Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комп'ютерна мережа школи з розмежуванням доступу
Назва теми

КРКІ 2001125.24.01.03 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Програмування та захист комп'ютерних систем і мереж»
Назва

Виконав: студент III курсу, група КІ1с–20–1 _____ В.О. Пасічник
Підпис Ініціали, прізвище

Керівник _____ Ю.П. Кльоц
Підпис, дата Ініціали, прізвище

Нормоконтролер 15.06.23 С.В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри
кібербезпеки _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

«_____» _червня_ 2023 р.

Хмельницький 2023

№ рядка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КРКІ 200225.20.01.03 ПЗ	Комп'ютерна мережа	65		
			школи з розмежуванням			
			доступу			
			пояснювальна записка			
2		КРКІ 200225.20.01.03 Е8	Логічна топологія мережі	1		
3		КРКІ 200225.20.01.03 Е8	Фізична топологія мережі	1		
4		КРКІ 200225.20.01.03 Е8	Система адресації мережі	1		

Зм	Арк	№ докум	Підпис	Дата	КРКІ 200225.20.01.03 ВП		
Розробив		Пасічник В.О.			Комп'ютерна мережа школи з розмежуванням доступу Відомість проєкту	Літера	Аркуш	Аркушів
Перевір.		Кльоц Ю.П.				У	1	1
						ХНУ, КІ1с-20-1		
Н. контр.				15.06				
Затв.								

6. Консультанти розділів дипломного проекту (роботи)

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

7. Дата видачі завдання «_1_»_____03_____2023 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	Лютий	
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	Березень	
3	Робота над розділом 1 – дослідження предметної області та постановка задачі	Березень	
4	Робота над розділом 2 – формування вимог	Квітень	
5	Робота над розділом 3 –реалізація комп'ютерної мережі	Квітень	
6	Оформлення пояснювальної записки згідно вимог	Травень	
7	Попередній захист ВКР	Травень	
8	Захист ВКР на засіданні ЕК	Червень	

Студент _____ В.О. Пасічник
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Ю.П. Кльоц
Підпис Ініціали, прізвище

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Програмування та захист комп'ютерних систем і мереж»

ЗАТВЕРДЖУЮ

Зав. кафедри Ю.П. Кльоц

" 1 " 03 2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Пасічнику Владиславу Олеговичу

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Комп'ютерна мережа школи з розмежуванням доступу.
Керівник проекту (роботи) Кльоц Юрій Павлович к.т.н., доцент

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 01.03.2022 р. № 5

2. Строк подання студентом проекту (роботи) на кафедру 8.06.2022 р.

3. Вихідні дані до проекту (роботи) Завдання кваліфікаційної роботи полягає в проектуванні комп'ютерної мережі школи, яка дозволить розмежувати доступи до ресурсів мережі. Забезпечення покриття школи швидким Wi-Fi. Забезпечити відеоспостереження в кожному класі та місцях загального використання з мінімізацією «сліпих зон». Систему відеоспостереження реалізувати відокремленою кабельною мережею. Забезпечити дротовим інтернетом стаціонарні комп'ютери (директори, завучі, вчительська, допоміжні підрозділи, комп'ютерні класи) та інші стаціонарні пристрої (телевізори, мультимедійні панелі тощо).

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Дослідити предметну область, існуючі рішення та провести аналіз наявних проблем та вимог до мережі, свормувати постановку задачі.
Розробити політики безпеки для уіх користувачів мережі
Розробити логічну та фізичну топологію мережі

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

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Комп'ютерна мережа школи з розмежуванням доступу».

Автор роботи: Пасічник Владислав Олегович.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 63 с., 22 рис., 4 табл., 3 дод., 40 джерел.

Ключові слова: комп'ютерна мережа, Cisco, віртуальні мережі, права доступу, ролі доступу.

Метою роботи є проєктування та реалізація комп'ютерної мережі школи з розмежуванням доступу.

Об'єктом дослідження є комп'ютерна мережа школи з розмежованим доступом користувачів в інструментарії візуального моделювання Cisco Packet Tracer.

Предметом дослідження є комп'ютерні мережі з розмежованим доступом користувачів, способи реалізації демілітаризованої зони в комп'ютерних системах.

Практична цінність роботи полягає в спроектованій та змодельованій комп'ютерній мережі школи з розмежованим доступом користувачів, що забезпечує на високому рівні потреби усіх груп користувачів на має можливості розширення кількості користувачів.

07.06.2023

ABSTRACT

Topic of the qualification work: "School Computer Network with Access Segmentation."

Author of the work: Vladyslav Olegovich Pasichnyk.

Supervisor of the work: Yuriy Pavlovich Klots.

Explanatory note: 63 pages, 22 figures, 4 tables, 3 appendices, 40 sources.

Graphiv part: 3 posters.

Keywords: computer network, Cisco, virtual networks, access rights, access roles.

The aim of the work is to design and implement a computer network for a school with access segmentation.

The object of the research is the computer network of the school with segmented user access using Cisco Packet Tracer visual modeling tools.

The subject of the research is computer networks with segmented user access and methods of implementing a demilitarized zone in computer systems.

The practical value of the work lies in the designed and modeled computer network for the school with segmented user access, which meets the high-level needs of all user groups and allows for scalability in terms of the number of users.

07.06.2023

ЗМІСТ

					КРКІ 2001125.24.01.03 ПЗ		
Зм.	Арк	№докум.	Підпис	Дата			
Виконав		*Пасічник В.О.*			Комп'ютерна мережа школи з розмежуванням доступу Пояснювальна записка	Літера	Аркуш 2 / Аркушів 63
Перевір.		*Кльоц Ю.П.*					
Н.контр.				15.06		ХНУ, КІ1с-20-1	
Затвер.							

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

AAA – Authentication, authorization and accounting

CLI – Command line interface

DMZ – Demilitarized zone

DNS – Domain name system

DHCP – Dynamic host configuration protocol

FTP – File transfer protocol

LAN – Local area network

NAT – Network address translation

PAT – Port Address Translation

SSH – Secure shell

VLAN – Virtual local area network

WAN – Wide area network

WLAN – Wireless local area network

ВСТУП

У сучасних умовах неможливо уявити школу без комп'ютерної мережі та доступу до Інтернету. Ця технологія значно покращує роботу будь-якої компанії, надаючи доступ до інформації, обміну документами та різними типами даних. Однак, разом з усіма перевагами, з'являються й певні виклики. Використання Інтернету вимагає вирішення проблеми безпеки і захисту інформації, а також забезпечення захисту всієї локальної мережі.

Питання безпеки стає особливо важливим, коли компанія має публічні інтернет-сервіси, такі як веб-сервери, файлові сервери і сервіси для поштової розсилки, які розміщені в локальній комп'ютерній мережі. Ці сервери доступні для загального використання, що означає, що будь-який користувач може отримати доступ до ресурсів, розміщених на веб-сервері або до файлового сервера без авторизації або автентифікації. Це створює ризик того, що разом із електронним листом може потрапити шкідливе програмне забезпечення, а серед тисяч користувачів можуть бути особи, які з мотивів конкуренції або особистих цілей намагатимуться отримати доступ до локальної мережі організації.

Якщо хакер отримає доступ до одного з комп'ютерів локальної мережі, він може отримати доступ до широкого спектру паролів, від простих користувачів до адміністраторів. Це дозволить йому отримати доступ до всієї інформації, що обробляється або зберігається в мережі. Крім того, якщо він отримає доступ до веб-сервера, зловмисник може навмисно заблокувати доступ до всіх ресурсів, що може призвести до недоступності важливих послуг та збоїв у роботі організації.

Основною метою роботи є розробка та впровадження комп'ютерної мережі школи з розмежованим доступом користувачів.

Об'єктом дослідження є інформаційні потоки, та дії користувачів мережі школи, які будуть моделюватись з використанням інструментарію візуального моделювання Cisco Packet Tracer.

1 ДОСЛІДЖЕННЯ ВИМОГ, ЗАСОБІВ ТА ПІДХОДІВ ДО ПРОЕКТУВАННЯ МЕРЕЖІ ШКОЛИ

1.1 Потреби та вимоги до комп'ютерної мережі школи

Успішна реалізація комп'ютерної мережі в школі вимагає ретельного аналізу потреб та вимог, які можуть виникнути в освітньому середовищі. Ці вимоги та потреби можуть варіюватися залежно від конкретної школи та освітніх вимог, але їх аналіз може допомогти визначити оптимальний підхід до розробки рішень з розмежуванням доступу в комп'ютерній мережі школи.

Основні потреби та вимоги, які можуть виникати у багатьох шкіл, включають [xxx]:

– Забезпечення високої доступності та надійності мережі. Мережа школи повинна бути доступною для використання вчителями та учнями під час всього робочого дня. Вона повинна бути надійною, безперебійною та забезпечувати стабільний доступ до ресурсів мережі, таких як Інтернет, електронні ресурси, електронна пошта тощо.

– Забезпечення високої швидкості та пропускної здатності. Шкільна мережа повинна мати достатню швидкість та пропускну здатність, щоб забезпечити ефективну роботу вчителів та учнів з використанням різноманітних мультимедійних ресурсів, веб-додатків, відео- та аудіоматеріалів тощо.

– Забезпечення безпеки мережі. Мережа школи повинна бути захищена від загроз безпеки, таких як несанкціонований доступ до мережі, віруси, шкідливі програми, зловмисники тощо. Забезпечення захисту персональних даних учнів та вчителів є також важливою вимогою.

– Забезпечення відповідності до нормативно-правових вимог. Мережа школи повинна відповідати вимогам національного та регіонального законодавства щодо використання Інтернету в освітніх установах, зокрема щодо захисту дітей від шкідливого контенту, дотримання авторських прав, захисту персональних даних, використання безпечних інтернет-ресурсів тощо.

– Забезпечення ефективного управління мережею. Мережа школи повинна мати зручний і ефективний механізм управління, який дозволяє адміністраторам мережі керувати ресурсами, контролювати доступ користувачів, проводити моніторинг стану мережі, здійснювати резервне копіювання та відновлення даних, вирішувати технічні проблеми тощо.

– Забезпечення розширених можливостей мережі. Залежно від освітніх потреб школи, можуть виникати вимоги до розширених можливостей мережі, таких як підтримка відеоконференцій, використання віртуальних середовищ для навчання, підтримка віддаленого доступу до ресурсів мережі тощо.

– Забезпечення відповідності бюджетним обмеженням. Однією з важливих вимог є відповідність мережі бюджетним обмеженням школи. Вимоги до мережі повинні бути в межах фінансових можливостей школи, забезпечуючи оптимальний баланс між функціональністю мережі та фінансовими ресурсами.

Основними чинниками, що впливають на проектовану мережу є:

– Загальна кількість користувачів мережі впливає на потужність обладнання та вибір топології мережі.

– Кількість груп користувачів, що відрізняються вимогами до мережі та правами доступу.

– Трафік, що споживається користувачем, ритмічність завантаження каналу, потреба в пріоритезації трафіку, що використовується для голосового зв’язку та відеоконференцій.

– Необхідність доступу до локальних та зовнішніх ресурсів мережі, як то локальні сервери для зберігання навчального контенту,

– Способи підключення до мережі, а саме стаціонарні користувачі кабелем або Wi-Fi, рухомі користувачі – Wi-Fi.

– Площа, на якій розгорнута мережа впливає на вибір місця розташування вузлів мережі, комутаторів, точок доступу, їх типу та розташування.

1.2 Огляд мережевих архітектур для реалізації мережі школи.

Для побудови мережі школи можна використати різні архітектури мережі, залежно від вимог та потреб школи.

1.2.1 Ієрархічна архітектура мережі.

Ієрархічна архітектура мережі - це підхід до побудови комп'ютерної мережі, де вузли мережі організовані в ієрархічну структуру з різними рівнями абстракції та функцій. Кожен рівень має свої визначені обов'язки і виконує конкретні функції, що дозволяє розподілити навантаження та забезпечити ефективну організацію та керування мережею.

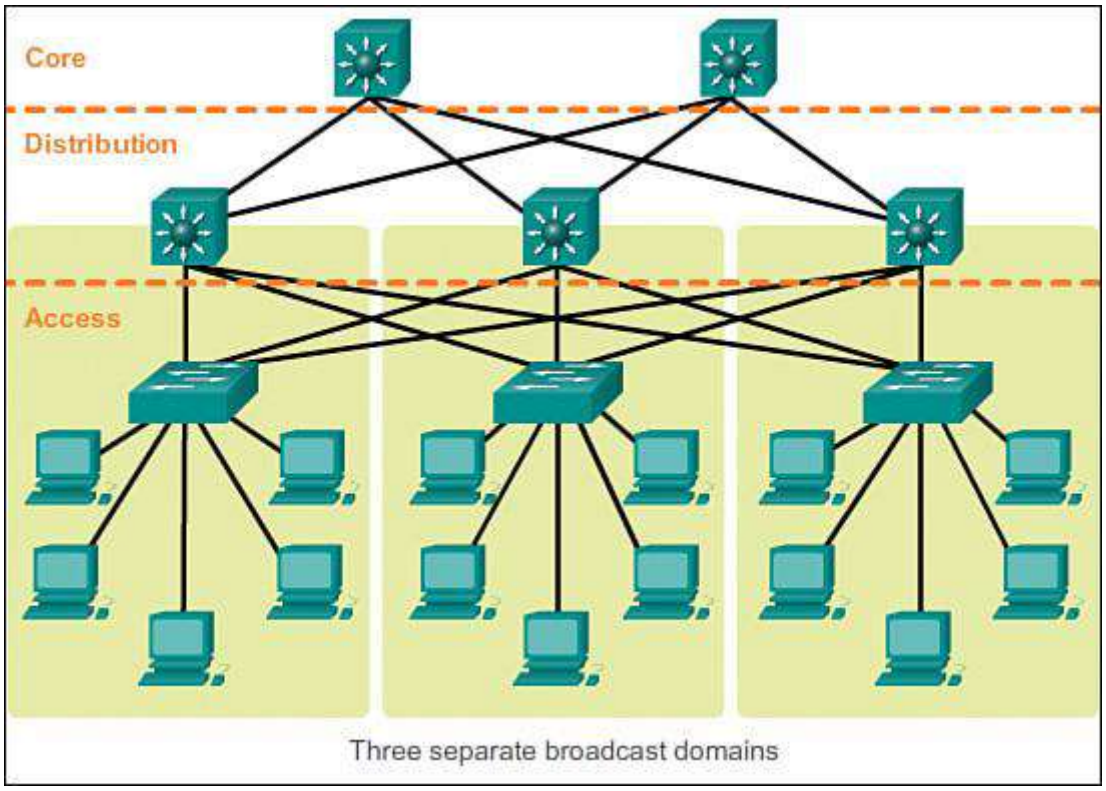


Рисунок 1.1 Ієрархічна архітектура мережі

Ієрархічна архітектура передбачає використання різних рівнів мережі зі строгим розподілом функцій та відповідальностей між ними. Наприклад, використовуються центральні комутатори на рівні корпусу школи, що

забезпечують зв'язок між різними відділеннями або підсистемами школи, а також розподіляють мережевий трафік до рівнів мережі в кожному відділенні чи класі.

Визначають наступні рівні ієрархічної архітектури мережі.

Рівень доступу (Access Layer). Це найнижчий рівень, який забезпечує з'єднання мережевих кінцевих пристроїв, таких як комп'ютери, телефони, принтери і т. д., з мережевою інфраструктурою. Він використовує комутатори або точки доступу до мережі (Access Points) для забезпечення локального доступу до мережі та розподілу трафіку між різними пристроями в мережі.

Рівень дистрибуції (Distribution Layer). Цей рівень виконує функції розподілу трафіку, маршрутизації, керування політиками безпеки та керування багатошвидкісними зв'язками між різними сегментами мережі. Він використовує мережеві пристрої, такі як маршрутизатори, комутатори серії Distribution, файрволи тощо.

Рівень корпоративного ядра (Core Layer). Це центральний рівень мережі, який забезпечує високошвидкісний обмін даними між різними розподіленими ресурсами. Він використовує високопродуктивні мережеві пристрої, такі як комутатори серії Core, маршрутизатори великого масштабу, оптичні мережеві пристрої тощо. Рівень корпоративного ядра забезпечує швидкий та надійний обмін даними між різними вузлами мережі та є основою для побудови високопродуктивних та відмовостійких мереж.

До ієрархічної архітектури мережі також можуть входити інші рівні в залежності від потреб конкретної мережі, такі як рівень кампусу (Campus Level) або рівень провайдера послуг (Service Provider Level) у випадку великих мереж, що включають кілька кампусів або мають підключення до різних провайдерів послуг.

Рівень підключення до зовнішніх мереж (WAN Connectivity). Це може бути окремий рівень, що забезпечує зв'язок з зовнішніми мережами, такими як Інтернет або віддалені підрозділи. В цьому рівні використовуються мережеві пристрої, такі як маршрутизатори, мережеві шлюзи для забезпечення зовнішнього зв'язку компанії зі світовою мережею.

Рівень сервісів (Services). Це може бути окремий рівень, де розташовані різноманітні мережеві сервіси, такі як сервери DHCP, DNS, проксі-сервери,

файрволи, системи безпеки та інші сервіси мережі, які забезпечують додаткові функції мережі.

Ієрархічна архітектура мережі дозволяє розділити мережеві функції на різні рівні, забезпечує масштабованість, керованість та ефективність мережі. Кожен рівень може мати свої особливості, такі як налаштування безпеки, маршрутизацію, комутацію та інші, відповідно до потреб мережі і бізнес-вимог організації.

Зазвичай, в ієрархічній архітектурі мережі використовуються різні типи мережевих пристроїв на кожному рівні. Наприклад, на рівні доступу можуть бути використані комутатори або точки доступу Wi-Fi для підключення кінцевих пристроїв, таких як комп'ютери, телефони або інші мережеві пристрої. На рівні дистрибуції можуть бути використані маршрутизатори або комутатори з розширеними функціями мережі, які забезпечують розподіл трафіку між різними сегментами мережі та реалізацію політик безпеки. На рівні корпоративного ядра можуть використовуватись маршрутизатори великого масштабу або комутатори з високою пропускною здатністю, які забезпечують високий рівень доступності та надійності мережі.

Інша важлива характеристика ієрархічної архітектури мережі - це керованість. Керування може здійснюватися централізовано або розподілено між різними рівнями. Наприклад, на рівні доступу може бути локальне керування для налаштування параметрів доступу до мережі на рівні вузлів, тоді як на рівні дистрибуції та корпоративного ядра може бути централізоване керування, включаючи налаштування маршрутизації, політик безпеки та інші настройки.

Ще одна важлива перевага ієрархічної архітектури мережі – це масштабованість. Додавання нових вузлів або збільшення обсягу трафіку в мережі може бути відносно простим, оскільки мережа може бути розширена на рівні доступу або дистрибуції без необхідності перепроектування корпоративного ядра. Це робить ієрархічну архітектуру мережі гнучкою та масштабованою.

Однак, також варто враховувати, що ієрархічна архітектура мережі може мати свої недоліки. Наприклад, вона може бути складною в налаштуванні та управлінні, особливо в великих мережах з багатьма рівнями. Також, введення

зайвих рівнів в архітектурі може призвести до збільшення затримок та зменшення продуктивності мережі.

Загалом, ієрархічна архітектура мережі є поширеним підходом до проектування мережі, який дозволяє досягти масштабованості, керованості та ефективності роботи мережі. Вона використовує різні рівні мережевих пристроїв, розподіляє функції та відповідальність між різними рівнями та забезпечує гнучкість та розширюваність мережі.

1.2.2 Стелс-архітектура мережі.

Ця архітектура передбачає використання різних місцевих мереж, які фізично розділені одна від одної і підключені до центрального комутатора або мережевого сервісу. Це дозволяє забезпечити фізичний розподіл мережі, що забезпечує високу надійність та незалежність різних відділень або підсистем школи.

Стелс-архітектура мережі - це підхід до проектування та розгортання комп'ютерних мереж, який має на меті забезпечення високого рівня захисту від виявлення та блокування мережевої активності з боку зовнішніх або внутрішніх загроз. Цей підхід використовує ряд технік, протоколів, алгоритмів та технологій для зниження відслідкованості мережі та забезпечення конфіденційності, цілісності, автентифікації та доступності даних.

Основні риси стелс-архітектури мережі включають набір параметрів.

Прихованість (Concealment). Стелс-мережі прагнуть знизити свою візуальну та радіопомітність, тобто забезпечити прихованість своєї наявності в мережі. Це може бути досягнуто за допомогою різних методів, таких як шифрування, стеганографія, застосування мережевих тунелей, техніків камуфляжу та інших приховувальних технік.

Розподілена архітектура (Distributed Architecture). Стелс-мережі можуть використовувати розподілену архітектуру, де функції мережі розподіляються між різними вузлами, що робить важким виявлення центральних точок атаки або однієї точки входу.

Мінімальні сліди (Minimal Footprint). Стелс-мережі прагнуть мінімізувати сліди, які залишаються в мережі, такі як логи, аудит-записи та інші відомості, які можуть використовуватися для виявлення мережевої активності. Це може бути досягнуто за допомогою використання криптографії, анонімізації даних, видалення слідів активності та інших технік, що забезпечують мінімальний відбиток діяльності мережі.

Захист від виявлення (Detection Avoidance). Стелс-архітектура мережі включає заходи, що запобігають виявленню мережевої активності з боку зовнішніх або внутрішніх загроз. Це може бути досягнуто шляхом використання різних методів, таких як динамічна зміна мережевих характеристик, випадковий вибір шляхів, використання різноманітних портів, технік обхилу від виявлення та інших підходів, які ускладнюють виявлення мережевої активності.

Резистентність до атак (Resilience to Attacks). Стелс-мережі розробляються з урахуванням резистентності до різних видів атак, таких як аналіз трафіку, атаки на протоколи, злам паролів та інші загрози. Для цього використовуються різноманітні заходи, такі як криптографічні методи, фільтрація трафіку, системи виявлення вторгнень (IDS), багатоетапна автентифікація та авторизація, контроль доступу та інші техніки захисту.

Гнучкість та масштабованість (Flexibility and Scalability). Стелс-архітектура мережі дозволяє розгортати та налаштовувати мережу залежно від потреб, забезпечуючи гнучкість та масштабованість. Це дозволяє адаптувати мережу до змінних умов, забезпечувати високий рівень ефективності та надійності, а також реагувати на нові загрози та виклики без значних переребудов або деградації функціональності.

Шифрування та автентифікація (Encryption and Authentication). Захист даних в стелс-мережах забезпечується за допомогою різних методів шифрування та автентифікації. Використання криптографічних алгоритмів дозволяє захистити дані від несанкціонованого доступу та забезпечити конфіденційність та цілісність даних, переданих через мережу.

Захист від внутрішніх загроз (Insider Threat Protection). Стелс-архітектура мережі включає заходи для захисту від внутрішніх загроз, таких як

несанкціонований доступ зсередини мережі, виток даних від внутрішніх користувачів та інші атаки, що можуть виникнути зсередини мережі. Це може бути досягнуто за допомогою різних методів, таких як використання ролей та прав доступу, систем виявлення вторгнень, аудиту та моніторингу діяльності користувачів та інші підходи.

Незалежність від певних технологій (Technology Independence). Стелс-архітектура мережі дозволяє використовувати різні технології та протоколи залежно від потреб і вимог організації. Це забезпечує незалежність від певних виробників або технологій, що дозволяє використовувати найкращі рішення на ринку та забезпечити високий рівень гнучкості та розширюваності мережі.

Це загальні принципи стелс-архітектури мережі, які можуть бути використані для розробки різних типів стелс-мереж, таких як стелс-мережі зв'язку, стелс-мережі даних, стелс-мережі IoT (розумних речей) та інші. Кожен тип стелс-мережі може мати свої властивості та вимоги, але загальні принципи захисту та незамітності є спільними для всіх стелс-мереж.

Ціль стелс-архітектури мережі - забезпечити високий рівень захисту від різних видів загроз, таких як розпізнавання, виявлення та атаки, зберігаючи при цьому непомітність мережі для потенційних загроз. Використання таких технік, як камуфляж, маскування, захист від аналізу, шифрування, автентифікація та інші, допомагає забезпечити стійкість мережі до різних атак та зберегти її конфіденційність, цілісність та доступність.

Стелс-архітектура мережі може бути застосована в різних сферах, таких як військова та розвідувальна діяльність, комерційний сектор, промисловість, медична техніка, автономні транспортні засоби та інші, де конфіденційність, захист даних та незамітність мережі є важливими факторами.

Важливо відзначити, що стелс-архітектура мережі не є універсальним рішенням та має свої обмеження. Вона може вимагати високого рівня експертизи та ресурсів для реалізації та підтримки, а також може мати певні обмеження в продуктивності та ефективності мережі. Застосування стелс-архітектури мережі повинно бути відповідно до вимог та контексту конкретної організації або проекту.

1.2.3 Комбінована архітектура мережі.

Ця архітектура передбачає використання різних типів мереж, таких як провідні мережі (Ethernet), бездротові мережі (Wi-Fi) та віртуальні приватні мережі (VPN), для реалізації мережевої інфраструктури школи. Наприклад, провідна мережа може використовуватися для підключення стаціонарних комп'ютерів та серверів, Wi-Fi може використовуватися для мобільних пристроїв та доступу віддалених користувачів, а віртуальні приватні мережі (VPN) можуть використовуватися для забезпечення безпеки та захисту даних мережі.

1.2.4 Мережа з розподіленою архітектурою.

Ця архітектура передбачає використання розподіленої мережевої інфраструктури, де різні відділення або підсистеми школи можуть мати власні мережеві ресурси, такі як комутатори, маршрутизатори, сервери тощо. Це дозволяє забезпечити локальний контроль та керування мережею в кожному відділенні, а також знижує вплив на мережевий трафік між відділеннями.

1.2.5 Віртуалізована архітектура мережі.

Ця архітектура передбачає використання віртуалізації для створення віртуальних мереж та ресурсів. Наприклад, може бути використана віртуалізація комутаторів, маршрутизаторів, серверів та інших мережевих пристроїв для створення гнучкої та масштабованої мережі школи.

Фізичні мережеві ресурси групуються і абстрагуються від віртуальних об'єктів, які можуть бути легко керуватися та конфігуруватися за допомогою програмного забезпечення. При використанні віртуалізованої архітектури мережі можна розділити мережеві служби і функціональність, що дозволяє вирішувати різні задачі на різних рівнях. Віртуалізована архітектура мережі дозволяє забезпечити більшу безпеку шляхом централізованого керування доступом та застосуванням політик безпеки на рівні віртуальних об'єктів.

Застосування віртуалізованої архітектури мережі вимагає використання відповідного вартісного обладнання.

1.3 Потреби у розмежуванні доступу для користувачів мережі.

Розмежування доступу для користувачів мережі є важливим аспектом управління мережевою інфраструктурою та забезпечення безпеки. Основна потреба у розмежуванні доступу полягає в тому, щоб кожен користувач мав обмежений доступ лише до ресурсів і даних, необхідних для виконання його ролі та обов'язків.

Користувачі мережі можуть мати різні рівні доступу залежно від їхньої ролі або положення в організації. Наприклад, адміністратори мають права по налаштуванню системи, ресурсів та адміністрування користувачів, звичайні користувачі мають обмежений доступ лише до необхідних додатків та даних. Мережу варто розділити на логічні сегменти, щоб розділити трафік та ресурси. Це допомагає запобігти небажаному доступу до конфіденційної інформації, забезпечити локалізацію проблем у мережі. Кожен користувач мережі повинен бути автентифікований перед отриманням доступу до ресурсів. Додатково, можуть бути встановлені політики безпеки, що визначають які ресурси і функції доступні для кожного користувача. Розмежування доступу також сприяє можливості моніторингу та аудиту дій користувачів. Це дозволяє виявляти незвичайну або підозрілу активність, встановлювати журнали подій та виконувати аналіз безпеки мережі.

Загалом, розмежування доступу допомагає забезпечити конфіденційність, цілісність та доступність мережевих ресурсів, а також мінімізувати ризики зовнішніх атак і внутрішніх загроз у мережі.

Реалізація розмежування доступу може бути проведена різними способами. Серед них найбільш поширеними є розподіл мережі на віртуальні підмережі. VLAN дозволяють розділити мережу на логічні групи, незалежно від фізичної структури. Кожна VLAN може мати власні правила доступу та політики безпеки, що дозволяє

контролювати комунікацію між користувачами в різних VLAN. Для контролю комунікації між різними VLAN використовують міжмережеві екрани (фаєрволи). Фаєрвол використовується для контролю трафіку між різними сегментами мережі. Вони можуть фільтрувати трафік на основі IP-адрес, портів, протоколів та інших параметрів. Файерволи дозволяють встановлювати правила доступу, обмежувати певні види трафіку та забезпечувати безпеку мережі. Використання систем управління доступом дозволяє централізовано керувати правами користувачів по доступу до мережевих ресурсів. Вони використовують різні методи автентифікації, такі як логіни/паролі, сертифікати, двофакторну аутентифікацію тощо, та забезпечують авторизацію користувачів залежно від їхніх прав доступу.

Застосування шифрування трафіку, наприклад, за допомогою протоколу SSL/TLS, дозволяє забезпечити конфіденційність інформації, що передається по мережі. Це допомагає захистити дані від несанкціонованого доступу. Використання шифрованого трафіку передбачає отримання усіма користувачами апаратних або програмних ключів доступу. Зазвичай використання шифрованого трафіку використовується в системах, де циркулює секретна інформація. Для веб-додатків, що не використовують секретні дані достатньо використання протоколу HTTPS, що базується на сертифікатах SSL/TLS.

1.4 Постановка задачі.

Проведений аналіз можливих рішень реалізації мережі школи підтверджує, що використання архітектури SOHO мережі не прийнятний для школи, оскільки не забезпечує належний рівень безпеки мережі та користувачів.

З огляду на це необхідно розробити мережу, що має відповідати таким вимогам:

– топологія мережі – зірка;

– кабельна мережа між основними вузлами – одномодове оптоволокно, від вузла до кінцевого пристрою – мідний кабель UTP cat. 5E;

– фізично відокремлений сегмент відеоспостереження;

– ядро мережі – маршрутизатор та файрвол;

– рівень дистрибуції – керовані комутатори L3 з вхідними оптичними портами;

– розподіл мережі на VLAN з метою ізоляції різних частин мережі;

– використання ролей користувачів для розмежування доступу до ресурсів мережі;

– використання точок доступу Wi-Fi, що підтримують multySSID;

– маршрутизатори, сервери та файрволи повинні бути розміщені в спеціалізованому приміщенні з обмеженим доступом – серверній;

– необхідно використати сервер LDAP для зберігання облікових записів користувачів, їх ролей та авторизації при доступі до ресурсів мережі;

– розробити логічну та фізичну топології мережі.

2 ПРОЕКТУВАННЯ МЕРЕЖІ ШКОЛИ

2.1 Політики безпеки та правила розмежування доступу

Політика безпеки встановлює загальні принципи та цілі, які визначаються організацією або компанією для забезпечення конфіденційності, цілісності та доступності інформації. Вона визначає, які види діяльності є припустимими і недопустимими, а також встановлює відповідальності за порушення політики безпеки.

Правила розмежування доступу визначають, які користувачі або групи користувачів мають доступ до певних ресурсів або функцій інформаційної системи. Ці правила встановлюються для обмеження доступу лише до тих ресурсів, які є необхідними для виконання роботи або обов'язків користувача. Вони можуть бути засновані на різних критеріях, таких як ролі користувачів, рівні довіри, поточний контекст автентифікації тощо.

Існує кілька основних методів реалізації політики безпеки та правил розмежування доступу:

– Автентифікація і авторизація. Цей метод включає процес ідентифікації користувачів (автентифікацію) та надання прав доступу до ресурсів на основі їхньої ідентифікації (авторизація). Часто використовуються паролі, сертифікати, біометричні дані або токени для автентифікації користувачів.

– Ролева модель доступу. Цей підхід включає визначення різних ролей, які мають доступ до певних ресурсів, і надання прав доступу на основі приналежності до певної ролі. Користувачі можуть мати одну або декілька ролей, і кожній ролі призначається набір дозволених дій.

– Модель дозволів на основі принципу "найменшого привілею". Ця модель передбачає, що користувачеві надаються лише ті дозволи, які необхідні для виконання його роботи або обов'язків. Це зменшує ризик випадкового або зловмисного доступу до конфіденційної інформації.

– Аудит та моніторинг. Цей аспект включає збір і аналіз журналів подій та дій користувачів для виявлення потенційних загроз безпеці інформації. Системи аудиту можуть зафіксовувати спроби несанкціонованого доступу, зміни конфігурацій і інші підозрілі дії.

Оскільки розробляється мережа школи основними користувачами будуть учні, вчителі та адміністрація школи. Додатковими користувачами можуть бути допоміжний персонал, батьки учнів та інші відвідувачі.

Виходячи з цього потрібно провести аналіз потреб усіх користувачів мережі.

Тому необхідно визначити права, якими мають володіти користувачі мережі.

Права учнів:

– доступ до особистого кабінету веб-системи підтримки навчання (перегляд оцінок та домашніх завдань);

– доступ до корпоративної поштової скриньки;

– доступ до системи відеозв’язку;

– доступ до локальних навчальних ресурсів мережі школи;

– доступ до хмарних навчальних ресурсів мережі школи;

– доступ до месенджерів;

– доступ до обмеженого типу веб-ресурсів мережі інтернет.

Права вчителів:

– доступ до особистого кабінету веб-системи підтримки навчання (внесення уроків, виставлення оцінок, внесення домашніх завдань, контроль успішності учнів);

– доступ до корпоративної поштової скриньки;

– доступ до системи відеозв’язку;

– доступ до локальних навчальних ресурсів мережі школи;

– доступ до хмарних навчальних ресурсів мережі школи;

– доступ до месенджерів;

– доступ до веб-ресурсів мережі інтернет.

Права адміністрації:

– доступ до особистого кабінету веб-системи підтримки навчання (формування навчальних планів, розкладу занять, контроль роботи вчителів, аналіз якості навчання учнів);

– доступ до корпоративної поштової скриньки;

– доступ до системи відеозв’язку;

– доступ до локальних навчальних ресурсів мережі школи;

– доступ до хмарних навчальних ресурсів мережі школи;

– доступ до месенджерів;

– доступ до веб-ресурсів мережі інтернет.

Права допоміжного персоналу:

– доступ до особистого кабінету веб-системи підтримки навчання (перегляд розкладу занять);

– доступ до корпоративної поштової скриньки;

– есурсів мережі школи;

– доступ до месенджерів;

– доступ до веб-ресурсів мережі інтернет.

Права батьків:

– доступ до особистого кабінету веб-системи підтримки навчання (перегляд оцінок та домашніх завдань);

– доступ до локальних навчальних ресурсів мережі школи;

– доступ до хмарних навчальних ресурсів мережі школи;

– доступ до месенджерів;

– доступ до веб-ресурсів мережі інтернет.

Права гостей:

– доступ до месенджерів;

– доступ до веб-ресурсів мережі інтернет.

Аналіз прав користувачів мережі вказує, що лише адміністрація може мати дві ролі (адміністрація і вчитель), решта користувачів постійно працюють з мережею з однією роллю.

Відповідно до цього прийняте рішення забезпечити рольовий доступ для користувачів, авторизацію та автентифікацію користувачів.

Визначено такі ролі в системі:

– адміністратор мережі (має права на зміну налаштувань мережевого обладнання, адміністрування, резервне копіювання та відновлення серверів, реєстрація та зміна ролей користувачів, зміна правил ролей, адміністрування та користування корпоративною поштою);

– адміністратор школи (має права на створення і коригування навчальних планів, формування та перегляд розкладу, формування і перегляд журналів успішності учнів та звітів по роботі вчителів, користування корпоративною поштою);

– вчитель (має права на ведення журналів, виставлення оцінок, формування домашніх завдань, перегляд успішності учнів у класі та розкладу, користування корпоративною поштою);

– учень (має права на перегляд журналів успішності класу та домашніх завдань та розкладу, користування корпоративною поштою);

– допоміжний персонал (має права на перегляд розкладу);

– батьки (має права на перегляд журналів успішності своєї дитини – учня школи, розкладу та домашніх завдань);

– гості (не мають прав на доступ до системи, виключно приєднання до інтернет).

2.2 Топологія мережі та підключення кінцевих користувачів

Топологія комп’ютерної мережі визначає спосіб, яким комп'ютери розташовані і з'єднані між собою. Ця форма або фізичне розташування визначає вимоги щодо типу кабелю, мережевих пристроїв, методів керування обміном даними, можливості розширення мережі та надійності роботи [8-11, 23]. Загалом існує кілька основних типів топології, таких як шина, зірка, кільце або змішана.

В топології "Шина", всі комп'ютери підключаються паралельно до однієї лінії зв'язку, інформація, що надходить від кожного комп'ютера, передається одночасно всім іншим комп'ютерам. В цій топології вимагається, щоб мережеве обладнання було однаковим, а всі абоненти мали однакові права. Оскільки комп'ютери можуть передавати дані лише послідовно через єдину лінію зв'язку, інакше інформація може бути спотворена через конфлікти. В даній топології немає можливості мати сервер, через який передається вся інформація. Також на кінцях шини (кабелю) розташовуються термінатори, які запобігають відображенню сигналу.

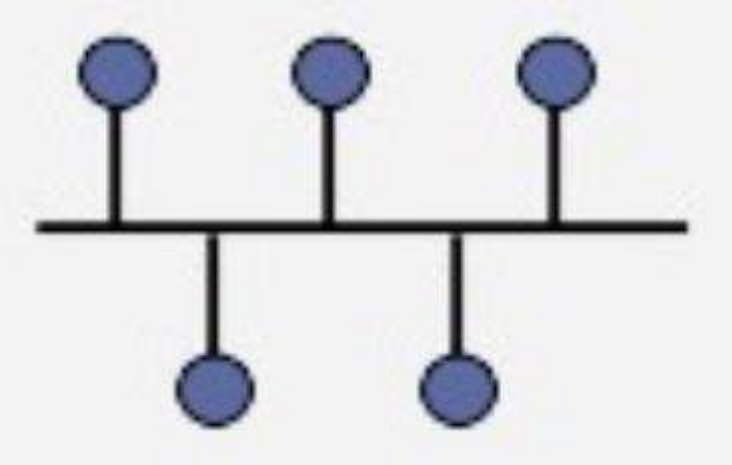


Рисунок 2.1 Топологія «Шина»

Топологія "Зірка" передбачає, що інші периферійні комп'ютери підключаються до одного центрального комп'ютера, використовуючи окремі лінії зв'язку для кожного з них. У цій топології вся комунікація відбувається через центральний вузол, через який іде значне навантаження. Зазвичай центральним вузлом є комутатор, на якому зосереджені функції керування обміном даних.

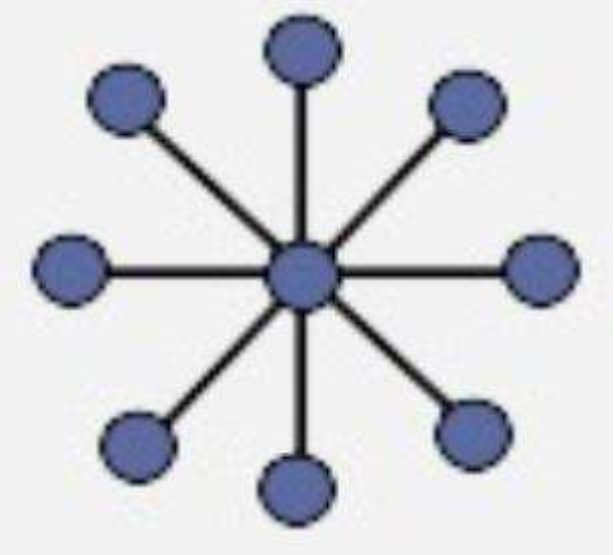


Рисунок 2.3 Топологія «Зірка»

Оскільки керування повністю централізоване, в даній топології виключені конфлікти.

У топології "Кільце" комп'ютери передають інформацію по ланцюжку, постійно передаючи її наступному пристрою в кільці, а отримують інформацію лише від попереднього пристрою в кільці.

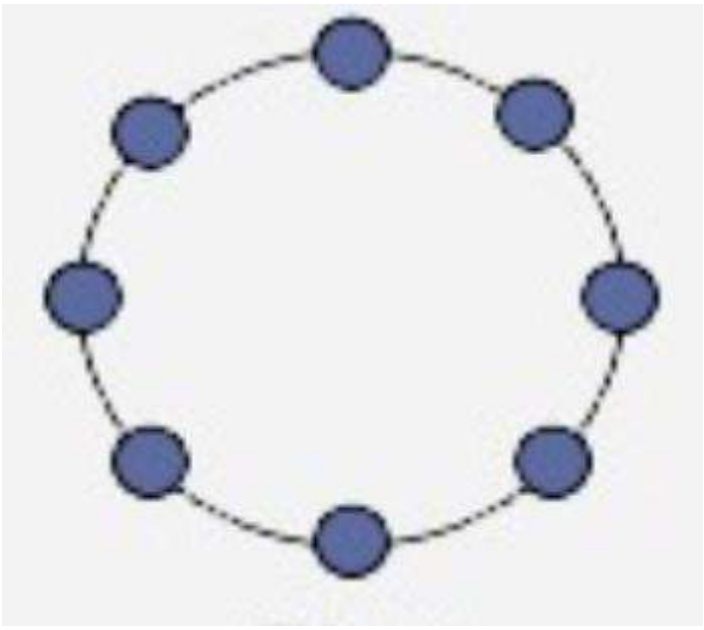


Рисунок 2.3 Топологія «Кільце»

У цій топології відсутній окремий центральний пристрій, але, на відміну від топології "Шина", комп'ютери не є повністю рівноправними. Однак часто в

"Кільці" виділяють спеціального абонента, який виконує керування або контроль над обміном даними. Внаслідок цього, наявність керуючого абонента знижує надійність комп'ютерної мережі, оскільки в разі відмови цього пристрою мережа може припинити свою роботу.

У топології "Змішана" пристрої знаходяться на одному рівні і можуть передавати повідомлення безпосередньо один одному. Це дозволяє знизити навантаження на канали передачі даних. Однак, з такою організацією мережі виникають проблеми з керованістю. В топології "Змішана" відсутня "третя сторона" або арбітр, який міг би вирішувати конфліктні ситуації між різними організаціями або підрозділами в межах однієї організації.

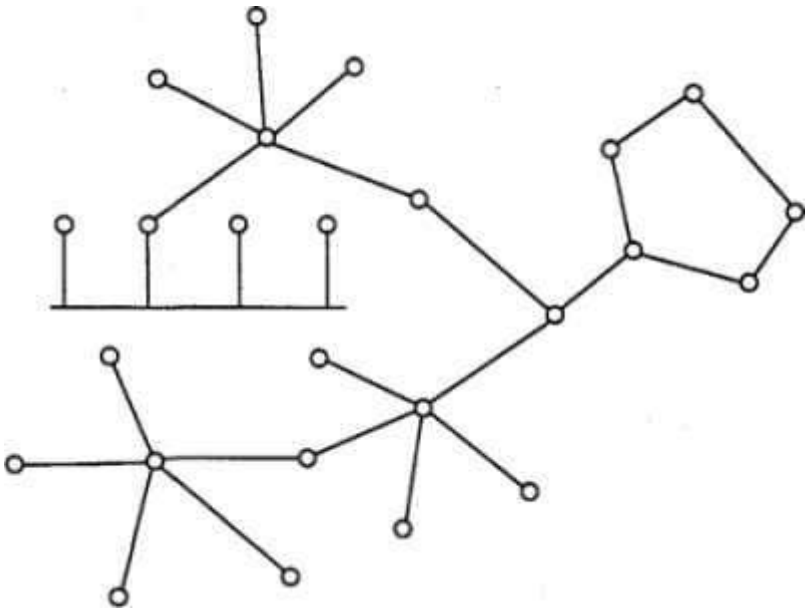


Рисунок 2.3 Топологія «Змішана»

Якщо створюється комп'ютерна мережа школи, рекомендовано використовувати топологію "зірка". Ця топологія є найпоширенішою в сучасних комп'ютерних мережах через наступні переваги, які вона надає:

– вихід з ладу периферійного комп'ютера не має впливу на решту мережі;

– на лінії зв'язку присутні лише два абоненти - периферійний комп'ютер і центральний, що значно спрощує мережеве обладнання порівняно з топологією "шина" і не вимагає додаткових зовнішніх термінаторів;

– пошкодження кабелю в конкретній точці або коротке замикання впливають тільки на один кінцевий пристрій, і решта комп'ютерів можуть продовжувати свою роботу;

– легко виявляти несправності та локалізувати їх;

– висока продуктивність комп'ютерної мережі.

До недоліків топології "Зірка" можна віднести:

– залежність від централізованих систем, таких як мережеве обладнання;

– великі витрати на кабель, у порівнянні з іншими топологіями, що може суттєво підвищити загальну вартість мережі.

Мережа школи займає достатньо велику за площею територію та має досить велику кількість підключених користувачів. Користувачі використовують як дротовий так і бездротовий способи підключення. Зазвичай стаціонарне обладнання (персональні комп’ютери, багатофункційні пристрої, телевізори, камери спостереження) підключається за допомогою кабелю. В свою чергу також має бути розвинена бездротова мережа для підключення ноутбуків та смартфонів.

З огляду на те, що школа має підключення лише до одного провайдера і не має критичних задач по доступу до ресурсів доцільно сформувати єдине ядро, що складається з високопродуктивного маршрутизатора та файрвола.

З іншого боку мережеві пристрої розміщені по території школи достатньо рівномірно та на значній відстані один від одного. Це не дозволяє підвести кабелі від усіх проводових пристроїв в серверну та забезпечити єдиний вузол рівня дистрибуції.

Тому для забезпечення ефективного використання кабельних мереж доцільно рівень дистрибуції реалізувати за допомогою трьох вузлів, що розташовані за межами серверної та з’єднані між собою та з серверною оптоволоконними лініями зв’язку. Для реалізації вузлів рівня дистрибуції доцільно використати керовані комутатори, оскільки вони забезпечать підтримку поділу мережі на віртуальні підмережі. Також в вузлах дистрибуції варто розмістити POE комутатори для підключення камер системи відеоспостереження та бездротових точок доступу.

Необхідно врахувати, що для систем відеоспостереження доцільно використати окрему кабельну мережу, в яку крім камер і POE комутаторів включений відеореєстратор.

Оскільки вузел ядра складається з одного маршрутизатора і файрвола, має підключення до одного провайдера, кабельна мережа розміщена всередині приміщення, немає вимог до гарантованого доступу до інтернету то можна не забезпечувати резервування каналів зв'язку рівня дистрибуції. Однак доцільно врахувати, що в школі займаються діти та підлітки, які можуть з особистих мотивів, не усвідомлюючи ступеню відповідальності за наслідки пошкодити лінії зв'язку рівня дистрибуції. Враховуючи це варто резервувати оптоволоконні лінії зв'язку між комутаторами рівня дистрибуції та серверною, це забезпечить стійкість ядра мережі від збоїв та актів вандалізму.

2.3 Обґрунтування вибору мережевих пристроїв для реалізації мережі

Для забезпечення функцій високопродуктивного маршрутизатора варто використовувати маршрутизатори Cisco. Маршрутизатори Cisco представлені серіями: Cisco ISR 4000, Cisco ASR 1000, Cisco ASR 9000, Cisco Catalyst серії 9000, Cisco Nexus серії 9000, Cisco Catalyst серії 6000, Cisco Catalyst серії 4000, Cisco Catalyst серії 3000, Cisco Catalyst серії 2000.

Для забезпечення функцій ядра з урахуванням вартості пристроїв варто використати маршрутизатор Cisco Catalyst 3650 24TS. Він поєднує в собі надійність, продуктивність та технічні можливості по налаштуванню.

Рисунок 2.4 – Маршрутизатор Cisco Catalyst 3650 24TS.

Комутатори Cisco Catalyst 3650 належать до серії пристроїв з фіксованою конфігурацією, які підтримують стекування і мають вбудований бездротовий контролер ASIC. Вони використовують операційну систему IOS XE. Аналогічні ASIC також використовуються в комутаторах Catalyst 3850 і Supervisor 8-E для Catalyst 4500-E. Комутатори Cisco Catalyst 3650 забезпечують політику безпеки та якість обслуговування QoS для провідного та бездротового трафіку клієнтів. Вони також надають можливість моніторингу та оптимізації цього трафіку на рівні доступу до корпоративної мережі.

Основні характеристики моделей Catalyst 3650 включають фіксовану конфігурацію з 24 або 48 портами 10/100/1000 з підтримкою PoE+ (до 30 Вт на порт), вбудовані аплінки (4 x Gigabit Ethernet, 2 x 10 Gigabit Ethernet або 4 x 1) з підтримкою SFP і SFP+, підтримку до 2 відмовостійких джерел живлення змінного струму різної потужності та 3 вентиляторів для охолодження. Крім того, Catalyst 3650 підтримує стекування за допомогою технології StackWise з можливістю до 9 пристроїв у стеку і пропускною здатністю 160 Гб/с, а також технологію SSO (Stateful SwitchOver). Модель також має пропускну здатність бездротової мережі 40 Гб/с на основі ASIC UADP (Unified Access Data Plane) та підтримку до 25 точок доступу та 1000 бездротових клієнтів на один комутатор 3650 або один стек StackWise з комутаторів 3650.

На цей маршрутизатор покладено виконання функцій ядра системи.

В якості комутаторів рівня дистрибуції можна використати високопродуктивні комутатори Cisco Catalyst 2960-X серії, Cisco Catalyst 3650 серії, Cisco Catalyst 3850 серії, Cisco Catalyst 4500-X серії, Cisco Catalyst 6500-E серії, Cisco Nexus 3000 серії, Cisco Nexus 5000 серії, Cisco Nexus 7000 серії, Cisco Nexus 9000 серії.

З огляду на вартість та технічні характеристики доцільно використати керований комутатор Cisco Catalyst 2960.

Рисунок 2.5 – Комутатор Cisco Catalyst 2960

Комутатори Cisco Catalyst 2960 представляють собою лінійку комутаторів з фіксованою конфігурацією, які мають порти Fast Ethernet та Gigabit Ethernet. Вони розроблені для використання в початкових рівнях підприємств та мереж віддалених офісів і надають розширені сервіси локальної мережі (LAN). Комутатори Cisco Catalyst 2960 підтримують передачу голосу, даних та відео, а також забезпечують безпечний доступ до мережі. Вони також надають масштабоване управління, яке може адаптуватися до змін потреб вашого бізнесу.

Комутатори Cisco Catalyst 2960 мають розумні функції, такі як створення складних списків керування доступом (ACL), розширена безпека, комбіновані гігабітні аплінки (мідний Ethernet 10/100/1000BASE-T або SFP-модуль для переходу в інше середовище, таке як Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Крім того, комутатори Catalyst 2960 підтримують функції якості обслуговування (QoS), обмеження швидкості передачі, списки доступу (ACL) на основі MAC- або IP-адрес, портів UDP/TCP та мультикастові сервіси. Вони також дозволяють регулювати швидкість передачі на кожному порту з кроком 64 кбіт, використовувати Link Aggregation для створення швидкісних з'єднань між комутаторами та серверами, налаштовувати транкові з'єднання з використанням тегів 802.1q. Комутатори Catalyst 2960 підтримують до 255 віртуальних локальних мереж (VLAN) на комутатор, до 4000 ідентифікаторів VLAN та керування через Cisco Network Assistant. Вони також доступні з різними версіями прошивки, такими як LAN Base та Lan Lite Image, з різними рівнями функціональності, включаючи покращену безпеку (ACLs), DHCP Snooping, Web authentication, розширення 802.1x, можливості установок якості обслуговування (QoS), підтримку надлишкового живлення RPS та велику кількість SFP-портів. Крім того, вони мають функції Flex Links, Link State Tracking,

підтримують до 256 VLAN, IPv6 Host, MLD Snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82, IP SLA (responder) та інші.

Для забезпечення бездротового сегменту необхідно вибрати точки доступу. В якості точок доступу аналізувались такі: Cisco Aironet 1800 серії, Cisco Aironet 2800 серії, Cisco Aironet 3800 серії, Cisco Catalyst 9100 серії, Cisco Meraki MR серії, Cisco Small Business WAP серії, Cisco Mobility Express серії.

Cisco Aironet 4800 – це серія універсальних точок доступу високої продуктивності з чотирма вбудованими внутрішніми антенами. Вона відрізняється унікальною функцією гнучкого змінювання режиму роботи радіо модулів.

Також точки доступу підтримують Hyperlocation і мають вбудовані модулі Bluetooth Low Energy.

Рисунок 2.6 – Точка доступу Cisco AIR-AP4800-E-K9

Основні особливості:

– Підтримка поточного бездротового протоколу 802.11ac Wave 2, що забезпечує теоретичну пропускну здатність до 2,6 Гбіт/с.

– Підтримка архітектури віртуальної цифрової мережі Cisco DNA.

– Унікальна радіочастотна архітектура, включаючи запатентовані технології шумоподавлення "Cross-AP Noise Reduction" та оптимізованого роумінгу, для створення надійного бездротового покриття в густонаселених мережах.

– Технологія MU-MIMO з трьома потоками 4x4, що дозволяє розділяти потоки даних від різних клієнтів і збільшує пропускну здатність.

– Підтримка Multigigabit Ethernet.

– Технологія Intelligent Capture для глибокого аналізу трафіку.

– Технологія Hyperlocation для визначення місцезнаходження з використанням WiFi і BLE.

– Інтелектуальна зміна режиму роботи радіомодулів на основі радіочастотного середовища 2,4 ГГц, 5 ГГц та подвійний режим 5 ГГц.

– Підтримка технологій ClientLink 4.0 і CleanAir.

– Можливість виділення радіостанції для моніторингу безпеки мережі.

З метою підключення точок доступу та камер відеоспостереження необхідно використати POE комутатори. Розглянемо моделі: Cisco Catalyst 2960-L Series, Cisco Catalyst 2960-X Series, Cisco Catalyst 3650 Series, Cisco Catalyst 3850 Series, Cisco Catalyst 9300 Series, Cisco Catalyst 9400 Series, Cisco Catalyst 9500 Series.

З огляду на необхідність розвитку мережі та передачі значних обсягів відеотрафіку доцільно використати комутатори з Gigabit Ethernet портами. Це дозволить уніфікувати типи комутаторів, використовувати меншу кількість моделей пристроїв та мати резерв для відновлення роботоздатності мережі після виходу з ладу обладнання.

Комутатори серії Cisco Business 220 є доступними Smart комутаторами, які пропонують безпечність, надійність та простоту використання для бізнес-мереж. З їх інтуїтивно зрозумілою панеллю управління, можливістю Power over Ethernet (PoE) і налаштовуваними функціями, ці комутатори дозволяють створити надійну мережу, не надто навантажуючи бюджет.

Рисунок 2.7 – Комутатор Cisco CBS220-16P-2G-EU

Cisco CBS220-16P-2G-EU є пристроєм, який забезпечує швидкість передачі даних та керування мережею для малих і середніх підприємств. Він оснащений 16 портами Gigabit Ethernet і 2 портами Gigabit SFP, що дозволяє досягти високої швидкості передачі даних. Окрім того, цей комутатор підтримує функцію PoE (Power over Ethernet), яка дозволяє передавати живлення через мережевий кабель, спрощуючи підключення пристроїв і уникнення потреби в додаткових джерелах живлення. Компактний розмір та зручна монтажна конструкція роблять його легким у встановленні навіть в обмеженому просторі.

Цей комутатор також забезпечує надійність і відмовостійкість, що дозволяє йому працювати стабільно і ефективно в будь-яких умовах мережі.

2.4 Структура адрес та підмережі школи

З метою забезпечення роботи комп’ютерної мережі школи її необхідно розділити на віртуальні підмережі (VLAN).

З огляду на задачі, що стоять перед мережею і групи користувачів, які будуть нею користуватись визначимо підмережі, орієнтовну кількість користувачів підмережі, спосіб призначення адрес пристроям та необхідність реєстрації пристрою для доступу до мережі.

Підмережа системи відеоспостереження.

Призначена для постійного моніторингу та запису подій на території школи з метою недопущення крадіжок, булінгу та інших протиправних дій.

Оскільки в школі налічується 27 приміщень та 5 загальних зон доцільно використати не менше 33 камер.

Визначимо адресу мережі 192.168.0.0/24 та призначимо VLAN id = 21. В такій мережі може бути розміщено до 254 відеореєстраторів та IP камер. Визначимо, що IP адреса маршрутизатора, що буде виконувати функції шлюза буде 192.168.0.1. Оскільки відеореєстратори та камери відеоспостереження повинні працювати постійно і не передбачається часта зміна їх налаштувань з метою спрощення закріплення камер за реєстраторами їм буде встановлюватись фіксована IP адреса на етапі налаштування. Широковживані відеореєстратори зазвичай можуть обслуговувати до 32 камер, тому для обслуговування до 254 IP камер необхідно максимум 8 реєстраторів. Визначимо IP адреси, зарезервовані для відеореєстраторів в діапазоні 192.168.0.2-10. Приймемо, що для IP адрес камер відеоспостереження будуть використовуватись IP адреси в діапазоні 192.168.0.20-254.

Серверна демілітаризована зона призначена для розміщення серверів школи. В ній розміщені веб-сервери, DNS-сервер, DHCP-сервер, сервери відеоконференцій. DMZ зона

Демілітаризована зона або підмережа розташовується між захищеною внутрішньою мережею (Intranet) і незахищеною зовнішньою мережею (інтернет).

У DMZ можуть розташовуватися публічні сервери, такі як веб-сервери, поштові сервери або сервери VPN, які повинні бути доступні з інтернету. Розміщення цих серверів у DMZ дозволяє обмежити доступ до внутрішньої мережі, зменшити потенційну небезпеку для внутрішніх ресурсів та поліпшити безпеку.

Зазвичай у DMZ встановлюються файерволи та інші пристрої безпеки для фільтрації мережевого трафіку та контролю доступу. Це дозволяє забезпечити обмежений доступ з DMZ до внутрішньої мережі, а також контролювати і моніторити зовнішній трафік, що надходить до серверів у DMZ.

Створення DMZ є важливим елементом в плануванні мережевої безпеки, оскільки воно допомагає зменшити ризик злому або зловживання, коли системи зовнішньої мережі мають доступ до внутрішніх ресурсів.

Визначимо адресу мережі 192.168.2.0/24 та призначимо VLAN id = 22. В такій мережі може бути розміщено до 253 серверів, що більше чим достатньо для потреб школи. Визначимо, що IP адреса маршрутизатора, що буде виконувати функції шлюза буде 192.168.2.1. Ця сама адреса повинна використовуватись локальним DNS-сервером як адреса зовнішнього DNS сервера. Всі решта серверів мають в якості адреси DNS-сервера використовувати адресу локального DNS-сервера. IP - адреси серверам призначаються вручну.

З метою ізоляції комп'ютерів в комп'ютерних класах школи кожен клас виділений в окремий VLAN. Таке рішення прийнято з метою недопущення можливих шкідливих впливів з комп'ютерів класу на усю мережу школи.

Визначимо адресу мережі класу №1 як 192.168.3.0/24 та призначимо VLAN id = 23. В такій мережі може бути розміщено до 253 комп'ютерів. Визначимо, що IP адреса маршрутизатора, що виконує функції шлюза буде 192.168.3.1. Ця сама адреса повинна використовуватись як адреса локального DNS-сервера. IP - адреси комп'ютерам призначаються за допомогою сервісу DHCP .

Налаштування підмережі класу №2 відрізняються від налаштувань класу №1 лише номером підмережі 192.168.4.0/24 та VLAN id = 24.

Комп'ютери адміністрації, з метою недопущення атак на них з боку школярів та інших зловмисників також відокремлені в окремий VLAN. До мережі адміністрації відносяться комп'ютери директора школи, його заступників, та бухгалтерії.

Визначимо адресу мережі адміністрації 192.168.5.0/24 та призначимо VLAN id = 25. Визначимо, що IP адреса маршрутизатора, що виконує функції шлюза буде 192.168.5.1. Ця сама адреса повинна використовуватись як адреса локального DNS-сервера. IP - адреси комп'ютерам призначаються за допомогою сервісу DHCP.

Комп'ютери, з метою недопущення атак на них з боку школярів та інших зловмисників також відокремлені в окремий VLAN.

Визначимо адресу мережі вчителів 192.168.6.0/24 та призначимо VLAN id = 26. Визначимо, що IP адреса маршрутизатора, що виконує функції шлюза буде 192.168.6.1. Ця сама адреса повинна використовуватись як адреса локального DNS-сервера. IP - адреси комп'ютерам призначаються за допомогою сервісу DHCP.

Безпроводовий сегмент мережі пропонується розділити на 2 підмережі відкриту та закриту, для цього використати 2 VLAN.

Для закритого Wi-Fi учнів та вчителів визначимо адресу мережі 192.168.8.0/21 та призначимо VLAN id = 30. Визначимо, що IP адреса маршрутизатора, що виконує функції шлюза буде 192.168.8.1. Ця сама адреса повинна використовуватись як адреса локального DNS-сервера. IP - адреси клієнтам призначаються за допомогою сервісу DHCP. Маска для VLAN використана 21, забезпечить приєднання щонайменше двох тисяч користувачів. Та гарантовано забезпечить учнів та вчителів школи доступом до мережі, навіть коли кожен з них буде використовувати по три Wi-Fi пристрої. Передбачається, що доступ в закриту Wi-Fi мережу будуть мати лише користувачі, що зареєстрували свої пристрої у адміністратора мережі. Фіксація MAC адреси користувача забезпечить отримання постійної IP адреси навіть при повторних перепідключеннях з тривалими перервами. Це зроблено з метою чіткої ідентифікації пристроїв та користувачів в мережі з метою спрощення розслідування кіберінцедентів.

Публічний Wi-Fi також виокремлений в окремий VLAN. Як і для закритого сегменту визначимо адресу мережі 192.168.16.0/21 та призначимо VLAN id = 40, що також дозволить одночасно приєднатись не менше двом тисячам користувачів. Визначимо, що IP адреса маршрутизатора, що виконує функції шлюза буде 192.168.16.1. Ця сама адреса повинна використовуватись як адреса локального DNS-сервера. IP - адреси клієнтам призначаються за допомогою сервісу DHCP. Також для цього сегменту доступ надається лише до мережі інтернет і на обмеженій швидкості.

Таблиця 2.1 – IP-план підмереж комп’ютерної мережі школи

IP-адреса	Призначення	VLAN
1	2	3
192.168.0.0/24	Система відеоспостереження	21
192.168.0.1	Шлюз системи відеоспостереження	

Таблиця 2.1 (Продовження) – IP-план підмереж комп’ютерної мережі школи

1	2	3
192.168.0.2-10	Відеореєстратори	
192.168.0.20-254	Камери відеоспостереження	
192.168.2.0/24	Серверна (DMZ)	22
192.168.2.1	Шлюз	
192.168.2.3	Веб-сервер	
192.168.2.4	DNS-сервер	
192.168.2.5	DHCP-сервер	
192.168.2.6	FTP-сервер	
192.168.3.0/24	Клас №1	23
192.168.3.1	Шлюз, DHCP, DNS – сервери	
192.168.3.20-50	Робочі станції класу	
192.168.4.0/24	Клас №2	24
192.168.4.1	Шлюз, DHCP, DNS – сервери	
192.168.4.20-50	Робочі станції класу	
192.168.5.0/24	Адміністрація	25
192.168.5.1	Шлюз	
192.168.5.20-50	Комп’ютери адміністрації	
192.168.6.0/24	Вчительська	26
192.168.6.1	Шлюз	
192.168.6.20-50	Комп’ютери вчителів	
192.168.8.0/21	Закритий Wi-Fi учнів та вчителів	30
192.168.8.1	Шлюз	
192.168.8.10-192.168.15.254	Зареєстровані Wi-Fi пристрої	
192.168.16.0/21	Публічний Wi-Fi	40
192.168.16.1	Шлюз	
192.168.16.10-192.168.23.254	Публічні Wi-Fi пристрої	

Такий розподіл адрес дозволить розмежувати доступи між різними групам користувачів, використати групові правила фільтрації трафіку та реалізувати розмежувати доступи користувачів в залежності від призначених їм ролей. Такий підхід дозволить мінімізувати атаки школярів на комп'ютери та сервери школи.

2.5 Логічна топологія мережі

Логічна топологія розроблюваної мережі проектується з урахуванням початкових даних, а саме кількість провайдерів, кількість та типи кінцевих пристроїв, відстані між приміщеннями, де встановлюється кінцеве обладнання.

Рисунок 2.8 – План школи

На плані школи, представленому на рисунку 2.8, наявно 25 кабінетів різного призначення, їдальня, коридори та приміщення серверної.

Мережу школи можна поділити на 2 зони – внутрішня мережа школи, що забезпечує доступ до ресурсів школи і мережі інтернет з приміщення школи та зовнішня мережа, яка відображає способи доступу легальних користувачів шкільної мережі до її ресурсів.

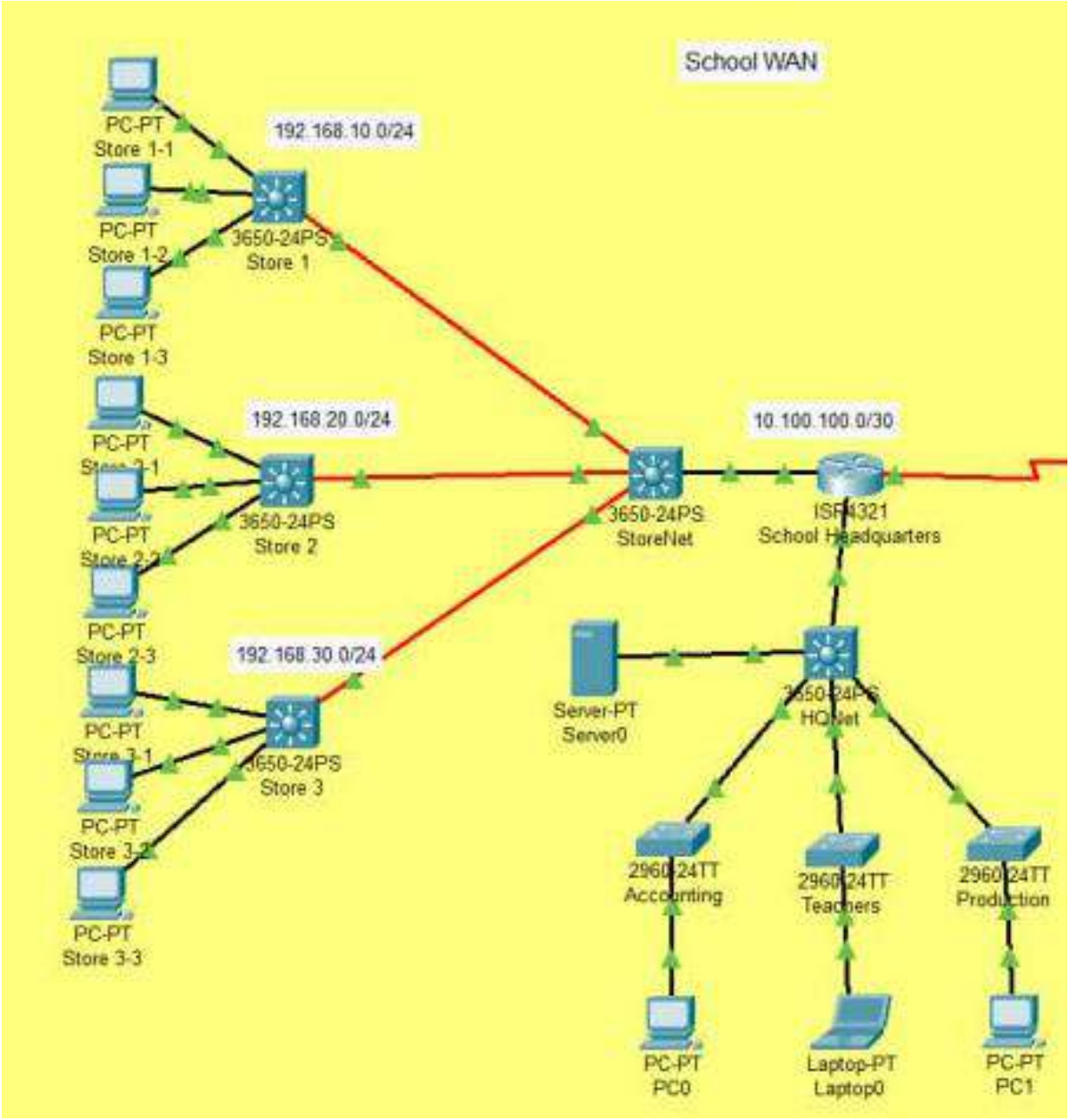


Рисунок 2.9 – Узагальнена логічна топологія внутрішньої мережі

Представлена на рис. 2.9 узагальнена логічна топологія внутрішньої мережі показує загальну організацію мережі та логіку під'єднання до неї пристроїв.

Представлена на рис. 2.10 узагальнена логічна топологія зовнішньої мережі показує яким чином користувачі шкільної мережі можуть отримати доступ до ресурсів мережі школи. Таке необхідно за умови коли учні або вчителі з різних причин не можуть бути присутніми в школі на уроці.

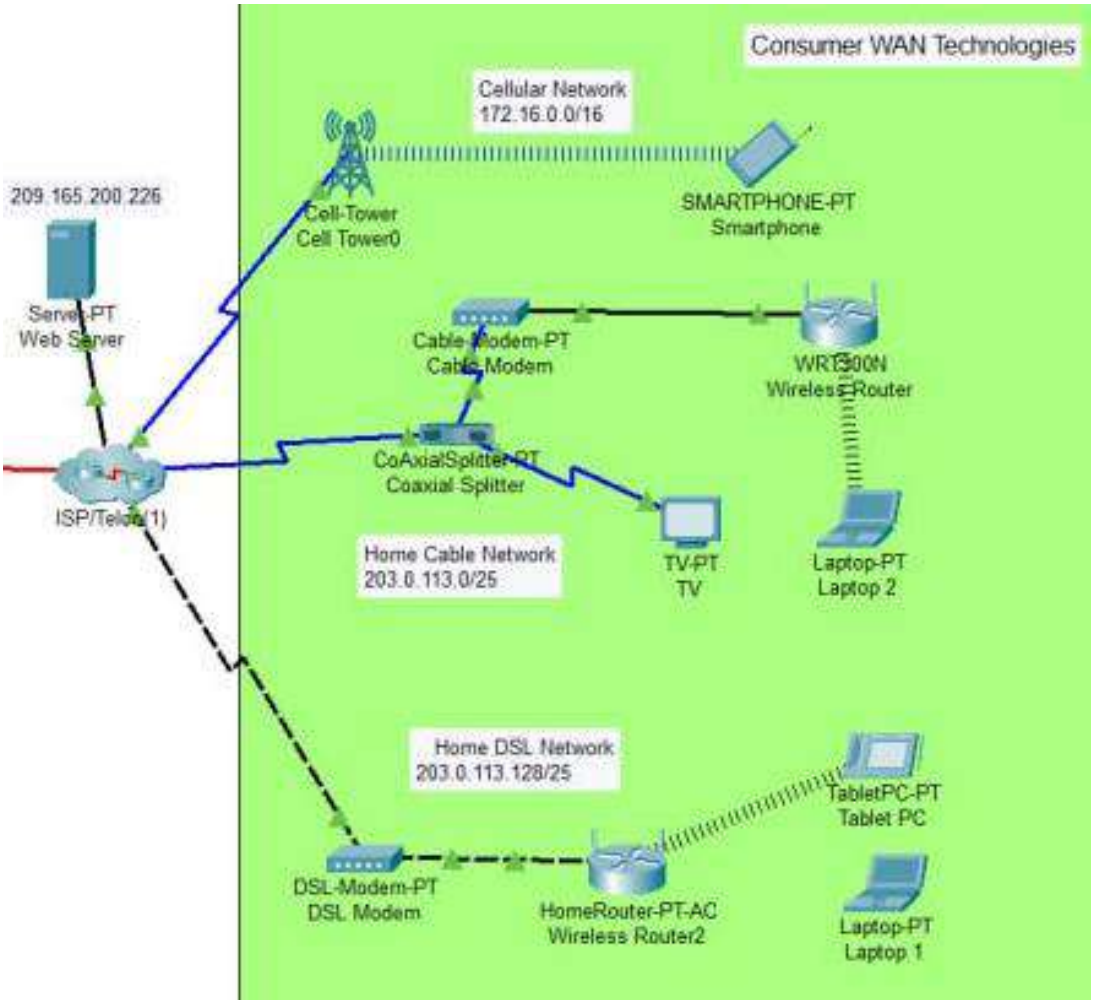


Рисунок 2.10 – Узагальнена логічна топологія зовнішньої мережі

На рисунку 2.11 представлено логічну топологію ядра мережі.

Ядро мережі складається з файрвола, що забезпечує фільтрацію трафіку та захист мережі від зовнішніх атак. Вхідного маршрутизатора, на якому створені VLAN, та відбувається маршрутизація між підмережами. Та магістральні комутатори, що формують рівень дистрибуції та за рахунок резервних ліній забезпечують стійкість мережі у випадку виходу з ладу одного з комутаторів чи кабельної лінії, що їх з'єднує. Також безпосередньо до вхідного маршрутизатора приєднані сервери демілітаризованої зони.

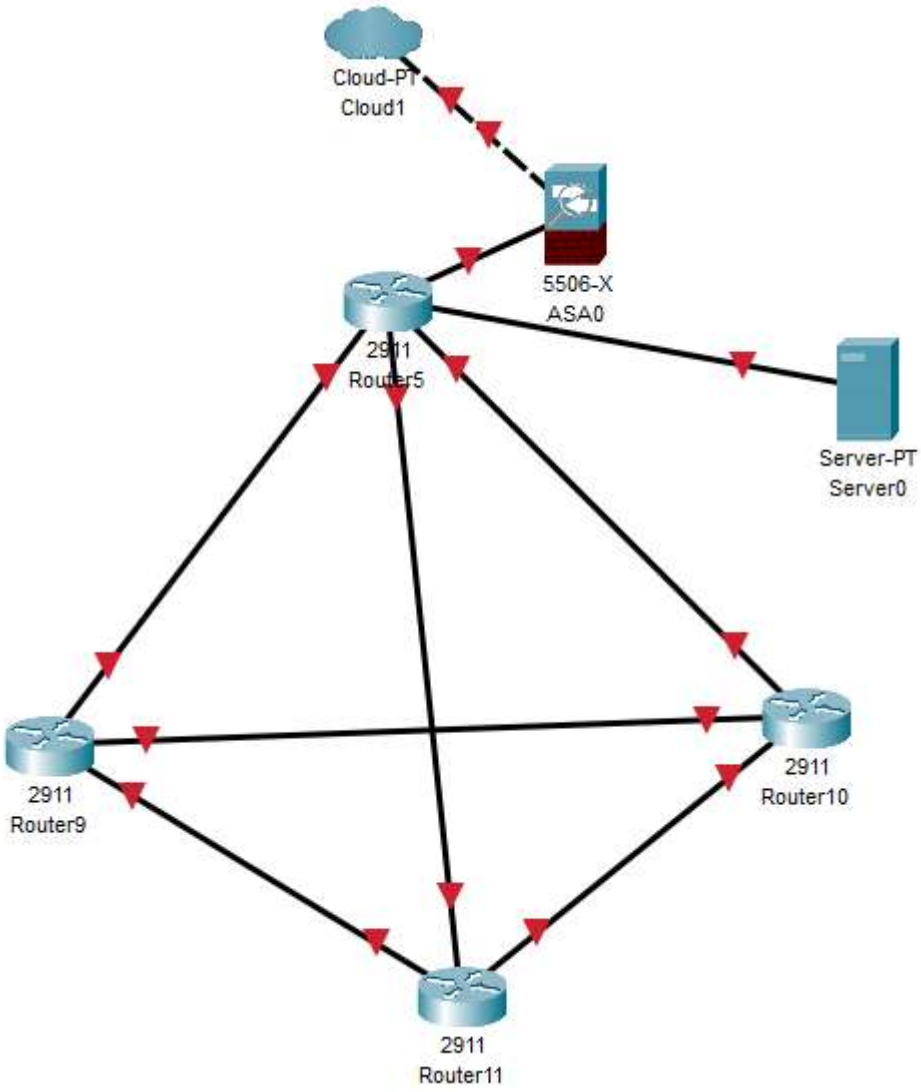


Рисунок 2.11 – Логічна топологія ядра мережі

На рисунку 2.12 представлено фрагмент логічної топології системи відеоспостереження. IP камери повинні розміщуватись по одній в класі, в коридорах та інших місцях загального користування. Для системи відеоспостереження передбачено окремий VLAN, за рахунок цього досягається достатній рівень ізоляції трафіку системи відеоспостереження. Реєстратор системи відеоспостереження розміщується в серверній.

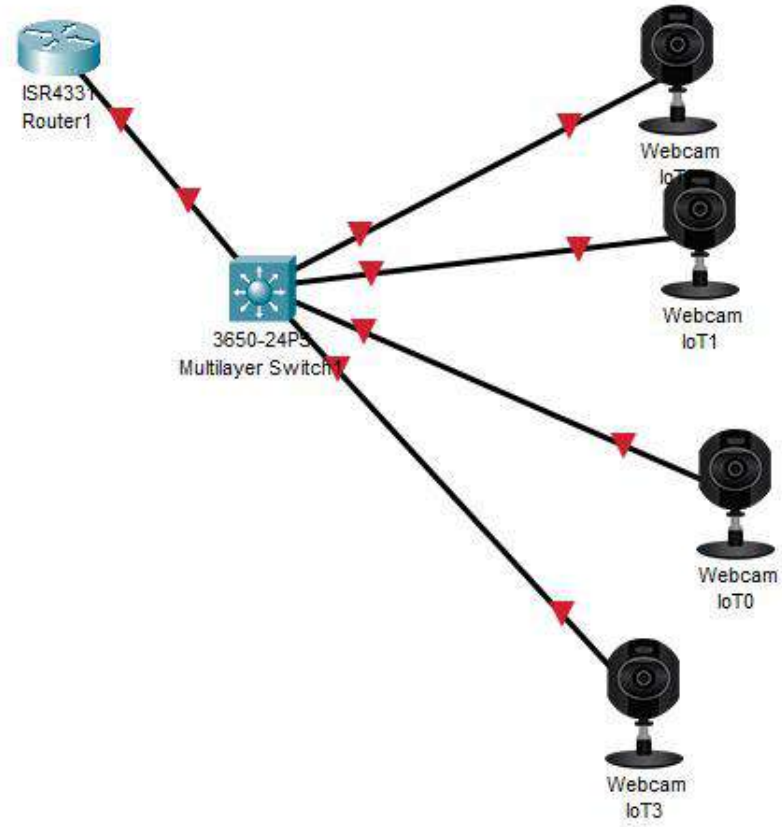


Рисунок 2.12 – Логічна топологія фрагменту системи відеоспостереження

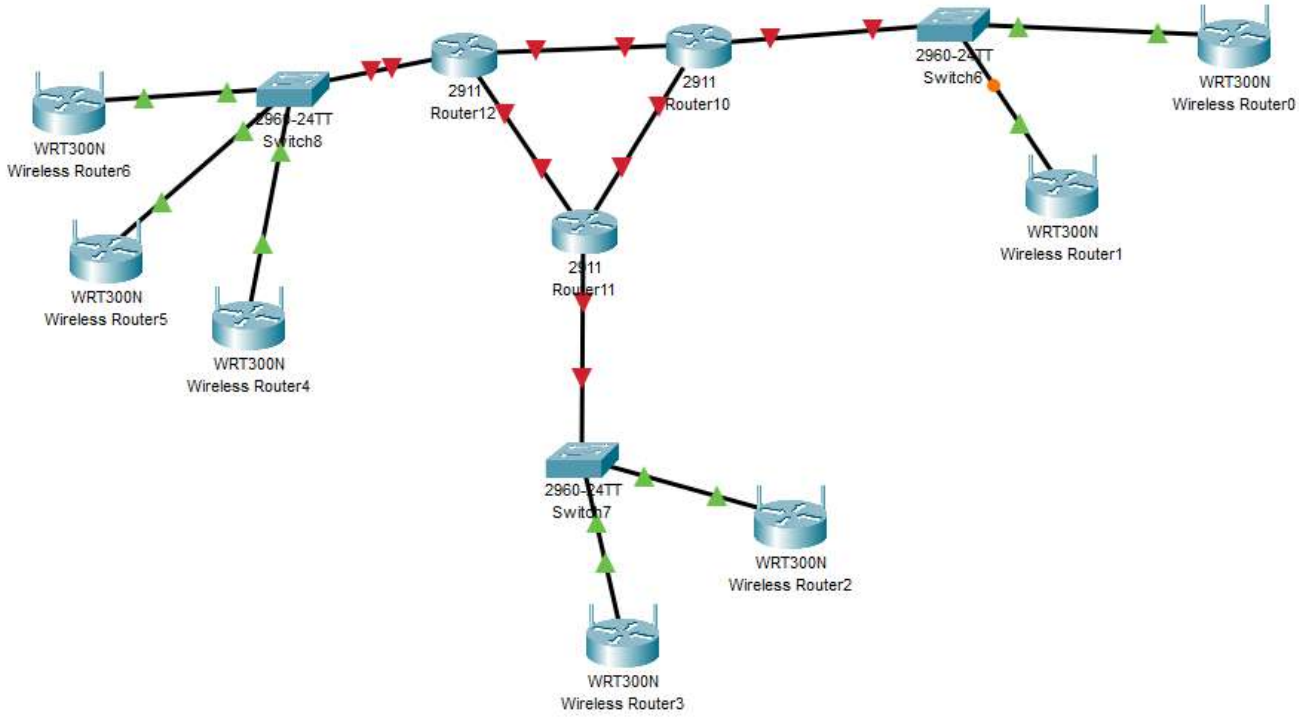


Рисунок 2.13 – Логічна топологія бездротового сегменту мережі

На рисунку 2.13 представлено логічну топологію бездротового сегмента мережі. Для забезпечення якісного покриття приміщення школи використано 7 високопродуктивних точок доступу. Запропоновані точки доступу підтримують технологію MultySSID та дозволяють підключати різних користувачів до визначених vlan. З метою раціонального використання мережевого кабелю та зменшення пристроїв в сегментах мережі точки доступу розділені між магістральними вузлами. Точки доступу з номерами 0 та 1, приєднуються до першого магістрального вузла, що розміщений в коридорі біля кабінету №116. Точки з номерами 2 та 3 приєднуються до магістрального вузла, що розміщений в коридорі біля аудиторії 106, решта точок, з номерами 4,5 та 6 під'єднуються до магістрального вузла номер 3, що розміщений в коридорі біля аудиторії 122. Усі точки приєднуються до гігабітних портів керованих POE- комутаторів. До цих-же комутаторів приєднуються камери відеоспостереження.

Запропонована логіна топологія мережі забезпечує високі показники швидкодії та має можливості для її розширення.

2.6 Фізична топологія мережі

Фізична топологія мережі визначає фізичну організацію пристроїв, кабелів та інших з'єднувальних елементів в мережі. Вона описує розташування та підключення фізичних компонентів мережі.

Фізична топологія представлена на рисунку 2.14.

Магістральне обладнання розміщене в серверній (вхідний маршрутизатор, файєрвол, магістральний комутатор №1). Також в серверній розміщуються сервери, що обслуговують мережу та інформаційні системи школи.

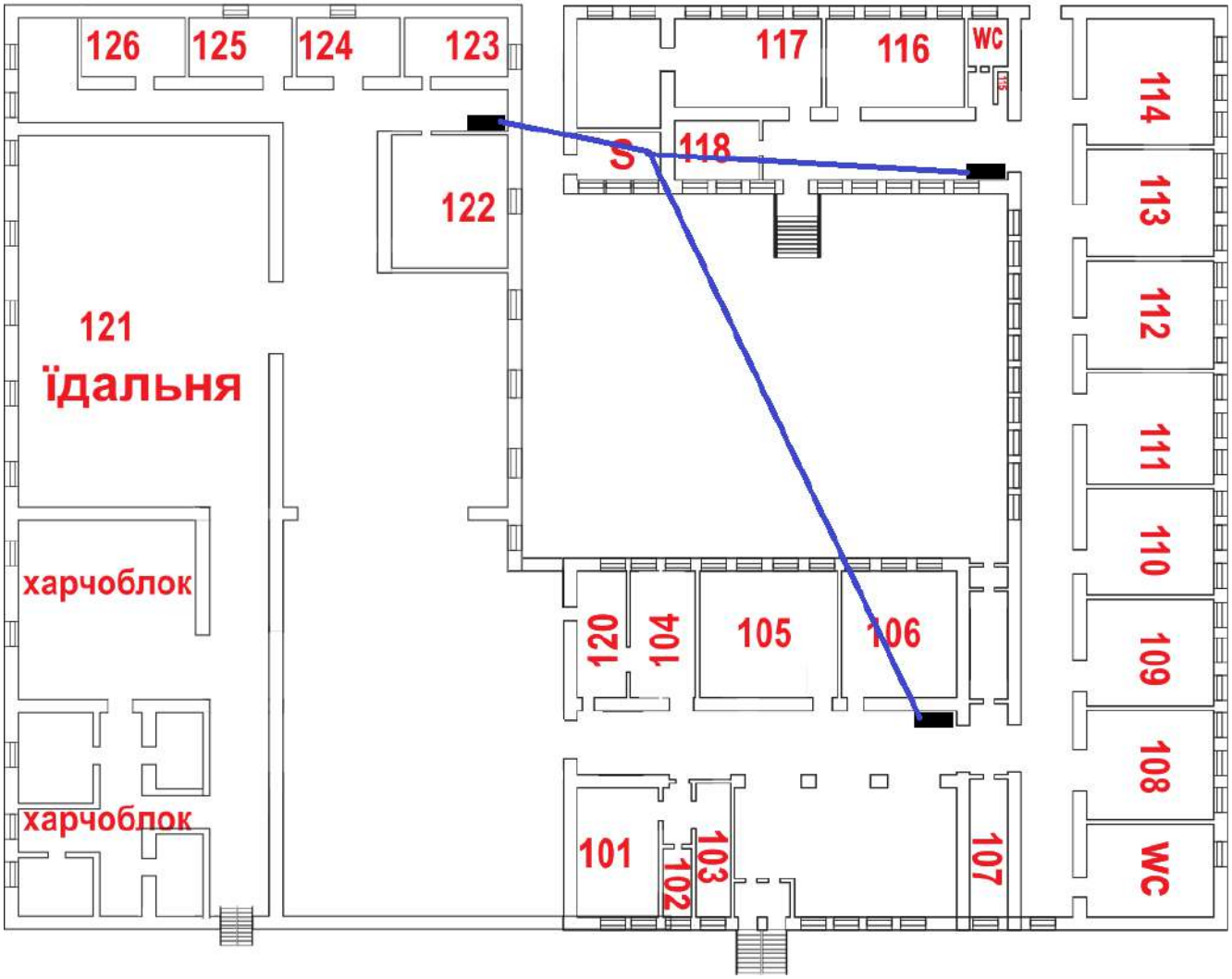


Рисунок 2.14 – фізична топологія ядра мережі

На рисунку 2.15 представлено узагальнено фізичну топологію внутрішнього сегменту мережі. Дротовий сегмент мережі має розгалужену структуру та складається з двох частин оптичного та мідного. Вхід мережі від провайдера виконується оптоволоконним кабелем. Також оптоволоконні кабелі прокладено від серверної до магістральних вузлів. Використання оптоволоконних кабелів не призводить до суттєвого здорожчення, однак дозволяє, за потреби, збільшити швидкість передачі даних навіть до 10Гб/с. Монтаж кабелів магістральних ліній слід виконати в недоступному до потенційних зловмисників місці (над підвісною стелею в коридорах.)

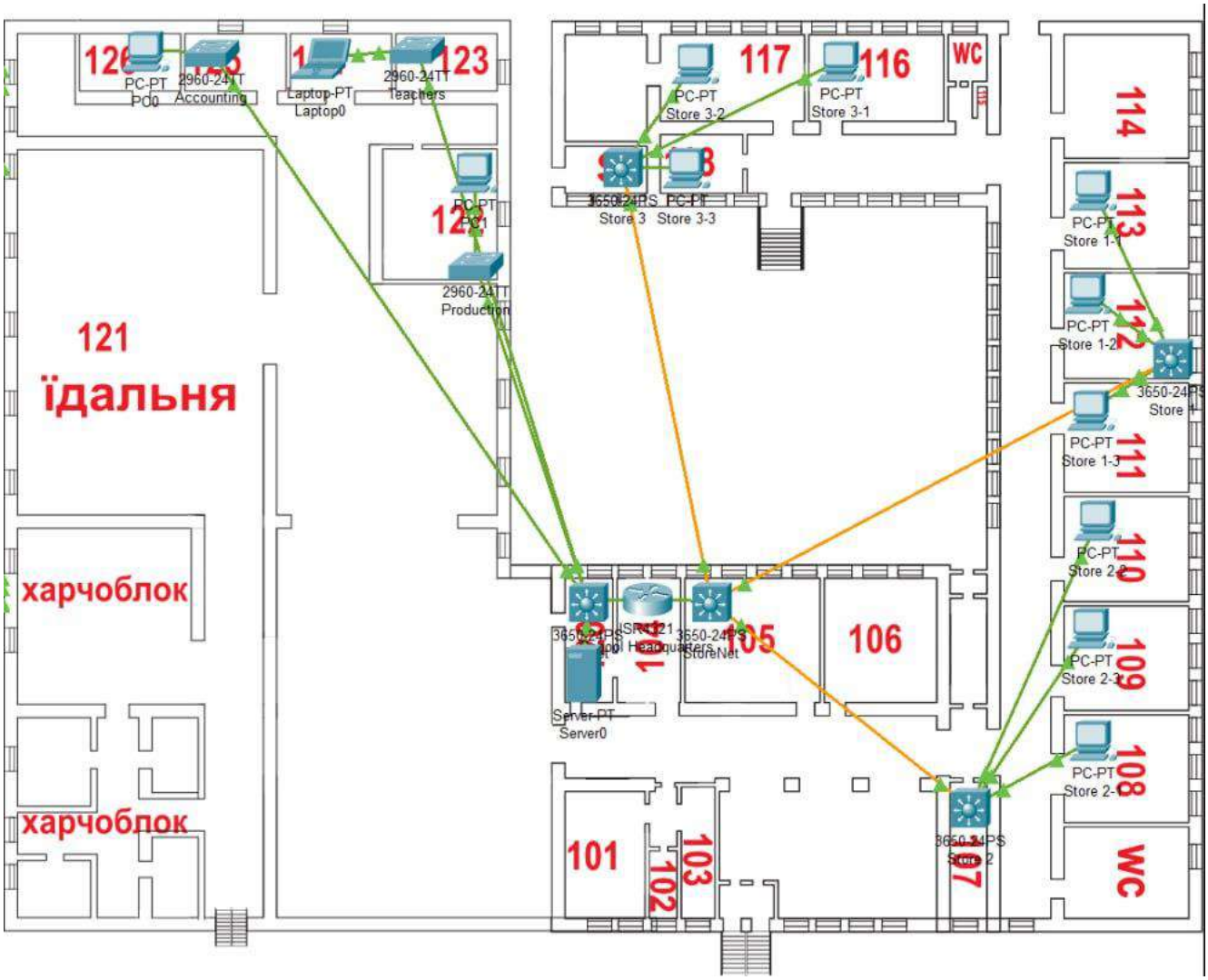


Рисунок 2.15 - Узагальнена фізична топологія внутрішньої мережі

Фізична топологія, представлена на рисунку 2.15 передбачає встановлення трьох магістральних вузлів, що складається з вхідного керованого комутатора та POE комутатора. В порти вхідного комутатора підключаються комп'ютери або інші пристрої, що потребують кабельного підключення та розміщені в класах або інших приміщеннях.

Представимо фізичну топологію бездротового сегменту мережі на рис. 2.16, вона розроблена у відповідності до логічної топології, представленої на рисунку 2.13. На фізичній топології представлено 6 Wi-Fi точок. Запропоновані точки мають функцію Multi-SSID та можуть в залежності від SSID, до якої підключений користувач, направляти трафік у відповідний VLAN.

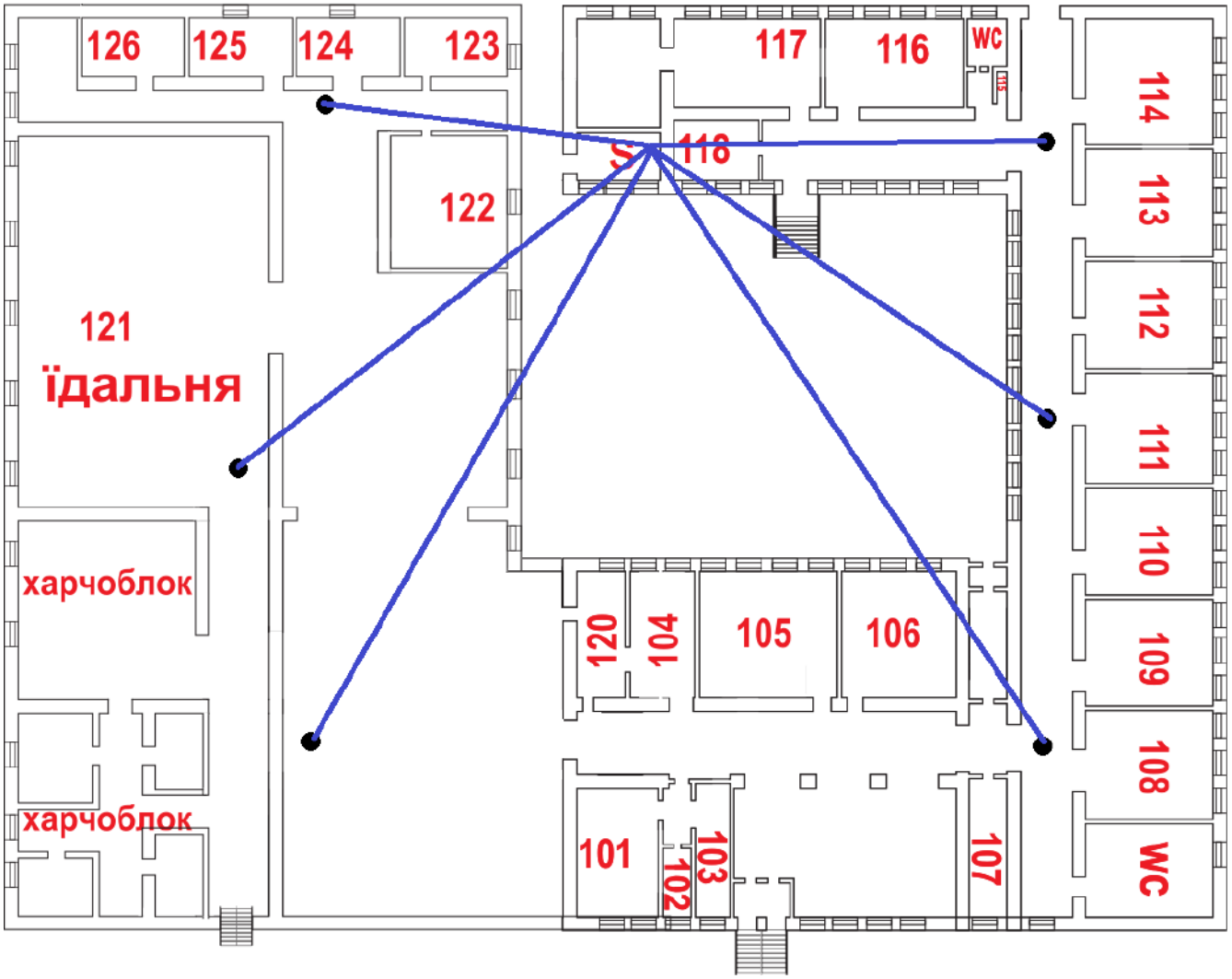


Рисунок 2.16 – Фізична топологія бездротового сегменту мережі

Реалізація системи відеоспостереження передбачає розміщення відеокамер в класних кабінетах, коридорах, холах та їдальні. Вчительська, кабінети адміністрації та санітарні місця системою відеоспостереження не обладнуються. Також передбачено окрема кабельна система для відеоспостереження.

Оскільки IP-камери системи відеоспостереження отримують живлення за технологією POE, з метою недопущення перевантаження мережевих комутаторів підмережа відеоспостереження розділена на 3 сегмента. Сформовані сегменти в середньому мають по 15 камер, що дозволяє використати стандартні POE комутатори. Для зменшення трафіку від камер до реєстратора прокладено окрему кабельну мережу саме для підсистеми відеоспостереження. Фізична топологія системи відеоспостереження представлена на рисунку 2.17

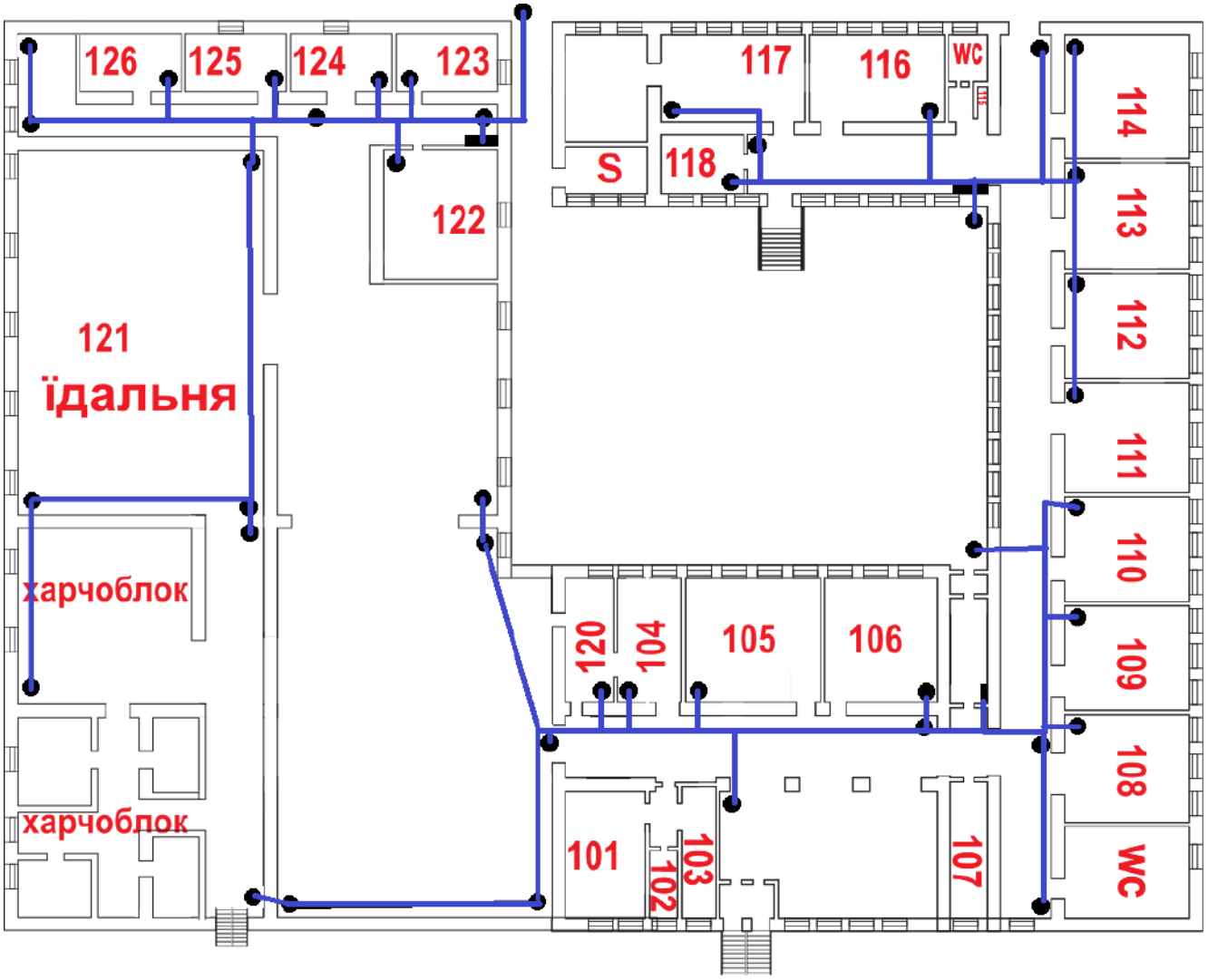


Рисунок 2.17 – Фізична топологія системи відеоспостереження

Запропонована фізична топологія враховую особливості будівлі та вимоги до мережі.

2.7 Висновки

В розділі представлено етапи проектування мережі від розподілу мережі на підмережі в залежності від задач, що виконуються користувачами в мережі. Проведено визначення адресних просторів для кожного VLAN. Це дозволить в подальшому провести ефективне налаштування мережевого обладнання та налаштувати маршрутизацію між VLAN та забезпечити доступ до ресурсів як локальної мережі так і інтернет.

3 НАЛАШТУВАННЯ ТА ТЕСТУВАННЯ МЕРЕЖІ ШКОЛИ

3.1 Налаштування мережевого обладнання школи

Підібране і розміщене обладнання з розділів 1 та 2 необхідно налаштувати і підготувати до роботи.

Першим етапом налаштування мережевого обладнання є налаштування файєрвола ASA 5506.

```
Перший крок – відключення nat-control
SC-SCHOOLCONFIG-1(config)#
no nat-control
SC-SCHOOLCONFIG (config)#
interface Ethernet 1
nameif inside
security-level 100
ip address 10.10.10.95/32
no shut
Outside-інтерфейс:
SC-SCHOOLCONFIG (config)#
interface Ethernet 0
nameif outside
security-level 0
ip address 172.20.0.1
no shut
```

Рисунок 3.1 – початкове налаштування ASA

Створення VLAN:

ASA (config)# vlan 10

ASA (config-vlan)# name 10

ASA (config-vlan)# exit

Налаштування портів ASA:

ASA (config)# interface 1

ASA (config-if)# switchport mode access

ASA (config-if)# switchport access vlan 10

ASA (config-if)# exit

Налаштування підінтерфейсу ASA для кожної VLAN:

ASA(config)# interface GigabitEthernet0/0

ASA(config-if)# nameif 10

ASA(config-if)# security-level 100

ASA(config-if)# ip address 192.168.0.1 24

ASA(config-if)# no shutdown

ASA(config-if)# exit

Додавання маршруту за замовчуванням:

ASA(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1

Налаштування ACL:

ASA(config)# access-list indns extended permit tcp 0.0.0.0 192.168.0.1

Налаштування NAT:

ASA(config)# object network object_1

ASA(config-network-object)# subnet 192.168.0.1 24

ASA(config)# nat (inside,outside) dynamic interface

Застосування ACL до інтерфейсу:

ASA(config)# access-group indns in interface GigabitEthernet0/0

Збереження налаштувань:

ASA(config)# write memory

Налаштування вхідного маршрутизатора.

Першим етапом потрібно створити VLAN на маршрутизаторі, для чого потрібно додати їх до бази даних.

vlan database

vlan 20

vlan 21

vlan 22

vlan 23

vlan 24

vlan 25

vlan 26

vlan 30

vlan 40

exit

Потрібно провести налаштування інтерфейсів VLAN.

interface GigabitEthernet0/1

switchport mode access

switchport access vlan 20

exit

interface GigabitEthernet0/2

switchport mode access

switchport access vlan 21

exit

Відповідні налаштування потрібно провести для усіх VLAN.

Проводиться налаштування підінтерфейсів для VLAN на порту маршрутизатора:

interface GigabitEthernet0/0

no shutdown

interface GigabitEthernet0/0.10

encapsulation dot1Q 20

ip address 192.168.20.1 255.255.255.0

exit

interface GigabitEthernet0/0.20

encapsulation dot1Q 21

ip address 192.168.21.1 255.255.255.0

exit

exit

Налаштування NAT:

ip nat inside source list 1 interface GigabitEthernet0/1 overload

ip nat inside source static tcp 192.168.20.1 80 interface GigabitEthernet0/1 80

ip nat inside source static tcp 192.168.21.1 80 interface GigabitEthernet0/1 80

access-list 1 permit 192.168.20.0 0.0.0.255

access-list 1 permit 192.168.21.0 0.0.0.255

interface GigabitEthernet0/1

ip nat outside

exit

Аналогічні налаштування необхідно провести на решті маршрутизаторів, що створюють ядро мережі.

enable

configure terminal

hostname Switch1

Цей набір команд дозволяє змінювати налаштування комутатора та задає його ім’я.

Аналогічно до вхідного маршрутизатора в базу даних комутатора вносяться номери VLAN.

vlan database

vlan 20

vlan 21

…

Далі, так само як і на маршрутизаторі прив’язуються VLAN до відповідних портів.

Наступним етапом є налаштування тегованого порту для зв’язку з маршрутизатором.

interface GigabitEthernet0/24

switchport mode trunk

switchport trunk allowed vlan all

exit

налаштування завершується встановленням IP адреси комутатора та збереженням налаштувань.

interface Vlan1

ip address 192.168.0.5 255.255.255.0

exit

end

write memory

виконання цих команд забезпечує налаштування комутатора.

3.2 Вимірювання продуктивності мережі

Вимірювання продуктивності мережі передбачає використання метрик.

До таких метрик можна віднести:

– швидкість передачі даних. Вимірювання пропускної здатності мережі шляхом передачі файлів різного розміру та запису часу, необхідного для завершення передачі. Використання такої метрики передбачає тестування готової мережі та дозволяє оцінити якість вибору та налаштування мережевого обладнання та пропускну здатність каналів зв’язку.

– Затримка передачі пакету. Вимірювання часу затримки між двома вузлами мережі. Це можна зробити за допомогою утиліти ping, яка надає інформацію про час, необхідний для відправки пакету даних від одного вузла до іншого та повернення його. Оцінку затримок в мережі можна провести як на реальній мережі так і на її моделі.

– Втрата пакетів. Вимірювання кількості втрачених пакетів під час передачі даних. Це можна зробити за допомогою утиліти ping або спеціальних інструментів, таких як traceroute, які дають змогу відстежувати маршрут пакетів і визначати місце втрати. Можна провести на реальній мережі, є інформативним у випадку неналежного конфігурування мережі. За мови відсутності критичних помилок може бути інформативним лише за умови значного завантаження каналів передачі даних. Зазвичай для працездатних мереж не застосовується.

– Пропускна здатність. Вимірювання фактичної швидкості передачі даних через мережу. Це можна здійснити за допомогою інструментів, таких як iPerf або вбудованих засобів моніторингу мережевого обладнання. Може бути реалізовано виключно на реальній мережі.

– Вимірювання навантаження. Застосування спеціальних інструментів, таких як Apache JMeter або Gatling, для створення імітованого трафіку на мережевому обладнанні та вимірювання продуктивності під навантаженням. Вимірювання за цією метрикою може бути реалізоване на реальній мережі.

З метою перевірки продуктивності мережі використаємо метрику «Затримка передачі пакету». Результати тестування представлено в таблиці 3.1.

Таблиця 3.1 – Перевірка продуктивності мережі метрикою «Затримка передачі пакету»

Джерело / Отримувач	Система відеоспостереження	Серверна (DMZ)	Клас №1	Клас №2	Адміністрація	Вчительська	Закритий Wi-Fi	Публічний Wi-Fi	Зовнішня мережа
1	2	3	4	5	6	7	8	9	10
Система відеоспостереження	*	3мс	-	-	+	-	-	-	-
Серверна (DMZ)	-	*	4мс	4мс	3мс	3мс	24мс	26мс	10мс
Клас №1	-	-	*	-	-	4мс	-	-	11мс
Клас №2	-	-	-	*	-	4мс	-	-	-
Адміністрація	-	-	-	-	*	-	25мс	-	-
Вчительська	-	-	-	-	4мс	*	26мс	-	-

Таблиця 3.1 (Продовження) – Перевірка продуктивності мережі метрикою «Затримка передачі пакету»

1	2	3	4	5	6	7	8	9	10
Закритий Wi-Fi учнів та вчителів	-	-	-	-	26мс	26мс	*	-	-
Публічний Wi-Fi	-	-	-	-	-	-	-	*	36мс
Зовнішня мережа	-	-	11мс	10мс	12мс	10мс	27мс	28мс	*

Отримані результати тестування показують прийнятні значення метрики, які зазвичай, є типовими для комп'ютерних мереж такого класу.

3.3 Тестування розмежування доступу в мережі школи

Тестування розмежування доступу в мережі зазвичай включає перевірку правильності налаштування правил файєрвола, контролю доступу до ресурсів та рівня безпеки мережевих сегментів.

Зазвичай таке тестування проводиться в декілька етапів:

– перевірка правил файєрвола;

– перевірка контролю доступу;

– перевірка безпеки мережевих сегментів, а саме обмежень доступів між VLAN.

Виконання сканування відкритих портів на вхідному інтерфейсі файєрвола командою nmap -p 0-65535 10.10.90.1 показало, що відкритими є лише порти, які перенаправляються до серверів в демілітаризовану зону. Файєрвол та вхідний маршрутизатор не мають відкритих вхідних портів та адмініструються виключно з внутрішньої мережі.

Перевірка контролю доступу передбачає запуск утиліти ping з кожного vlan, включаючи зовнішній, до ресурсів мережі. Результати виконання утиліти ping представлені в таблиці 3.2.

В результаті проведеного тестування можна зробити висновок, що правила фільтрації трафіку між VLAN збудовані правильно, та забезпечують виконання поставлених на завдань. Такий набір правил мінімізує ймовірність проведення хакерських атак на інфраструктуру школи, оскільки як внутрішні так і зовнішні користувачі мають доступ до серверів виключно через дозволені для веб-доступу порти.

Таблиця 3.2 – Тестування доступності між VLAN в мережі школи

З мережі / Доступний ресурс	Система відеоспостереження	Серверна (DMZ)	Клас №1	Клас №2	Адміністрація	Вчительська	Закритий Wi-Fi	Публічний Wi-Fi	Зовнішня мережа
1	2	3	4	5	6	7	8	9	10
Система відеоспостереження	*	+	-	-	+	-	-	-	-
Веб-сервер	-	*	+	+	+	+	+	+	+
DNS-сервер	-	*	+	+	+	+	+	-	-
DHCP-сервер	-	*	+	+	+	+	+	+	-
FTP-сервер	-	*	+	+	+	+	+	-	-
Клас №1	-	-	*	-	-	+	-	-	-
Клас №2	-	-	-	*	-	+	-	-	-
Адміністрація	-	-	-	-	*	-	+	-	-
Вчительська	-	-	-	-	+	*	+	-	-

Таблиця 3.2 (Продовження) – Тестування доступності між VLAN в мережі школи

1	2	3	4	5	6	7	8	9	10
Закритий Wi-Fi учнів та вчителів	-	-	-	-	+	+	*	-	-
Публічний Wi-Fi	-	-	-	-	-	-	-	*	+
Зовнішня мережа	-	-	+	+	+	+	+	+	*

Користувачі мережі мають доступи до внутрішніх ресурсів мережі, обґрунтовані виключно потребою навчання або виконання посадових обов'язків.

3.4 Розрахунок вартості обладнання та кабельних мереж для комп'ютерної мережі

Розрахуємо вартість обладнання та матеріалів, необхідних для реалізації мережі. Для цього внесемо в таблицю 3.3 моделі пристроїв, їх вартість та необхідну кількість. Оскільки планується розробка нової мережі та придбання комплекту обладнання ціни обрано з офіційного сайту виробника з офіційними ліцензіями та гарантією.

Вартість обладнання, необхідного для розвертання мережі складає 14707,63$. Окрім вартості обладнання необхідно врахувати вартість кабелів зв'язку. Для прокладання оптоволоконного сегменту мережі необхідно використати 150 метрів кабелю з мінімум 4-ма оптичними волокнами. Вартість такого кабелю – 1$ за метр. Загальна вартість оптоволоконного кабелю – 150$. Провівши аналіз фізичної топології мережі на предмет визначення довжини кабелю виявлено, що його необхідно 890м. Вартість UTP кабелю категорії 5е складає 0,25$ за 1 метр. З урахуванням технологічних витрат при прокладанні кабелю в розмірі не менше 10% загальна вартість кабелю складе 250$. Вартість прокладання оптоволоконного та мідного кабелів в середньому дорівнює вартості кабелю. Тому приймемо вартість кабелів з прокладанням рівною 800$.

Таблиця 3.3 – Таблиця розрахунку вартості мережевих пристроїв

Пристрій	Ціна за одиницю в $	Кількість	Загальна вартість в $
Брандмауер, Cisco ASA 5505	418,89	1	418,89
Маршрутизатор, CISCO2811	1259,65	4	5038,60
Комутатор, Cisco WS-C2960-24TT-L	941,02	8	3764,08
IP камера, Cisco Video Surveillance 7530PD	150,17	36	5406,12
Бездротовий маршрутизатор, Cisco-Linksys WRT300N	39,97	6	79,94
Разом			14707,63

Загальна вартість побудови мережі складе приблизно 15,5 тис. $.

3.5 Висновки

В розділі представлено налаштування мережевого обладнання, в якому враховано вимоги до мережі. Проведено чисельне вимірювання затримок в спроектованій мережі, визначено що затримки знаходяться в допустимих межах як для кабельних сегментів мережі, так і для безпроводових.

Проведено тестування доступності кінцевого обладнання між vlan. Отримані результати вказують, що правила фільтрації трафіку збудовані правильно та використовуються в правильному порядку, що в результаті забезпечило виконання поставлених до мережі вимог.

ВИСНОВКИ

Автором в процесі виконання кваліфікаційної роботи було розроблено проект мережі школи.

Для виконання цього завдання було проаналізовано вимоги до шкільних комп'ютерних мереж, визначено які ресурси потрібні в мережі та перспективи розвитку освітніх підходів з метою врахування їх в архітектурі мережі. Проведено аналіз підходів до проектування мережі та побудови топологій шкільних мереж.

В ході виконання кваліфікаційної роботи розроблено узагальнену логічну топологію шкільної мережі, розроблено логічну топологію ядра мережі. Також розроблено логічні топології системи відеоспостереження та бездротового сегменту мережі.

Також розроблено узагальнену фізичну топологію мережі, фізичну топологію рівня дистрибуції, фізичну топологію системи відеоспостереження та бездротового сегменту мережі.

В процесі роботи налаштовано мережеве обладнання, що забезпечить функціонування мережі згідно поставленого завдання та проведено тестування розмежування доступу, що підтвердило правильність налаштування обладнання.

Загальна вартість мережі склала 15,5 тис. $.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Стасєв Ю.В. Комп’ютерні мережі. Технології, протоколи та моделювання: навчал. посібн. / І.В. Рубан, С.В. Дуденко, О.І. Тимочко. – Х.: ХУПС, 2019. – 359 с

2. Корпоративна мережа. URL: http://wikipedia.ua.nina.az/wiki/%D0%9A%D0 (дата звернення 01.06.2023)

3. Трояновська Т. І. Корпоративна мережа, як засіб організації роботи підприємства URL: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2017/paper/viewFile/1844/1562 (дата звернення 01.05.2023).

4. Computer Network Architecture. URL: https://www.javatpoint.com/computer-network-architecture (дата звернення: 23.04.2023)

5. Комплексна безпека інформаційних мережевих систем. Навчальний посібник/ А.Г. Микитишин, М.М. Митник, П.Д. Стухляк. Львів, «Магнолія 2006», 2016. 256 с.

6. Коробейнікова Т. І., Захарченко С. М. Комп'ютерна мережа. Львів : Вид-во Львів. політехніки, 2022. 228 с.

7. Принципи побудови і призначення комп’ютерних мереж. URL: https://tdmuv.com/kafedra/internal/informatika/classes_stud/uk/nurse/and/03.Принципи%20побудови%20і%20призначення%20компютерних%20мереж.html (дата звернення: 24.04.2023)

8. Hierarchical Network Model. URL: https://networkdirection.net/articles/network-theory/hierarchicalnetworkmodel/ (дата звернення: 30.04.2023)

9. Що таке демілітаризована зона (DMZ)?. URL: https://uk.itpedia.nl/2023/01/28/wat-is-een-demilitarized-zone-dmz (дата звернення: 30.04.2023)

10. Stateful inspection URL: https://www.techtarget.com/searchnetworking/definition/stateful-inspection. – (дата звернення 01.06.2023).

11. Ліхтарников О.М, Хорошко М.П, Слободяник В.О. Основи комп'ютерних мереж: навчальний посібник. Київ : Ленвіт, 2018. 320 с.

12. Демілітаризована зона URL: http://nickshevtsov.blogspot.com/2017/11/blog-post_86.html (дата звернення 01.05.2023).

13. DMZ Network: How It Works, Its Uses, and Benefits in Network Security. URL: https://www.linkedin.com/pulse/dmz-network-how-works-its-uses-benefits-security-valdemar-závadský (дата звернення: 10.05.2023)

14. Організація комп'ютерних мереж «демілітаризована зона» URL: https://kremenetskyy.blogspot.com/2017/11/blog-post.html (дата звернення 25.05.2023).

15. DMZ URL: https://www.fortinet.com/resources/cyberglossary/what-is-dmz (дата звернення 07.05.2023)

16. Gary A. Donahue Network Warrior / Gary A. Donahue. – Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2011. – 627 p.

17. Cisco IOS. URL: https://docs.oracle.com/en-us/iaas/Content/Network/Reference/ciscoiosCPE.htm (дата звернення: 28.04.2023)

18. Tanenbaum A.S, Wetherall D.J. Computer networks. Pearson, 2010. 960 p.

19. Основні вимоги до проектування кампусних мереж. URL: https://studfile.net/preview/5199546/page:2/ (дата звернення: 15.05.2023)

20. Yanko A., Vyhivskyi R. Система захисту комп'ютерної мережі. Системи управління, навігації та зв'язку. Збірник наукових праць. 2022. Т. 2, № 68. С. 91–94. URL: https://doi.org/10.26906/sunz.2022.2.091 (дата звернення: 10.05.2023)

21. Комп'ютерні мережі. URL: https://comp-net.at.ua/index/topologija_komp_39_juternikh_merezh/0-6 (дата звернення: 16.05.2023)

22. Тарбаєв С.І. Проектування інфокомунікаційних мереж. 2015. 268 с.

23. Мережева модель OSI URL: https://uk.wikipedia.org/wiki/Мережева_модель_OSI. (дата звернення 01.05.2023)

24. Топології комп’ютерних мереж. URL: http://blogkkzshnika.blogspot.com/2017/10/blog-post_10.html (дата звернення: 17.05.2023)

25. Hari Subedi. A guide to network topology: 2020 URL: https://www.itjones.com/blogs/2020/11/22/a-guide-to-network-topology (дата звернення: 17.05.2023)

26. Топологія комп'ютерних мереж. URL: https://stud.com.ua/53329/informatika/topologiya_kompyuternih_merezh (дата звернення: 17.05.2023)

27. Організація комп'ютерних мереж. URL: http://nickshevtsov.blogspot.com/2017/10/blog-post.html (дата звернення: 17.05.2023)

28. Канальний рівень моделі OSI URL: https://static-course-assets.s3.amazonaws.com/ITE50UK/course (дата звернення 01.05.2023).

29. Канальний рівень моделі OSI URL: https://uk.wikipedia.org/wiki/Канальний_рівень. (дата звернення 01.05.2023)

30. Комутатор URL: https://uk.wikipedia.org/wiki/Мережевий_комутатор. (дата звернення 01.05.2023).

31. Що таке корпоративний сервер? URL: https://uk.icyscience.com/enterprise-server (дата звернення 25.05.2023).

32. Топологія локальних мереж. URL: https://ua5.org/lan/125-topologja-lokalnikh-merezh.html (дата звернення: 17.05.2023)

33. David Scott The IT Professional's Guide To Corporate Networks URL: https://www.techopedia.com/the-it-professionals-guide-to-corporate-networks/2/25665 (дата звернення: 18.05.2023)

34. Топологія комп’ютерних мереж. Класифікація комп’ютерних мереж з топології. URL: https://creativnost.com.ua/topologiya-kompyuternix-merezh-klasifikaciya-kompyuternix-merezh-z-topologii/ (дата звернення: 18.05.2023)

35. Топологія мережі: 6 пояснених та порівняних мережевих топологій. URL: https://instagalleryapp.com/chistij-administrator-2/topologija-merezhi-6-pojasnenih-ta-porivnjanih/ (дата звернення: 18.05.2023)

36. Докучаєв А.В, Засов А.В, Казакевич П.В. Інформаційна безпека комп'ютерних систем: навчальний посібник. Київ : Наук. думка, 2017. 152 с.

37. Інформаційні мережі / Полоневич О.В та ін. Київ, 2019. 94 с.

38. Setting up an FTP Server URL: https://www.ocf.berkeley.edu/reinholz/freebsd/ftp.html (дата звернення 15.05.2023).

39. Kim D.J, Solomon, M.G. Network security bible. Wiley, 2019. 816 с.

40. Vulnerabilities of network OS and mitigation withstate-based permission system [Electronic resource] / J. Noh, S. Lee, J. Park, S. Shin, B. B. Kang // Graduate School of Information Security, School of Computing, Korea Advanced Institute of Science and Technology, Daejeon, Korea. – URL: https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1369 (дата звернення: 18.05.2023)

41. Методика розрахунку конфігурації мережі Ethernet URL: http://um.co.ua/7/7-8/7-87320.html (дата звернення 25.05.2023).

42. Configuring dynamic NAT in Cisco devices URL: https://www.manageengine.com/network-configuration-manager/configlets/configure-dynamic-nat-cisco.html (дата звернення: 18.05.2023)

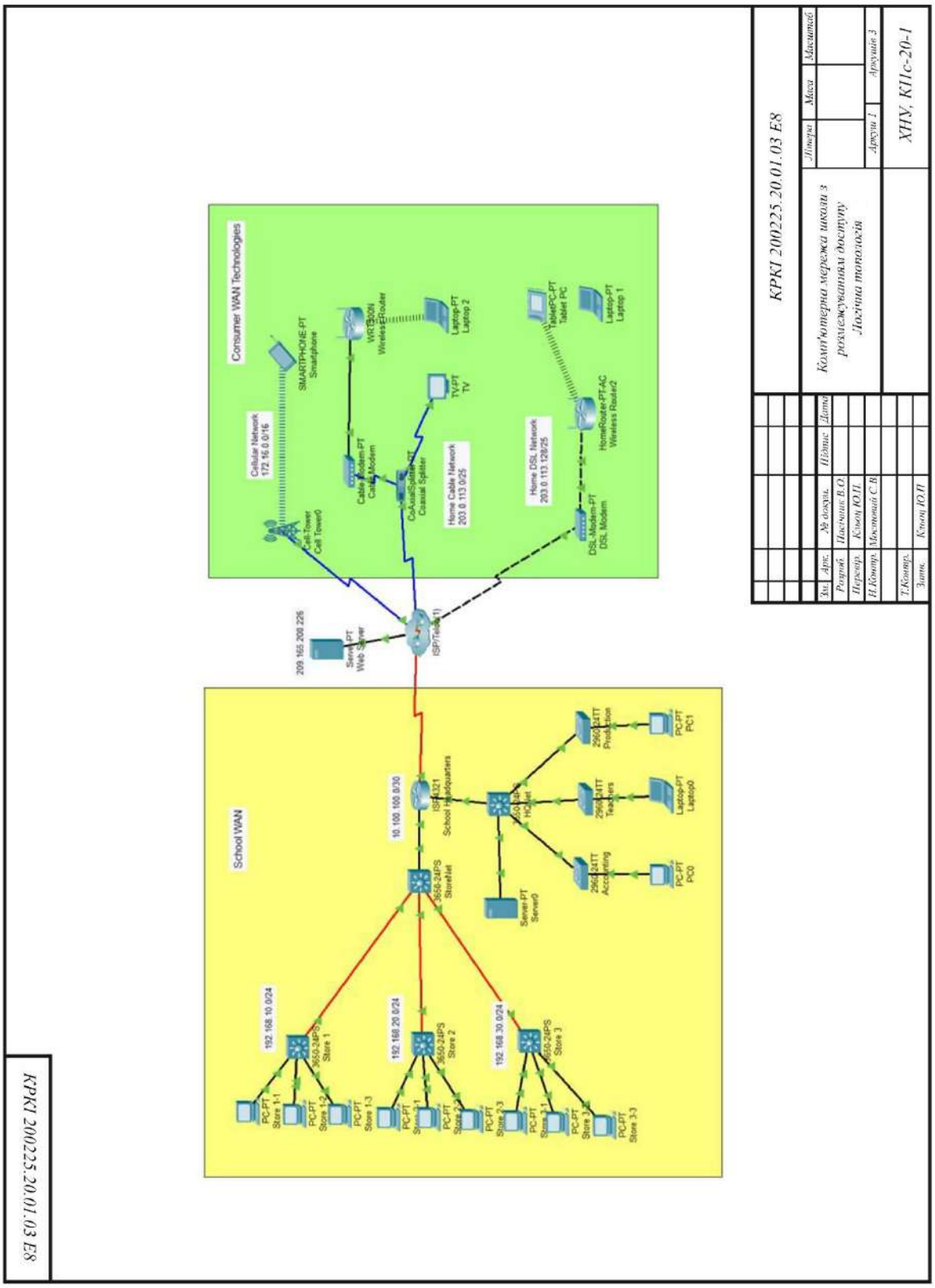
43. Configuring IP Access Lists URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html (дата звернення: 18.05.2023)

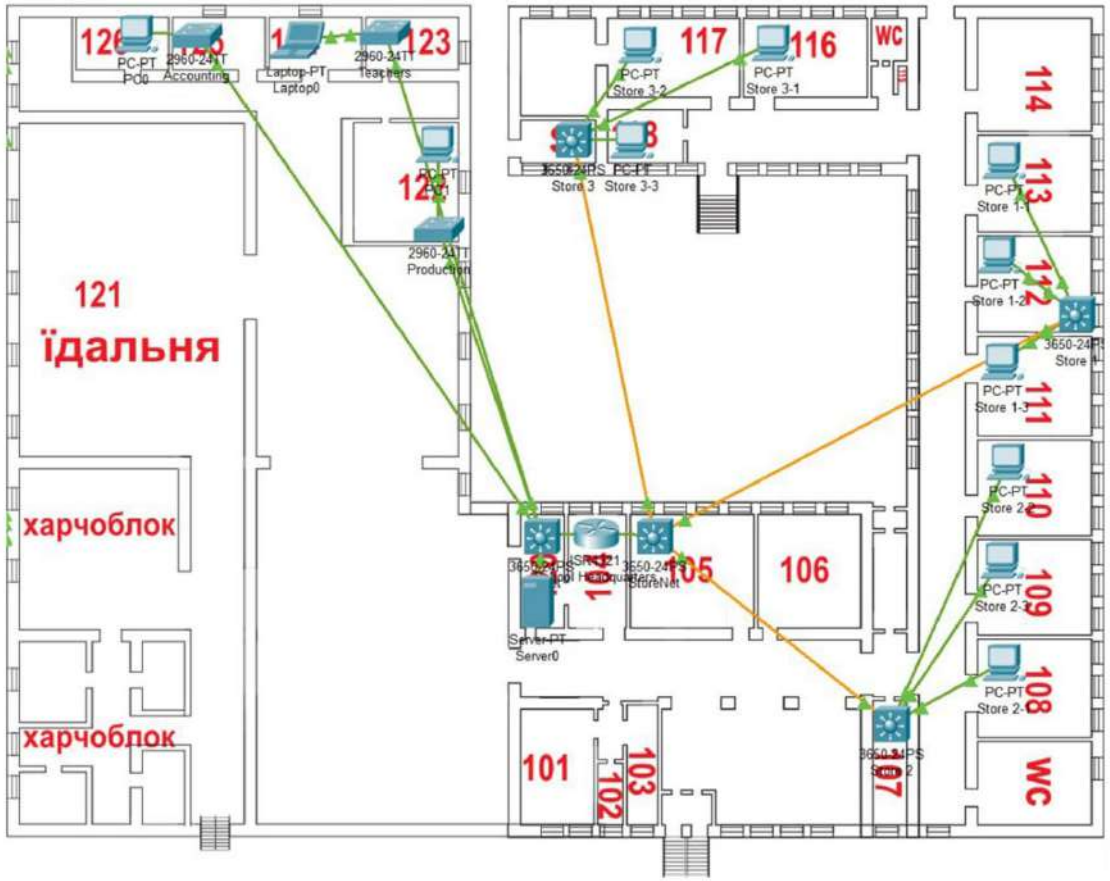
44. How to Enable SSH on Cisco Switch, Router and ASA URL: https://www.thegeekstuff.com/2013/08/enable-ssh-cisco/ (дата звернення: 18.05.2023)

45. Whitman M. E, Mattord H. J. Principles of information security. 7-ме вид. Cengage Learning, 2018. 658 p.

ДОДАТОК А

Графічні матеріали





					КРКІ 200225.20.01.03 Е8	
Зм.	Арк.	№ докум.	Підпис	Дата	Комп'ютерна мережа школи з розмежуванням доступу Фізична топологія	Літера / Маса / Масштаб
Розроб.		Пасічник В.О.				
Перевір.		Кльоц Ю.П.				Аркуш 2 / Аркушів 3
Н.Контр.		Мостовий С.В.				
Т.Контр.						ХНУ, КІ1с-20-1
Затв.		Кльоц Ю.П.				

IP-адреса	Призначення	VLAN
192.168.0.0/24	Система відеоспостереження	21
192.168.0.1	Шлюз системи відеоспостереження	
192.168.0.2-10	Відеореєстратори	
192.168.0.20-254	Камери відеоспостереження	
192.168.2.0/24	Серверна (DMZ)	22
192.168.2.1	Шлюз	
192.168.2.3	Веб-сервер	
192.168.2.4	DNS-сервер	
192.168.2.5	DHCP-сервер	
192.168.2.6	FTP-сервер	

IP-адреса	Призначення	VLAN
192.168.3.0/24	Клас №1	23
192.168.3.1	Шлюз, DHCP, DNS – сервери	
192.168.3.20-50	Робочі станції класу	
192.168.4.0/24	Клас №2	24
192.168.4.1	Шлюз, DHCP, DNS – сервери	
192.168.4.20-50	Робочі станції класу	
192.168.5.0/24	Адміністрація	25
192.168.5.1	Шлюз	
192.168.5.20-50	Комп'ютери адміністрації	
192.168.6.0/24	Вчительська	26
192.168.6.1	Шлюз	
192.168.6.20-50	Комп'ютери вчителів	
192.168.8.0/21	Закритий Wi-Fi учнів та вчителів	30
192.168.8.1	Шлюз	
192.168.8.10-192.168.15.254	Зареєстровані Wi-Fi пристрої	
192.168.16.0/21	Публічний Wi-Fi	40
192.168.16.1	Шлюз	
192.168.16.10-192.168.23.254	Публічні Wi-Fi пристрої	

Зм.	Арк.	№ докум.	Підпис	Дата	КРКІ 200225.20.01.03 Е8			
Розроб.		Пасічник В.О.			Комп'ютерна мережа школи з розмежуванням доступу Система адресації	Літера	Маса	Масштаб
Перевір.		Кльоц Ю.П.						
Н.Контр.		Мостовий С.В.				Аркуш 3	Аркушів 3	
Т.Контр.						ХНУ, КІ1с-20-1		
Затв.		Кльоц Ю.П.						

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітньо-кваліфікаційного рівня «бакалавр»

Студент Пасічник Владислав Олегович
Тема: «Комп'ютерна мережа школи з розмежуванням доступу»
Галузь знань 12 «*Інформаційні технології*» Спеціальність 123 «*Комп'ютерна інженерія*» Освітня програма «Програмування та захист комп'ютерних систем і мереж»

Обсяг дипломної роботи освітньо-кваліфікаційного рівня «бакалавр»: кількість листів креслень 3; кількість сторінок записки 63;

1. Короткий зміст КР та прийнятих рішень Кваліфікаційна робота присвячена дослідженню питань, пов'язаних з розробкою комп'ютерної мережі з розмежуванням доступу.Для досягнення цієї мети було проведено аналіз топологій мереж та підходи до розмежування доступу. Створено і розроблену мережу, яка дозволяє забезпечити надійну роботу мережі з гарантованими затримками та належним рівнем безпеки. Робота має на меті забезпечити належний рівень доступу до ресурсів мережі всіма учасниками освітнього процесу та мінімізувати ризики витоку персональних даних.
2. Висновок про відповідність КР завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній так і у практичній частині роботи.
3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі обґрунтовується актуальність теми роботи, її зв'язок з галуззю знань «Інформаційні технології» та спеціальністю «Комп'ютерна інженерія», формулюється мета та основні завдання кваліфікаційної роботи. У першому розділі було проведено аналіз вимог та засобів до проектування мережі школи. У другому розділі розроблено політики безпеки та правила розмежування доступу користувачів. Обґрунтовано вибір топології мережі та способу підключення кінцевих пристроїв. Розроблено логічну та фізичну топології мережі. У третьому розділі проведено налаштування мережевого обладнання школи, проведено вимірювання продуктивності роботи мережі та перевірено відповідні доступи.
4. Позитивні сторони кваліфікаційної роботи полягають у тому що, застосування розробленої мережі забезпечить гарантований доступ користувачів мережі як до локальних ресурсів так і до ресурсів, що розміщені в хмарних сервісах та до інтернету. Використання обґрунтованих політик та обмеження в доступах до ресурсів забезпечують високу швидкість доступу до навчальних ресурсів при забороні доступу учнів до розважального контенту, що в свою чергу, сприяє покращенню якості навчального процесу без відволікання учнів.

5. Негативні сторони проекту: _варто приділити більше уваги налаштуванню QoS

6. Оцінка графічного оформлення та пояснювальної записки роботи. Графічне оформлення виконане відповідно до теми кваліфікаційної роботи із дотриманням усіх стандартів. У загальному графічне оформлення виконане на достатньому технічному рівні. Пояснювальна записка відповідає нормам для її оформлення та вимогам

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. У пояснювальній записці багато наглядних пояснень, однак деякі розділи варто розширити. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої задачі проектування.

8. Інші зауваження -

9. Оцінка дипломної роботи Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що робота заслуговує оцінки «добре/ B (4,25)».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) __завідувач кафедри автоматизації, комп'ютерно-інтегрованих технологій та робототехніки, д.т.н., професор Мартинюк Валерій Володимирович__

« __5___ » ____червня_____ 2023 . _____ (підпис)

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Комп'ютерна мережа школи з розмежуванням доступу

Автор: Пасічник Владислав Олегович

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: Програмування та захист комп`ютерних систем і мереж

Науковий керівник: Кльоц Ю.П.

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) запозичення розміщені в розділах аналізу існуючих методів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 16.3% і адресується до 192 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Ю.П. Кльоц

Завідувач кафедри КБ _____ Ю.П. Кльоц

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1015672772

Дата перевірки:
22.06.2023 09:21:03 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
22.06.2023 09:42:53 EEST

ID користувача:
100008300

Назва документа: **Пасічник**

Кількість сторінок: **59** **Кількість слів:** **9925** **Кількість символів:** **76123** **Розмір файлу:** **2.68 MB** ID **файлу:** **1015317667**

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

11.4%
Схожість

Найбільша схожість: **3.78%** **з джерелом з Бібліотеки** (ID **файлу:** **1011379802**)

10.8% Джерела з Інтернету	**695**	**Сторінка** 61
8.99% Джерела з Бібліотеки	**119**	**Сторінка** 64

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи	**3**
Підозріле форматування	**11 сторінок**

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 1.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 13%**

	Документ		Сумарний збіг по Базі Даних	
ID: 117625 Назва: Комп'ютерна мережа школи з розмежуванням доступу Додано в БД: 2023-06-22 Автора: Пасічник В.О. Керівники: Кльоц Ю.П. Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	66488	552	1929 (3%)	23 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми