Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Інфокомунікацій_____
(повна назва)

Кафедра _____Інформаційно-мережної інженерії_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____перший (бакалаврський)_____
_____ Проєктування інфокомунікаційної мережі будівельного підприємства _____
_____
(тема)

Виконав:
здобувач ____4____ року навчання,
групи _____ТРІМІ-21-1_____
_____Денис Мірза_____
(власне ім'я, прізвище)

Спеціальність __172 Телекомунікації_____
_____та радіотехніка_____
(код і повна назва спеціальності)
Тип програми ____освітньо-професійна_____
Освітня програма _____
_*Інформаційно-мережна інженерія*_____
(повна назва освітньої програми)

Керівник ___ст.викл. Галина Ляшенко_____
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри _____ _____ _Валерій Безрук___
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти перший (бакалаврський)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма *Інформаційно-мережної інженерії*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Мірза Денису Станіславовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Проєктування інфокомунікаційної мережі будівельного підприємства*

затверджена наказом університету від 23 травня 2025 р. № 410 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вихідні дані до роботи *Інфокомунікаційна мережа офісу підприємства, активне та пасивне мережеве обладнання інфокомуніаційної мережі*

4. Перелік питань, що потрібно опрацювати в роботі

1 Теоретичні аспекти побудови інфокомунікаційних мереж.

2 Аналіз потреб та планування інфокомунікаційної мережі офісу підприємства.

3 Вибір необхідного обладнання, оцінка сумісності та ефективності.

4 Моделювання інфокомунікаційної мережі офісу підприємства.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *Слайди у форматі Power Point*

_____
_____
_____
_____
_____
_____
_____
_____
_____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
	Отримання завдання.	26.05.25	виконано
	Підбір літератури за темою роботи.	27.05.25-28.05.25	виконано
	Розробка 1 розділу	29.05.25-1.06.25	виконано
	Розробка 2 розділу	02.06.25-05.06.25	виконано
	Розробка 3 розділу	06.06.25-08.06.25	виконано
	Розробка 4 розділу	09.06.25-10.06.25	виконано
	Розробка 5 розділу	11.06.25-12.06.25	виконано
	Оформлення кваліфікаційної роботи	13.06.25-14.06.25	виконано
	Оформлення презентаційного матеріалу	15.06.25-17.06.25	виконано

Дата видачі завдання _____26.05.2025___

Здобувач _____Денис Мірза
(підпис)

Керівник роботи _____ ___ст. викл. Галина Ляшенко
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 73 с., 20 рис., 8 табл., 21 джерел, 2 додатки

Об'єкт дослідження – інфокомунікаційна мережа будівельного підприємства, яка забезпечує зв’язок між підрозділами, обмін даними та доступ до інформаційних ресурсів.

Мета роботи – розробка ефективної інфокомунікаційної мережі для будівельного підприємства з використанням сучасних технологій і програмних засобів для забезпечення стабільної роботи, оптимізації інформаційних потоків та підвищення рівня безпеки.

У роботі проведено аналіз потреб будівельного підприємства в інфокомунікаційній інфраструктурі, досліджено сучасні технології проєктування мереж, такі як VLAN, протоколи маршрутизації та засоби кіберзахисту (ACL, VPN). Для створення моделі мережі використано програмне середовище Cisco Packet Tracer, у якому розроблено топологію, налаштовано обладнання та проведено тестування працездатності мережі.

ІНФОКОМУНІКАЦІЙНА МЕРЕЖА, ПРОЄКТУВАННЯ МЕРЕЖІ, МЕРЕЖЕВА ІНФРАСТРУКТУРА, VLAN, МАРШРУТИЗАЦІЯ, КІБЕРБЕЗПЕКА, CISCO PACKET TRACER.

THE ABSTRACT

Explanatory note: 73 p., 20 fig., 8 tabl., 21 sources, 2 app.

Object of research: the info-communication network of a construction enterprise, which provides connectivity between departments, data exchange, and access to information resources.

Purpose of the work: to design an efficient info-communication network for a construction enterprise using modern technologies and software tools to ensure stable operation, optimize information flows, and enhance security.

The work involved analyzing the construction enterprise's needs for an info-communication infrastructure, researching modern network design technologies such as VLAN, routing protocols, and cybersecurity tools (ACL, VPN). The Cisco Packet Tracer software environment was used to create a network model, develop the topology, configure equipment, and test the network's functionality.

INFO-COMMUNICATION NETWORK, CONSTRUCTION ENTERPRISE, NETWORK DESIGN, NETWORK INFRASTRUCTURE, VLAN, ROUTING, CYBERSECURITY, CISCO PACKET TRACER.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ

IP – (Internet protocol) Інтернет-протокол;

VPN – Virtual Private Network (технологія віртуальних приватних мереж)

VLAN – (virtual local area network) віртуальна локальна мережа;

TCP/IP – Transmission Control Protocol/Internet Protocol (протокол управління передачею/міжмережевий протокол)

OSI – OpenSystems Interconnection Basic Reference Model (базова еталонна модель взаємодії відкритих систем)

LAN – Local area network (локальна комп'ютерна мережа)

СКС – структурована кабельна система

ACL (Access Control List) – список контролю доступу

VoIP (Voice over IP) – голос через IP;

MAC – (media access control) управління доступом до середовища

ВСТУП

У сучасних умовах цифрової трансформації бізнесу ефективне функціонування будь-якого підприємства неможливе без надійної та гнучкої інфокомунікаційної інфраструктури [1]. Професійно спроєктована мережа забезпечує швидкий обмін даними, координацію а також захист конфіденційної інформації. У будівельній галузі, де проєкти потребують інтеграції великих обсягів даних, таких як креслення, 3D-моделі та системи Building Information Modeling (BIM), якісна мережева інфраструктура є критично важливою для підвищення продуктивності та зниження ризиків.

Саме тому питання проєктування сучасної інфокомунікаційної мережі для будівельного підприємства набуває особливого значення.

Інфокомунікаційна мережа забезпечує передачу даних, голосу, відео та іншої інформації між офісами, будівельними майданчиками та партнерами. Її належне проєктування дозволяє не лише підвищити продуктивність праці, а й забезпечити безпеку інформації, стабільність зв’язку та масштабованість системи відповідно до потреб підприємств [2].

Метою кваліфікаційної роботи є проєктування комплексної інфокомунікаційної мережі для будівельного підприємства з урахуванням технічних та організаційних аспектів, яка інтегрує локальну мережу з глобальними інформаційними системами, забезпечуючи високу стійкість до збоїв і оптимальну продуктивність.

Завдання дослідження:

– Проаналізувати призначення, основні характеристики та сучасні технології інфокомунікаційних мереж.

– Розробити план приміщення та розміщення робочих місць для будівельного підприємства.

– Вибрати оптимальну топологію мережі.

– Спроєктувати структуровану кабельну систему та розрахувати

кількість кабелю.

– Підібрати обладнання.

– Змоделювати мережу в Cisco Packet Tracer, включаючи налаштування заходів безпеки.

Об’єкт дослідження: інфокомунікаційна мережа будівельного підприємства, що включає апаратне та програмне забезпечення для передачі даних.

Предмет дослідження: процес проєктування, налаштування та тестування інфокомунікаційної мережі з урахуванням специфіки будівельної галузі.

Методи дослідження: аналіз літератури, порівняльний аналіз топологій, моделювання в Cisco Packet Tracer.

Практична цінність: створення готового до впровадження проєкту мережі, який підвищує ефективність роботи будівельного підприємства, забезпечує захист даних і може бути адаптований для інших компаній галузі.

1 ТЕОРЕТИЧНІ ОСНОВИ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Інфокомунікаційні мережі є ключовим елементом сучасних інформаційних систем, призначеним для забезпечення ефективної передачі, обробки та зберігання даних між різними користувачами та пристроями [2]. Їхня головна мета — створення надійного каналу зв'язку, що дозволяє інтегрувати різні підсистеми організації, забезпечуючи швидкий доступ до інформації та координацію діяльності. У загальному контексті такі мережі слугують основою функціонування бізнес-процесів, сприяючи оптимізації обміну даними, підвищенню продуктивності та зниженню операційних ризиків, що актуально для будь-якої сфери діяльності, включаючи будівельну галузь [2].

Для будівельної компанії інфокомунікаційні мережі забезпечують об'єднання всіх етапів роботи — від проєктування до реалізації об'єктів. Вони дозволяють передавати великі обсяги даних, такі як креслення, 3D-моделі або проєктну документацію, Таким чином, головною метою таких мереж є гарантування стабільного та безпечного зв'язку між відділами, будівельними майданчиками та віддаленими співробітниками, що сприяє пришвидшенню реалізації проєктів та покращенню якості управління.

1.1 Призначення інфокомунікаційної мережі

Інфокомунікаційні мережі забезпечують передачу та обмін інформацією між різними підрозділами та користувачами. Для будівельного підприємства, яке характеризується складною структурою та розподіленими об’єктами, такі мережі використовуються для безперебійної комунікації між офісами, та віддаленими співробітниками [2]. Основне призначення інфокомунікаційної мережі – спрощення процесів управління проєктами, забезпечення спільного доступу до документації, креслень, а також підтримка використання

спеціалізованих технологій,, що дозволяє покращити якість проєктування та будівництва [2].

Крім того, інфокомунікаційні мережі в будівельних підприємствах сприяють підвищенню рівня безпеки даних, що є досить важливим у галузі, де конфіденційність проєктної документації та фінансової інформації має високий пріоритет [3]. Такі мережі також дозволяють інтегрувати локальні системи підприємства з глобальними інформаційними ресурсами, забезпечуючи доступ до оновлень програмного забезпечення, онлайн-сервісів та хмарних технологій, що спрощує масштабування бізнесу та адаптацію до змінюючихся ринкових умов [4]. Завдяки високій стійкості до збоїв та швидкості відновлення, інфокомунікаційні мережі гарантують стабільність операцій, це важливо для підтримки репутації підприємства та своєчасного виконання контрактних зобов’язань. Крім того, впровадження таких мереж дозволяє знизити операційні витрати шляхом оптимізації процесів та збільшити загальну ефективність діяльності підприємства.

1.2 Вимоги до мережевої інфраструктури будівельного підприємства

У будівельній галузі, де проєкти часто є розподіленими та включають велику кількість учасників, мережа має відповідати специфічним вимогам, щоб забезпечити швидкий обмін даними, безпеку та надійність. Цей розділ описує ключові вимоги до мережевої інфраструктури, які є необхідними для успішного виконання будівельних проєктів.

Масштабованість є однією з головних вимог. Будівельні проєкти можуть розширюватися або ускладнюватися, тому мережа повинна бути гнучкою, дозволяючи додавати нові пристрої, користувачів чи навіть цілі майданчики без значних змін у структурі [4]. Наприклад, на початку проєкту може бути лише кілька користувачів, але з часом їх кількість може зрости, що потребує додаткових ресурсів мережі. Масштабованість допомагає уникнути дорогих переробок і забезпечує адаптивність до змін.

Висока пропускна здатність необхідна для роботи з великими обсягами даних, характерними для будівельної галузі. Архітектурні креслення, 3D-моделі, відеоспостереження чи дані з BIM-систем потребують швидкої передачі між офісами, майданчиками та підрядниками [4]. Недостатня пропускна здатність може спричинити затримки, наприклад, коли інженери чекають на завантаження великих файлів. Мережа повинна підтримувати сучасні протоколи, такі як Ethernet або Wi-Fi 6, щоб забезпечити високу швидкість і ефективність.

Оскільки будівельні підприємства працюють з конфіденційною інформацією, такою як проєктна документація, контракти чи фінансові звіти потрібно, щоб захист та безпека даних були на належному рівні. Мережа повинна мати засоби захисту, включаючи шифрування даних, брандмауери, системи автентифікації. Наприклад, використання протоколів SSL/TLS або VPN може захистити дані під час передачі. Крім того, мережа має відповідати стандартам безпеки, таким як GDPR, щоб уникнути юридичних проблем і забезпечити довіру клієнтів [5].

Інтеграція з будівельними технологіями є необхідною для підтримки сучасних інструментів, таких як Building Information Modeling (BIM), Інтернет речей (IoT) чи дрони для моніторингу об’єктів. Мережа повинна забезпечувати безперебійну взаємодію між цими технологіями, дозволяючи, наприклад, IoT-пристроям передавати дані про стан обладнання чи безпеку в реальному часі . BIM-системи, які використовуються для створення цифрових моделей будівель, потребують високої пропускної здатності та низької затримки для ефективної роботи.

Простота управління є також важливою, оскільки не всі працівники будівельного підприємства мають технічні навички. Мережа повинна мати інтуїтивно зрозумілі інтерфейси для виконання базових завдань, таких як підключення нових пристроїв чи перевірка стану мережі. Наприклад, веб-панель управління може дозволити адміністратору швидко виявити проблему без залучення IT-фахівців.

На завершення, мережева інфраструктура будівельного підприємства повинна бути гнучкою, надійною, безпечною та адаптованою до потреб галузі. Ці вимоги дозволяють забезпечити ефективну комунікацію, швидкий обмін даними та підтримку сучасних технологій, що є ключем до успіху в будівельних проєктах.

1.3 Дослідження та порівняння сучасних інструментів моделювання мереж

Моделювання мереж дозволяє перевірити працездатність мереж до їх фактичного впровадження. Cisco Packet Tracer є популярним вибором, адже дозволяє створювати віртуальні мережі з маршрутизаторами, комутаторами та серверами, тестуючи їхню роботу. За допомогою Cisco Packet Tracer можна налаштувати IP-адресацію, створити VLAN, впровадити маршрутизацію та навіть перевірити безпекові протоколи, такі як ACL чи VPN. Для будівельного підприємства це важливо, адже мережа має обробляти великі файли, як-от креслення, і забезпечувати стабільний зв’язок між офісом і віддаленими працівниками. Наприклад, можна моделювати, як мережа поводитиме себе під час передачі великого обсягу інформації, перевіряючи затримки чи пропускну здатність [5].

Іншим важливим аспектом є можливість тестувати різні сценарії. У Cisco Packet Tracer можна симулювати відмови обладнання, наприклад, якщо маршрутизатор виходить з ладу, або перевірити, як мережа витримує пікове навантаження, коли багато користувачів одночасно завантажують дані. Це особливо корисно для будівельного підприємства, де затримки можуть призвести до простоїв. Інструмент також має інтуїтивно зрозумілий інтерфейс, що робить його зручним для використання навіть для людей без практичного досвіду.

Окрім Cisco Packet Tracer, є й інші інструменти, які варто згадати. Riverbed Modeler (раніше OPNET) є більш просунутим рішенням, яке дозволяє

аналізувати мережевий трафік, прогнозувати поведінку мережі під час пікових навантажень і навіть моделювати складні сценарії, такі як вплив погодних умов на бездротові мережі. Однак для невеликих проєктів, він може бути надто складним і дорогим. GNS3, у свою чергу, дозволяє створювати віртуальні мережі з використанням реального мережевого обладнання Cisco, що є корисним для тих, хто прагне до більш реалістичного досвіду [6]. Але GNS3 вимагає більше технічних знань і ресурсів, тому Cisco Packet Tracer залишається найкращим вибором через свою універсальність і поширеність [7].

Таблиця 1.1 – Порівняння основних інструментів моделювання мереж

Інструмент	Основні функції	Переваги	Недоліки	Придатність для проєкту
Cisco Packet Tracer	Симуляція мереж, налаштування VLAN, маршрутизація	Безкоштовний, простий у використанні, підтримує навчання	Обмеження для складних сценаріїв	Висока
Riverbed Modeler	Аналіз трафіку, прогнозування навантаження	Докладний аналіз, професійне використання	Дорогий, складний	Низька
GNS3	Робота з реальним обладнанням Cisco	Реалістичність, гнучкість	Вимагає більше ресурсів, складність	Середня

2 БЕЗПЕКА ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ

Безпека інфокомунікаційних мереж є основою для захисту інформації, яку компанії передають і зберігають. Вона запобігає крадіжкам даних, хакерським атакам і збоїв у роботі, що може коштувати підприємствам багато грошей і репутації.

Безпека інфокомунікаційних мереж є важливою з кількох причин, особливо для будівельної галузі:

Захист чутливих даних: будівельні підприємства працюють з конфіденційною інформацією, включаючи проєктні плани, фінансові дані та контракти. Втрата чи викрадення цих даних може призвести до фінансових втрат і юридичних проблем. Наприклад, витік інформації про проєкт може дати конкурентам перевагу або спричинити порушення контрактів.

Підтримка операційної стабільності: кібератаки, такі як витік даних чи порушення роботи систем, можуть призвести до затримок у виконанні проєктів. У будівництві, де час є критичним, такі затримки можуть бути дорогими, адже затримка одного етапу може вплинути на весь графік.

Захист сучасних технологій: використання BIM (Building Information Modeling) і IoT (Інтернет речей) збільшує ризики, оскільки ці системи можуть бути цілями для хакерів. Наприклад, злом BIM-системи може призвести до спотворення проєктної документації, що загрожує безпеці будівельного об’єкта, а злом IoT-пристроїв, таких як камери чи датчики, може створити фізичні ризики на майданчику.

Дотримання регуляторних вимог: багато країн мають законодавчі вимоги щодо захисту даних, і невиконання цих вимог може призвести до штрафів та юридичних наслідків. Наприклад, у Європейському Союзі діють правила GDPR, які вимагають захисту персональних даних, що може стосуватися і будівельних компаній.

Фінансові та репутаційні наслідки: дослідження показують, що

кібератаки можуть коштувати будівельній індустрії мільярди доларів щороку через втрати даних, простої та відновлення систем. Крім того, втрата довіри клієнтів може серйозно підірвати репутацію компанії, особливо якщо інформація про проєкти стане публічною.

Для будівельних підприємств безпека мереж є ключовою, адже вони працюють з конфіденційними даними, такими як проєкти і контракти. Кібератаки можуть затримати проєкти або навіть створити небезпеку на майданчиках через вразливість IoT-пристроїв.

2.1 Загрози та вразливості в інфокомунікаційних мережах

Інфокомунікаційні мережі піддаються різноманітним загрозам, які можуть вплинути на їхню безпеку та функціональність. Серед найпоширеніших:

Малварі: віруси, черви, троянці, шифровальні віруси (ransomware), шпигунське програмне забезпечення (spyware) та рекламні програми (adware) можуть викрадати дані, пошкоджувати системи або блокувати доступ до інформації [8].

Атаки на мережу: атаки типу "людина посередині" (man-in-the-middle, MitM), перехоплення пакетів, атаки відмови в обслуговуванні (DoS і DDoS), захоплення сеансів, підробка (spoofing) і сканування портів можуть порушити роботу мережі або викрасти дані [8].

Атаки на додатки: ін’єкції SQL, ін’єкції команд і кросдоменний скриптинг (XSS) використовуються для отримання доступу до баз даних або веб-додатків [8].

Бездротові загроз: підроблені точки доступу, атаки "злого близнюка" (evil twin) і підслуховування Wi-Fi загрожують безпеці бездротових мереж, які часто використовуються в офісах [8].

Соціальна інженерія: фішинг, спір-фішинг, атаки на керівників (whaling) і приманка (baiting) обманом змушують працівників розкривати конфіденційну

інформацію [8].

Шифрові загрози: експлойти протоколів SSL/TLS і слабке шифрування дозволяють хакерам перехоплювати захищені дані [8].

Загрози апаратного забезпечення: захоплення DNS, атаки на пристрої IoT і шкідливі USB-пристрої можуть компрометувати мережеве обладнання [8].

Постійні просунуті загрози (APT): Використання вразливостей нульового дня і складна розвідка дозволяють хакерам довгостроково проникати в мережі [8].

Загрози IoT та OT: Компрометація пристроїв Інтернету речей (IoT) і операційних технологій (OT) може порушити контроль над обладнанням [8].

Ці загрози є актуальними для будь-якого підприємства, але для будівельних компаній вони набувають особливої ваги через використання спеціалізованих технологій, таких як Building Information Modeling (BIM), IoT-пристрої для моніторингу будівельних майданчиків і хмарні сервіси для управління документацією.

2.2 Методи захисту: VPN, ACL, firewall

Інфокомунікаційні мережі будівельного підприємства потребують надійних методів захисту для запобігання кібератакам, несанкціонованому доступу та витоку даних. У цьому підрозділі розглядаються три ключові методи захисту — VPN (Virtual Private Network), ACL (Access Control Lists) та firewall. Ці методи є основою для забезпечення безпеки даних, стабільності мережі та відповідності стандартам кібербезпеки, що є критично важливим для офісу будівельного підприємства, де обробляються чутливі дані, такі як проєктна документація чи фінансові звіти.

2.2.1 VPN (Virtual Private Network)

VPN створює зашифрований тунель між користувачем і мережею, що дозволяє безпечно передавати дані через публічні мережі, такі як інтернет. Це

особливо важливо для будівельного підприємства, де працівники можуть працювати віддалено або на будівельних майданчиках, потребуючи доступу до корпоративних ресурсів, таких як BIM-системи чи бази даних. VPN захищає дані від перехоплення, використовуючи протоколи, такі як IPsec або GRE. У Cisco Packet Tracer можна налаштувати VPN для симуляції віддаленого доступу, перевіряючи його ефективність у захисті даних і забезпеченні стабільного з'єднання. Наприклад, можна змоделювати сценарій, де віддалений працівник підключається до серверів підприємства через зашифрований канал, що гарантує конфіденційність інформації [9].

2.2.2 ACL (Access Control Lists)

ACL — це інструмент для контролю доступу до мережевих ресурсів, який дозволяє фільтрувати трафік на основі IP-адрес, портів чи протоколів. Вони налаштовуються на маршрутизаторах або комутаторах і визначають, які пристрої чи користувачі можуть отримувати доступ до певних сегментів мережі. Для будівельного підприємства ACL можуть обмежувати доступ до серверів з проєктною документацією, дозволяючи лише авто ризованим користувачам працювати з цими даними. У Cisco Packet Tracer ACL можна використовувати для створення правил, які, наприклад, дозволяють лише певним IP-адресам доступ до фінансових систем, блокуючи всі інші запити. Це допомагає зменшити ризик несанкціонованого доступу та підвищує безпеку мережі [10].

2.2.3 Firewall

Firewall (мережевий екран) захищає мережу від зовнішніх загроз, аналізуючи вхідний і вихідний трафік і блокуючи шкідливі пакети, такі як ті, що походять від malware чи DDoS-атак. Він працює на основі заздалегідь визначених правил, які дозволяють або забороняють трафік залежно від його характеристик. Для будівельного підприємства firewall є необхідним для захисту від кібератак, які можуть призвести до витоку даних чи порушення

роботи систем. У Cisco Packet Tracer firewall можна налаштувати за допомогою віртуальних пристроїв, таких як Cisco ASA, для моделювання захисту від зовнішніх атак. Наприклад, можна створити правило, яке блокує всі вхідні запити з невідомих IP-адрес, дозволяючи лише авторизований трафік [11].

2.3 Стандарти та найкращі практики безпеки

Безпека інфокомунікаційних мереж є критично важливою для будівельних підприємств, які працюють із конфіденційними даними, такими як проєктна документація, фінансові звіти та інформація клієнтів. Міжнародні стандарти та найкращі практики безпеки допомагають систематично захищати ці дані, зменшувати ризики кібератак і забезпечувати відповідність регуляторним вимогам. У цьому підрозділі розглядаються ключові стандарти, такі як ISO/IEC 27001, NIST Cybersecurity Framework і GDPR, а також практичні заходи, які можна налаштувати в Cisco Packet Tracer для моделювання безпечної мережі офісу будівельного підприємства.

Стандарти безпеки встановлюють чіткі вимоги до захисту інфокомунікаційних мереж. ISO/IEC 27001 є міжнародним стандартом, який визначає рамки для управління інформаційною безпекою, включаючи ідентифікацію ризиків, захист даних і контроль доступу. Цей стандарт допомагає підприємствам систематично підходити до кібербезпеки, що є важливим для будівельної галузі, де витік даних може призвести до значних фінансових втрат [12]. NIST Cybersecurity Framework пропонує структурований підхід до управління кібербезпекою, який включає п’ять основних функцій: ідентифікація, захист, виявлення, реагування та відновлення. Цей фреймворк є гнучким і підходить для організацій, які потребують адаптивної моделі безпеки [12]. Для будівельних підприємств, які працюють у Європейському Союзі, GDPR є обов’язковим, оскільки він регулює захист персональних даних клієнтів і працівників, вимагаючи впровадження шифрування та інших заходів безпеки [13].

Найкращі практики безпеки включають технічні та організаційні заходи, які можна реалізувати для захисту мережі. VPN (Virtual Private Network) забезпечує безпечний віддалений доступ до мережі, шифруючи дані, що передаються через інтернет. Це особливо важливо для будівельних підприємств, де працівники можуть підключатися до мережі з будівельних майданчиків чи віддалених локацій [12]. ACL (Access Control Lists) дозволяють контролювати доступ до мережевих ресурсів, фільтруючи трафік на основі IP-адрес, портів чи протоколів. Наприклад, ACL можна налаштувати для обмеження доступу до серверів із проєктною документацією лише для авторизованих користувачів [10]. Firewall захищає мережу від зовнішніх загроз, таких як malware чи DDoS-атаки, блокуючи шкідливі пакети на основі заздалегідь визначених правил [11]. Регулярне оновлення програмного забезпечення є необхідним для запобігання експлуатації відомих вразливостей, оскільки застаріле ПЗ є однією з основних причин кібератак у будівельній галузі. Навчання персоналу щодо розпізнавання фішингових атак і соціальної інженерії також є ключовим, оскільки працівники часто є найслабшою ланкою в системі безпеки.

2.4 Специфіка інфокомунікаційної мережі для будівельної галузі

Будівельні підприємства мають унікальні виклики щодо кібербезпеки через використання спеціалізованих технологій, таких як Building Information Modeling (BIM) та Інтернет речей (IoT). BIM-системи містять детальні цифрові моделі будівель, які є цінною інтелектуальною власністю, тому їхній захист є пріоритетним. Наприклад, компрометація BIM-системи може призвести до спотворення проєктних даних, що загрожує безпеці будівельного об’єкта [8]. IoT-пристрої, такі як датчики чи камери на будівельних майданчиках, також є вразливими до атак, оскільки часто мають слабкі механізми безпеки. Впровадження стандартів, таких як ISO/IEC 27001, і практик, таких як шифрування та firewall, допомагає захистити ці системи [5]. Крім того, будівельні

підприємства часто співпрацюють із численними підрядниками, що збільшує кількість точок доступу до мережі. Використання ACL і VPN дозволяє обмежити доступ сторонніх осіб до чутливих даних [9,10].

2.5 Практичне застосування в Cisco Packet Tracer

Cisco Packet Tracer є популярним інструментом для моделювання стандартів і практик безпеки в інфокомунікаційних мережах. За допомогою цього інструмента VPN налаштовується для забезпечення безпечного віддаленого доступу до серверів із BIM-даними, ACL застосовуються для обмеження доступу до фінансових чи проєктних серверів лише для певних IP-адрес.

Firewall конфігурується для блокування зовнішніх атак, таких як DDoS чи спроби несанкціонованого доступу. Такі симуляції дозволяють перевірити ефективність заходів безпеки, виявити потенційні вразливості та оптимізувати конфігурацію мережі перед її реальним впровадженням. Наприклад, можна змоделювати сценарій, де хакер намагається отримати доступ до мережі, і перевірити, як firewall і ACL реагують на цю загрозу.

Стандарти безпеки, такі як ISO/IEC 27001, NIST Cybersecurity Framework і GDPR, разом із найкращими практиками, такими як VPN, ACL, firewall, оновлення ПЗ і навчання персоналу, є необхідними для створення захищеної інфокомунікаційної мережі будівельного підприємства. Ці заходи забезпечують захист чутливих даних, стабільність роботи мережі та відповідність регуляторним вимогам. Для будівельної галузі, яка використовує BIM та IoT, ці стандарти та практики є особливо важливими для запобігання витокам інформації та забезпечення безперебійної роботи проєктів. Моделювання цих заходів у Cisco Packet Tracer дозволяє отримати практичні навички та підготуватися до реального впровадження мережі.

3 ПЛАНУВАННЯ МЕРЕЖІ БУДІВЕЛЬНОГО ПІДПРИЄМСТВА

3.1 Фізичне планування мережі

Для реалізації проєкту інфокомунікаційної мережі підприємства необхідно створити її структурну схему, яка наочно відобразить усі потреби системи. Під час розробки такої схеми важливо пов’язати її з планом приміщень, де буде розгорнута мережа. Це дозволить чітко визначити вимоги до топології, типів кабелю та сформувати реалістичне уявлення про майбутню мережу.

Було створено план розміщення кімнат, а також їх взаємозв’язок відповідно до поставленого завдання. Для цього використано програмний комплекс Microsoft Visio.

Горизонтальна підсистема на поверсі реалізована на основі кабелю типу кручена пара категорії 5е.

План будівлі, розроблений у Microsoft Visio, зображено на рисунку 3.1.

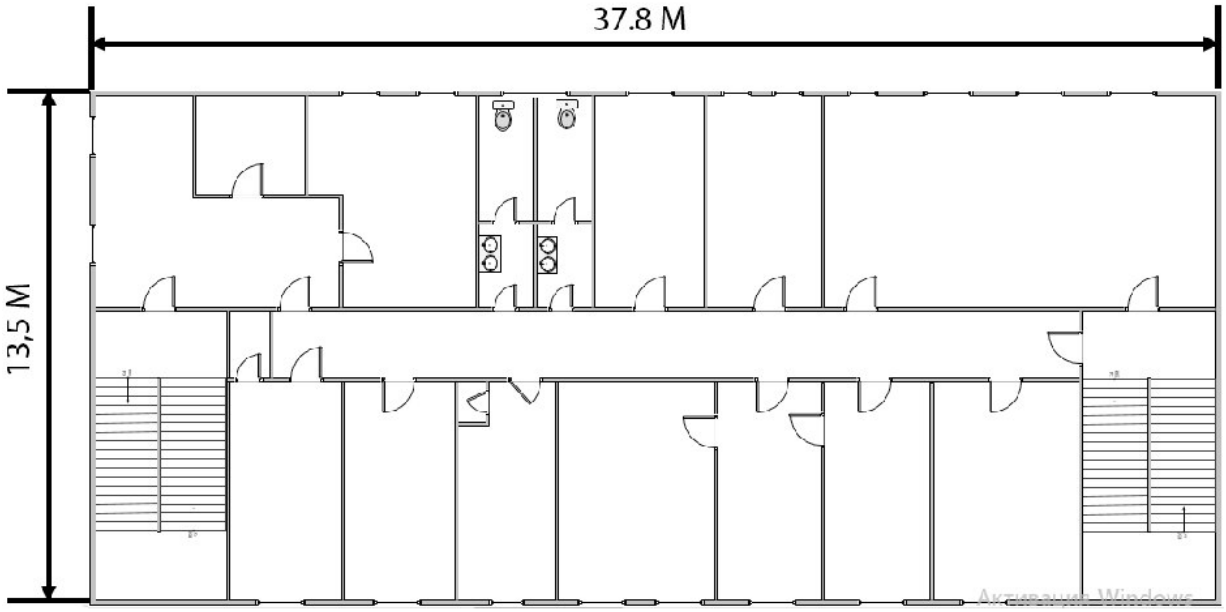

Рисунок 3.1 – План будівлі підприємства

3.2 Вибір топології мережі

Топологія мережі визначає спосіб фізичного та логічного з’єднання пристроїв у комп’ютерній мережі, впливаючи на її продуктивність, надійність, масштабованість і легкість управління. Для будівельного підприємства з двоповерховою будівлею розміром 37.8×13.5 м на кожному поверсі, вибір оптимальної топології є першим етапом проєктування інфокомунікаційної мережі. У цьому підрозділі розглядаються основні типи топологій, їх порівняння та обґрунтування вибору зіркової топології для даного підприємства.

Для вибору оптимальної топології розглянуто п’ять основних типів, які найчастіше використовуються в локальних мережах (LAN).

При використанні шинної топології (Bus Topology) усі пристрої підключені до єдиної кабельної магістралі, яка діє як основа мережі. Дані передаються через цю магістраль, і кожен пристрій отримує їх, але обробляє лише призначені для нього пакети (рис. 3.2).

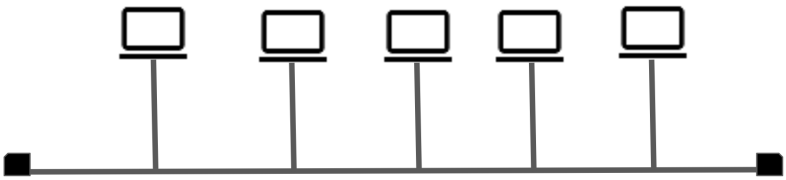

Рисунок 3.2 – Топологія «шина»

Переваги: простота встановлення, мінімальна кількість кабелів, низька вартість.

Недоліки: вихід з ладу магістралі призводить до відмови всієї мережі; складність виявлення помилок; низька масштабованість через обмеження пропускної здатності [14].

У зірковій топології (Star Topology) кожен пристрій підключений до центрального комутатора або концентратора окремим кабелем. Усі дані проходять через центральний пристрій, який керує трафіком (рис. 3.3).

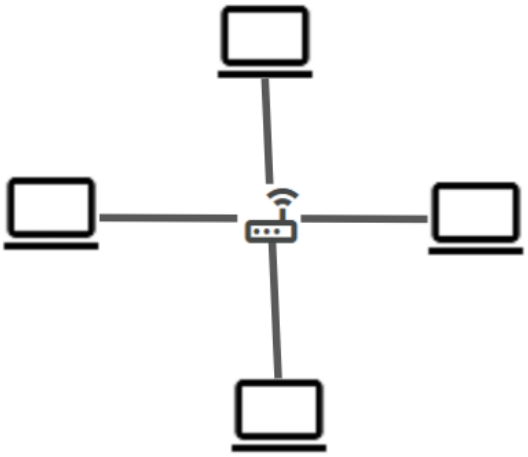

Рисунок 3.3 – Топологія «зірка»

Переваги: легкість управління та діагностики; ізоляція помилок (проблема з одним пристроєм не впливає на інші); простота додавання нових пристроїв; висока продуктивність завдяки окремим з’єднанням.

Недоліки: залежність від центрального комутатора (єдина точка відмови); більша кількість кабелів підвищує початкові витрати [14].

У кільцевій топології (Ring Topology) пристрої з’єднані у замкнуте коло, де кожен пристрій передає дані наступному. Дані циркулюють у мережі, доки не досягнуть адресата (рис. 3.4).

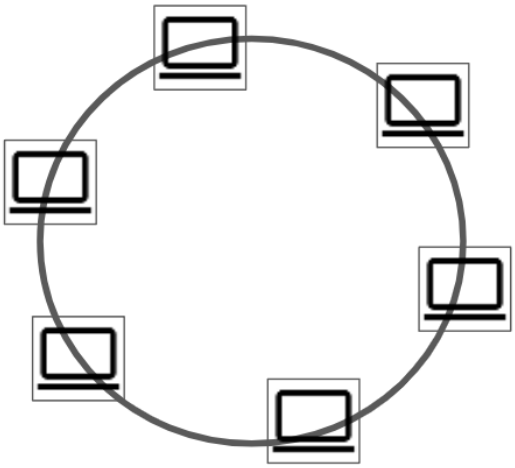

Рисунок 3.4 – Топологія «кільце»

Переваги: рівний доступ до ресурсів; висока продуктивність при високих навантаженнях; низький ризик колізій у подвійному кільці.

Недоліки: вихід з ладу одного пристрою може порушити роботу мережі; складність додавання чи видалення пристроїв; потреба в постійному управлінні [14].

У сітчастій топології (Mesh Topology) кожен пристрій з'єднаний з усіма іншими пристроями (повна сітка) або з кількома (часткова сітка) (рис. 3.5).

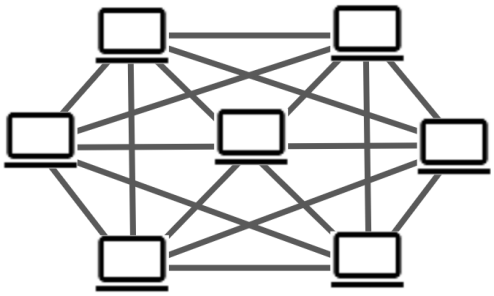

Рисунок 3.5 – Сітчаста топологія

Переваги: висока надійність через відсутність єдиної точки відмови; стійкість до збоїв; висока безпека та масштабованість.

Недоліки: висока вартість через велику кількість кабелів; складність налаштування та управління; значне споживання ресурсів [14].

У деревоподібній топології (Tree Topology) комбінується зіркова та шинна топології, де кілька зіркових мереж з'єднані через магістраль, утворюючи ієрархічну структуру (рис. 3.6).

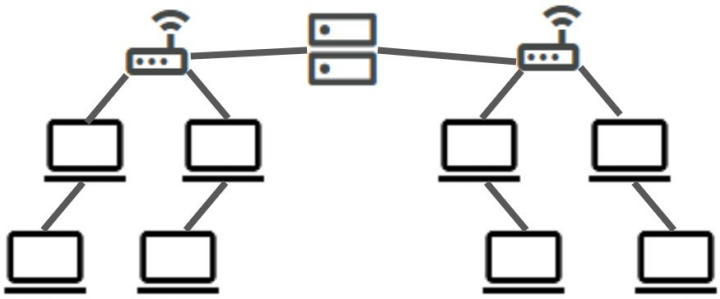

Рисунок 3.6 – Топологія «дерево»

Переваги: висока масштабованість; легкість управління завдяки ієрархії; підтримка різних типів носіїв.

Недоліки: залежність від магістралі та центральних вузлів; складність конфігурації; вищі витрати на кабелі [14].

3.3 Порівняння топологій для будівельного підприємства

Для вибору топології враховувалися вимоги, визначені в підрозділі 3.1, зокрема фізична структура будівлі (один поверх (37.8×13.5м), 15 робочих станцій), потреба в надійності, масштабованості, легкості управління та економічній ефективності. Нижче наведено порівняння топологій за ключовими критеріями:

Таблиця 3.1 – Порівняння топологій

Топологія	Надійність	Масштабованість	Легкість управління	Вартість	Продуктивність
Шинна	Низька (єдина точка відмови – магістраль)	Низька (обмеження пропускної здатності)	Складна (важко виявляти помилки)	Низька	Низька при високому навантаженні
Зіркова	Висока (ізоляція помилок)	Висока (легке додавання пристроїв)	Висока (централізоване управління)	Низька	Висока (окремі з’єднання)
Кільцева	Середня (залежить від одного вузла)	Низька (складність змін)	Середня (постійне управління)	Низька	Висока (надлишкові з’єднання)
Сітчаста	Дуже висока (немає єдиної точки відмови)	Висока (але складна)	Низька (складність конфігурації)	Висока	Висока (надлишкові з’єднання)
Деревоподібна	Висока (залежить від магістралі)	Висока (ієрархічна структура)	Висока (структуроване управління)	Середня	Висока (залежить від магістралі)

3.4 Аналіз розглянутих топологій для мережі будівельного підприємства

Шинна топологія не підходить через низьку надійність і масштабованість. Вихід з ладу магістралі може зупинити всю мережу, що неприпустимо для підприємства, яке залежить від постійного доступу до даних (наприклад,

креслень і BIM-моделей).

Кільцева топологія ускладнює додавання нових пристроїв і має ризик збою через залежність від кожного вузла, що не відповідає потребам гнучкості та простоти управління.

Сітчаста топологія є надто дорогою та складною для середнього підприємства з 20–50 станціями, оскільки потребує значних ресурсів на кабелі та конфігурацію.

Деревоподібна топологія є перспективною для більших мереж, але для одноповерхової будівлі з відносно невеликою кількістю пристроїв вона додає непотрібну складність і витрати на магістраль.

Зіркова топологія забезпечує баланс між надійністю, масштабованістю, легкістю управління та вартістю, що робить її ідеальною для даного підприємства. Центральний комутатор (або кілька комутаторів для кожної робочої групи) дозволяє адміністраторам легко моніторити та керувати мережею через централізовані інструменти. Це особливо важливо для підприємства, де мережа підтримує офісні програми, VoIP і спеціалізоване ПЗ, таке як CAD і BIM (Cisco Network Topology).

У зірковій топології проблема з одним пристроєм або кабелем не впливає на інші, що спрощує діагностику та ремонт. Це критично для будівельного підприємства, де простої мережі можуть затримувати проєктні роботи (Comparitech Network Topologies).

Додавання нових робочих станцій або пристроїв здійснюється шляхом підключення до центрального комутатора, що не вимагає значних змін у мережі. Це відповідає потребі підприємства в гнучкості для майбутнього розширення (GeeksforGeeks Topologies).

Кожен пристрій має власне з’єднання з комутатором, що забезпечує високу пропускну здатність і мінімізує затримки. Це важливо для передачі великих файлів, таких як проєктна документація, і для роботи хмарних сервісів.

Згідно з описом фізичного плану (5 робочих груп, 2–5 станцій у групі), зіркова топологія підходить для структурованої кабельної системи. Кожна

робоча група може мати власний комутатор, підключений до головного комутатора в серверній кімнаті, що забезпечує ефективне розподілення трафіку.

Основний недолік зіркової топології — залежність від центрального комутатора — можна пом’якшити шляхом використання високонадійних комутаторів (наприклад, Cisco Catalyst) і резервного обладнання. Крім того, початкові витрати на кабелі виправдані довгостроковими перевагами у вигляді зниження витрат на обслуговування та підвищення продуктивності (Comparitech Network Topologies) [14].

Фізична структура мережі, передбачає розміщення комутаторів для кожної робочої групи (5 на поверх) і головного комутатора в серверній кімнаті. Кабелі категорії 5e з’єднують робочі станції з комутаторами, а точки доступу WiFi підключаються до тих самих комутаторів для бездротового доступу. Така конфігурація відповідає зірковій топології, де кожен пристрій має пряме з’єднання з центральним вузлом. У деяких випадках, як видно з плану будівлі, кілька зіркових мереж можуть бути з’єднані через магістраль, утворюючи ієрархічну зіркову або деревоподібну топологію, але основна структура залишається зірковою.

Зіркова топологія є оптимальним вибором для інфокомунікаційної мережі будівельного підприємства завдяки своїй надійності, масштабованості, легкості управління та відповідності фізичним і функціональним вимогам. Вона забезпечує ефективну підтримку офісних і спеціалізованих будівельних додатків, мінімізуючи ризики збоїв і спрощуючи адміністрування.

3.5 Проєктування кабельної системи

Структурована кабельна система (СКС) є основою фізичної інфраструктури мережі будівельного підприємства, забезпечуючи надійне з’єднання 15 робочих комп’ютерів у одноповерховій будівлі розміром 13,5 м × 37,8 м (площа 510 м²). Проєкт відповідає стандартам ANSI/TIA-568 та ISO/IEC 11801, забезпечуючи високу продуктивність, масштабованість і легкість

управління.

Будівля має один поверх із 15 робочими станціями, розподіленими по приміщенню. Мережа підтримує офісні програми, VoIP і спеціалізоване ПЗ (наприклад, CAD, BIM), що вимагає пропускної здатності до 1 Гбіт/с. Використовується зіркова топологія.

Метою є створення СКС, яка має абезпечувати швидку передачу даних для великих файлів, буде надійною та з мінімальними простоями, дозволятиме легко додавати нові пристрої, також вона повинна відповідати стандартам безпеки та управління.

Структурована кабельна система (СКС) будівельного підприємства складається з компонентів, які забезпечують ефективну організацію мережевої інфраструктури.

Компоненти СКС можна розділити на серверну, яка містить основний комутатор, маршрутизатор і сервер, робочу зона що включає стінні розетки та патч-корди для підключення комп'ютерів, а вхідні приміщення слугують точкою підключення до кабелів провайдера.

При проєктуванні системи телекомунікаційна кімната (серверна) була розташована в лівій частині будівлі поруч із входом. В серверній розміщений серверний стелаж із обладнанням таким як: комутатор із портами для 5 свічів, патч-панелі та маршрутизатор (який з'єднаний із головним комутатором оптичним кабелем за технологією Gigabit Ethernet), при цьому забезпечені вентиляція, безперебійне живлення та обмежений доступ для безпеки. У робочій зоні встановлено 15 стінних розеток, які розміщені відповідно до розташування робочих станцій із урахуванням плану приміщення.

Зіркова топологія забезпечує пряме з'єднання кожної станції з комутатором через окремий кабель, що відповідає принципам ізоляції помилок і легкості управління.

Проєкт СКС для будівельного підприємства забезпечує надійну інфраструктуру для 15 робочих станцій та чіткого маркування. Відповідає потребам підприємства та стандартам.

Для цієї підсистеми було обрано технологію Fast Ethernet з використанням витої пари категорії 5е.

3.6 Розміщення робочих місць

Будівельне підприємство, яке є об’єктом проєкту, складається з п’яти відділів, кожен із яких має свої завдання та вимоги до інфокомунікаційної мережі. Загалом на підприємстві передбачено 15 робочих місць, розподілених наступним чином: бухгалтерія – 2 робочі місця, директорат – 1 робоче місце, інженерний відділ – 4 робочі місця, відділ постачання – 3 робочі місця та конференц-зал – 5 робочих місць. Нижче наведено опис функцій кожного відділу та їхніх потреб у мережевій інфраструктурі (рис 3.7).

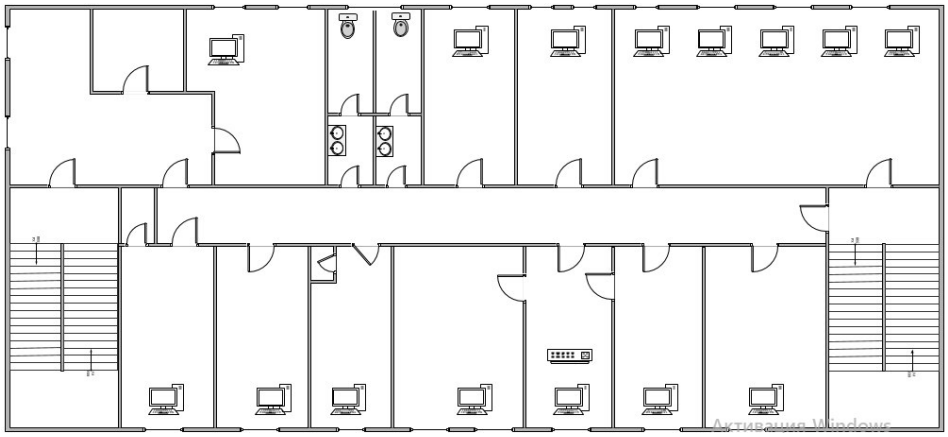

Рисунок 3.7 – План розміщення робочих місць підприємства

Бухгалтерія (2 робочі місця). Відділ бухгалтерії відповідає за фінансову діяльність підприємства, включаючи облік витрат на будівельні проєкти, обробку платежів підрядникам, нарахування заробітної плати та підготовку фінансових звітів.

Директорат (1 робоче місце). Директорат, представлений одним робочим місцем, займається стратегічним управлінням підприємством, прийняттям ключових рішень щодо проєктів, координацією роботи всіх відділів і

спілкуванням із клієнтами та партнерами. Директор потребує постійного доступу до всіх інформаційних ресурсів компанії, включаючи звіти, проєктну документацію та електронну пошту, а також можливості для відеоконференцій із віддаленими партнерами.

Інженерний відділ (4 робочі місця). Інженерний відділ є основним підрозділом, який відповідає за розробку будівельних проєктів, створення креслень, 3D-моделей та роботу з Building Information Modeling (BIM)-системами. Цей відділ обробляє великі обсяги даних, що потребує високої пропускної здатності мережі для швидкої передачі файлів між робочими станціями та сервером, а також низької затримки для роботи з BIM у реальному часі. Інженери також співпрацюють із будівельними майданчиками, тому мережа повинна підтримувати безпечний віддалений доступ до проєктних даних, наприклад, через налаштування VLAN для ізоляції трафіку та використання ACL для обмеження доступу.

Відділ постачання (3 робочі місця). Відділ постачання займається організацією закупівель матеріалів, логістикою та координацією доставки на будівельні майданчики, а також веде облік складських запасів. Працівники цього відділу використовують програми для управління ланцюгами постачання, які потребують стабільного доступу до баз даних і можливості обміну інформацією з постачальниками через інтернет. Мережа для цього відділу повинна забезпечити безперебійний доступ до хмарних сервісів, захист даних під час передачі та ізоляцію трафіку для уникнення перевантаження основних каналів зв’язку.

Конференц-зал (5 робочих місць). Конференц-зал використовується для проведення нарад, презентацій проєктів клієнтам, а також навчання персоналу, що передбачає використання мультимедійного обладнання, такого як проєктори, та відеоконференцій із віддаленими учасниками. У залі передбачено 5 робочих місць. Мережа в конференц-залі повинна мати високу пропускну здатність для передачі відео у високій якості, підтримувати бездротове підключення через Wi-Fi для гостей і забезпечувати безпеку через ізоляцію

гостьового доступу від основної мережі підприємства, наприклад, за допомогою окремої VLAN.

Приміщення має площу 510,3 м^2. Поверх вміщає у собі 13 кімнат, коридор, вбиральню, та сходи. Всього на поверсі розташовано 15 робочих місць.

Для даної СКС використовується кручена пара для внутрішньої прокладки та оптичний кабель для зовнішньої (рис 3.8).

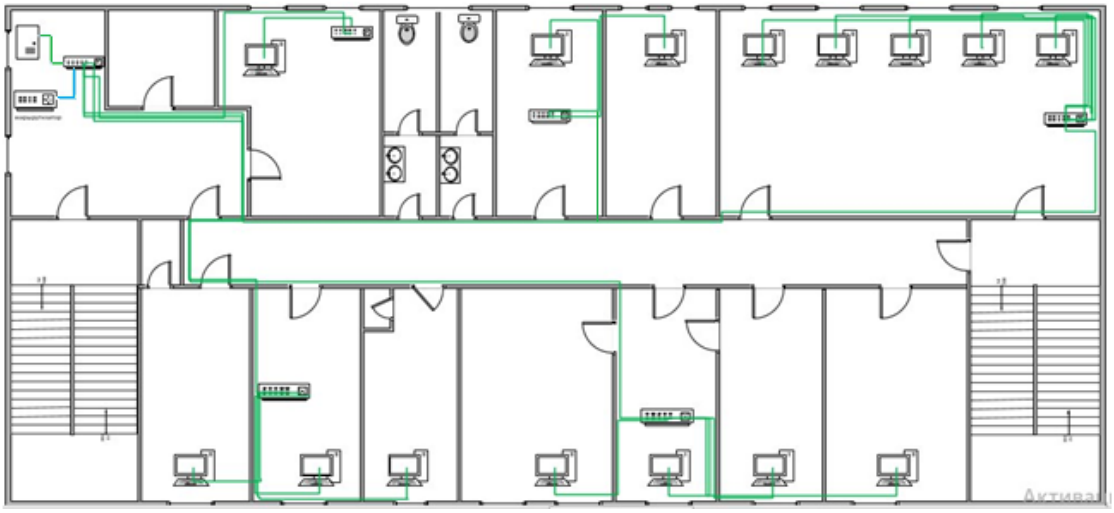

Рисунок 3.8 – Схема розведення крученої пари і розташування мережевого обладнання

Згідно з технічними параметрами, поверх має розміри 37,8 м на 13,5 м. Для мережі використано два види кабелю: кручена пара 5е категорії 408 м та 3 м оптичного кабелю.

4 ВИБІР МЕРЕЖЕВОГО ОБЛАДНАННЯ

Мережеве обладнання — це сукупність спеціалізованих пристроїв, які забезпечують створення, підтримку та управління інфокомунікаційними мережами, дозволяючи передачу, обробку та обмін даними між різними пристроями та користувачами.

До основних типів мережевого обладнання належать комутатори (switches), маршрутизатори (routers), сервери, джерела безперебійного живлення (UPS), оптичні термінали (ONT) та кабельні бокси [15].

4.1 Критерії вибору обладнання

Обладнання має відповідати технічним потребам підприємства, зокрема забезпечувати достатню пропускну здатність для передачі великих обсягів даних, таких як креслення та 3D-моделі, що є характерним для інженерного відділу.

4.2 Аналіз та вибір обладнання

Alcatel-Lucent I-010G – це оптичний мережевий термінал (ONT) (рис 4.1-4.2) призначений для використання в мережах пасивного оптичного доступу (PON). Цей пристрій забезпечує підключення кінцевих користувачів до оптичної мережі, перетворюючи оптичні сигнали в електричні для передачі даних через Ethernet. Він підтримує високошвидкісний доступ до Інтернету, голосового зв’язку (VoIP) та інших мережевих сервісів, що робить його оптимальним для використання в офісах, житлових будинках або підприємствах [16].

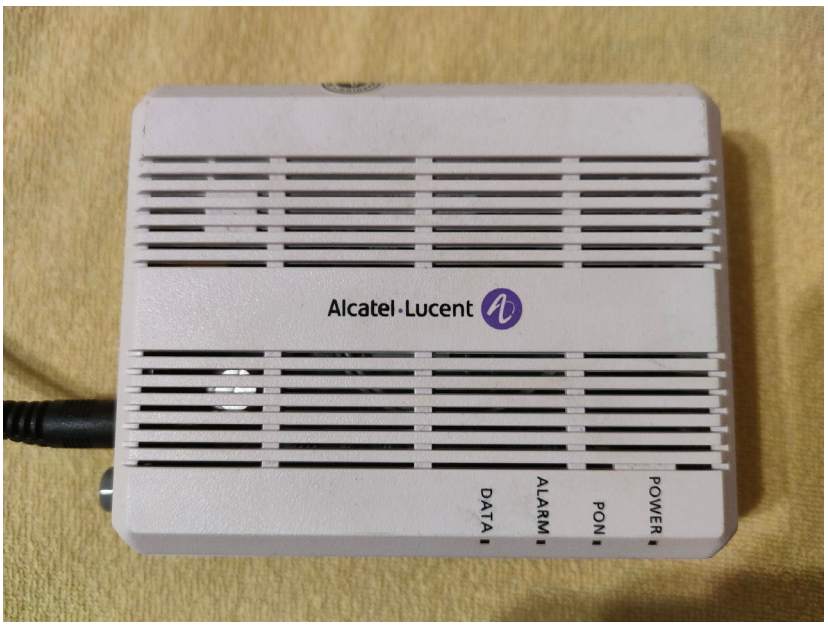

Рисунок 4.1 – Оптичний мережевий термінал Alcatel-Lucent I-010G

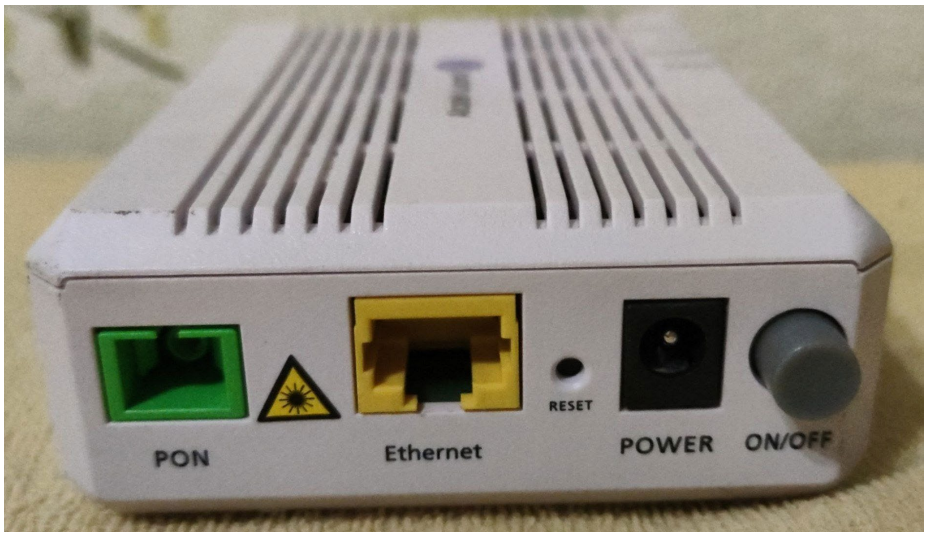

Рисунок 4.2 – Оптичний мережевий термінал Alcatel-Lucent I-010G

ONT оснащений кількома портами, включаючи оптичний порт (PON) для підключення до оптичної лінії, порт Ethernet (DATA) для підключення кінцевих пристроїв. Пристрій відповідає стандарту Class 1 Laser Product, що свідчить про безпечність його лазерного випромінювання при правильному використанні (табл. 4.1) [16].

Таблиця 4.1 – Технічні характеристики оптичного мережевого терміналу Alcatel-Lucent I-010G

Характеристика	Опис
Інтерфейс	1 порт 10/100/1000 Мбит/с (RJ45) 1 порт GPON (SC/UPC)
Оптичний стандарт	ITU-T G.984 (GPON)
Швидкість передачі даних	До 1 Гбіт/с на порт Ethernet
Лазерний клас	Class 1 Laser Product (безпечний для використання)
Кнопки	1 Reset Button (перезавантаження) 1 Power Button (харчування)
Зовнішній блок живлення	12 В постійного струму / 0,5 А
Відстань	0~20 км макс
Розміри	Довжина: 105 мм, Ширина: 82 мм, Висота: 36.5 мм
Оптичний модуль	Двонаправлений оптичний підвузол (BOSA) В Чутливість модуля від -8 до -28 RX
Стандарти IEEE	IEEE 802.3, 802.3u, 802.1Q, 802.1p, 802.1D, 802.1w ITU-T Y.1291, ITU-T G.984/G988
Довжина хвилі	Вхідна: 1490 нм Вихідна: 1310 нм
Робоча температура	-5°C ~ 55°C
Температура зберігання	-40°C ~ 80°C
Робоча вологість	5% ~ 90% без конденсації

Оптичний мережевий термінал Alcatel-Lucent I-010G використовується для підключення кінцевих користувачів до оптичної мережі за технологією GPON. Він забезпечує високошвидкісний доступ до Інтернету, підтримуючи швидкість до 1 Гбіт/с на порт Ethernet. Пристрій дозволяє підключати

комп’ютери, маршрутизатори або інші мережеві пристрої через порт Ethernet [16].

Цей ONT підходить для використання в офісах, багатоквартирних будинках або на підприємствах, де потрібен стабільний і швидкий доступ до Інтернету, а також можливість інтеграції з іншими мережевими сервісами, такими як VoIP або IPTV. Завдяки компактним розмірам і простоті встановлення, він є ефективним рішенням для розгортання сучасних оптичних мереж.

D-Link DES-1008D — це 8-портовий настільний комутатор Fast Ethernet (рис. 4.3), призначений для створення локальної мережі (LAN) у малих офісах або домашніх умовах. Цей пристрій забезпечує підключення кількох пристроїв, таких як комп’ютери, принтери та мережеві накопичувачі, для ефективного обміну даними. Комутатор працює на канальному рівні (рівень 2 моделі OSI), використовуючи MAC-адреси для передачі пакетів даних між підключеними пристроями [17].

Рисунок 4.3 – Комутатор D-Link DES-1008D

D-Link DES-1008D є активним мережевим обладнанням із підтримкою швидкості 10/100 Мбіт/с на кожному порті, що дозволяє забезпечити гнучкість підключення як старіших, так і сучасних пристроїв [17]. Його компактний

дизайн і відсутність необхідності в конфігурації роблять його простим у використанні та оптимальним для розгортання невеликих мереж (табл. 4.2).

Таблиця 4.2 – Технічні характеристики комутатора D-Link DES-1008D

Характеристика	Опис
Інтерфейс	8 портів 10/100 Мбіт/с RJ45, автоузгодження, авто MDI/MDIX
Світлодіодні індикатори	Живлення (Power), Link/Activity на кожному порті
Джерело живлення	Зовнішній адаптер (9 В, 0,6 А)
Метод комутації	Store-and-forward
Протокол	CSMA/CD
Розміри	Довжина: 162 мм, Ширина: 106 мм, Висота: 28 мм
Стандарти	IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX, IEEE 802.3x Flow Control
Метод комутації	Збереження і пересилання
Швидкість передачі даних	10/100 Мбіт/с (напівдуплекс), 20/200 Мбіт/с (повний дуплекс)
Ємність комутаційної матриці	1,6 Гбіт/с
Таблиця MAC-адрес	2K записів, автоматичне навчання і старіння
Робоча температура	0°C ~ 40°C
Температура зберігання	-10°C ~ 70°C
Робоча вологість	10% ~ 90% без конденсації

Комутатор D-Link DES-1008D призначений для підключення кількох пристроїв у локальну мережу, забезпечуючи швидкий і надійний обмін даними. Він ідеально підходить для малих офісів, домашніх мереж або робочих груп, де потрібно з’єднати до восьми пристроїв, таких як комп’ютери, мережеві

принтери або IP-телефони. Завдяки підтримці авто MDI/MDIX і автоматичного визначення швидкості, пристрій спрощує встановлення, усуваючи потребу в крос-кабелях [17].

Цей комутатор підвищує ефективність мережі, спрямовуючи пакети даних лише до призначених одержувачів, що зменшує завантаженість і покращує продуктивність порівняно з концентраторами. Його компактність і відсутність потреби в налаштуванні роблять його зручним рішенням для користувачів, які шукають просте та економічне мережеве обладнання.

Настінний бокс для кабелю Category 5e (Cat 5e) (рис. 4.4) призначений для монтажу на стіну. Забезпечує точку підключення для мережних кабелів через роз'єм RJ45, що робить його придатним для структурованих кабельних систем. На верхній поверхні пристрою є маркування CAT 5E, що вказує на підтримку кабелю категорії 5e, який забезпечує передачу даних зі швидкістю до 1 Гбіт/с і частотою до 100 МГц.

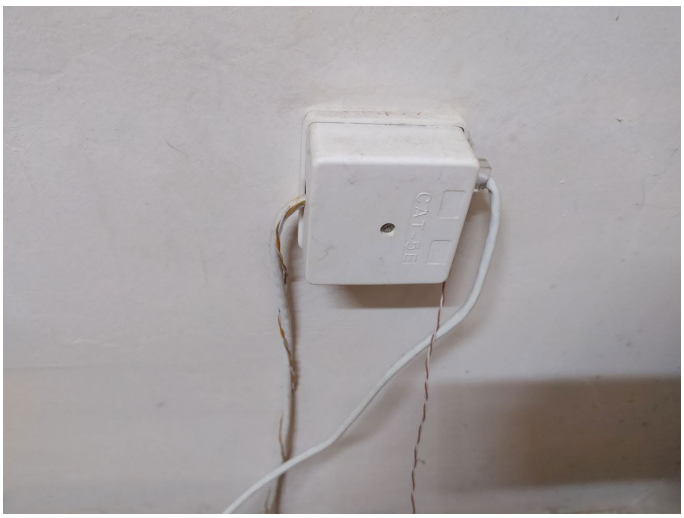

Рисунок 4.4 – Настінний бокс для кабелю

Використовується для створення зручної точки підключення мережевих пристроїв, таких як комп'ютери, телефони або принтери до локальної мережі через стандартний роз'єм RJ45. Завдяки настінному монтажу він забезпечує акуратне та організоване розміщення кабелів, що особливо важливо в офісних приміщеннях або житлових будинках з великою кількістю мережевих з'єднань.

Сервер CSV Rackmount призначений для обробки великих обсягів даних у серверних стійках (рис. 4.5).

Рисунок 4.5 – Сервер CSV Rackmount

Цей пристрій підходить для корпоративних мереж, де потрібна висока обчислювальна потужність і надійне зберігання даних (табл. 4.3).

Таблиця 4.3 – Технічні характеристики сервера CSV Rackmount

Характеристика	Опис
Форм-фактор	2 U Rackmount
Процесор	AMD Athlon 64 X2 (~2.0–3.0 GHz)
Кількість дисків	6 слотів для HDD/SSD (Hot-Swap)
Інтерфейси	USB, CD/DVD-ROM (LG)
Вентиляція	Вбудований вентилятор
Світлодіодні індикатори	Світло (зелений), живлення (червоний)
Розміри	Стандартний 2U, висота ~8.9 см
Робоча температура	0-40°C

Додаткові функції:

– підтримка гарячої заміни дисків для безперервної роботи;
– вбудований вентилятор для ефективного охолодження;
– можливість розширення через слоти PCI або аналогічні;
– сумісність та підтримувані системи.

Пристрій сумісний із серверними операційними системами, такими як Windows Server, Linux, та іншими платформами для корпоративного використання.

Сервер CSV Rackmount є надійним рішенням для корпоративних мереж, забезпечуючи високу продуктивність, гнучкість у зберіганні даних і ефективне охолодження.

TP-Link TL-WR841N — це бездротовий маршрутизатор стандарту N, призначений для створення локальної мережі з доступом до Інтернету в домашніх або невеликих офісних умовах (рис.4.4) [18].

Рисунок 4.6 – Маршрутизатор TP-Link TL-WR841N

і

Пристрій оснащений двома зовнішніми антенами для забезпечення стабільного Wi-Fi-покриття та має кілька портів для дротового підключення. На передній панелі розташовані світлодіодні індикатори, які відображають стан живлення, бездротового з’єднання, WAN і LAN-портів, а також функції WPS і безпеки [18].

Маршрутизатор підтримує сучасні технології бездротового зв’язку, що дозволяє ефективно розподіляти Інтернет між кількома пристроями, такими як комп’ютери, смартфони та планшети (табл. 4.5).

Таблиця 4.4 – Технічні характеристики маршрутизатора TP-Link TL-WR841N

Характеристика	Опис
1	2
Стандарти бездротового зв’язку	IEEE 802.11b/g/n (2.4 ГГц)
Швидкість передачі даних	До 300 Мбіт/с (бездротова), 10/100 Мбіт/с (дротове підключення)
Частотний діапазон	2.4 ГГц
Антени	2 зовнішні антени, 5 дБі
Порти	1 порт WAN 10/100 Мбіт/с, 4 порти LAN 10/100 Мбіт/с (Auto MDI/MDIX)
Безпека	WEP, WPA/WPA2-PSK, WPA-PSK/WPA2-PSK, WPS
Джерело живлення	9 В, 0.6 А (зовнішній адаптер)
Розміри	Довжина: 173 мм, Ширина: 118 мм, Висота: 33 мм
Режими роботи	Маршрутизатор, Точка доступу (AP), Повторювач, Клієнт
Робоча температура	0°C ~ 40°C
Температура зберігання	-40°C ~ 70°C
Робоча вологість	10% ~ 90% без конденсації

Бездротовий маршрутизатор TP-Link TL-WR841N призначений для створення локальної мережі з доступом до Інтернету в домашніх умовах, невеликих офісах або навчальних закладах. Він забезпечує підключення до Інтернету через порт WAN, розподіляючи його між пристроями як через

бездротове з’єднання (Wi-Fi зі швидкістю до 300 Мбіт/с), так і через чотири порти LAN. Завдяки підтримці стандарту 802.11n і двом антенам пристрій забезпечує стабільне покриття в межах середнього приміщення [18].

Маршрутизатор підтримує функцію WPS для швидкого безпечного підключення пристроїв та пропонує кілька рівнів шифрування (WEP, WPA/WPA2) для захисту мережі [18]. Його компактний дизайн і простота налаштування роблять TP-Link TL-WR841N зручним рішенням для користувачів, які шукають доступний і надійний спосіб організації бездротової мережі.

APC SUA 1000 RMI 2U – це компактний безперебійник баштового типу (рис. 4.7), призначений для забезпечення резервного живлення критичних електронних пристроїв, таких як комп’ютери, сервери або мережеве обладнання, у разі відключення електроенергії [19].

Рисунок 4.7 – Безперебійник APC SUA 1000 RMI 2U

Пристрій має міцний пластиковий корпус чорного кольору з перфорованою передньою панеллю для вентиляції та оснащений дисплеєм із світлодіодними індикаторами, які показують рівень заряду батареї, режим

роботи та статус живлення. На передній панелі також розташовані кнопки для тестування (Test) і включення/виключення пристрою.

Безперебійник інтегрований у стійку, використається в серверних кімнатах або центрах обробки даних. Технічні характеристики наведено в таблиці 4.5.

Таблиця 4.5 – Технічні характеристики безперебійника APC SUA 1000 RMI 2U

Характеристика	Опис
Тип	Джерело безперебійного живлення (UPS), баштовий
Потужність	600-1000 ВА
Вихідні роз’єми	4x IEC C13 (резервне живлення)
Час автономної роботи	31,6 хвилин при половинному навантаженні (335 Вт), 9,1 хвилин при повному навантаженні (670 Вт
Типовий час зарядки	3 години
Світлодіодні індикатори	Рівень заряду батареї, режим роботи (лінія/батарея), статус
Тип батареї	Герметична свинцево-кислотна батарея без обслуговування, із суспендованим електролітом
Розміри	Довжина: 432 мм, Ширина: 89 мм, Висота: 457 мм
Технологія	Лінія-інтерактивна (Line-Interactive)
Робоча температура	0°C ~ 40°C
Температура зберігання	-15°C ~ 45°C
Робоча вологість	0% ~ 95% без конденсації
Тип хвилі	Синусоїдальна
Інтерфейси	USB, DB-9 RS-232, SmartSlot.
Номінальна вихідна напруга	220-240 В
Номінальна вхідна напруга	230 В
Діапазон вхідної напруги	160–280 В (для основної роботи), 151–302 В (регульований
Частота входу	50/60 Гц ± 3 Гц (автовиявлення)

Безперебійник APC SUA 1000 RMI 2U призначений для захисту серверів, робочих станцій, комутаторів, маршрутизаторів та іншого мережевого обладнання від перебоїв електроенергії. Завдяки підтримці USB і SmartSlot він дозволяє інтегрувати програмне забезпечення для автоматичного збереження даних і безпечного вимкнення систем. Пристрій також забезпечує захист від стрибків напруги завдяки рейтингу енергії 480 Дж, що робить його придатним для офісних мереж, де важлива безперервність роботи. Технологія Line-Interactive стабілізує напругу, захищаючи пристрої від стрибків і падінь напруги [19].

APC SUA 1000 RMI 2U включає кілька вихідних роз'ємів для підключення пристроїв і підтримує функцію автоматичного регулювання напруги (AVR), що стабілізує електроживлення під час коливань. Завдяки інтелектуальному управлінню батареєю пристрій максимізує термін служби акумулятора та забезпечує безпечне вимкнення обладнання при повному розряді [19].

Пристрій забезпечує автономну роботу на 15 хвилин (залежно від навантаження), що дозволяє завершити критичні операції або переключитися на альтернативне джерело живлення. Його компактний дизайн і можливість монтажу в стійку роблять безперебійник APC SUA 1000 RMI 2U зручним для використання в технічних середовищах, де простір обмежений [19].

Було встановлено серверну стійку з комутаційними панелями (patch panel) і мережевими комутаторами (switch) (рис. 4.8-4.9), які є основою структурованої кабельної системи підприємства. Ці пристрої організовують, маршрутизують і розподіляють локальний мережевий трафік між усіма комп'ютерами в мережі офісу.

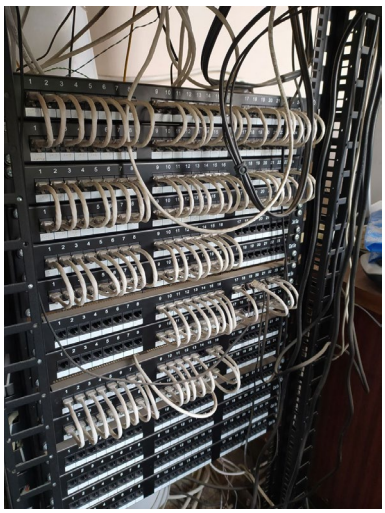

Рисунок 4.8 – Нижня частина серверів

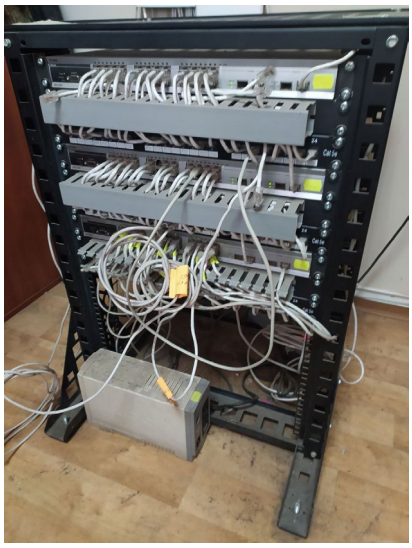

Рисунок 4.9 – Триярусний свіч

На рисунку 4.8 зображена нижня частина серверів яка дозволяє розподіляти запити від комп'ютерів. Патч-панелі (Patch Panels) – використовуються для впорядкування підключень мережевих кабелів. Кожен порт панелі відповідає за з'єднання з робочим місцем.

На рисунку 4.9 триярусний свіч який дозволяє розподіляти інтернет та доступ до серверу по всім комп'ютерам. Це мережеве обладнання дозволяє оптимально організувати кабельну систему, підключити до мережі всі відділи (бухгалтерія, інженерний, постачання, директорат тощо), забезпечуючи швидкий і надійний обмін даними. Через комутатори відбувається розподіл

доступу до локальних серверів, до інтернету та до хмарних сервісів, що необхідні для роботи з 3D-моделями, BIM-системами і проєктною документацією. Завдяки правильному фізичному і логічному проєктуванню цієї частини мережі гарантується безперебійна передача даних, кібербезпека (через ізоляцію VLAN) та легкість масштабування, що є критично важливим у динамічному середовищі будівельного бізнесу.

4.3 Обґрунтування вибору обладнання

Оптичний термінал Alcatel-Lucent I-010G забезпечує високошвидкісний доступ до Інтернету зі швидкістю до 2,5 Гбіт/с у напрямку до користувача, що відповідає потребам у стабільному з’єднанні для хмарних сервісів

Мережа повинна бути здатною до розширення в майбутньому, якщо кількість робочих місць чи відділів зросте. Комутатор D-Link DES-1008D має достатню кількість портів для підключення додаткових пристроїв, а сервер CSV Rackmount із 6 слотами для дисків із підтримкою гарячої заміни дозволяє легко додавати нові накопичувачі для збільшення обсягу зберігання даних. Маршрутизатор TP-Link TL-WR841N із підтримкою Wi-Fi забезпечує гнучкість для підключення тимчасових пристроїв у конференц-залі через бездротовий зв’язок.

Обладнання має бути сумісним із сучасними мережевими технологіями, такими як VLAN, VoIP і бездротові мережі, що використовуються в будівельній галузі. Маршрутизатор TP-Link TL-WR841N підтримує стандарт 802.11n і швидкість Wi-Fi до 300 Мбіт/с, що дозволяє організувати бездротовий доступ для гостей у конференц-залі, а також підтримує VoIP для голосового зв’язку директорату. Оптичний термінал Alcatel-Lucent I-010G підтримує технологію GPON, що забезпечує інтеграцію з оптичними мережами для високошвидкісного доступу до Інтернету.

З огляду на роботу з конфіденційними даними, такими як фінансові звіти та проєктна документація, обладнання має забезпечувати захист мережі.

Маршрутизатор TP-Link TL-WR841N підтримує шифрування WPA/WPA2, що захищає бездротову мережу від несанкціонованого доступу. Комутатор D-Link DES-1008D спрямовують пакети даних лише до призначених одержувачів, зменшуючи ризик перехоплення. Джерело безперебійного живлення APC SUA 1000 RMI 2U забезпечує стабільність роботи серверів і мережевих пристроїв у разі відключення електроенергії, що запобігає втраті даних.

Для невеликого підприємства важливим є співвідношення ціни та якості. Комутатор D-Link DES-1008D є економічним рішенням для малих офісів, забезпечуючи достатню продуктивність без складного налаштування. Маршрутизатор TP-Link TL-WR841N і настінний бокс Category 5e також є доступними, але водночас ефективними для створення структурованої кабельної системи. Сервер CSV Rackmount, хоча й дорожчий, виправдовує свою ціну завдяки підтримці гарячої заміни дисків і високій продуктивності для обробки даних.

Обладнання має бути зручним у встановленні та управлінні, оскільки не всі працівники підприємства мають технічні навички. Комутатор D-Link DES-1008D підтримує авто MDI/MDIX, що усуває потребу в крос-кабелях і спрощує підключення. Маршрутизатор TP-Link TL-WR841N має інтуїтивно зрозумілий інтерфейс для базового налаштування, а настінний бокс Category 5e забезпечує акуратне розміщення кабелів із простим монтажем. Джерело безперебійного живлення APC SUA 1000 RMI 2U оснащене світлодіодними індикаторами для легкого моніторингу стану.

Обладнання має бути надійним, щоб мінімізувати збої в роботі мережі. Сервер CSV Rackmount із вбудованим вентилятором і підтримкою гарячої заміни дисків забезпечує безперервну роботу навіть у разі відмови одного з компонентів. Джерело безперебійного живлення APC SUA 1000 RMI 2U захищає обладнання від стрибків напруги, подовжуючи термін його служби. Комутатор D-Link DES-1008D має міцний корпус і перевірену репутацію для використання в офісних умовах.

5 МОДЕЛЮВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖІ В CISCO PACKET TRACER

5.1 Розбиття мережі на підмережі на основі IP-адресів.

Проєктування IP-адресного простору є важливим етапом створення інфокомунікаційної мережі будівельного підприємства, оскільки воно забезпечує логічну організацію мережі, ефективне управління трафіком і безпеку даних. Для офісу з 15 робочими місцями, розподіленими між 5 відділами (бухгалтерія – 2 місця, директорат – 1 місце, інженерний відділ – 4 місця, відділ постачання – 3 місця, конференц-зал – 5 місць), необхідно створити структурований план IP-адресації, який враховує потреби кожного відділу та можливість масштабування в майбутньому. У цьому підрозділі описано підхід до розподілу IP-адрес із використанням приватного діапазону та сегментації мережі через VLAN.

Для мережі будівельного підприємства обрано приватний діапазон IP-адрес класу A – 10.16.1.0/24, який забезпечує до 254 доступних адрес для пристроїв (256 адрес мінус 2 зарезервовані для мережевої адреси та широкомовної адреси). Цей діапазон є стандартним для невеликих локальних мереж (LAN) і дозволяє уникнути конфліктів із публічними адресами в Інтернеті. Маска підмережі /24 (255.255.255.0) забезпечує достатню кількість адрес для 15 робочих місць із запасом для майбутнього розширення (табл. 5.1).

Для підвищення безпеки та ефективності управління трафіком мережа розділена на 5 підмереж, кожна з яких відповідає окремому VLAN для кожного відділу. Використання VLAN дозволяє ізолювати трафік між відділами, зменшуючи ризик несанкціонованого доступу та широкомовних штормів, що є важливим для захисту конфіденційних даних, таких як фінансові звіти в бухгалтерії чи проєктна документація в інженерному відділі [20]. Кожна підмережа отримує свій діапазон адрес із загального пулу 10.16.1.0/24, а також

зарезервовано адреси для мережевого обладнання, такого як маршрутизатор і сервер.

Розподіл IP-адрес для забезпечення достатньої кількості адрес у кожній підмережі використано підхід із фіксованим розміром підмереж. Загальна кількість пристроїв (15 робочих місць плюс мережеве обладнання, таке як маршрутизатор, сервер і шлюз) становить приблизно 18. Кожна підмережа розрахована на мінімум 8 адрес (6 пристроїв плюс 2 зарезервовані), що відповідає масці /29 (255.255.255.248).

Таблиця 5.1 – Розподіл IP-адрес

VLAN	Відділ	Діапазон адрес	Шлюз	Кількість пристроїв	Запас адрес
VLAN 10	Бухгалтерія	10.16.1.8–10.16.1.15	10.16.1.9	2	4
VLAN 20	Директорат	10.16.1.16–10.16.1.23	10.16.1.17	1	5
VLAN 30	Інженерний відділ	10.16.1.24–10.16.1.31	10.16.1.25	4	2
VLAN 40	Відділ постачання	10.16.1.32–10.16.1.39	10.16.1.33	3	3
VLAN 50	Конференц-зал	10.16.1.40–10.16.1.47	10.16.1.41	5	1

5.2 Створення моделі мережі

Для вивчення інструментів, які використовуються для захисту мережі, у рамках підприємсва було створено модель мережі офісу будівельного підприємства з використанням програмного забезпечення Cisco Packet Tracer. Побудована модель включає 5 комутаторів відділів, 1 головний комутатор,

1 маршрутизатор та сервер (рис. 5.1) [21].

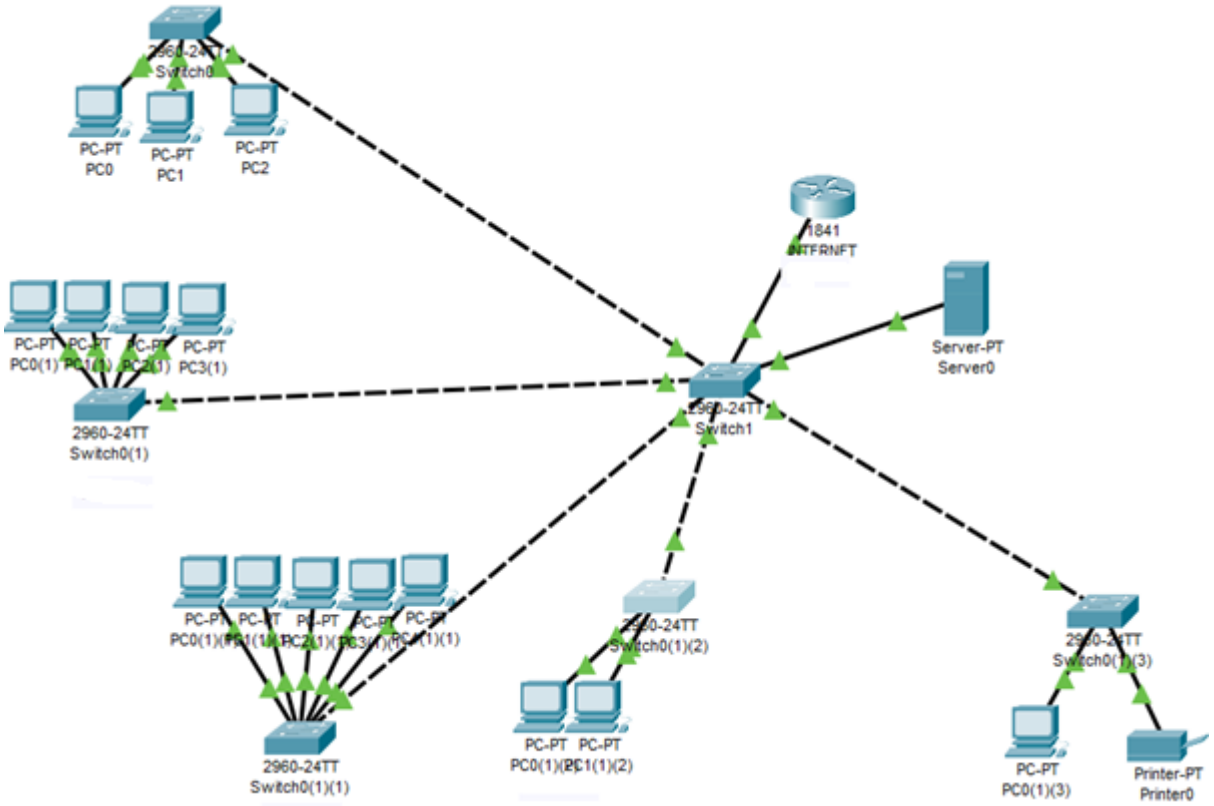

Рисунок 5.1 – Логічна структура інфокомунікаційної мережі підприємства

На рисунку 5.1 можна побачити, що індикатори портів світяться зеленим кольором, це означає що порти налаштовані вірно та здатні передавати дані.

Розроблена модель офісу складається з шести сегментів, з них п’ять це відділи, у яких розташовано 1-5 робочих станцій які з’єднані із комутаторами, та кожен відділ має свою IP-адресацію для зв’язку між іншими дозволеними сегментами мережі. Окрема кімната де розташована серверна, головний комутатор і роутер.

5.3 Налаштування маршрутизаторів і комутаторів

Кожен VLAN функціонує як окрема локальна мережа, що забезпечує

ізоляцію трафіку між сегментами на рівні канального шару моделі OSI (рівень 2). Для зв’язку між VLAN застосовується маршрутизація через маршрутизатор або Layer 3 комутатор [20].

На підприємстві були налаштовані комутатори які поділяють мережу на підрозділи до яких під’єднані персональні комп’ютери та комутатори. Для налаштування одного із комутаторів були виконані наступні команди.

Принцип розподілу VLAN для робочих груп:

1) робоча група 1 – VLAN 10;

2) робоча група 2 – VLAN 20;

3) робоча група 3 – VLAN 30;

4) робоча група 4 – VLAN 40;

5) робоча група 5 – VLAN 50.

Лістінг 5.1 – Налаштування комутатора першої робочої групи

```
Switch>enable
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#name Accounting
Switch(config-vlan)#interface range fa0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 10
Switch(config-if)#exit
Switch(config)#end
```

5.4 Впровадження VLAN

В роботі було створено VLAN для кожного відділу (лістинг 5.2).

Лістінг 5.2 – Команди створення та конфігурування VLAN:

```
enable
configure terminal
vlan 10
name Accounting
exit
vlan 20
name Directorate
exit
vlan 30
name Engineering
exit
vlan 40
name Supply
exit
vlan 50
name Conference
exit
interface range fa0/1-2
switchport mode access
switchport access vlan 10
exit
interface range fa0/3
switchport mode access
switchport access vlan 20
exit
interface range fa0/4-7
switchport mode access
switchport access vlan 30
exit
interface range fa0/8-10
switchport mode access
switchport access vlan 40
exit
interface range fa0/11-15
switchport mode access
switchport access vlan 50
exit
```

Ці команди створюють VLAN для кожної робочої групи та прив’язують відповідні порти комутатора до них, забезпечуючи ізоляцію трафіку.

Налаштування маршрутизатора для міжмережевої комунікації.

Для забезпечення зв’язку між VLAN використовується маршрутизатор із конфігурацією міжмережевої маршрутизації (Inter-VLAN Routing). Маршрутизатор підключається до комутатора через порт із режимом trunk, який передає трафік усіх VLAN. На маршрутизаторі створюються віртуальні інтерфейси (subinterfaces) для кожного VLAN із відповідними IP-адресами, що виступають шлюзами для підмереж.

Лістінг 5.3 – Налаштування trunk і subinterfaces:

```
enable
configure terminal
interface gigabitEthernet0/0
no shutdown
exit
interface gigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 10.16.1.9 255.255.255.248
no shutdown
exit
interface gigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 10.16.1.17 255.255.255.248
no shutdown
exit
interface gigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 10.16.1.25 255.255.255.248
no shutdown
exit
interface gigabitEthernet0/0.40
encapsulation dot1Q 40
ip address 10.16.1.33 255.255.255.248
no shutdown
exit
interface gigabitEthernet0/0.50
encapsulation dot1Q 50
ip address 10.16.1.41 255.255.255.248
no shutdown
exit
ip routing
```

Ця конфігурація активує маршрутизацію між VLAN, дозволяючи пристроям у різних підмережах обмінюватися даними через шлюзи.

Принцип розподілу VLAN базується на логічному розділенні мережі для кожної робочої групи, що забезпечує ізоляцію трафіку та підвищує безпеку. Кожному VLAN призначається унікальний ідентифікатор і діапазон IP-адрес, що відповідає кількості робочих місць у групі з урахуванням запасу.

Наприклад, VLAN 30 для інженерного відділу (4 місця) отримує 6 адрес (10.16.1.26–10.16.1.29 для пристроїв, плюс шлюз і запас). Такий підхід дозволяє:

Забезпечити безпеку: ізоляція трафіку між VLAN запобігає несанкціонованому доступу, наприклад, до фінансових даних бухгалтерії з інших відділів.

Оптимізувати продуктивність: зменшення широкомовного трафіку підвищує швидкість роботи, що важливо для інженерного відділу з великими файлами.

Спростити управління: прив’язка портів до VLAN дозволяє централізовано контролювати доступ до ресурсів.

Після налаштування в Cisco Packet Tracer необхідно перевірити працездатність мережі за допомогою команд, таких як ping між пристроями різних VLAN через маршрутизатор. Наприклад, відправка пакета з 10.16.1.10 (бухгалтерія) до 10.16.1.26 (інженерний відділ) має бути успішною, якщо маршрутизація коректно налаштована.

5.5 Налаштування ACL

Access Control Lists (ACLs) є важливим інструментом для забезпечення безпеки в інфокомунікаційних мережах. Налаштування ACL виконується через командний рядок (CLI) маршрутизатора в Cisco Packet Tracer. Нижче наведено покрокову інструкцію для створення та застосування розширеного ACL, який забороняє відділу постачання (VLAN 40, діапазон IP 10.16.1.32–10.16.1.39)

доступ до фінансового сервера (IP 10.16.1.100), але дозволяє решту трафіку.

Лістінг 5.4 – Налаштування ACL

```
enable
Configure terminal
Ip access-list extended 101
deny ip 10.16.1.32 0.0.0.7 10.16.1.100 0.0.0.0
permit ip any any
exit
interface gigabitEthernet0/0.40
ip access-group 101 in
exit
exit
```

access-list extended 101: визначає номер розширеного ACL (100–199).

deny ip: забороняє IP-трафік.

10.16.1.32 0.0.0.7: джерело — підмережа VLAN 40 (діапазон 10.16.1.32–10.16.1.39, маска /29).

10.16.1.100 0.0.0.0: призначення — фінансовий сервер.

permit ip any any: дозволяє весь інший трафік.

interface gigabitEthernet0/0.40: вибирає субінтерфейс для VLAN 40.

ip access-group 101 in: застосовує ACL 101 до вхідного трафіку.

Це гарантує, що трафік від відділу постачання фільтрується перед маршрутизацією до інших частин мережі.

Для дослідження роботи ACL було проведено тест із відділу постачання: ПК у VLAN 40 IP 10.16.1.35 виконуємо команду ping 10.16.1.100 (рис. 5.2).

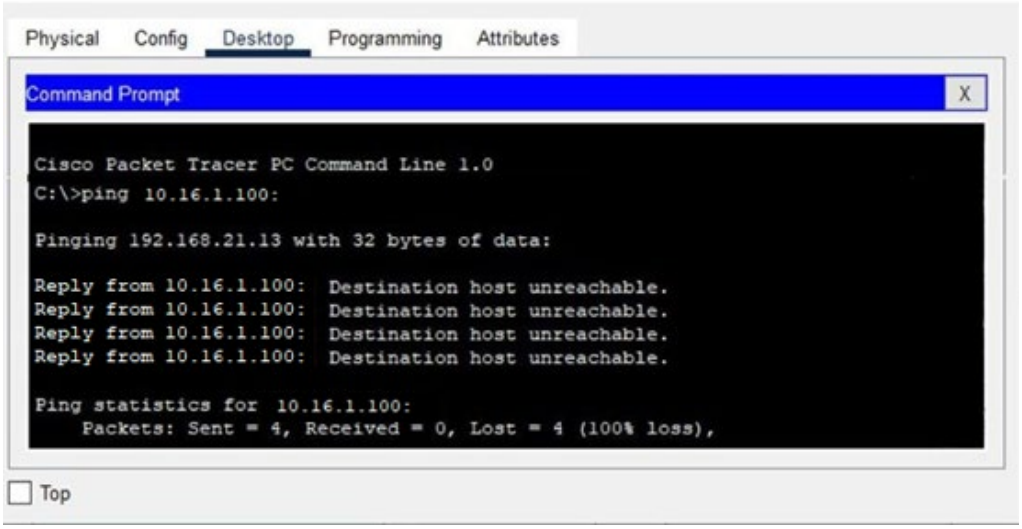

Рисунок 5.2 – Перевірка запиту від ПК у VLAN 40 до серверу

Ping невдалий через правило заборони.

Тест мережі з відділу бухгалтерії:

З ПК у VLAN 10 IP 10.16.1.10 виконуємо ping 10.16.1.100. Ping успішний(рис. 5.2), оскільки немає правила заборони для цього відділу (рис. 5.3).

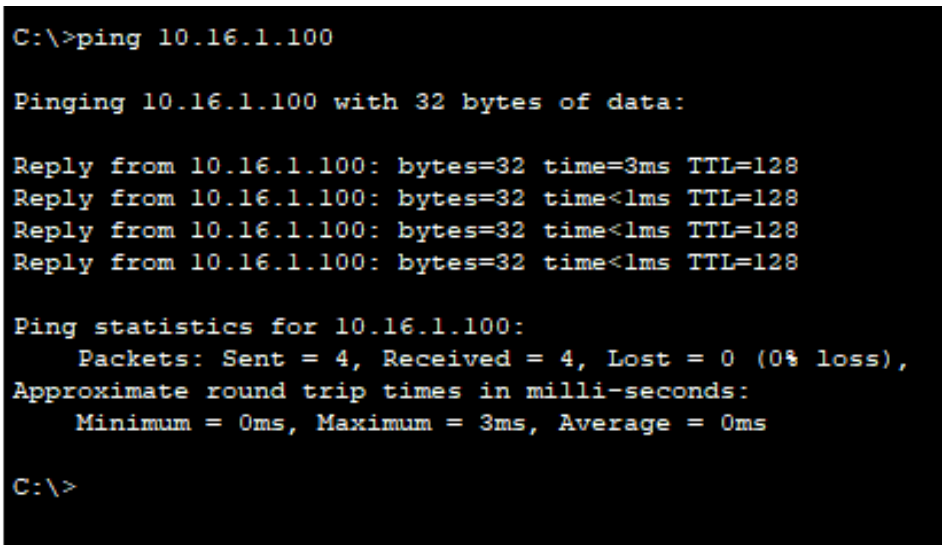

Рисунок 5.3 – Перевірка запиту від ПК у VLAN 10 до серверу

Ці тести підтверджують, що ACL коректно обмежує доступ до фінансового сервера, захищаючи чутливі дані підприємства.

ВИСНОВКИ

У результаті виконаної роботи проведено дослідження основ інфокомунікаційних мереж, розглянуто загрози та вразливості сучасним мережам, а також досліджено методи захисту, такі як VPN, ACL і firewall, які забезпечують безпеку даних.

Розроблено проєкт інфокомунікаційної мережі для будівельного підприємства, який відповідає сучасним вимогам і стандартам. У процесі роботи розроблено план розміщення 15 робочих місць, розподілених між 5 відділами, обрано оптимальну топологію мережі та спроєктовано структуровану кабельну систему, розраховано необхідну кількість кабелю. Виконано всі ключові етапи: проаналізовано потреби користувачів мережі, здійснено підбір мережевого обладнання такого як комутатори, маршрутизатор, сервер, безперебійник, та проведено моделювання мережі в Cisco Packet Tracer.

Впроваджено технологію VLAN для логічного розділення трафіку між відділами, що підвищило безпеку та продуктивність. Крім того, налаштовано заходи безпеки, зокрема ACL, для контролю доступу та захисту конфіденційних даних, таких як фінансові звіти та проєктна документація.

Проєкт відповідає міжнародним стандартам, зокрема ISO/IEC 11801, що регулює структуровані кабельні системи. Для реалізації кабельної системи використано 408 метрів кабелю категорії 5e для горизонтальних підсистем, а також 3 метри оптичного кабелю. Мережу розділено на 5 віртуальних локальних підмереж.

Розроблений проєкт повністю відповідає поставленим завданням і готовий до впровадження, забезпечуючи ефективну та безпечну роботу мережі підприємства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Васильців, Н., & Заставний, В. (2024). ОСОБЛИВОСТІ ЦИФРОВОГО ПРОДУКТУ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ БІЗНЕСУ. Економіка та суспільство, (59). [Електронний ресурс]. – Режим доступу до ресурсу https://doi.org/10.32782/2524-0072/2024-59-98

2. Воробієнко П. П. Телекомунікаційні та інформаційні мережі / П. П. Воробієнко, Л. А. Нікітюк, П. І. Резніченко. – Київ: САММІТ-Книга, 2010. – 708 с. – (Підручник для вищих навчальних закладів).

3. Проектування інфокомунікаційних мереж / С. І.Тарбаєв, К. О. Домрачева, В. Ф. Заїка, М. П. Трембовецький. – Київ: ННІТІ ДУТ, 2019. – 186 с. – (Посібник для самостійної роботи студентів вищих навчальних закладів з кредитно-модульною організацією навчального процесу).

4. Cheng, E.W.L., Li, H., Love, P.E.D. and Irani, Z. (2001), "Network communication in the construction industry", Corporate Communications: An International Journal, Vol. 6 No. 2, pp. 61-70. https://doi.org/10.1108/13563280110390314

5. Недашківський О. Л. Технології та протоколи інфокомунікаційних мереж / О. Л. Недашківський., 2017. – 297 с.

6. Cisco Packet Tracer [Електронний ресурс] — Режим доступу до ресурсу: https://www.netacad.com/

7. Getting Started with GNS3 [Електронний ресурс] — Режим доступу до ресурсу: https://docs.gns3.com/docs/

8. Dean Dorton. (2019). Cybersecurity in the Construction Industry: Understanding the Risks. [Електронний ресурс] – Режим доступу:https://deandorton.com/cybersecurity-risks-for-the-construction-industry/

9. Cisco. (2023). What is a VPN? [Електронний ресурс] — Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-a-vpn.html

10. Cisco. (2023). Access Control Lists (ACLs) [Електронний ресурс] — Режим доступу до ресурсу: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

11. Cisco. (2023). What is a Firewall? [Електронний ресурс] — Режим доступу до ресурсу: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

12. Mantha, B. R. K., & García de Soto, B. (2020). Assessment of the cybersecurity vulnerability of construction networks. Engineering, Construction and Architectural Management, 28(10), 3078-3105. [Електронний ресурс]. – Режим доступу: https://doi.org/10.1108/ECAM-06-2020-0400

13. General Data Protection Regulation (GDPR). [Електронний ресурс]. – Режим доступу: https://gdpr-info.eu/

14. A Guide To Network Topology [Електронний ресурс] / Jones IT. – Режим доступу: https://www.itjones.com/blogs/2020/11/22/a-guide-to-network-topology.

15. Routers, Switches, And Hubs - Understanding Your Network Components [Електронний ресурс]/Jones IT.–Режим доступу: https://www.itjones.com/blogs/2021/8/15/routers-switches-and-hubs-understanding-your-network-components .

16. ONU Alcatel Lucent I-010G [Електронний ресурс]/deps.ua –Режим доступу: https://deps.ua/katalog/ru-abonentskie-terminalyi-onu/alcatel-lucent-i-010g.html

17. D-Link DES-1008D — Коммутатор неуправляемый 8xFast Etherne [Електронний ресурс]/Jones IT. –Режим доступу: https://comtrade.ua/ua/d-link-des-1008d/

18. TL-WR841N [Електронний ресурс]/tp-link.com – Режим доступу: https://www.tp-link.com/uk-ua/home-networking/wifi-router/tl-wr841n/#specifications

19. Smart-UPS 1000VA SUA1000RMI2U [Електронний ресурс]/ek.ua – Режим доступу: https://ek.ua/APC-SMART-UPS-1000VA-

SUA1000RMI2U.htm

20. Віртуальні локальні мережі VLAN / С. І.Приходько, С. О. Жученко, М. А. Штомпель, С. В. Сколота. // Українська державна академія залізничного транспорту. – 2018. – С. 5–8.

21. Мірза Д. С. Проєктування інфокомунікаційної мережі будівельного підприємства / Мірза Д.С., Ляшенко Г. Є. // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління : тез. доп. п’ятнадцятої міжнародної науково - технічної конференції, 24–25 квітня 2025 р. – Т. 3. – Баку–Харків–Жиліна, 2025. – С. 50.