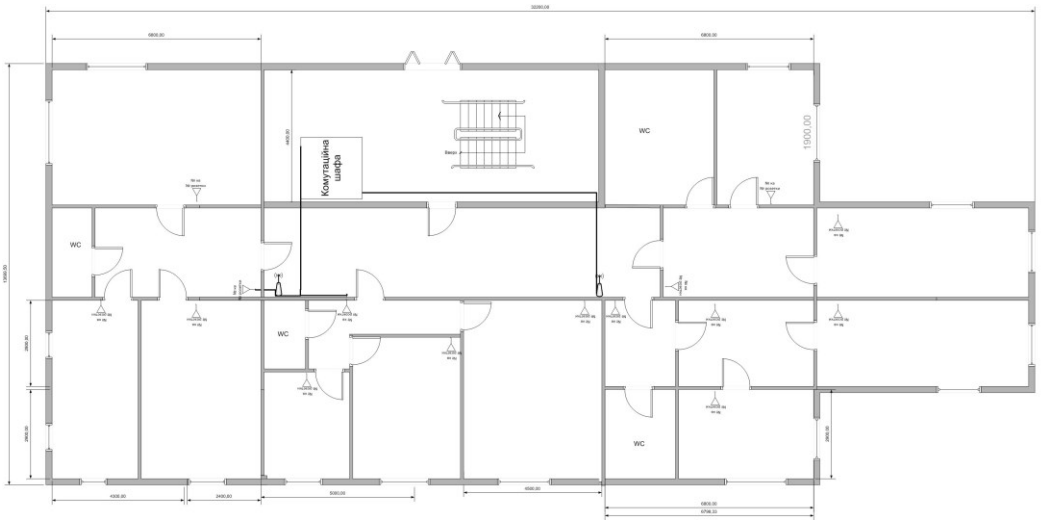

Рисунок 2.2 – Планування фізичної топології на основі будівлі школи с.Катеринівка

У процесі планування визначаються місця розташування активного мережевого обладнання та можливості підключення дротових користувачів. Кабельна інфраструктура прокладається у підвісній стелі, використовуючи спеціальні короби та кріплення для забезпечення надійності. Усі кабелі маркуються відповідно до задокументованої схеми кодування, що полегшує пошук і усунення несправностей.

Поняття “живучість” у мережевому плануванні означає здатність мережі функціонувати, незважаючи на часткові пошкодження, такі як вихід з ладу вузлів або з’єднань. Важливо проектувати мережу таким чином, щоб вона залишалася працездатною і могла забезпечувати безперервну передачу даних та стабільне надання послуг навіть у разі відмови окремих компонентів.

Відмовостійкі мережі автоматично перенаправляють трафік альтернативним маршрутом при виникненні несправностей. Це досягається за рахунок резервування – встановлення дублюючих мережевих пристроїв та використання кількох з'єднань для передачі однакових даних, що підвищує надійність мережі.

Альтернативні підходи до забезпечення відмовостійкості включають автоматизовані механізми обходу несправностей, технології виявлення та корекції помилок під час передачі даних, а також спеціалізовані мережеві протоколи та алгоритми, розроблені для підтримки стабільної роботи системи.

На етапі проектування аналізуються потенційні збої, які можуть вплинути на мережу, їхня ймовірність та можливі наслідки для продуктивності. Відповідно до цих оцінок у структуру мережі інтегруються механізми, що гарантують її надійність та безперебійне функціонування.

2.3 Підбір обладнання для локальної мережі школи с.Катеринівка

Мережеві пристрої, що відповідають за передачу та маршрутизацію даних у комп'ютерній мережі, належать до активного мережевого обладнання. Завдяки вбудованому процесору та оперативній пам'яті, вони можуть керувати потоками інформації та виконувати обробку даних. Це сприяє підвищенню швидкості передачі даних та спрощенню управління мережею. Таким чином, активне обладнання контролює, обробляє та пересилає дані між вузлами мережі [10-20].

Важливою характеристикою активного мережевого обладнання є його інтелектуальна складова. Завдяки розширеному функціоналу мережа працює стабільно, безперебійно та безпечно, з мінімальним втручанням людини.

Комутатор, до якого підключаються всі пристрої мережі, є одним із найбільш поширених видів активного мережевого обладнання. Сучасні комутатори оснащені великою кількістю портів, що дозволяє ефективно організувати єдину мережу без проблем із підключенням і володіють функціями керування мережею.

Пасивне мережеве обладнання, навпаки, відповідає лише за передачу даних, не виконуючи їх обробку. Воно не має власного джерела живлення і не може контролювати трафік. До таких компонентів належать:

– розгалужувачі та сплайс-бокси – використовуються для об’єднання або розділення оптоволоконних ліній зв’язку;

– патч-панелі, коннектори та кросові поля – забезпечують з’єднання між кабелями та пристроями;

– кабелі – служать для передачі даних між підключеними вузлами.

Пасивне мережеве обладнання відповідає за стабільність та ефективність функціонування мережі без необхідності складних налаштувань чи додаткової конфігурації. Воно виконує роль основи для створення єдиного мережевого середовища, використовуючи інформаційні розетки, повторювачі та інші елементи, що спрощує процес інтеграції. Оскільки таке обладнання не має інтелектуальних можливостей, його функції обмежуються виключно передачею даних.

Щоб визначити оптимальне рішення для мережі школи, варто порівняти комутатори Cisco 1000 серії та Mikrotik CRS326 серії, проаналізувавши їхні ключові характеристики та можливості.

Порівняльний аналіз комутаторів цих двох серій дасть змогу вибрати більш оптимальний для школи варіант з можливістю впровадження сучасних технологій та подальшого розвитку мережі. Може виглядати, що покупка пристрою рівня малого бізнесу є неоправданою для школи, проте з іншої сторони необхідність заміни в більш дешевого через його обмеженість має бути розглянута.

У таблиці 2.1 подано порівняння характеристик двох комутаторів.

Таблиця 2.1 – Порівняння характеристик Cisco 1000 та Mikrotik CRS326

Характеристика	Cisco Catalyst 1000	MikroTik CRS326
Порти	8/16/24/48 × 1 Gb + 2/4 SFP/SFP+	24 × 1 Gb + 2 × SFP+ (1/10 Gb)
PoE	PoE+ (до 740 Вт)	лише PoE-in
Охолодження	Fanless (крім PoE-48), ~20 Вт	Пасивне / rack fan, ~20–24 Вт
L2 продуктивність	Лінійна на всіх портах	Лінійна, швидше при bridge
L3	Статичні маршрути, 1 SVI, до 64 VLAN	Інтер-VLAN HW-offload, NAT до ~700 Mbps
CPU	800 MHz ARM, 512 MB	650-800 MHz ARM, 512 MB
Управління	CLI (IOS), web UI, SNMP, Bluetooth	SwOS/RouterOS CLI/API
Підтримка	Cisco підтримка до 2028	Спільнота, регулярні оновлення
Цільова аудиторія	Edge-комутатори SMB з PoE	Homelab / edge L2 з 10 Gb uplink

На рисунку 2.3 показано можливості налаштування комутатора Cisco 1000 через використання графічного інтерфейсу, що в умовах роботи у школі і не дуже високій кваліфікації адміністратора може суттєво спростити налаштування через інтуїтивно зрозумілий дизайн.

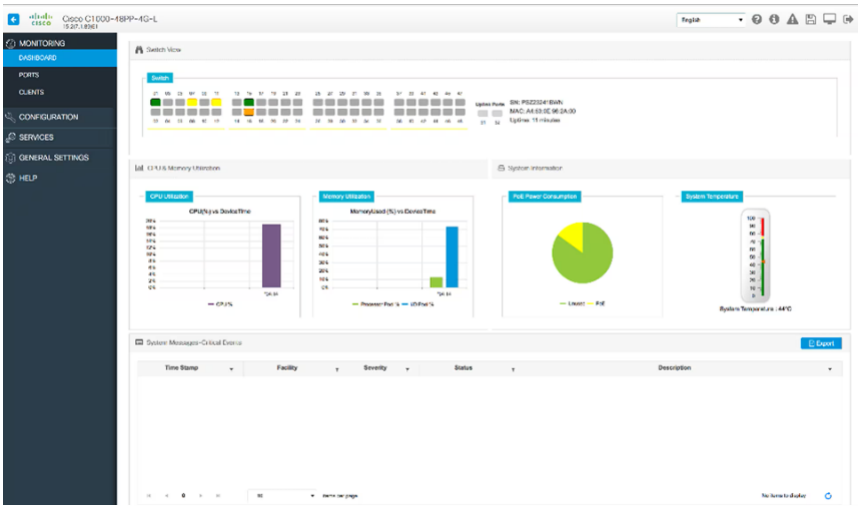

Рисунок 2.3 – Візуалізації графічного інтерфейсу управління комутатором Cisco C1000-24P-4G-L

Іншою корисною опцією є можливість налаштування через використання інтерфейсу Bluetooth, що дасть змогу використовувати носимі пристрої для швидкого та захищеного доступу до налаштувань. На рисунку 2.4 показано приклад такого підключення.

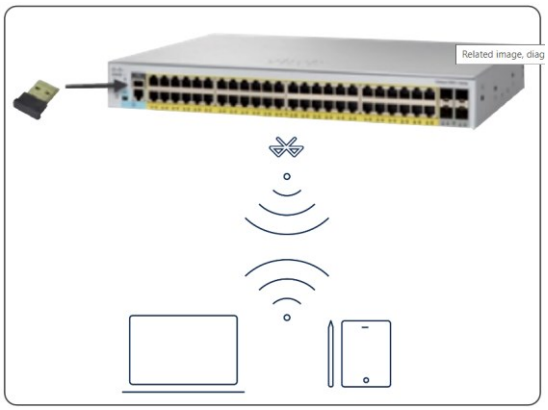

Рисунок 2.4 – Опційне налаштування через Bluetooth

Для реалізації функцій маршрутизації прийнято рішення використовувати Cisco CBS350-16P-2G-EU як частину екосистеми Cisco, що була обрана для створення локальної комп’ютерної мережі у школі с.Катеринівка. Це обладнання забезпечує оптимальне співвідношення продуктивності та вартості, що робить його ефективним рішенням для даної мережі.

Вибір між пристроями Cisco та Mikrotik залежить від потреб мережі, фінансових можливостей і вимог до функціональності та масштабованості. Cisco пропонує надійні та високопродуктивні рішення для корпоративних мереж, тоді як Mikrotik забезпечує доступніші варіанти для малого та середнього бізнесу, з хорошою функціональністю та широкими можливостями налаштування. На основі аналізу прийнято рішення на користь обладнання Cisco, яке гарантує високу гнучкість, тривалу підтримку та стабільність роботи мережі.

2.4 Проектування необхідних налаштувань та тестування роботи мережі школи с.Катеринівка

Логічна топологія мережі стосується способу передачі даних у мережі. Вона відображає логічні зв'язки та шляхи між мережевими пристроями, такими як маршрутизатори, комутатори та сервери. На відміну від фізичної топології мережі, яка описує фізичне розташування мережевих пристроїв та кабелів, логічна топологія мережі зосереджується на тому, як дані проходять через мережу [21-34].

Створення логічної топології мережі школи залежить від кількох факторів:

- кількість приміщень/кабінетів;
- наявність комп'ютерних класів, Wi-Fi;
- підключення до інтернету та шкільного сервера;
- вимоги до безпеки, сегментації, управління.

При створенні логічної топології мережі школи пропонується використати дворівневу модель організації зв'язків. На першому рівні, який буде відігравати роль кореневого буде використано маршрутизатор або комутатор L3 для забезпечення функцій доступу до Інтернету, маршрутизації між VLAN, організації функцій безпеки у якості фаєрволу та виконання NAT трансляції, базової фільтрації трафіку користувачів.

Створення мережі школи с.Катеринівка передбачає розроблення політики поділу на сегменти через використання віртуальних мереж VLAN. Для адміністрації та дирекції буде використано VLAN з номером 100, вчителі будуть у VLAN 200, для учнів VLAN 300, гостьовий доступ організується у VLAN 400, інші ресурси такі як принтери, системи дистанційного навчання та інші сервіси будуть у VLAN 500.

Для підключення користувачів на рівні доступу пропонується встановлення мінімум одного комутатора на поверх, а за необхідності

додавання додаткових у відповідних місцях. До цих пристроїв будуть доєднуватись комп’ютери та точки доступу, а також інші периферійні пристрої з потребою мережевого обміну даними. Основною вимогою окрім підтримання продуктивності на належному рівні є також робота з протоколом 802.1Q для забезпечення VLAN.

Для роботи точок доступу доцільним є розглянути можливість їх управління через контролер, що дасть змогу забезпечити централізоване керування та моніторинг. При цьому зросте безпечність бездротового з’єднання.

Доступ до Інтернету буде здійснюватись до мережі провайдера через використання функцій NAT з Firewall. При цьому хорошою ідеєю є забезпечити фільтрацію мережевого трафіку і швидко виявляти непотрібні дані. На рисунку 2.5 подано схематичну організацію мережі школи с.Катеринівка.

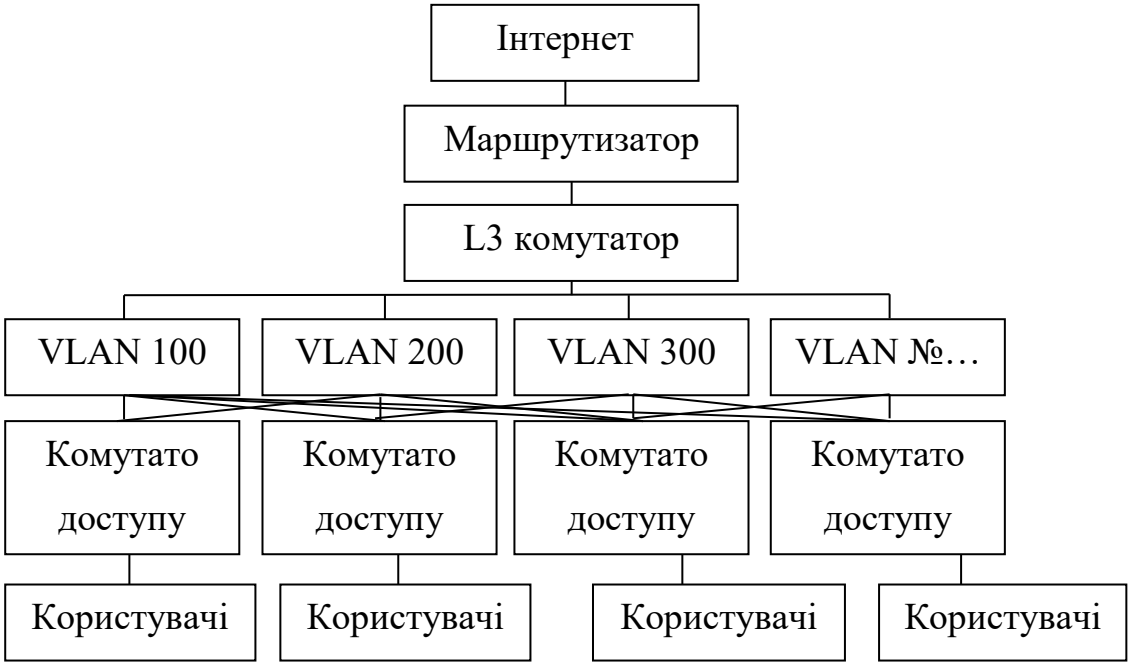

Рисунок 2.5 – Схематичне зображення мережі школи с.Катеринівка

Розрахунок адрес для мережі школи буде проводитись з використанням приватних адрес простору 10.0.0.0/8, що разом з

технологією NAT дасть змогу утворювати довільні конфігурації і масштабувати її при зміні вимог у школі.

Розрахунок адрес показано в таблиці 2.2.

Таблиця 2.2 – Призначення IP адрес у мережі школи

Ім’я	К-сть адрес	Загальна к-сть адрес	Адреси без використання	Адреса мережі	Корисні адреси	Широкомовна
Учні	110	126	16	10.0.0.0 /25	10.0.0.1 - 10.0.0.126	.127
Вчителі	50	62	12	10.0.0.128 /26	10.0.0.129 - 10.0.0.190	.191
Дирекція	15	30	15	10.0.0.192 /27	10.0.0.193 - 10.0.0.222	.223
Гості	25	30	5	10.0.0.224 /27	10.0.0.225 - 10.0.0.254	.255
Інші сервіси	12	14	2	10.0.1.0 /28	10.0.1.1 - 10.0.1.14	.15
Адміністрування	12	14	2	10.0.1.16 /28	10.0.1.17 - 10.0.1.30	.31

Тестування продуктивності мережі допомагає оцінити її ефективність, стабільність та здатність витримувати навантаження. Основні методи тестування включають:

– навантажувальне тестування при якому проводиться перевірка роботи мережі при стандартному навантаженні;

– стресове тестування дає змогу провести визначення меж пропускної здатності при екстремальних умовах;

– тестування стабільності здійснює оцінку продуктивності мережі при тривалому використанні;

– об’ємне тестування проводить перевірку роботи мережі при великій кількості даних;

– тестування стрибків забезпечує аналіз реакції мережі на раптові зміни навантаження.

Для тестування використовуються спеціальні інструменти, такі як ManageEngine OpManager, PRTG Network Monitor та Site24x7, які допомагають виявити проблеми та оптимізувати продуктивність

Результати розрахунків разом з даними триманими при тестуванні будуть поміщені в технічний журнал. Також буде заплановано періодичне перетестування для оцінювання змін у часі та виявлення необхідності проводити зміни чи модифікації.

2.5 Висновки до другого розділу

У другому розділі кваліфікаційної роботи проведено формування етапів проектування локальної комп’ютерної мережі школи с.Катеринівка, що дало змогу визначити її потреби та розробити архітектуру для успішного функціонування. Сформовано план впровадження, що допоможе уникнути неочікуваних ситуацій. Запропоновано оцінювати продуктивність мережі за визначеними показниками і враховувати фінансове планування для розвитку та модернізації мережі. Наведено перелік документів, що повинні зберігатись для ефективного та швидкого виявлення та виправлення несправностей у разі їх виникнення. На етапі вибору та проектування фізичної топології запропоновано використовувати з’єднання типу “точка-точка” для підключення провайдера послуг Інтернет і

використати розширену зірку для забезпечення з’єднанням користувачів. У процесі планування вибрано місце розташування активних мережевих пристроїв, а також кабелювання і розміщення розеток. Кабельна інфраструктура прокладається у підвісній стелі, використовуючи спеціальні короби та кріплення для забезпечення надійності. Усі кабелі маркуються відповідно до задокументованої схеми кодування, що полегшує пошук і усунення несправностей. В процесі вибору активного мережевого обладнання порівняно комутатори Cisco 1000 серії та Mikrotik CRS326 серії, проаналізувавши їхні ключові характеристики та можливості. Для реалізації функцій маршрутизації прийнято рішення використовувати Cisco CBS350-16P-2G-EU як частину екосистеми Cisco. На основі аналізу прийнято рішення на користь обладнання Cisco, яке гарантує високу гнучкість, тривалу підтримку та стабільність роботи мережі. Спроектовано логічну схему мережі де запропоновано використати дворівневу модель організації зв’язків. На першому рівні, який буде відігравати роль кореневого буде використано маршрутизатор або комутатор L3 для забезпечення функцій доступу до Інтернету, маршрутизації між VLAN, організації функцій безпеки у якості фаєрволу та виконання NAT трансляції, базової фільтрації трафіку користувачів. На другому будуть комутатори доступу рівня L2. Створення мережі школи с.Катеринівка передбачає розроблення політики поділу на сегменти через використання віртуальних мереж VLAN. Для адміністрації та дирекції буде використано VLAN з номером 100, вчителі будуть у VLAN 200, для учнів VLAN 300, гостьовий доступ організується у VLAN 400, інші ресурси такі як принтери, системи дистанційного навчання та інші сервіси будуть у VLAN 500. Проведено розрахунок відповідних адрес та їх розподіл для відповідних підрозділів.

3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ ЗМОДЕЛЬОВАНОЇ МЕРЕЖІ ШКОЛИ С.КАТЕРИНІВКА

3.1 Моделювання локальної комп'ютерної мережі школи с.Катеринівка

Cisco Packet Tracer – це ефективний засіб для моделювання локальних комп'ютерних мереж, який дає змогу створювати та перевіряти мережеві структури перед їх впровадженням. Ця платформа забезпечує широкий спектр можливостей для тестування мереж, даючи змогу експериментувати з різними конфігураціями та сценаріями без потреби у фізичних пристроях.

Рисунок 3.1 зображає модель мережі школи с.Катеринівка, що в подальшому може бути реалізована на реальному обладнанні.

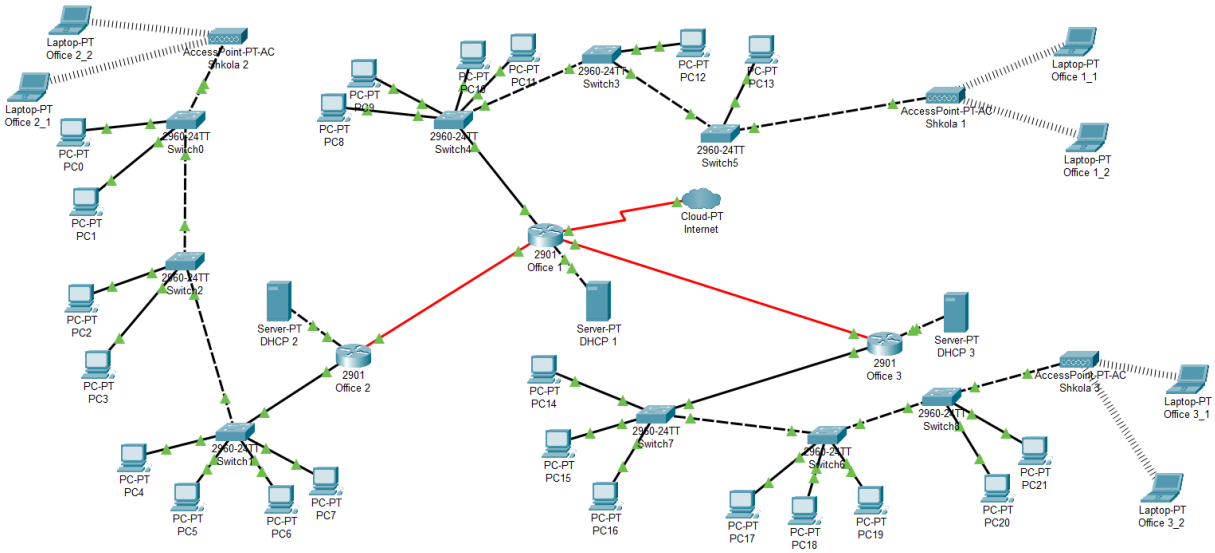

Рисунок 3.1 – Модельована мережа школи с.Катеринівка

На схемі відображено модель мережі школи, що складається з трьох офісів, з'єднаних між собою через маршрутизатори. В кожному офісі встановлена комутована мережа, яка включає три комутатори для підключення користувачів із застосуванням технології VLAN. Це

забезпечує базову мережеву безпеку, оскільки передача даних між різними VLAN здійснюється через маршрутизатор, де налаштовуються списки контролю доступу (ACL).

Додатково пропонується впровадити механізми захисту другого рівня на комутаторах. Це включає фільтрацію MAC-адрес для обмеження несанкціонованого доступу, а також автоматичне повідомлення адміністратора у разі спроби підключення стороннього пристрою.

Рисунок 3.2 демонструє параметри, які потрібно налаштувати на шлюзі з використанням статичних адрес. .

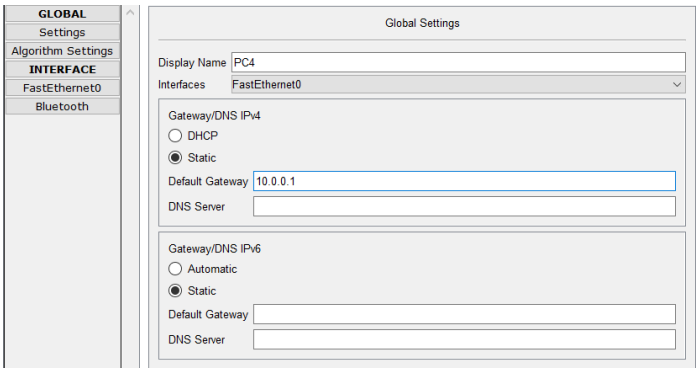

Рисунок 3.2 – Параметри налаштування маршрутизатора за замовчуванням

Відповідно рисунок 3.3 показує параметри встановлення статичних IP адрес на ключові комп’ютери, такі як файлові сервери чи спільного використання.

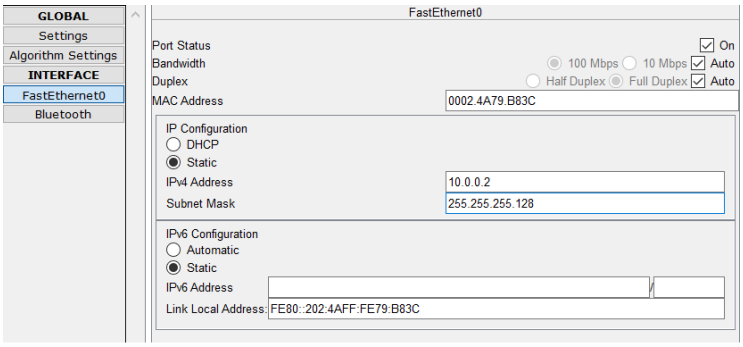

Рисунок 3.3 – Налаштування парамтерів статичної IP адреси

Щоб запобігти несанкціонованому доступу до налаштувань комутатора та забезпечити його правильну ідентифікацію серед інших мережевих пристроїв компанії, буде виконано конфігурацію відповідно до показаної 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 – Ідентифікація комутатора

Згідно вибраної схеми потрібно реалізувати сегментацію і присвоїти комп’ютери до відповідних VLAN. Рисунок 3.5 показує створення VLAN та співвідношення 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 – Процес налаштування VLAN

Як показано у налаштуванні, після створення VLAN було визначено діапазон портів з другого по п’ятий, які належать до цієї VLAN. На рисунку 3.6 представлено перевірку її працездатності.

```
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 – Огляд налаштування VLAN

Кожна віртуальна мережа буде об’єднувати користувачів чи додатки за їх спільним використанням. У випадку утворення нових потреб в мережі школи можна доналаштувати ще необхідні VLAN.

3.2 Налаштування безпеки та динамічних адрес для обладнання у мережі школи с.Катеринівка

На комутаторі виконано конфігурацію безпеки портів, що запобігає несанкціонованому підключенню сторонніх пристроїв. Візуальне представлення налаштувань можна побачити 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 – Безпека портів на комутаторі

Деяким користувачам передбачено автоматичне отримання IP-адрес завдяки використанню DHCP-сервера, який буде розташований окремо від інших пристроїв. Це дозволить ефективно керувати доступом до нього та забезпечити його захист. На рисунку 3.8 представлено конфігурацію DHCP-сервера. Потрібно також врахувати вразливість даного сервісу до затримок, що можуть виникнути з роботою протоколу запобігання петель Spanning Tree Protocol (STP). Тому бажано встановити його швидшу версію Rapid STP, яка покликана вирішувати ці питання.

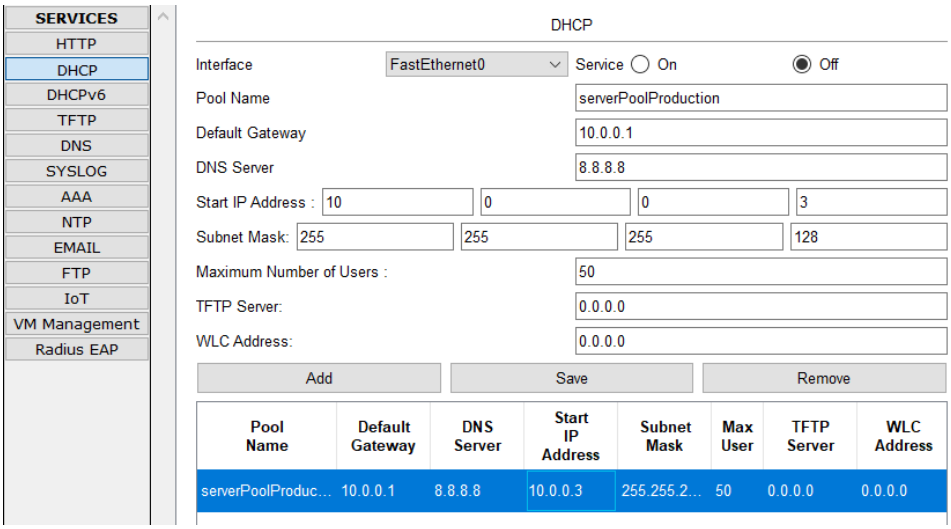

Рисунок 3.8 – Встановлення параметрів DHCP сервера

Для забезпечення коректної роботи міжмережевого з'єднання необхідно налаштувати IP-адреси на маршрутизаторі. Обмін даними між віртуальними мережами буде здійснюватися за допомогою протоколу 802.1Q, який підтримується маршрутизаторами Cisco. На рисунку 3.9 представлено конфігурацію підінтерфейсів для всіх 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 3.9 – Встановлення параметрів для протоколу 802.1Q

У нашому випадку DHCP сервер знаходиться за межами локальної мережі і для клієнтів потрібно здійснити додаткове налаштування маршрутизатора як на рисунку 3.10.

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

Рисунок 3.10 – Встановлення релей агента

Щоб запобігти втратам пакетів при роботі DHCP-сервера та інших протоколів, які критично залежать від мінімальних затримок, слід активувати прискорену версію протоколу Spanning Tree, яка миттєво вводить порти в робочий стан. Додатковий захист від випадкових підключень, що можуть спричинити петлю, буде забезпечений шляхом налаштування BPDU Guard. Приклад конфігурації цього механізму наведено на рисунку 3.11.

```
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 3.11 – Ввімкнення RSTP з BPDU Guard

Для перевірки роботи DHCP і отримання адреси здійснено виконання команди ipconfig /all результат якої подано на рисунку 3.12.

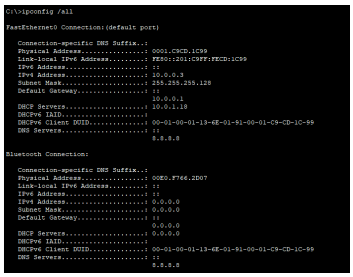

Рисунок 3.12 – Динамічне отримання адреси

На основі представлених даних можна зробити висновок, що налаштування та впровадження DHCP-сервера і клієнта виконані коректно, а отримані параметри відповідають очікуваним результатам.

Оскільки мережа має невеликі масштаби, для її моделювання було обрано протокол RIP для забезпечення маршрутизації. У реальних умовах планується використовувати статичну маршрутизацію. Конфігурація маршрутизації представлена на рисунку 3.13.

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

Рисунок 3.13 – Ввімкнення протоколу RIP

Оскільки в нашій мережі використовується поділ на підмережі з різними масками, друга версія протоколу маршрутизації має бути включена.

3.3 Висновок до третього розділу

Третій розділ кваліфікаційної роботи описує основні етапи моделювання роботи мережі школи с.Катеринівка у середовищі Cisco Packet Tracer. У моделі реалізовано функціонування технології VLAN, здійснено захист основних компонентів мережі від несанкціонованого доступу та описано повний процес налаштування кінцевого обладнання. При налаштуванні DHCP сервера також виконано додаткове налаштування обладнання для уможливлення роботи єдиного сервісу з різних мереж.

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" [35-38].

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 φ. 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 φ. Наприклад, якщо на блоці живлення комп'ютера написано «850 Вт» (cos φ 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 ≈ 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

У результаті виконання кваліфікаційної роботи проведено розроблення проекту та моделювання локальної комп’ютерної мережі школи с.Катеринівка і отримано наступні результати:

– проведено аналіз призначення та основних компонентів локальної комп’ютерної мережі школи с.Катеринівка. Як наслідок, визначено типи серверів, що можуть обслуговувати потреби школи. Одним з варіантів здешевлення проекту запропоновано використання тонких клієнтів у якості користувацього обладнання. Економію ліцензій можна здійснити через використання серверних версій програмного забезпечення і віддаленого доступу до нього;

– проаналізовано типи локальних мереж для школи та наведено кращі практики організації управління мережею. Проведено формування етапів проектування локальної комп’ютерної мережі школи с.Катеринівка, що дало змогу визначити її потреби та розробити архітектуру для успішного функціонування. Сформовано план впровадження, що допоможе уникнути неочікуваних ситуацій. Запропоновано оцінювати продуктивність мережі за визначеними показниками і враховувати фінансове планування для розвитку та модернізації мережі. Наведено перелік документів, що повинні зберігатись для ефективного та швидкого виявлення та виправлення несправностей у разі їх виникнення. На етапі вибору та проектування фізичної топології запропоновано використовувати з’єднання типу “точка-точка” для підключення провайдера послуг Інтернет і використати розширену зірку для забезпечення з’єднанням користувачів.

– вибрано місце розташування активних мережевих пристроїв, а також кабелювання і розміщення розеток. Кабельна інфраструктура прокладається у підвісній стелі, використовуючи спеціальні короби та кріплення для забезпечення надійності. Усі кабелі маркуються відповідно до

задокументованої схеми кодування, що полегшує пошук і усунення несправностей.

– в процесі вибору активного мережевого обладнання порівняно комутатори Cisco 1000 серії та Mikrotik CRS326 серії, проаналізувавши їхні ключові характеристики та можливості. Для реалізації функцій маршрутизації прийнято рішення використовувати Cisco CBS350-16P-2G-EU як частину екосистеми Cisco. На основі аналізу прийнято рішення на користь обладнання Cisco, яке гарантує високу гнучкість, тривалу підтримку та стабільність роботи мережі.

– спроектовано логічну схему мережі де запропоновано використати дворівневу модель організації зв'язків. На першому рівні, який буде відігравати роль кореневого буде використано маршрутизатор або комутатор L3 для забезпечення функцій доступу до Інтернету, маршрутизації між VLAN, організації функцій безпеки у якості фаєрволу та виконання NAT трансляції, базової фільтрації трафіку користувачів. На другому будуть комутатори доступу рівня L2. Створення мережі школи с.Катеринівка передбачає розроблення політики поділу на сегменти через використання віртуальних мереж VLAN. Для адміністрації та дирекції буде використано VLAN з номером 100, вчителі будуть у VLAN 200, для учнів VLAN 300, гостьовий доступ організується у VLAN 400, інші ресурси такі як принтери, системи дистанційного навчання та інші сервіси будуть у VLAN 500. Проведено розрахунок відповідних адрес та їх розподіл для відповідних підрозділів.

– змодельовано мережу школи с.Катеринівка у середовищі Cisco Packet Tracer. У моделі реалізовано функціонування технології VLAN, здійснено захист основних компонентів мережі від несанкціонованого доступу та описано повний процес налаштування кінцевого обладнання. При налаштуванні DHCP сервера також виконано додаткове налаштування обладнання для уможливлення роботи єдиного сервісу з різних мереж.

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 Local Area Network (LAN)? Definition, Types, Architecture, and Best Practices [Електронний ресурс] – Режим доступу: https://www.spiceworks.com/tech/networking/articles/what-is-local-area-network/#_002. – Назва з екрану. – Дата звернення: 9. 05.2025

2. What is LAN [Електронний ресурс] – Режим доступу: https://cyble.com/knowledge-hub/what-is-lan/. – Назва з екрану. – Дата звернення: 9. 05.2025

3. What is LAN. [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/switches/what-is-a-lan-local-area-network.html. – Назва з екрану. – Дата звернення: 9.05.2025.

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: 9.05.2025.

5. Type of LANs [Електронний ресурс] – Режим доступу: https://www.networkacademy.io/ccna/ethernet/type-of-lans. – Назва з екрану. – Дата звернення: 10. 05.2025

6. Types of area networks - LAN, MAN and WAN [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/. – Назва з екрану. – Дата звернення: 10. 05.2025

7. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids/. – Назва з екрану. – Дата звернення: 10. 05.2025

8. БІДЮК, О., & МАРЦЕНКО, С. (2025). МЕТОДИ ТА ЗАСОБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІТ ІНФРАСТРУКТУР. Herald of Khmelnytskyi

National University. Technical Sciences, 347(1), 47-58. https://doi.org/10.31891/2307-5732-2025-347-6

9. 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: 10. 05.2025

10. NETWORK EQUIPMENT: CONCEPT AND TYPES [Електронний ресурс] – Режим доступу: https://newserverlife.com/articles/network-equipment-concept-and-types/. – Назва з екрану. – Дата звернення: 10. 05.2025

11. 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: 11. 05.2025

12. Karnaukhov, O., Duda, O., Martsenko, S., & Yatsyshyn, V. (2023). Cyber-physical systems at" Digital University". In ITTAP (pp. 306-314).

13. Комутатор мережевий Cisco C1000-24T-4G-L [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/288249428/p288249428/. – Назва з екрану. – Дата звернення: 11. 05.2025

14. 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: 11. 05.2025

15. 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: 11. 05.2025

16. Комутатор D-LINK DGS-1100-24PV2. [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/342410224/p342410224/. – Назва з екрану. – Дата звернення: 11. 05.2025

17. Zyxel GS1915-24EP [Електронний ресурс]. – Режим доступу: https://rozetka.com.ua/ua/zyxel-gs1915-24ep-eu0101f/p357602781/. – Назва з екрану. – Дата звернення: 11. 05.2025

18. 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. 11. 05.2025

19. 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: 11. 05.2025

20. “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: 12. 05.2025

21. Private-wireless-networking-logistics-industry [Електронний ресурс]. – Режим доступу: https://www.nokia.com/blog/private-wireless-networking-logistics-industry/. – Назва з екрану. – Дата звернення: 12. 05.2025

22. 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: 12. 05.2025).

23. 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: 12. 05.2025).

24. What Is Network Virtualization? [Електронний ресурс]. – Режим доступу: https://blog.gigamon.com/2018/01/04/network-virtualization-optimize/ – Назва з екрану. – Дата звернення: 12. 05.2025.

25. Solving the Network Virtualization Conundrum [Електронний ресурс]. – Режим доступу: https://www.arista.com/en/solutions/network-virtualization – Назва з екрану. – Дата звернення: 12. 05.2025.

26. 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: 12. 05.2025).

27. 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.

28. 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.

29. 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.

30. 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: 12. 05.2025).

31. 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

32. 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: 12. 05.2025.

33. Network functionality [Електронний ресурс]. – Режим доступу: https://www.sciencedirect.com/topics/computer-science/network-functionality – Назва з екрану. – Дата звернення: 12. 05.2025.

34. Functionality of computer networks [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/functionality-of-computer-network/ – Назва з екрану. – Дата звернення: 12. 05.2025.

35. 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: 14. 05.2025.

36. 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: 14. 05.2025.

37. 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%9

D%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%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B1%D1%83%D0%B4%D0%B8%D0%BD%D0%BA%D1%96%D0%B2%20%D1%96.pdf – Назва з екрану. – Дата звернення: 14. 05.2025.

38. 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: 14. 05.2025.