Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій та робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи
бакалавр
(ступінь вищої освіти)

на тему **«Оптимізація інтегральної цифрової мережі зв'язку підприємства критичної інфраструктури»**

Виконав: студент 4 курсу, групи 401ТТ
спеціальності 172 «Телекомунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)

Дубина В.С.
(прізвище та ініціали)

Керівник Косенко В.В.
(прізвище та ініціали)

Рецензент Фомін О.С.
(прізвище та ініціали)

Полтава – 2025 рік

РЕФЕРАТ

кваліфікаційної роботи бакалавра «Оптимізація інтегральної цифрової мережі зв’язку підприємства критичної інфраструктури»

Кваліфікаційна робота бакалавра присвячена дослідженню особливостей побудови, експлуатації та оптимізації мереж зв’язку, що забезпечують функціонування об'єктів критичної інфраструктури. Актуальність теми обумовлена підвищеними вимогами до надійності, безперервності та безпеки обміну даними в умовах зростаючих кіберзагроз, цифровізації управління та складної геополітичної ситуації.

У роботі розглянуто загальні принципи організації цифрових телекомунікаційних мереж для підприємств критичної інфраструктури, таких як теплопостачальні організації, енергетичні компанії, транспортні вузли тощо. Особливу увагу приділено побудові багаторівневих мереж із використанням сучасних технологій IP-зв’язку, оптоволоконних каналів, резервних радіоканалів, а також впровадженню систем централізованого моніторингу, шифрування та авторизації доступу.

Об'єкт дослідження – інтегральна цифрова мережа зв'язку Полтавське обласне комунальне виробниче підприємство теплового господарства «Полтаватеплоенерго» як підприємства критичної інфраструктури.

Предмет дослідження – методи та засоби оптимізації інтегральної цифрової мережі зв'язку підприємства теплоенергетики.

Методи дослідження. У роботі використано комплекс загальнонаукових та спеціальних методів: аналізу і синтезу – для дослідження структури та функцій мереж зв'язку; моделювання – для розробки оптимізованої архітектури мережі; системного аналізу – для вивчення взаємозв'язків між компонентами мережі; порівняння – для оцінки ефективності різних технічних рішень..

Практичне значення роботи полягає в розробці технічних рішень з оптимізації інтегральної цифрової мережі зв'язку ПОКВПТГ

«Полтаватеплоенерго», впровадження яких дозволить підвищити надійність функціонування підприємства, покращити контроль за технологічними процесами, забезпечити захист від несанкціонованого доступу з урахуванням стандартів кіберзахисту, вимог до швидкодії, резервування та управління інцидентами. Проведено техніко-економічне обґрунтування, що включає розрахунок вартості обладнання, монтажу та термінів окупності впровадження, що дасть знизити експлуатаційні витрати в майбутньому. Запропонована модель дає змогу забезпечити стабільну та захищену роботу цифрових сервісів підприємства в режимі 24/7.

Кваліфікаційна робота складається зі вступу, трьох розділів основної частини, висновків, списку використаних джерел та додатків. У першому розділі подано аналіз сучасних підходів до побудови цифрових мереж. Та здійснено аналізу існуючої мережевої інфраструктури підприємства. У другому та третьому розділах розробляється концепція оптимізації мережі, проводяться відповідні розрахунки та техніко-економічне обґрунтування проекту. У висновку сформульовано підсумки дослідження та рекомендації.

Обсяг роботи: 88 сторінок, 3 розділи, 17 таблиць, 7 рисунків, 17 джерел.

Ключові слова: критична інфраструктура, мережа зв’язку, кібербезпека, IP-телефонія, VPN, SD-WAN, резервування, диспетчеризація.

SUMMARY

bachelor's qualification thesis: “Optimization of the integrated digital communication network of a critical infrastructure enterprise”

This bachelor's thesis focuses on the analysis, design, and optimization of communication networks that support the operation of critical infrastructure facilities. The relevance of the topic is driven by growing demands for reliability, continuity, and data security in the face of increasing cyber threats, the digitalization of management processes, and a complex geopolitical environment.

The thesis explores the general principles of building digital telecommunication networks for critical infrastructure enterprises such as district heating providers, energy companies, and transportation hubs. Special attention is given to the design of multi-tier network architectures utilizing modern IP-based communication technologies, fiber-optic channels, redundant radio links, and the deployment of centralized monitoring systems, encryption mechanisms, and access authorization controls.

Object of study: the integrated digital communication network of Poltava Regional Municipal Production Enterprise of Heat Supply “Poltavateploenergo,” categorized as a critical infrastructure enterprise.

Subject of study: methods and tools for optimizing the integrated digital communication network of a district heating utility.

Research methods: The study applies a comprehensive set of general scientific and specialized methods: analysis and synthesis — for examining the structure and functions of communication networks; modeling — for designing an optimized network architecture; systems analysis — for evaluating interdependencies among network components; and comparative analysis — for assessing the effectiveness of various technical solutions.

The practical value of this work lies in the development of technical solutions aimed at optimizing the integrated digital communication network of “Poltavateploenergo.” The proposed solutions are intended to enhance operational reliability, improve real-time monitoring of technological processes, and ensure

protection against unauthorized access in compliance with cybersecurity standards, performance requirements, redundancy principles, and incident management protocols. A techno-economic assessment is conducted, including cost estimation for hardware, installation, and payback periods, contributing to reduced operational expenses in the long term. The proposed model ensures stable and secure 24/7 operation of the enterprise's digital services.

The thesis consists of an introduction, three main chapters, conclusions, a list of references, and appendices. Chapter one analyzes current approaches to digital network design and evaluates the existing network infrastructure of the enterprise. Chapters two and three present a conceptual framework for network optimization, including technical calculations and a techno-economic feasibility study. The conclusion summarizes the key findings and provides practical recommendations.

Scope: 88 pages, 3 chapters, 17 tables, 7 figures, 17 references.

Keywords: critical infrastructure, communication network, cybersecurity, IP telephony, VPN, SD-WAN, redundancy, dispatching.

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій та робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Ступінь вищої освіти Бакалавр
Спеціальність 172 «Телекомунікації та радіотехніка»

ЗАТВЕРДЖУЮ

Завідувач кафедри автоматики, електроніки та телекомунікацій
_____О.В. Шефер
«01» квітня 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА СТУДЕНТУ

Дубині Вадиму Сергійовичу

1. Тема роботи «Оптимізація інтегральної цифрової мережі зв'язку підприємства критичної інфраструктури»
керівник роботи Косенко Віктор Васильович, д.т.н., професор
затверджена наказом вищого навчального закладу від 03 . 03 . 2025 року № 306/1-ф,а .

2. Строк подання студентом проєкту (роботи) 10.06.2025 р.

3. Вихідні дані до проекту (роботи) Мережа цифрового зв'язку ПОКВПТГ «Полтаватеплоенерго». Розробити заходи оптимізації для забезпечення надійної та безперебійної роботи мережі зв'язку у відповідності до вимог побудови цифрових мереж зв'язку об'єктів критичної інфраструктури.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд сучасних технологій цифрового зв'язку. Аналіз стану цифрової мережі зв'язку підприємства та визначенні її недоліків. Постановка задач на кваліфікаційну роботу. Розробка заходів оптимізації, включаючи вибір архітектури, протоколів, проєктування нової топології та вибір технічних рішень і програмного забезпечення. Проведення розрахунків техніко-економічного обґрунтування, що демонструють доцільність і економічний ефект від впровадження оптимізованої мережі.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
   1) актуальність теми і мета кваліфікаційної роботи;
   2) завдання кваліфікаційної роботи;
   3) об'єкт та методи дослідження;
   4) аналіз існуючого стану мережі зв'язку, виявлені недоліки;

5) запропонована архітектура мережі і оцінка надійності запропонованої моделі;
6) розрахунки навантаження на мережу зв’язку за категоріями мережевого трафіку;
7) техніко-економічне обґрунтування запропонованих рішень і очікуваний ефект;
8) висновки.

6. Дата видачі завдання 01.04.2025 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів кваліфікаційної роботи бакалавра	Термін виконання етапів роботи			Примітка (плакати)
1	Характеристика існуючої мережі цифрового зв’язку. Аналіз недоліків і постановка задачі на кваліфікаційну роботу.	22.04.25	I	20%	Пл. 1,2
2	Вибір архітектури мережі, протоколів та схем зв’язку.	08.05.25		40%	Пл. 3
3	Вибір обладнання та варіантів програмного забезпечення. Розрахунок ефективності взаємодії компонентів мережі.	22.05.25	II	60%	Пл. 4,5
4	Визначення оптимальних технічних параметрів мережевого обладнання. Розрахунок вартості запропонованих рішень	30.05.25		80 %	Пл. 6,7
5	Оформлення кваліфікаційної роботи бакалавра	10.06.25	III	100%	Пл. 8

Студент _____ Дубина В.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Косенко В.В.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CDP – Cisco Discovery Protocol – закритий протокол другого рівня

VPN – Virtual Private Network – узагальнена назва технології, яка дозволяє створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри

MPLS – Multiprotocol Label Switching – багатопротокольна комутація за мітками) – механізм високопродуктивної телекомунікаційної мережі, що здійснює передачу даних від одного вузла мережі до іншого за допомогою міток

SCADA – Supervisory Control and Data Acquisition – програмний пакет або система, що використовується для збору, обробки, відображення та архівування даних в реальному часі для моніторингу та управління різними об'єктами

ВСТУП

Актуальність теми дослідження. У сучасних умовах цифровізації та підвищення загроз кібербезпеці підприємства критичної інфраструктури відіграють ключову роль у забезпеченні сталого функціонування держави. До таких підприємств належать об'єкти енергетики, водопостачання, зв'язку, транспорту, які мають високий рівень залежності від надійної інформаційно-комунікаційної інфраструктури. Особливого значення набуває оптимізація цифрових мереж зв'язку в умовах військової агресії, коли зростає ризик фізичного пошкодження та кібератак на об'єкти критичної інфраструктури. Ефективність функціонування інтегральної цифрової мережі зв'язку є критично важливою для оперативного управління, безперервного моніторингу технологічних процесів, захисту даних та швидкого реагування на позаштатні ситуації.

Підприємства критичної інфраструктури в місті Полтава, як і в інших регіонах України, зазнають викликів, пов'язаних зі зростанням обсягу переданих даних, необхідністю підвищення надійності мережі, забезпеченням кібербезпеки та впровадженням новітніх технологій зв'язку під час збройної агресії російської федерації проти України. В умовах обмежених ресурсів особливо важливим є не лише технічне оновлення, а й оптимізація існуючих рішень, яка дозволяє досягти високих результатів з мінімальними витратами.

Актуальність оптимізації інтегральної цифрової мережі зв'язку підтверджується сучасними тенденціями в галузі телекомунікацій та інформаційних технологій. Зокрема, зростають вимоги до швидкості передачі даних, надійності та відмовостійкості мережі, інформаційної безпеки та можливості інтеграції з системами автоматизації технологічних процесів. Особливої уваги потребує забезпечення функціонування критичної інформаційної інфраструктури в умовах енергетичних обмежень та фізичних загроз, характерних для воєнного стану.

Розробка та впровадження оптимізованих рішень для цифрової мережі зв'язку дозволяє суттєво підвищити ефективність управління підприємством теплового господарства, забезпечити безперервність технологічних процесів, мінімізувати втрати ресурсів та своєчасно реагувати на аварійні ситуації. Тому дослідження методів та засобів оптимізації інтегральної цифрової мережі зв'язку для підприємств критичної інфраструктури є надзвичайно актуальним завданням, що має як теоретичне, так і практичне значення.

Метою дипломної роботи є розробка заходів з оптимізації інтегральної цифрової мережі зв'язку на прикладі Полтавського обласного комунального виробничого підприємства теплового господарства «Полтаватеплоенерго» з метою підвищення ефективності, надійності та безпеки інформаційно-комунікаційної інфраструктури.

Для досягнення цієї мети в роботі передбачено вирішення наступних завдань:

1. аналіз існуючої цифрової мережі зв'язку підприємства;
2. виявлення технічних та організаційних недоліків у її функціонуванні;
3. розробка технічних рішень для оптимізації мережевої інфраструктури;
4. моделювання і порівняння різних варіантів оптимізації;
5. техніко-економічне обґрунтування запропонованих змін.

Об'єкт дослідження – процеси передачі та обробки інформації в інтегральній цифровій мережі зв'язку підприємства критичної інфраструктури.

Предмет дослідження – методи та засоби оптимізації інтегральної цифрової мережі зв'язку для забезпечення надійного та безпечного функціонування підприємства теплового господарства.

Методи дослідження. У роботі використано комплекс загальнонаукових та спеціальних методів дослідження: системний аналіз для вивчення структури та функціонування цифрової мережі зв'язку підприємства; порівняльний аналіз для оцінки різних технологічних рішень; математичне моделювання для розрахунку параметрів мережі; методи теорії надійності для оцінки відмовостійкості системи; методи захисту інформації для забезпечення

кібербезпеки; методи техніко-економічного аналізу для обґрунтування запропонованих рішень.

Наукова новизна одержаних результатів полягає в розробці комплексного підходу до оптимізації інтегральної цифрової мережі зв'язку підприємства критичної інфраструктури, який, на відміну від існуючих, враховує специфіку функціонування об'єктів теплопостачання в умовах підвищених ризиків та обмежених ресурсів. Удосконалено методику оцінки надійності та відмовостійкості мережевої інфраструктури з урахуванням особливостей роботи в умовах надзвичайних ситуацій. Набули подальшого розвитку методи забезпечення інформаційної безпеки телекомунікаційних систем підприємств критичної інфраструктури.

Практичне значення одержаних результатів. Розроблені в дипломній роботі технічні рішення та рекомендації можуть бути безпосередньо впроваджені на ПОКВПТГ «Полтаватеплоенерго» для підвищення ефективності функціонування цифрової мережі зв'язку. Запропоновані підходи до оптимізації мережевої інфраструктури можуть бути адаптовані та використані на інших підприємствах критичної інфраструктури, зокрема в сфері теплопостачання, водопостачання та енергетики. Результати техніко-економічного обґрунтування дозволяють визначити пріоритетні напрями інвестицій у модернізацію телекомунікаційних систем з урахуванням обмежених фінансових ресурсів.

1. ОГЛЯД ІСНУЮЧИХ ТЕХНОЛОГІЙ І СТАНУ МЕРЕЖІ ЗВ’ЯЗКУ

1.1 Сучасні технології цифрового зв’язку

Цифрові мережі зв’язку є основою функціонування сучасних систем управління, моніторингу та передавання інформації. До основних технологій цифрової комунікації відносять: IP-телефонію, Ethernet, MPLS, VPN, SCADA, IoT-технології, а також бездротові технології передачі даних (Wi-Fi, LTE, LoRaWAN тощо).

Одним із ключових напрямів є впровадження індустріального Інтернету речей (IIoT), який забезпечує об’єднання тисяч пристроїв у єдину мережу та автоматизований обмін даними. Також активно розвиваються архітектури SDN (Software-Defined Networking) і NFV (Network Function Virtualization), які дозволяють гнучко керувати мережею та масштабувати її.

Інтегральна цифрова мережа зв'язку (ІЦМЗ) являє собою комплексне технологічне рішення, що забезпечує об'єднання різноманітних єдиних каналів передачі даних, голосу та відео в інформаційну систему з використанням цифрових технологій. Концепція інтегральних мереж виникла як відповідь на потребу підприємств у консолідації комунікаційних ресурсів та оптимізації інформаційних потоків.

На сучасному етапі розвитку телекомунікацій ІЦМЗ стала багатофункціональна телекомунікаційна система, що забезпечує передачу, обробку та зберігання інформації різного типу (даних, голосу, відео) на основі єдиних стандартів та протоколів, з використанням спільної інфраструктури та системи управління. Ключовою особливістю ІЦМЗ є інтеграція різних сервісів та додатків в єдиному середовищі з можливістю їх гнучкової конфігурації та масштабування.

Для підприємств критичної інфраструктури ІЦМЗ має особливе значення, забезпечує безперервність операційних процесів, високу надійність передачі критично важливої інформації та стійкість до зовнішніх впливів. У контексті таких підприємств ІЦМЗ можна застосувати як стратегічну складову

інформаційної інфраструктури, що гарантує своєчасну та достовірну передачу даних для прийняття управлінських рішень і забезпечення функціонування автоматизованої системи управління технологічними процесами.

Еволюція концепції ІЦМЗ пройшла шлях від базових цифрових мереж інтегрального обслуговування (ISDN) до сучасних конвергентних мереж нового покоління (NGN), які базуються на IP-технологіях та забезпечують широкий спектр телекомунікаційних послуг. Впровадження концепції програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV) відкрило нові можливості для гнучкого управління ресурсами ІЦМЗ та їх адаптації до змінних умов функціонування підприємств критичної інфраструктури.

Основні характеристики ІЦМЗ:

- мультисервісність (одночасна підтримка голосових, відео- та даних сервісів);
- модульність і масштабованість;
- підтримка QoS (Quality of Service) та SLA (Service Level Agreement);
- використання єдиної платформи для всіх типів зв’язку (IP-мережа);
- централізоване керування та моніторинг.

В основі сучасних ІЦМЗ лежать технології комутації пакетів (наприклад, IP/MPLS), що дозволяють оптимізувати використання каналів зв’язку, зменшити затримки та підвищити відмовостійкість системи.

Залежно від принципів побудови, топології, функціональності та масштабу, види організації (архітектури) цифрових мереж поділяються на кілька основних типів, а саме:

1) за топологією побудови

Шинна (bus)	Усі пристрої підключені до однієї загальної шини. Проста реалізація, але низька масштабованість.
Зіркова (star)	Усі пристрої підключаються до центрального комутатора або концентратора. Поширена в локальних мережах.

Кільцева (ring)	Передача даних відбувається по колу від одного вузла до іншого. Забезпечує чіткий порядок передачі, але чутлива до розривів.
Деревовидна (tree)	Розширення топології «зірка», що дозволяє будувати ієрархічну структуру. Підходить для великих мереж.
Повнозв'язна (mesh)	Кожен вузол з'єднаний з усіма іншими. Висока надійність і відмовостійкість, але дорога реалізація.
Гібридна	Поєднання кількох типів топологій, що дозволяє досягати оптимального балансу між вартістю, надійністю та продуктивністю.

2) за функціональним призначенням

Клієнт-сервер	Централізована модель, де сервери обслуговують запити клієнтів. Легка в адмініструванні, добре масштабується.
Одноранговa (P2P)	Всі вузли рівноправні, можуть бути як клієнтами, так і серверами. Дешева реалізація, але складне управління без централізації.
Хмарна (cloud-based)	Використовує ресурси віддалених дата-центрів. Масштабована, гнучка, але залежна від інтернет-з'єднання.

3) за рівнем інтеграції та інфраструктури

LAN (Local Area Network)	Обмежена територією (будівля, офіс). Висока швидкість, низька затримка.
MAN (Metropolitan Area Network)	Охоплює міські райони, часто використовується для підприємств із кількома філіями в місті.
WAN (Wide Area Network)	Розподілені мережі, що об'єднують віддалені офіси або країни. Зазвичай використовує канали зв'язку провайдерів.
SDN (Software-Defined Networking)	Інтелектуальна архітектура, що відокремлює контроль від фізичного обладнання. Гнучке управління, масштабованість.
IoT-мережі	Адаптовані для підключення великої кількості пристроїв з обмеженими ресурсами (датчики, контролери).

4) за моделлю взаємодії

OSI-модель	Теоретична 7-рівнева модель, яка описує, як дані передаються через мережу (фізичний, канальний, мережевий рівні тощо).
TCP/IP	Практична реалізація, яка лежить в основі сучасного Інтернету (мережевий, транспортний, прикладний рівні).

Відтак, правильний вибір архітектури цифрової мережі забезпечує ефективність, надійність та масштабованість інформаційної інфраструктури підприємства з урахуванням його технічних, економічних і функціональних вимог.

1.2 Особливості мереж зв’язку критичної інфраструктури

Підприємства критичної інфраструктури потребують високонадійних каналів зв’язку з гарантованою якістю обслуговування (QoS), низькою затримкою та відмовостійкістю. Такі мережі мають підтримувати резервування, кібербезпеку, безперервний моніторинг та автоматичне переключення у разі аварії.

Особливо актуальними є гібридні мережі, що поєднують оптоволоконну основу та бездротову передачу, а також інфраструктура для телеметрії, відеоспостереження, технічного обліку й керування (AMR, SCADA, BMS).

При побудові мереж підприємств критичної інфраструктури можна виділити такі вимоги:

- Надійність і резервування. Основні мережеві елементи повинні мати резерв, включаючи резервування каналів, серверів, маршрутизаторів і джерел живлення.
- Сегментація мережі. Використання VLAN, VPN, DMZ для розмежування технологічного, адміністративного і загальнодоступного трафіку.

- Індустріальні протоколи. Для автоматизації та диспетчеризації часто використовуються специфічні протоколи (Modbus, OPC, DNP3, IEC 60870-5-104 тощо).
- Захищений віддалений доступ. VPN, брандмауери, аутентифікація другого рівня.
- Централізоване управління. SCADA-системи інтегруються з корпоративними мережами та платформами моніторингу.

Архітектура інтегральної цифрової мережі зв'язку підприємств критичної інфраструктури складається з кількох взаємопов'язаних рівнів, кожен з яких виконує специфічні функції та містить відповідні компоненти.

1. Фізичний рівень (транспортна мережа):

- Кабельна система (оптоволоконні, мідні кабелі)
- Бездротові канали зв'язку (радіорелейні лінії, супутниковий зв'язок)
- Комутаційне обладнання (маршрутизатори, комутатори)
- Системи мультиплексування та демультиплексування сигналів
- Обладнання доступу до мережі (модеми, мультиплексори доступу)

2. Мережевий рівень:

- Системи маршрутизації та комутації пакетів
- Обладнання та програмне забезпечення для забезпечення якості обслуговування (QoS)
- Засоби віртуалізації мережевих функцій (NFV)
- Компоненти програмно-конфігурованої мережі (SDN)
- Системи балансування навантажень

3. Рівень управління та контролю:

- Системи управління мережею (NMS)
- Компоненти моніторингу та діагностики
- Засоби забезпечення інформаційної безпеки
- Системи резервування та відновлення працездатності
- Центри управління мережею (NOC)

4. Сервісний рівень:

- Сервери додатків і сервісів
- Системи обробки та зберігання даних
- Шлюзи інтеграції із зовнішніми системами
- Платформи надання телекомунікаційних послуг
- API для інтеграції з бізнес-системами

5. Рівень користувача:

- Термінальне обладнання (IP-телефони, відеотермінали)
- Програмні клієнти та додатки
- Системи диспетчеризації та оперативного управління
- Інтерфейси взаємодії з користувачами
- Засоби віддаленого доступу

У контексті підприємств критичної інфраструктури архітектура ІЦМЗ доповнюється спеціалізованими компонентами, що забезпечують підвищену надійність, безпеку та стійкість до зовнішніх впливів:

— Резервні центри обробки даних та вузли зв'язку

— Системи аварійного живлення та охолодження

— Дублюючі канали зв'язку з автоматичним перемиканням

— Спеціалізовані засоби захисту від кібератак

— Компоненти фізичного захисту елементів інфраструктури

Взаємодія між компонентами ІЦМЗ реалізується на основі стандартизованих протоколів та інтерфейсів, що забезпечує можливість інтеграції обладнання та програмного забезпечення від різних виробників. Ключовим аспектом архітектури ІЦМЗ є забезпечення відмовостійкості на всіх рівнях функціонування систем, що досягається за рахунок резервування критичних компонентів та каналів зв’язку, а також впровадження механізмів автоматичного відновлення працездатності.

Існують декілька видів організації (архітектури) цифрових мереж:

— Ієрархічна (трирівнева): ядро – агрегація – доступ. Забезпечує добру масштабованість і чітку логіку розгортання

— Плоска (flat network): мінімальна кількість рівнів, просте адміністрування,

швидка передача даних, але складніше масштабувати

— Мережа з SDN (Software Defined Networking): централізоване управління через контролер SDN, гнучкість у зміні топологій та маршрутів

— Меш (mesh): кожен вузол пов'язаний з кількома іншими, що забезпечує високу надійність і резервування, проте вимагає складного управління.

У межах критичної інфраструктури найчастіше використовується ієрархічна архітектура з елементами резервування та інтеграції промислових систем керування (рис.1.1), яка передбачає розподіл мережевих функцій на три логічні рівні:

1. Ядро (Core Layer)

- Функція: швидка пересилка великого обсягу трафіку між підмережами.
- Характеристики:
- високошвидкісне з’єднання між основними сегментами мережі.
- мінімальна обробка пакетів.
- висока надійність і відмовостійкість.
- відсутність прикладних сервісів.
- Пристрої: маршрутизатори або багатофункціональні комутатори з високою пропускною здатністю.

2. Агрегаційний або розподільний рівень (Distribution Layer)

- Функція: забезпечення політик маршрутизації, фільтрації, балансування навантаження, безпеки.
- Характеристики:
- обробка міжмережевого трафіку.
- контроль доступу та впровадження політик безпеки.
- VLAN-розмежування.
- Пристрої: L3-комутатори (із функціями маршрутизації), міжмережеві екрани, шлюзи.

3. Доступ або периферія (Access Layer)

- Функція: забезпечення доступу кінцевих користувачів до мережі.

- Характеристики
  - Підключення робочих станцій, принтерів, IP-телефонів тощо.
  - Контроль доступу на рівні портів.
  - Підтримка PoE (живлення через Ethernet).
- Пристрої. L2-комутатори, бездротові точки доступу, термінальні пристрої.

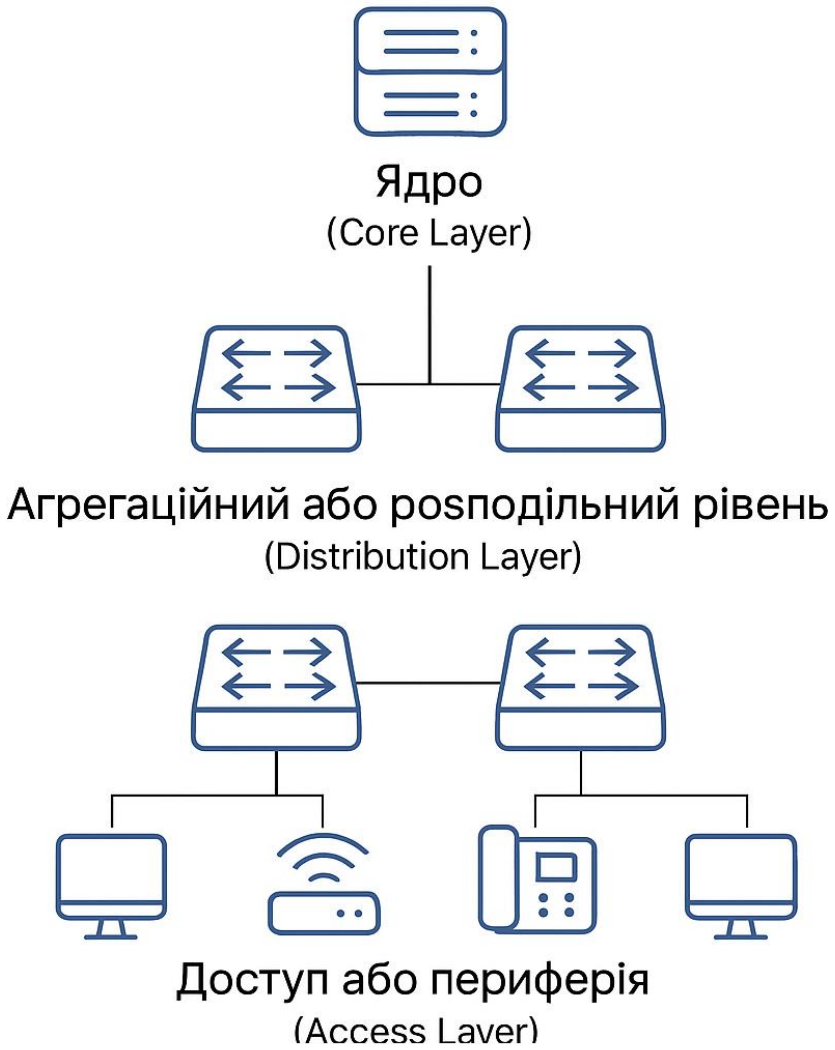


Рисунок 1.1 – Графічне зображення ієрархічної (трирівневої) архітектури цифрових мереж.

Така структура забезпечує масштабованість, керованість, високу продуктивність і безпеку мережі, особливо в середовищах критичної інфраструктури та корпоративного рівня

1.3 Аналіз об’єкта дослідження та його мережі зв’язку

Критична інфраструктура відіграє важливу роль у забезпеченні життєдіяльності населення, стабільного функціонування економіки та національної безпеки держави. До об’єктів критичної інфраструктури належать підприємства енергетики, транспорту, водопостачання, зв’язку тощо. Серед таких об’єктів у Полтавській області одним із найважливіших є Полтавське обласне комунальне виробниче підприємство теплового господарства «Полтаватеплоенерго», що є найбільшим постачальником теплової енергії в Полтавській області. Воно забезпечує теплопостачання понад 60% житлового фонду м. Полтава, об’єктів соціальної інфраструктури (лікарень, шкіл, дитячих садків), а також низки державних установ. Діяльність підприємства безпосередньо впливає на безпеку, добробут і здоров’я населення, особливо в опалювальний сезон. Будь-яке порушення в роботі тепломереж може спричинити соціальні кризи, масові відключення тепла та створити надзвичайні ситуації.

ПОКВПТГ «Полтаватеплоенерго» володіє розгалуженою системою теплопостачання, до складу якої входять:

- 90 котелень та теплогенераторних, встановленою потужністю 858,96 Гкал/год, котрі розташовані у містах Полтаві, Карлівці, Решетилівці, селищах міського типу Машівці та Котельві. Серед них:

— районна котельня (вул. Ціолковського, 36, потужністю 250 Гкал/год) – 1 од.;

— квартальні котельні з котлами КВГ-6,5, ТВГ-8М (потужністю від 19,5 до 41,5 Гкал/год) – 17 од.;

— групові котельні з котлами ВК-32 (потужністю від 5,2 до 11,6 Гкал/год) – 18 од.;

— групові котельні з котлами типу НІІСТУ-5 (потужністю від 0,66 до 5,1 Гкал/год) – 17 од.;

— індивідуальні та дахові котельні, теплогенераторні (потужністю від 0,08 до 1,9 Гкал/год) – 24 од.;

— автоматизовані котельні з котлами Buderus, SupeRac, Wolf, Ferroli і Viessmann – 11 од.;

— котельні з котлами Herz, що працюють на твердому паливі (потужністю від 0,43 до 0,86 Гкал/год) – 2 од.

- 28 центральних теплових пунктів (ЦТП);
- 8 теплові мережі та насосні;
- понад 250 індивідуальних теплових пунктів (ІТП) у багатоповерхових будинках і закладах соціальної сфери;
- диспетчеризована система керування технологічними процесами, що охоплює всі основні вузли тепломережі;
- теплові мережі довжиною понад 430 км у двотрубному обчисленні, з яких значна частина (понад 50%) потребує капітального ремонту або модернізації.

Котельні підприємства обладнані водогрійними та паровими котлами, які працюють на природному газі. Загальна встановлена теплова потужність становить понад 800 Гкал/год. Для зменшення втрат у тепломережах використовуються предізольовані труби, які встановлюються під час реконструкції. Система теплопостачання розділена на кілька гідравлічно незалежних зон, що дозволяє локалізувати аварії та зменшити зони відключення при пошкодженнях. Важливою технічною складовою є система автоматизованого диспетчерського управління (АСДУ), яка забезпечує:

- моніторинг параметрів теплоносія (тиск, температура, витрата);
- дистанційне керування насосним обладнанням і змішувальними вузлами;
- фіксацію аварійних ситуацій із можливістю оперативного реагування.

Усі великі котельні обладнані частотними перетворювачами на насосах, що дозволяє економити електроенергію за рахунок адаптації до змінних теплових навантажень. Також активно впроваджуються електронні теплолічильники та погодозалежне регулювання подачі теплоносія.

Для забезпечення надійності функціонування в умовах надзвичайних ситуацій підприємство має резервні джерела електроживлення (дизель-генератори),

аварійний запас труб, фітингів і комплектуючих. Значна частина обладнання потребує модернізації через зношеність і високі втрати тепла при транспортуванні. У зв’язку з цим підприємство реалізує програми з оптимізації та автоматизації управління тепловими процесами.

Сучасна діяльність ПОКВПТГ «Полтаватеплоенерго» ґрунтується на впровадженні цифрових технологій, що забезпечують ефективне управління виробничими процесами, облік ресурсів, оперативну комунікацію зі споживачами та підвищення рівня кіберзахисту критичних систем.

Основні компоненти цифрової інфраструктури підприємства:

1. Автоматизована система диспетчерського управління (АСДУ)

АСДУ охоплює всі великі котельні, центральні теплові пункти (ЦТП), насосні станції та головні вузли тепломережі. Система забезпечує:

— постійний моніторинг температури, тиску, витрати теплоносія;

— дистанційне керування насосами, засувками, регуляторами;

— реєстрацію аварійних ситуацій у реальному часі;

— архівацію даних для аналізу ефективності.

АСДУ функціонує на базі промислових контролерів (Siemens, Schneider Electric) та SCADA-систем.

2. Інформаційно-аналітична система обліку теплової енергії

Підприємство впровадило багаторівневу систему збору даних з приладів обліку теплової енергії:

— понад 90% об'єктів обладнано електронними теплолічильниками з дистанційним зчитуванням;

— дані автоматично передаються до центрального серверу через захищені канали зв’язку (GSM/LoRaWAN);

— впроваджено модулі для розрахунку тепловтрат і аналізу несанкціонованих втручань.

3. Система управління технічним обслуговуванням (CMMS)

Для управління технічним обслуговуванням використовується спеціалізоване програмне забезпечення, що включає:

— планування і контроль виконання ремонтних робіт;

— управління ресурсами та запасними частинами;

— ведення електронної технічної документації по обладнанню.

4. Особисті кабінети споживачів та мобільний застосунок

Платформа для споживачів дозволяє:

— переглядати нарахування та фактичне споживання;

— передавати показники лічильників;

— оплачувати рахунки онлайн;

— подавати звернення до служби підтримки.

5. Кібербезпека та захист інформації

У зв’язку з тим, що підприємство є об'єктом критичної інфраструктури, впроваджено комплекс заходів кіберзахисту:

— мережеві екрани та сегментація внутрішніх систем;

— багаторівнева система резервного копіювання;

— антивірусні та антишпигунські програми з автоматичним оновленням;

— обмеження доступу до критичних вузлів за допомогою політик доступу (role-based access control).

6. Системи енергоефективності та прогнозування

Використовуються математичні моделі для прогнозування теплового навантаження з урахуванням погодних умов, що дозволяє:

— мінімізувати перевитрати ресурсу;

— підвищити ефективність котелень;

— оптимізувати режими подачі теплоносія.

7. Заходи з підвищення надійності

Для підтримки стійкої роботи підприємства впроваджуються заходи з підвищення енергоефективності, резервування потужностей, автоматизації управління, посилення захисту інфраструктури. Підприємство взаємодіє з органами державної влади, службами з надзвичайних ситуацій та операторами критичної інфраструктури в інших галузях.

Існуюча мережа ПОКВПТГ «Полтаватеплоенерго» має фрагментарну архітектуру (рис.1.2), сформовану історично, з використанням різнорідного обладнання, основними компонентами якої є:

- локальні мережі на об’єктах (котельні, ЦТП) – переважно Ethernet 100 Мбіт/с або Wi-Fi;
- точка-доступу до інтернету – через міського провайдера;
- зв’язок між об’єктами – частково реалізований через VPN на базі публічного інтернету;
- серверне обладнання розміщене в центральному офіс;
- централізована диспетчерська система – частково інтегрована в IP-мережу, частково працює автономно;
- відеонагляд – локальні DVR-системи без централізованого архіву.

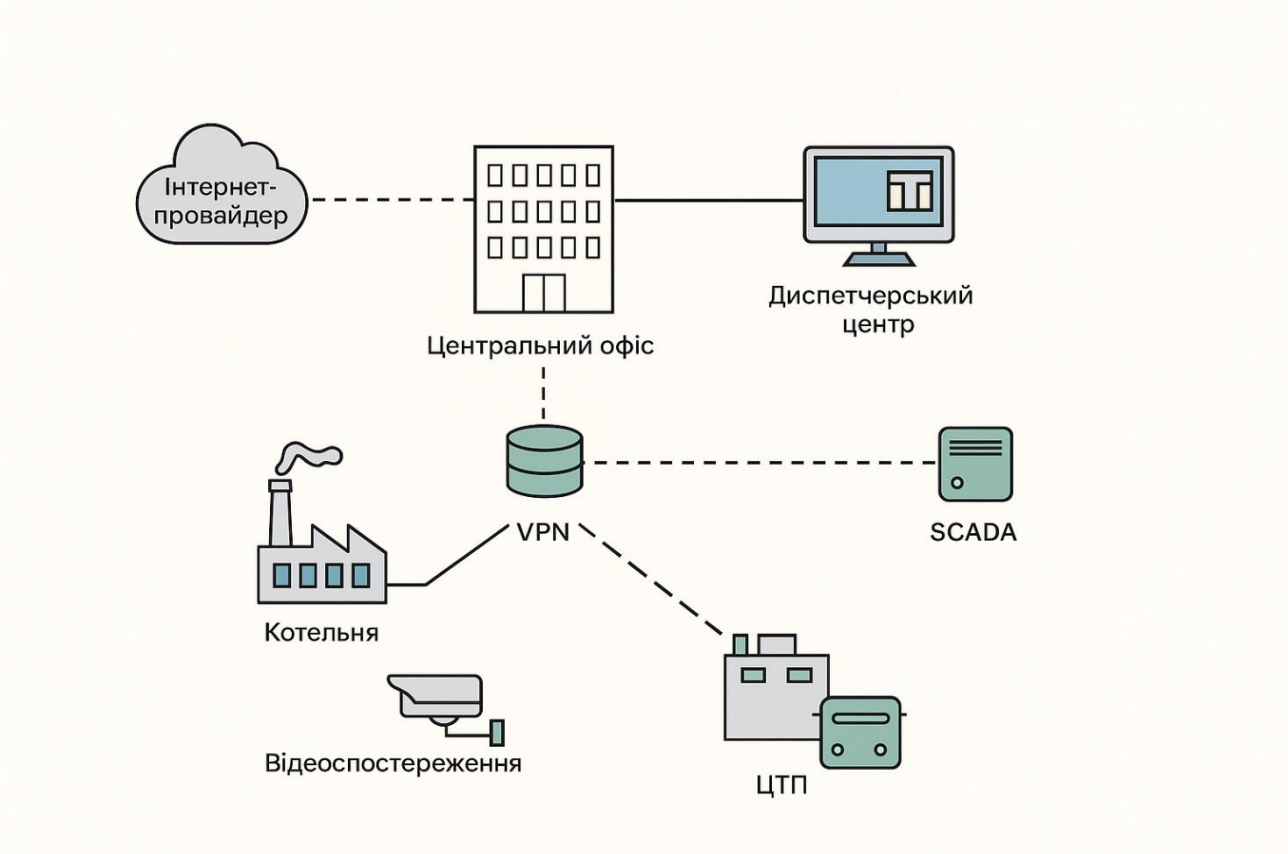


Рисунок 1.2 – Структура існуючої цифрової мережі зв’язку ПОКВПТГ «Полтаватеплоенерго»

У ході проведеного аналізу було виявлено, що мережа сформована без єдиного технічного підходу. Зв’язок між об’єктами реалізовано через комбінацію локальних Ethernet/Wi-Fi мереж, інтернет-з’єднання та VPN-тунелів, що забезпечує лише базовий рівень доступності та керованості. Частина об'єктів функціонує автономно. Також можна виділити такі ключові недоліки:

- відсутність єдиної архітектури мережі. Система сформована на базі застарілого обладнання без уніфікації стандартів.
- недостатнє резервування каналів. У разі збою інтернет-провайдера або окремого вузла спостерігається повна втрата зв’язку.
- низький рівень кіберзахисту. VPN використовуються не завжди, маршрутизатори часто з типовими налаштуваннями.
- неповна інтеграція SCADA-систем. Деякі об’єкти передають дані періодично, без автоматичного сповіщення про аварії.
- немає централізованого моніторингу відеоспостереження. Це ускладнює контроль за об’єктами в реальному часі.
- технічні обмеження старого обладнання. Деякі маршрутизатори не підтримують сучасні протоколи безпеки або QoS.

На основі виявлених недоліків сформовано перелік необхідних змін (табл.1.1):

Таблиця 1.1 – Перелік необхідних змін для оптимізації цифрової мережі зв’язку ПОКВПТГ «Полтаватеплоенерго»

№ п/п	Потреба	Обґрунтування
1	Централізація обробки даних	Забезпечить оперативність реагування
2	Побудова надійної LAN з VLAN	Розмежування доступу для підрозділів
3	Впровадження SCADA	Віддалене керування та автоматизація
4	Організація VPN	Безпечний віддалений доступ
5	Перехід на IP-зв’язок	Скорочення витрат, підвищення мобільності
6	Моніторинг Zabbix	Постійний контроль роботи систем

За результатами аналізу було сформовано висновок про те, що мережа зв’язку ПОКВПТГ «Полтаватеплоенерго» потребує системної оптимізації з урахуванням сучасних вимог до:

- резервування та відмовостійкості;
- безпеки передачі даних;
- централізованого моніторингу та управління;
- масштабованості та підтримки SCADA/IoT-сервісів;
- мінімізації втрат часу у разі аварій або порушень зв’язку.

1.4. Постановка задач на кваліфікаційну роботу

ПОКВПТГ «Полтаватеплоенерго» є ключовим елементом критичної інфраструктури регіону. Безперебійне функціонування підприємства забезпечує тепло і комфорт тисячам мешканців Полтави, а також стабільність у роботі важливих соціальних установ. Тому необхідно постійно вдосконалювати технічний стан, безпекові протоколи та цифрові системи управління підприємства.

На основі проведеного аналізу існуючої цифрової мережі зв’язку ПОКВПТГ «Полтаватеплоенерго» було виявлено низку критичних недоліків, що негативно впливають на стабільність, безпеку та ефективність функціонування систем управління та моніторингу. Це дозволяє сформулювати основні завдання, які необхідно вирішити в межах кваліфікаційної роботи:

— проаналізувати сучасні технології побудови цифрових мереж зв’язку для об’єктів критичної інфраструктури та визначити їх придатність для умов підприємства;

- розробити оптимізовану архітектуру інтегральної цифрової мережі зв’язку підприємства, що передбачає централізоване управління, підтримку телеметричних даних, scada-систем, відеоспостереження, службового зв’язку та захист інформації;
- запропонувати технічні рішення щодо вибору активного мережевого обладнання, топології, логічної сегментації (vlan) та протоколів безпеки;
- виконати розрахунок навантаження на мережу, визначити необхідну пропускну здатність каналів, кількість пристроїв та технічні параметри роботи;
- розробити техніко-економічне обґрунтування впровадження запропонованого рішення, оцінити витрати, переваги та строки окупності.
- передбачити заходи щодо охорони праці та безпеки при реалізації оптимізованої мережі зв’язку.

Виконання зазначених задач дозволить суттєво підвищити ефективність функціонування підприємства, зменшити ризики втрати керованості технологічними процесами та забезпечити належний рівень кібербезпеки.

2. ОПТИМІЗАЦІЯ ІНТЕГРАЛЬНОЇ МЕРЕЖІ ЗВ’ЯЗКУ

2.1 Розроблення заходів оптимізація інтегральної цифрової мережі зв’язку ПОКВПТГ «Полтаватеплоенерго» як об’єкта критичної інфраструктури

Модернізація цифрової мережі зв'язку підприємства ПОКВПТГ «Полтаватеплоенерго» представляє стратегічно важливе завдання, спрямоване на формування єдиної інтегрованої інформаційної інфраструктури. Призначення оновленої архітектури полягає у забезпеченні оперативної координації структурних підрозділів, автоматизованому управлінні тепловими об'єктами, високому рівні надійності та кіберзахисту, а також створенні передумов для масштабування та енергоефективності. Принципи оптимізації цифрової мережі включають централізацію управління через єдиний центр обробки та аналізу інформації, резервування критичних вузлів і каналів зв'язку, реалізацію сучасних засобів кіберзахисту, інтеграцію з системами SCADA та забезпечення можливості подальшого розширення без суттєвої перебудови.

Комплексний аналіз поточного стану мережевої інфраструктури дозволив виявити існуючі слабкі місця та сформувати перелік необхідних заходів. Першочергова інвентаризація наявного мережевого обладнання та топології показала значну гетерогенність технологічних рішень, несумісність окремих компонентів та відсутність уніфікованих стандартів. Оцінка пропускної здатності каналів передачі даних виявила критичні обмеження на рівні 10-100 Мбіт/с для магістральних ліній, що недостатньо для одночасної передачі телеметрії, відеоспостереження та інтеграції SCADA-систем.

Розрахунок необхідної пропускної здатності каналів зв'язку для різних типів даних можна виконати за формулою:

(2.1)

$$C = N \times R \times K$$

де C – сумарна необхідна пропускна здатність каналу (Мбіт/с);

N – кількість одночасних з'єднань;

R – середня швидкість передачі для одного з'єднання (Мбіт/с);

K – коефіцієнт запасу (1,2-1,5).

Застосовуючи дану формулу для оцінки вимог магістральних каналів при з'єднанні диспетчерської з котельнями отримуємо:

$$C = 90 \times 2{,}5 \times 1{,}3 = 292{,}5 \frac{\text{Мбіт}}{\text{с}}$$

Результати розрахунків пропускної здатності для різних сегментів мережі наведено у таблиці 2.1.

Таблиця 2.1 – Розрахункові вимоги до пропускної здатності каналів зв'язку

Сегмент мережі	**Кількість вузлів (N)**	**Швидкість на вузол (R), Мбіт/с**	**Коефіцієнт запасу (K)**	**Необхідна пропускна здатність (C), Мбіт/с**
Котельні	90	2,5	1,3	292,5
ЦТП	28	1,8	1,2	60,5
ІТП	250	0,8	1,5	300,0
Диспетчерські	5	50,0	1,4	350,0
Адміністрація	1	200,0	1,2	240,0

Аналіз рівня резервування показав, що 78% критичних вузлів не мають резервних каналів зв'язку, а коефіцієнт відмовостійкості системи (Кв) складає лише 0,65 при нормативному значенні 0,95 для об'єктів критичної інфраструктури. Розрахунок коефіцієнта відмовостійкості виконується за формулою:

(2.2)

$$Кв = 1 - П(1 - Ki)$$

де Кв – загальний коефіцієнт відмовостійкості системи;

Кі – коефіцієнт готовності і-го компонента системи;

П – добуток значень для всіх компонентів.

Ідентифікація вимог щодо інформаційної безпеки виявила невідповідність сучасним стандартам захисту критичної інфраструктури, зокрема відсутність комплексної системи захисту інформації та засобів моніторингу кіберзагроз.

Формування технічних вимог та розробка концепції оптимізації базувалися на детальному аналізі обсягів трафіку та типів передаваних даних. Результати аналізу представлені у таблиці 2.2.

Таблиця 2.2 – Характеристика типів даних в інтегральній мережі зв'язку

Тип даних	**Частка у загальному трафіку, %**	**Вимоги до затримки, мс**	**Пріоритет QoS**
Телеметрія	35	<100	Високий
SCADA	25	<50	Критичний
Відеоспостереження	20	<150	Середній
IP-телефонія	10	<80	Високий
Корпоративні дані	8	<300	Низький
Інтернет-трафік	2	<500	Найнижчий

Проєктування оптимізованої мережі зв'язку передбачає створення ієрархічної моделі з ядром, дистрибутивним та доступовим рівнями. Визначення надійності такої системи можна виконати за допомогою розрахунку коефіцієнта готовності:

(2.3)

$$K\text{г} = \frac{T\text{сер}}{T\text{сер} + T\text{відн}}$$

де Кг – коефіцієнт готовності системи;

Тсер – середній час безвідмовної роботи;

Твідн – середній час відновлення після відмови.

Для підвищення надійності мережі застосовується резервування каналів зв'язку. Коефіцієнт готовності системи з паралельним резервуванням розраховується за формулою:

(2.4)

$$К\text{г.рез} = 1 - (1 - К\text{г})^{n}$$

де Кг.рез – коефіцієнт готовності резервованої системи;

Кг – коефіцієнт готовності нерезервованої системи;

n – кількість паралельних каналів.

Економічна ефективність впровадження оптимізованих рішень оцінюється через розрахунок вартості володіння (ТСО) та рентабельності інвестицій (ROI). Оцінка ТСО на 5-річний період для основних компонентів мережі наведена у таблиці 2.3.

Таблиця 2.3 – Оцінка вартості володіння компонентами мережі на 5 років

Компонент мережі	**Початкові витрати, тис. грн**	**Операційні витрати за 5 років, тис. грн**	**ТСО, тис. грн**	**Питома вартість на 1 вузол, тис. грн**
Магістральне обладнання	2450	680	3130	626,0
Обладнання котелень	3870	1350	5220	58,0
Обладнання ЦТП	980	420	1400	50,0
Обладнання ІТП	2750	1250	4000	16,0
Системи безпеки	1860	930	2790	7,5
Програмне забезпечення	1540	2300	3840	10,3
Разом	13450	6930	20380	-

Розрахунок рентабельності інвестицій (ROI) виконується за формулою:

(2.5)

$$ROI = \frac{(\Delta P \times T) - I}{I} \times 100\%$$

де ROI – рентабельність інвестицій, %;

ΔP – щорічний економічний ефект від впровадження, тис. грн;

T – розрахунковий період, років; I – обсяг інвестицій, тис. грн.

Для проєкту оптимізації мережі зв'язку ПОКВПТГ «Полтаватеплоенерго» при річному економічному ефекті 4,2 млн грн та інвестиціях 13,45 млн грн на період 5 років ROI складає:

$$ROI = \frac{(4200 \times 5) - 13450}{13450} \times 100\% = 56{,}3\%$$

Позитивне значення ROI свідчить про економічну доцільність впровадження запропонованих заходів оптимізації.

Розробка плану впровадження оптимізованої мережі передбачає визначення пріоритетних об'єктів для оновлення з урахуванням їх критичності та наявності тимчасових схем комунікації для забезпечення безперервної роботи. Пріоритетність об'єктів визначається за допомогою інтегрального показника критичності (Ік), який розраховується за формулою:

(2.6)

$$Iк = 0{,}4 \times Nспож + 0{,}3 \times Mтепл + 0{,}2 \times Kзнос + 0{,}1 \times Sавар$$

де Ік – інтегральний показник критичності (від 0 до 100);

Nспож – нормалізована кількість споживачів (від 0 до 100);

Мтепл – нормалізована теплова потужність об'єкта (від 0 до 100);

Kзнос – нормалізований коефіцієнт зносу обладнання (від 0 до 100);

Sавар – нормалізована статистика аварійності (від 0 до 100).

Монтажні та наладочні роботи виконуються згідно з проєктною документацією та включають монтаж кабельної інфраструктури, встановлення активного обладнання, конфігурування мережевих пристроїв та впровадження систем моніторингу. Тестування та введення в експлуатацію передбачає перевірку швидкості, пропускної здатності, наявності затримок, проведення імітаційних сценаріїв відмови та перевірку на відповідність вимогам безпеки.

Оцінка ефективності та подальша оптимізація базується на аналізі ключових показників ефективності (KPI): доступність, середній час відновлення, рівень безпеки. Порівняння з базовими показниками до оптимізації дозволяє кількісно оцінити досягнутий ефект та сформувати рекомендації для подальшого масштабування або оновлення систем.

Реалізація запропонованих заходів оптимізації інтегральної цифрової мережі зв'язку ПОКВПТГ «Полтаватеплоенерго» забезпечить формування єдиної, масштабованої та керованої цифрової екосистеми, що значно підвищить якість управління тепловими процесами та створить надійну основу для подальшої цифрової трансформації підприємства.

2.2 Вибір архітектури та протоколів

Проєктування цифрової мережі зв'язку для підприємства критичної інфраструктури вимагає комплексного підходу до вибору архітектурної моделі та відповідних протоколів передавання даних. Оптимальна архітектура повинна забезпечувати високий рівень надійності, безперебійне функціонування, масштабованість, належний рівень захисту інформації та ефективну взаємодію між різнорідними компонентами системи.

Аналіз інфраструктури ПОКВПТГ «Полтаватеплоенерго» виявив складну територіально розподілену структуру об'єктів: центральний офіс, 3 адміністративні будівлі, 5 диспетчерських пунктів, 90 котелень різної потужності, 28 центральних теплових пунктів, понад 250 індивідуальних теплових пунктів, 8 насосних станцій та розгалужену систему теплових мереж. Подібна топологія потребує впровадження багаторівневої архітектури з чітким розмежуванням функціональних завдань кожного рівня.

Для оптимізації цифрової мережі зв'язку ПОКВПТГ «Полтаватеплоенерго» розроблено ієрархічну багаторівневу архітектуру IP-

мережі з розподілом функцій на три основні рівні: магістральний, розподільчий та периферійний (рис. 2.1).

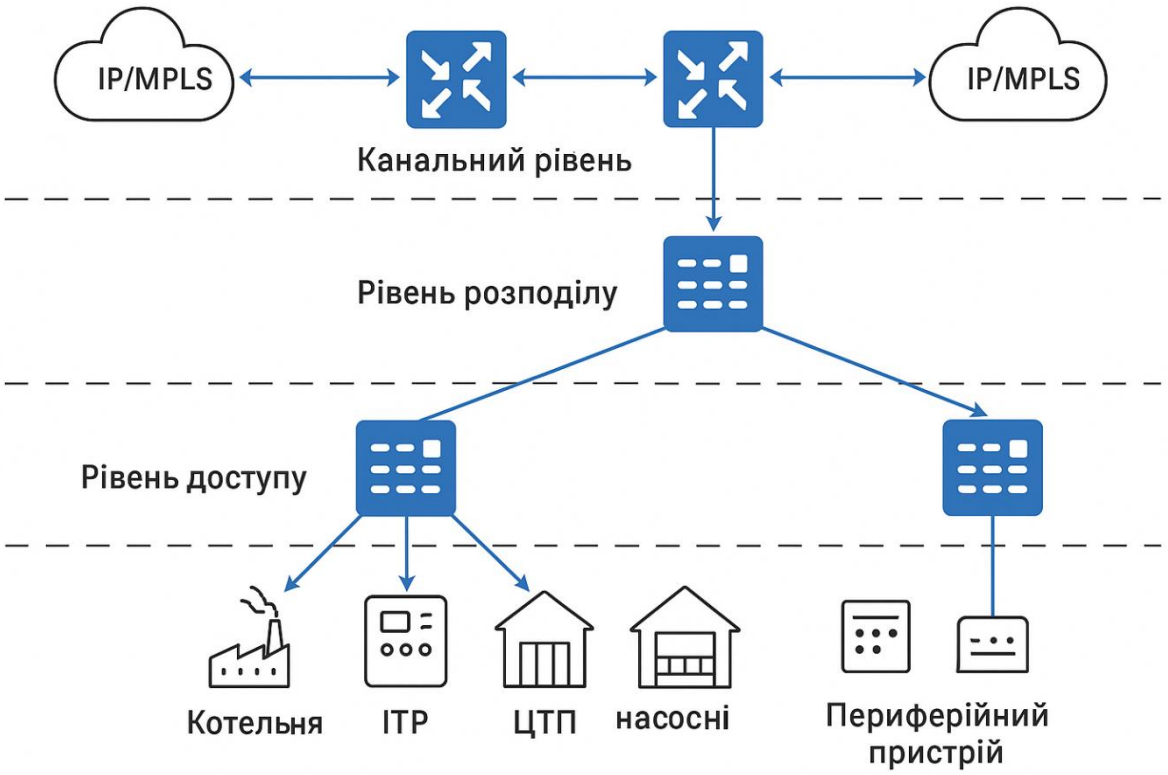


Рисунок 2.1 – Схема архітектури мережі

Надійність такої архітектурної моделі можна оцінити за допомогою розрахунку коефіцієнта структурної надійності (Кс), який визначає ймовірність працездатності системи при відмові окремих компонентів:

(2.7)

$$Kc = 1 - \prod(1 - Ri)$$

де Кс – коефіцієнт структурної надійності;

Ri – надійність і-го маршруту передачі даних;

$\prod$ – символ добутку значень.

При наявності двох незалежних маршрутів з надійністю

$R_1 = 0{,}98$ та $R_2 = 0{,}95$ загальна надійність складає:

$$Kc = 1 - (1 - 0{,}98) \times (1 - 0{,}95)$$

$$= 1 - 0{,}02 \times 0{,}05$$

$$= 1 - 0{,}001 = 0{,}999$$

Отриманий показник надійності 0,999 відповідає вимогам до систем критичної інфраструктури і забезпечує доступність мережі на рівні 99,9%, що еквівалентно допустимому часу простою не більше 8,76 годин на рік.

Магістральний рівень (Core) представляє собою ядро мережі, розташоване в центральному офісі підприємства. На цьому рівні розгортаються високошвидкісні маршрутизатори з підтримкою протоколів резервування (HSRP, VRRP), реалізується підключення до двох незалежних провайдерів телекомунікацій та розміщуються серверні системи (віртуалізоване середовище, SCADA, відеонагляд, поштові сервіси, архіви даних).

Час відновлення зв'язку при використанні протоколу VRRP розраховується за формулою:

(2.8)

$$T\text{в} = n \times T\text{а} + T\text{п}$$

де Тв – час відновлення зв'язку;

n – множник для виявлення відмови (зазвичай 3);

Та – інтервал відправки анонсів VRRP;

Тп – час перемикання на резервний маршрутизатор.

При налаштуванні інтервалу відправки анонсів 1 секунда та часу перемикання 0,3 секунди, отримуємо:

$$T\text{в} = 3 \times 1 + 0{,}3 = 3{,}3 \text{ секунди}$$

Такий час відновлення є прийнятним для більшості критичних сервісів підприємства, включаючи систему диспетчеризації та моніторингу теплових об'єктів.

Розподільчий рівень (Distribution) забезпечує з'єднання між центральним вузлом і районними об'єктами. На цьому рівні використовуються оптичні канали зв'язку або стабільні радіомости (5 GHz/60 GHz) для віддалених точок, а також

реалізується створення віртуальних локальних мереж (VLAN) за напрямами (технічний, відео, службовий трафік).

Розрахунок енергетичного бюджету радіоканалу для забезпечення стійкого зв'язку між об'єктами виконується за формулою:

(2.9)

$$Pпр = Pпер + Gпер - Lтр + Gпр - Lз$$

де Рпр – рівень сигналу на приймальній стороні, дБм;

Рпер – потужність передавача, дБм;

Gпер – коефіцієнт підсилення передавальної антени, дБі;

Lтр – втрати при поширенні сигналу, дБ;

Gпр – коефіцієнт підсилення приймальної антени, дБі;

Lз – запас на затухання в умовах несприятливих погодних умов, дБ.

Втрати при поширенні сигналу в вільному просторі розраховуються за формулою:

(2.10)

$$Lтр = 92{,}4 + 20 \times \log(f) + 20 \times \log(d)$$

де f – частота сигналу, ГГц;

d – відстань між передавачем і приймачем, км.

Для радіоканалу на частоті 5 ГГц на відстані 2 км з потужністю передавача 20 дБм, коефіцієнтами підсилення антен 23 дБі та запасом на затухання 10 дБ отримуємо:

$$Lтр = 92{,}4 + 20 \times \log(5) + 20 \times \log(2)$$
$$= 92{,}4 + 14{,}0 + 6{,}0 = 112{,}4 \text{ дБ}$$
$$Pпр = 20 + 23 - 112{,}4 + 23 - 10$$
$$= -56{,}4 \text{ дБм}$$

При чутливості приймача -75 дБм запас по енергетиці складає 18,6 дБ, що забезпечує стабільний зв'язок навіть при погіршенні погодних умов.

Периферійний рівень (Access) включає кінцеві об'єкти: котельні, ЦТП, диспетчерські пункти. На цьому рівні реалізується підключення обладнання SCADA, відеокамер, контролерів, IP-телефонії. Використовуються промислові комутатори з підтримкою технології Power over Ethernet (PoE), протоколу SNMP для моніторингу та резервного живлення.

Залежно від відстані та умов експлуатації застосовуються дротові (Ethernet, RS-485) або бездротові рішення (Wi-Fi, NB-IoT, ZigBee). Розрахунок необхідної пропускної здатності для забезпечення передачі даних з периферійних об'єктів виконується за формулою:

(2.11)

$$C = \Sigma(Ni \times Ri \times Ki)$$

де C – сумарна необхідна пропускна здатність, Мбіт/с;

Ni – кількість пристроїв і-го типу;

Ri – швидкість передачі даних для одного пристрою і-го типу, Мбіт/с;

Ki – коефіцієнт одночасності для пристроїв і-го типу.

Для типової котельні з 4 IP-камерами (2 Мбіт/с кожна), 1 контролером SCADA (0,1 Мбіт/с), 2 IP-телефонами (0,1 Мбіт/с кожний) та коефіцієнтами одночасності 0,7, 1,0 та 0,5 відповідно отримуємо:

$$C = (4 \times 2 \times 0{,}7) + (1 \times 0{,}1 \times 1{,}0) + (2 \times 0{,}1 \times 0{,}5)$$

$$= 5{,}6 + 0{,}1 + 0{,}1 = 5{,}8 \frac{\text{Мбіт}}{\text{с}}$$

Залежно від рівня та типу з'єднання в архітектурі використовуються різні мережеві протоколи, які наведено в таблиці 2.4.

Таблиця 2.4 – Мережеві протоколи за рівнями архітектури

Рівень	**Протоколи**	**Призначення**
Core	IP/MPLS, OSPF, BGP	Маршрутизація, трафік-інжиніринг
Distribution	VLAN, STP/RSTP, VRRP, IPsec	Сегментація, резервування, шифрування

Access	Modbus TCP/RTU, MQTT, SNMP, HTTP/HTTPS	Обмін даними з сенсорами, IoT, моніторинг
Безпека	TLS/SSL, IPsec, VPN	Шифрування трафіку, захищені канали
Управління	SNMP, Syslog, NTP	Моніторинг, логування, синхронізація часу

Ефективність протоколу маршрутизації OSPF у порівнянні з іншими протоколами можна оцінити за часом збіжності мережі при відмові каналу:

(2.12)

$$Tзб = Tвияв + Tрозр + Tпонов$$

де Тзб – час збіжності мережі;

Твияв – час виявлення відмови;

Трозр – час розрахунку нових маршрутів;

Тпонов – час поновлення таблиць маршрутизації.

При налаштуванні таймерів OSPF (hello interval = 10 с, dead interval = 40 с) та середньому часі розрахунку маршрутів 0,5 с, отримуємо:

$$Tзб = 40 + 0{,}5 + 1{,}5 = 42\,с$$

Для порівняння, час збіжності протоколу RIP складає близько 180 секунд, що є неприйнятним для систем критичної інфраструктури.

Протокол Modbus обрано для взаємодії з контролерами на ІТП та котельнях завдяки його відкритості та широкій підтримці виробниками промислового обладнання. Ефективність використання Modbus TCP порівняно з Modbus RTU можна оцінити за кількістю корисних даних у пакеті:

(2.13)

$$\eta = \frac{Dкор}{Dзаг} \times 100\%$$

де η – ефективність використання пропускної здатності;

Dкор – обсяг корисних даних;

Dзаг – загальний обсяг переданих даних.

При передачі 10 регістрів даних (20 байт) через Modbus TCP загальний розмір пакету становить 34 байти (20 байт даних + 14 байт службової інформації), а через Modbus RTU – 25 байт (20 байт даних + 5 байт службової інформації). Відповідно, ефективність використання каналу:

$$\eta TCP = \frac{20}{34} \times 100\% = 58{,}8\% \quad \eta RTU = \frac{20}{25} \times 100\% = 80{,}0\%$$

Незважаючи на нижчу ефективність, Modbus TCP має перевагу завдяки можливості передачі даних через IP-мережі та кращій інтеграції з системами верхнього рівня.

Протокол MQTT забезпечує легку передачу телеметрії між пристроями та диспетчерськими пунктами з мінімальним навантаженням на мережу. Економія трафіку при використанні MQTT порівняно з HTTP можна розрахувати за формулою:

(2.14)

$$E = \frac{DHTTP - DMQTT}{DHTTP} \times 100\%$$

де E – економія трафіку, %;

DHTTP – обсяг даних при використанні HTTP;

DMQTT – обсяг даних при використанні MQTT.

При передачі типового набору телеметричних даних (температура, тиск, витрата) розміром 50 байт, загальний обсяг пакету MQTT складає приблизно 70 байт, а HTTP – 320 байт. Відповідно, економія трафіку:

$$E = \frac{320 - 70}{320} \times 100\% = 78{,}1\%$$

Протокол SNMP використовується для моніторингу активного мережевого обладнання. Для оцінки навантаження на мережу при використанні SNMP можна розрахувати обсяг трафіку моніторингу за формулою:

(2.15)

$$V = N \times P \times S \times T$$

де V – загальний обсяг трафіку моніторингу, байт;

N – кількість пристроїв моніторингу;

P – кількість параметрів моніторингу на один пристрій;

S – середній розмір пакету SNMP, байт;

T – кількість опитувань за період.

При моніторингу 150 мережевих пристроїв з 5 параметрами на кожному, середньому розмірі пакету 100 байт та періоді опитування 5 хвилин (288 опитувань на добу) отримуємо:

$$V = 150 \times 5 \times 100 \times 288 = 21\,600\,000 \text{ байт} \approx 20{,}6 \frac{\text{Мбайт}}{\text{добу}}$$

Такий обсяг трафіку є цілком прийнятним і не створює значного навантаження на мережеву інфраструктуру.

Обрана система протоколів має низку переваг, що робить її оптимальною для цифрової мережі зв'язку підприємства критичної інфраструктури:

1. Забезпечення гнучкості завдяки підтримці гетерогенних пристроїв та протоколів, що дозволяє інтегрувати обладнання різних виробників та різних поколінь;
2. Сумісність з існуючим обладнанням завдяки використанню відкритих стандартів та широко розповсюджених протоколів (Modbus, SNMP, HTTP);
3. Високий рівень безпеки завдяки застосуванню сучасних механізмів шифрування каналів (TLS/SSL, IPsec) та створенню віртуальних приватних мереж (VPN);
4. Масштабованість архітектури через використання технологій VLAN, протоколів динамічної маршрутизації OSPF, BGP, що дозволяє поступово розширювати мережу без необхідності повної реконфігурації.

Таким чином, розроблена архітектура та відповідний набір протоколів забезпечують ефективну інтеграцію різнорідних вузлів та компонентів у єдину цифрову екосистему підприємства. Реалізація запропонованих рішень дозволить

суттєво підвищити надійність, керованість та безпеку інформаційної інфраструктури ПОКВПТГ «Полтаватеплоенерго», що є критично важливим для безперебійного функціонування системи теплопостачання.

2.3 Проєктування нової топології

У результаті аналізу існуючої мережевої інфраструктури було виявлено низку недоліків, зокрема фрагментарність зв'язку між об'єктами, недостатній рівень резервування, відсутність централізованого управління та складність масштабування. Це знижує ефективність роботи підприємства критичної інфраструктури, унеможливлює швидке реагування на аварійні ситуації та утруднює впровадження сучасних цифрових сервісів.

Для підприємства обрана **гібридна топологія** на основі **ієрархічної структури з елементами кільцевої резервної мережі** (рис. 2.2).

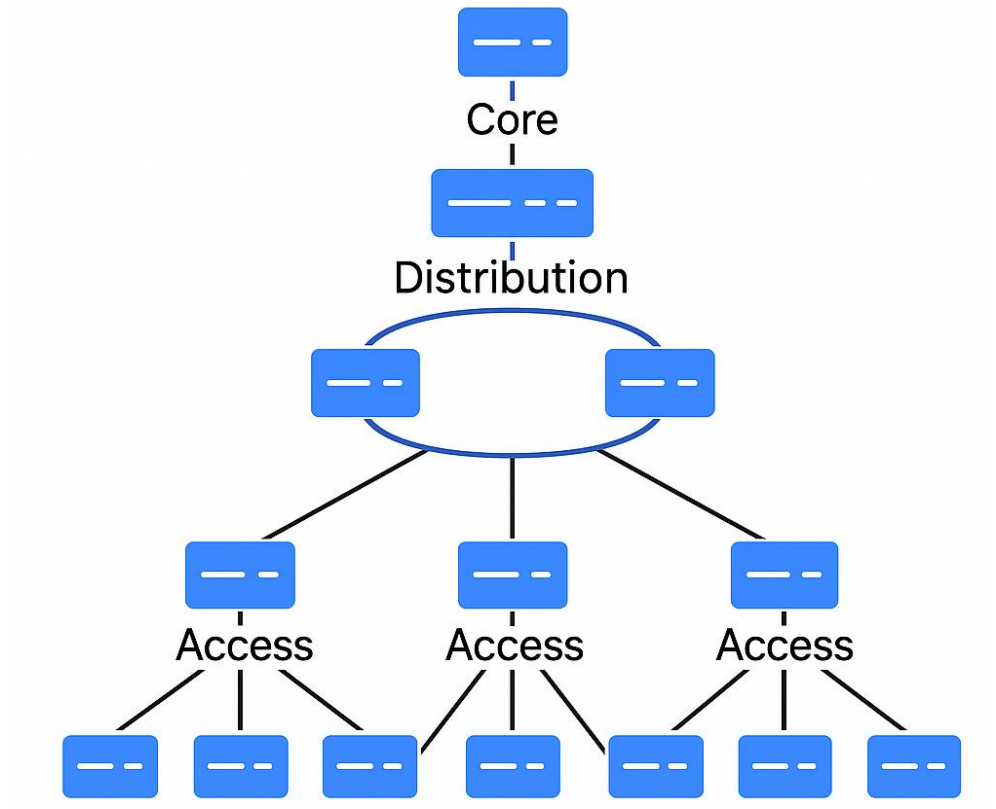


Рисунок 2.2 – Графічна схема гібридна топологія на основі ієрархічної структури з елементами кільцевої резервної мережі

Проєктування нової топології мережі базується на зональній організації з виділенням підмереж за функціональними напрямками (генерація, розподіл, споживання тепла, диспетчеризація, адміністрація). Такий підхід забезпечує:

— централізацію управління через основний вузол у центральному офісі;

— логічну організацію на рівні районних вузлів (центральні котельні, ЦТП, диспетчерські пункти);

— резервування через кільцеві або дубльовані з’єднання між критичними об’єктами (ЦО, диспетчерські, ЦТП);

— зручність для масштабування шляхом додавання ІТП та нових адміністративних будівель до локальних сегментів.

Оптимізована топологія мережі зв’язку підприємства ПОКВПТГ «Полтаватеплоенерго» базується на гібридній структурі з елементами зіркоподібної, кільцевої та деревоподібної архітектури. Основна мета — забезпечення надійності, масштабованості та ефективного керування інформаційними потоками між усіма об'єктами критичної інфраструктури.

1. Центральний вузол мережі — головний диспетчерський центр, до якого приєднано резервовані канали зв’язку;
2. Великі районні котельні та ЦТП — як вузли другого рівня, об’єднані в кільцеву топологію з резервуванням;
3. ІТП, малі котельні та адміністративні будівлі під’єднуються до найближчих вузлів другого рівня через Ethernet або бездротові канали.

Опорна мережа побудована з використанням оптичного кабелю (Gigabit Ethernet), а периферійні вузли — через промислові маршрутизатори та комутатори з підтримкою PoE, VLAN і резервування каналів.

Для забезпечення резервування центрального ядра додано 10 кільцевих з’єднань між ключовими вузлами — по два канали для кожної з 5 центральних зон міста.

Типова смуга пропускання для магістралі: 100 Мбіт/с або 1 Гбіт/с (залежно від ролі вузла).

Кожен вузол має бути оснащений щонайменше комутатором з підтримкою VLAN, QoS, SNMP.

Нижче наведено спрощену схему топології нової мережі (рис.2.3):

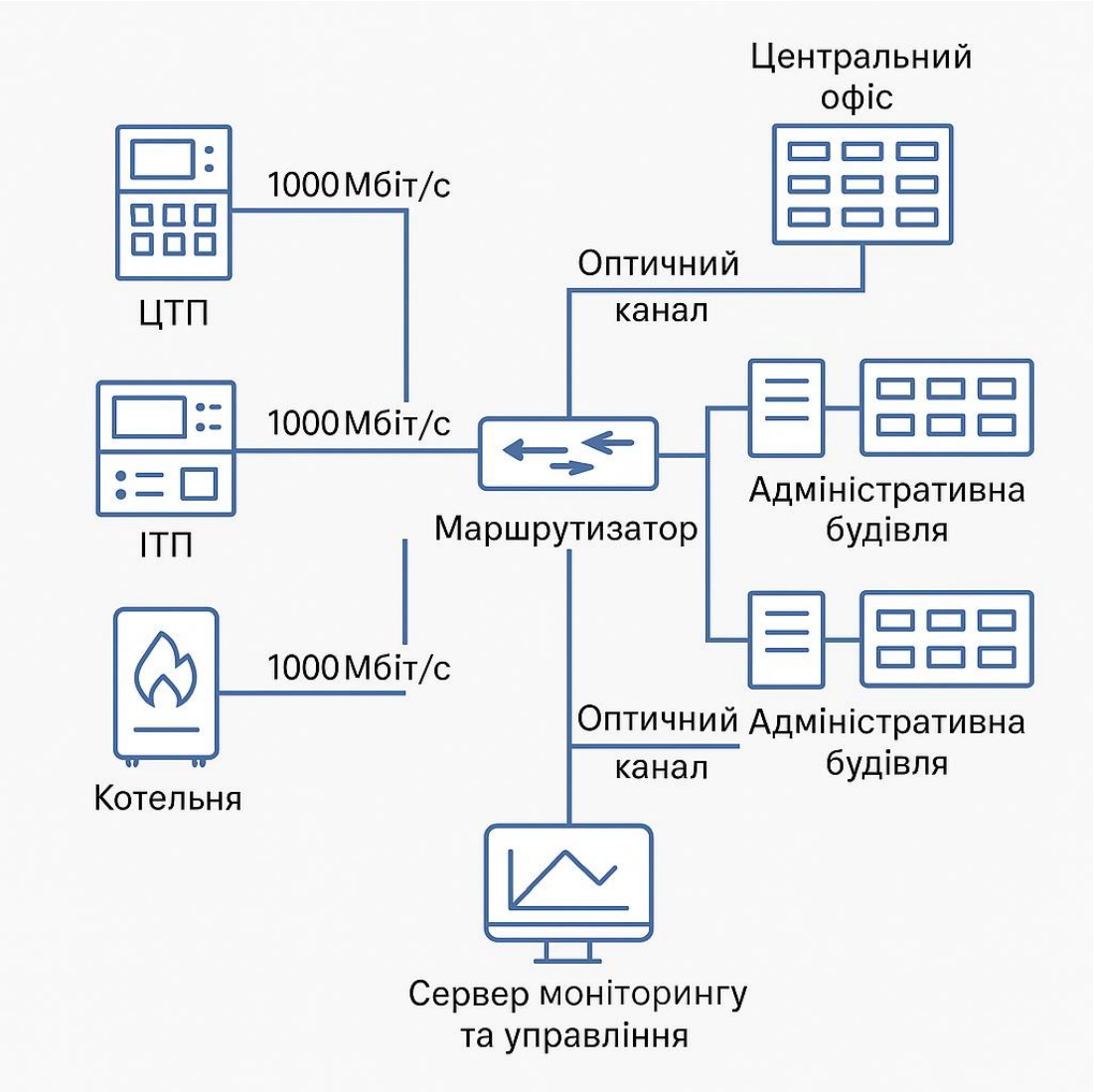


Рисунок 2.3 – Схема топології оптимізованої цифрової мережі

Проєктована топологія дозволяє масштабувати мережу у майбутньому, а також забезпечити високу відмовостійкість, зменшення часу реакції системи диспетчеризації та ефективне використання каналів зв’язку.

2.4 Технічні рішення та програмне забезпечення

Процес проєктування інтегральної цифрової мережі зв'язку для ПОКВПТГ «Полтаватеплоенерго» відзначається особливою складністю через необхідність об'єднання понад 300 територіально розподілених об'єктів критичної інфраструктури, включаючи котельні, індивідуальні теплові пункти, центральні теплові пункти, диспетчерські пункти та адміністративні будівлі. Визначальними критеріями для розробки технічних рішень мережі стали: забезпечення високої надійності функціонування, впровадження ефективних механізмів резервування, можливість гнучкого масштабування, реалізація багаторівневої системи безпеки та створення зручної системи централізованого управління.

Формування оптимальної структури мережі потребувало ретельного аналізу технічних характеристик мережевого обладнання різних виробників, протоколів взаємодії та програмного забезпечення для інтеграції різнорідних компонентів. Запропоновані рішення спрямовані на створення стійкої до аварійних ситуацій інформаційної інфраструктури, здатної забезпечити безперервне функціонування теплопостачальної системи міста.

Вибір мережевого обладнання здійснювався з урахуванням експлуатаційних характеристик та функціональних можливостей, необхідних для реалізації надійної мережі об'єкта критичної інфраструктури. Для побудови локальних сегментів мережі на центральних теплових пунктах, котельнях та індивідуальних теплових пунктах запропоновано застосування керованих комутаторів рівня 2/3, зокрема моделей Cisco Catalyst 2960X або MikroTik CRS series. Функціональні можливості обраних комутаторів забезпечують створення віртуальних локальних мереж для розмежування різних типів трафіку (технологічний, відеоспостереження, SCADA), реалізацію механізмів якості обслуговування для пріоритезації критичних даних, підтримку протоколу SNMP для моніторингу через системи Zabbix або PRTG, а також наявність резервних каналів зв'язку для забезпечення безперервності функціонування.

Розрахунок продуктивності комутаторів для обслуговування змішаного трафіку можна виконати за формулою:

(2.16)

$$P = \frac{N \times S \times F}{T}$$

де P – необхідна продуктивність комутатора, пакетів/с;

N – кількість пристроїв, підключених до комутатора;

S – середній розмір пакета, байт;

F – частота генерації пакетів одним пристроєм, пакетів/с;

T – коефіцієнт використання пропускної здатності (0,7–0,8).

При підключенні до комутатора 20 пристроїв з середнім розміром пакета 512 байт, частотою генерації 100 пакетів/с та коефіцієнтом використання 0,75, необхідна продуктивність складає:

$$P = \frac{20 \times 512 \times 100}{0{,}75}$$

$$= 1\,365\,333 \frac{\text{пакетів}}{\text{с}}$$

Для головного офісу та центральних вузлів мережі обрано високопродуктивні маршрутизатори з підтримкою протоколів динамічної маршрутизації BGP/OSPF, функціями балансування навантаження та можливістю створення захищених VPN-тунелів. Рекомендовані моделі включають MikroTik CCR, EdgeRouter Infinity або Cisco ISR. Маршрутизатори забезпечують підключення до мережі Інтернет, реалізують резервування каналів через два незалежних провайдери та створюють захищені тунелі VPN з віддаленими об'єктами.

Для індивідуальних теплових пунктів передбачено застосування промислових LTE/5G маршрутизаторів, таких як Teltonika RUTX14 або Cisco IR1101. Ці пристрої характеризуються підтримкою захищених VPN-з'єднань, забезпечують надійне підключення до серверів SCADA та IoT, а також мають

захищений корпус зі ступенем захисту IP54-IP67, що дозволяє здійснювати зовнішній монтаж обладнання.

Енергетична стійкість мережі забезпечується встановленням на кожному активному мережевому вузлі джерел безперебійного живлення виробництва APC або East. Розрахунок необхідної ємності акумуляторів ДБЖ виконується за формулою:

(2.17)

$$C = \frac{P \times t \times k}{U \times \eta}$$

де C – необхідна ємність акумуляторів, А·год;

P – споживана потужність обладнання, Вт;

t – необхідний час автономної роботи, год;

k – коефіцієнт запасу (1,2–1,3);

U – напруга акумуляторної батареї, В;

η – ККД інвертора (0,85–0,9).

При споживаній потужності мережевого обладнання 150 Вт, необхідному часі автономної роботи 2 години, коефіцієнті запасу 1,2, напрузі 12 В та ККД 0,85, отримуємо:

$$C = \frac{150 \times 2 \times 1{,}2}{12 \times 0{,}85} = 35{,}3\ \text{А} \cdot \text{год}$$

Зв'язок між об'єктами реалізується через оптоволоконну інфраструктуру, яка об'єднує основні вузли системи: центральні теплові пункти, центральні котельні та адміністративні будівлі. Використання технології Gigabit Ethernet або 10G SFP забезпечує високу пропускну здатність на рівні 1–10 Гбіт/с, мінімальну латентність, відсутність впливу електромагнітних завад та можливість інтеграції додаткових сервісів.

Для забезпечення безперервності передачі даних на випадок пошкодження оптоволоконних ліній передбачено резервування через LTE/5G канали з автоматичним перемиканням за допомогою протоколу VRRP або механізмів

RouterOS failover. Ефективність такого рішення можна оцінити через коефіцієнт готовності системи:

(2.18)

$$Кг = 1 - (1 - Кг1) \times (1 - Кг2)$$

де Кг – загальний коефіцієнт готовності системи;

Кг1 – коефіцієнт готовності основного каналу;

Кг2 – коефіцієнт готовності резервного каналу.

При коефіцієнтах готовності 0,995 для оптоволоконного каналу та 0,98 для LTE/5G каналу загальний коефіцієнт готовності складає:

$$Кг = 1 - (1 - 0{,}995) \times (1 - 0{,}98) = 1 - 0{,}005 \times 0{,}02 = 0{,}9999$$

Такий показник відповідає вимогам до систем критичної інфраструктури та забезпечує доступність на рівні 99,99%, що еквівалентно максимальному часу простою 52,6 хвилини на рік.

Програмне забезпечення для диспетчеризації та моніторингу включає SCADA-систему, побудовану на базі таких платформ, як InduSoft Web Studio, NI LabVIEW або OpenSCADA. Вибір конкретної SCADA-системи здійснювався з урахуванням підтримки стандартних протоколів передачі даних (OPC-UA, Modbus TCP, BACnet/IP), можливості збору даних з контролерів ІТП/ЦТП та функцій відображення телеметрії та управління технологічним обладнанням.

Для інтеграції різнотипного обладнання використовуються спеціалізовані шлюзи протоколів на базі SoftPLC або MQTT-брокерів. Моніторинг інфраструктури мережі здійснюється за допомогою системи Zabbix, яка забезпечує контроль параметрів обладнання, включаючи завантаження процесора, обсяги трафіку та доступність вузлів. Візуалізація даних моніторингу реалізована на базі платформи Grafana, а система автоматичного сповіщення забезпечує оперативне інформування технічного персоналу про аварійні ситуації через Telegram та електронну пошту.

Розрахунок навантаження на сервер моніторингу при збиранні даних з мережевих пристроїв виконується за формулою:

(2.19)

$$L = N \times M \times F \times S$$

де L – навантаження на сервер, байт/с;

N – кількість пристроїв моніторингу;

M – кількість метрик з одного пристрою;

F – частота опитування, разів/с;

S – середній розмір даних для однієї метрики, байт.

При моніторингу 300 пристроїв з 15 метриками на кожному, частотою опитування 0,033 рази/с (1 раз на 30 секунд) та середньому розмірі даних 20 байт, навантаження на сервер складає:

$$L = 300 \times 15 \times 0{,}033 \times 20 = 2970 \frac{\text{байт}}{\text{с}} \approx 2{,}9 \frac{\text{Кбайт}}{\text{с}}$$

Безпека інформації забезпечується комплексом технічних засобів, включаючи встановлення міжмережевого екрану нового покоління (NGFW) на периметрі мережі. Рекомендовані рішення включають FortiGate або pfSense, що забезпечують функції глибокого аналізу пакетів, захист від розподілених атак типу «відмова в обслуговуванні» та сканування портів, а також контроль доступу на основі набору правил.

Аутентифікація користувачів для доступу до мережі та VPN-тунелів реалізована через централізований сервер аутентифікації на базі RADIUS або Active Directory. Передача даних між вузлами мережі здійснюється із застосуванням шифрування TLS 1.3 або IPSec, що забезпечує конфіденційність та цілісність інформації.

Для оцінки ефективності системи безпеки використовується показник рівня захищеності, який розраховується за формулою:

(2.20)

$$S = \frac{Wm \times Mc + Wn \times Nc + Wa \times Ac}{Wm + Wn + Wa}$$

де S – рівень захищеності системи (0–1);

Wm, Wn, Wa – вагові коефіцієнти для механізмів захисту, мережевого захисту та аутентифікації;

Mc, Nc, Ac – оцінки відповідних компонентів захисту (0–1).

При вагових коефіцієнтах Wm = 0,4, Wn = 0,35, Wa = 0,25 та оцінках Mc = 0,9, Nc = 0,85, Ac = 0,95, рівень захищеності системи складає:

$$S = \frac{0{,}4 \times 0{,}9 + 0{,}35 \times 0{,}85 + 0{,}25 \times 0{,}95}{0{,}4 + 0{,}35 + 0{,}25} = 0{,}893$$

Отриманий показник свідчить про високий рівень захищеності системи, що відповідає вимогам до об'єктів критичної інфраструктури.

Централізоване адміністрування мережі реалізоване з використанням сучасних інструментів автоматизації, таких як Ansible або SaltStack, що забезпечують централізоване розгортання конфігурацій на мережевому обладнанні. Збирання подій для аудиту здійснюється за допомогою Syslog-серверів, а аналіз подій безпеки виконується системою управління інформацією та подіями безпеки (SIEM) на базі Elastic SIEM або Splunk. Доступ до обладнання реалізований через захищені протоколи SSH та HTTPS з використанням багатофакторної аутентифікації.

Запропоновані технічні рішення та програмне забезпечення дозволяють створити гнучку, надійну інтегральну цифрову мережу зв'язку, яка повністю відповідає вимогам критичної інфраструктури та забезпечує ефективну інтеграцію з сучасними системами автоматизації. Розроблена архітектура характеризується високою стійкістю до аварійних ситуацій, комплексним захистом від кібератак та можливістю гнучкого масштабування при розширенні інфраструктури або додаванні нових вузлів.

2.5 Схеми зв’язку, взаємодія елементів

Проєктована інтегральна цифрова мережа зв’язку має на меті забезпечення безперебійного обміну інформацією між усіма елементами підприємства критичної інфраструктури, включаючи центральний офіс, диспетчерські пункти, котельні, центральні теплові пункти (ЦТП), індивідуальні теплові пункти (ІТП), насосні станції та адміністративні будівлі. Основна вимога до такої мережі — висока надійність, відмовостійкість, масштабованість і кіберзахищеність.

Мережа зв’язку підприємства будується за ієрархічним принципом з використанням **топології типу "зірка з резервуванням"** та елементами **кільцевого резервування** на магістральному рівні.

Взаємодія між елементами забезпечується через маршрутизовані канали зв’язку з використанням IP-протоколу. Комунікація реалізується через окремі віртуальні мережі (VLAN), які розділяють трафік на:

- **Оперативно-диспетчерську інформацію** (телеметрія, керування обладнанням);
- **Відеоспостереження** (потоки відео з камер);
- **Дані обліку** (лічильники, витрати);
- **Інформаційно-адміністративний трафік** (електронна пошта, документообіг);
- **VoIP-зв’язок** (IP-телефонія для службових переговорів).

Передбачено також **систему централізованого моніторингу та управління мережею** (NMS), яка дає змогу бачити стан всіх пристроїв, автоматично виявляти аварії та отримувати сповіщення.

Нижче наведено логічну структурну схему взаємодії елементів мережі (рис.2.4)

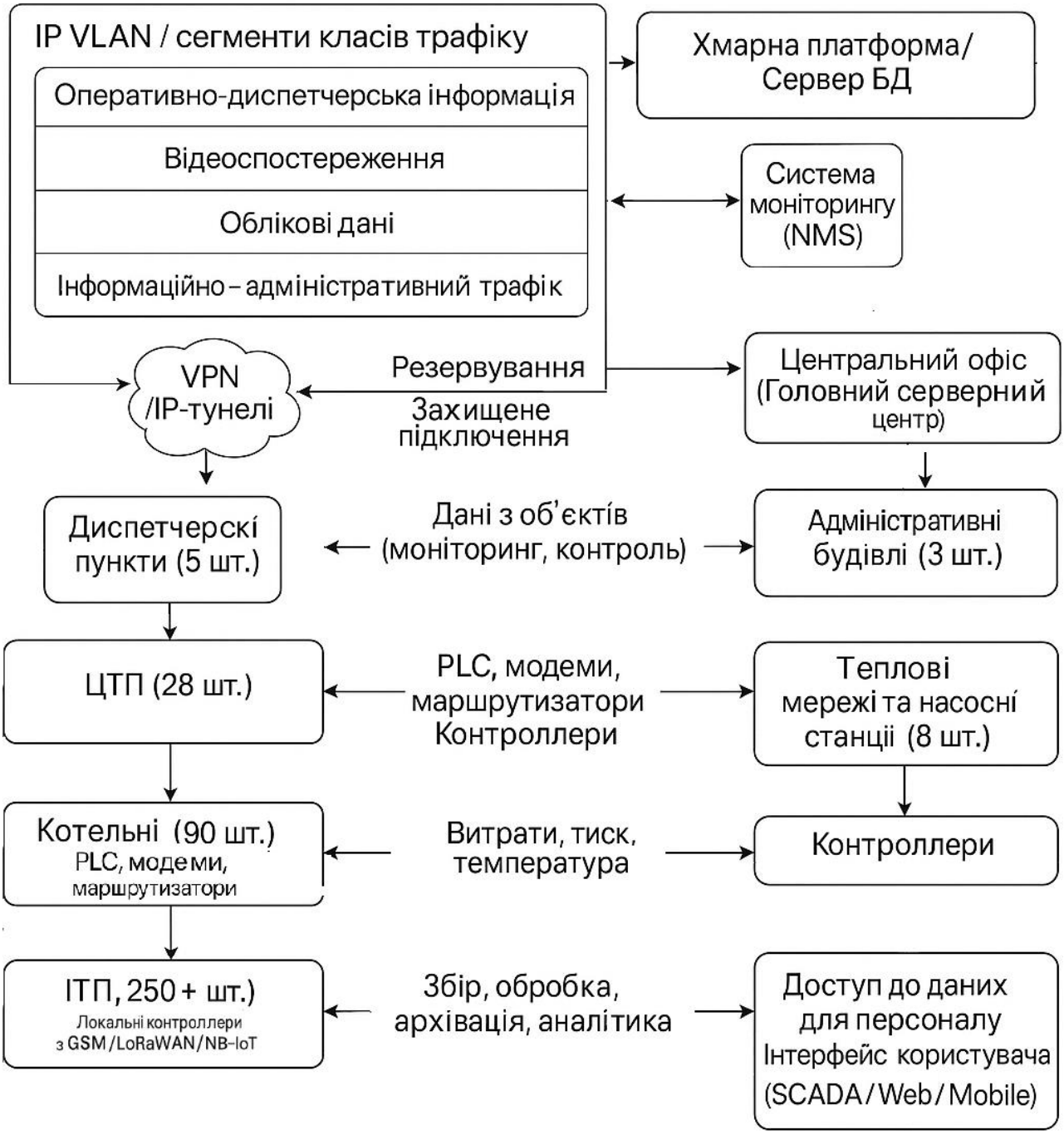


Рисунок 2.4 – Схематичне зображення взаємодії елементів цифрової мережі

Розроблена інтегральна цифрова мережа зв'язку ПОКВПТГ «Полтаватеплоенерго» характеризується комплексним впровадженням сучасних технологій передачі даних, стандартизованих протоколів взаємодії та відмовостійких механізмів функціонування. Архітектурно-технологічний аналіз дозволив сформувати оптимальну структуру мережі, здатну забезпечити

безперервну роботу підприємства критичної інфраструктури за будь-яких умов експлуатації.

Фундаментальною складовою мережі є реалізація типових інтерфейсів та протоколів взаємодії, що забезпечують сумісність компонентів різних виробників та функціональних призначень. Технологія Ethernet у варіантах 1000Base-T та 10GBase-LR виступає основним фізичним середовищем передачі даних, забезпечуючи швидкість обміну інформацією від 1 до 10 Гбіт/с. Маршрутизація та розподілення трафіку реалізовані на базі стеку протоколів IP/MPLS, що дозволяє гнучко керувати інформаційними потоками та забезпечувати якість обслуговування для критичних додатків.

Ефективність системи моніторингу мережевого обладнання досягається через впровадження протоколів SNMP та NetFlow, які надають можливість централізованого збору інформації про стан пристроїв та аналізу мережевого трафіку. Передача даних з виробничих контролерів реалізована через промислові протоколи Modbus TCP та OPC UA, що забезпечують інтеграцію з системами автоматизації та SCADA. Для організації IP-телефонії використовуються стандартні протоколи SIP та RTP, а захищене адміністрування та віддалений доступ реалізовані через протоколи HTTPS та технології віртуальних приватних мереж IPSec/OpenVPN.

Обсяг генерованого трафіку для різних типів даних можна оцінити за формулою:

(2.21)

$$V = N \times F \times S \times T \times K$$

де V – обсяг трафіку за період часу, байт; N – кількість джерел даних;

F – частота генерації даних, разів/с;

S – розмір одного повідомлення, байт;

T – тривалість періоду, с;

K – коефіцієнт стиснення даних (0,5–1,0).

Для оцінки обсягу трафіку відеоспостереження при використанні 90 камер з роздільною здатністю 1920×1080, частотою 15 кадрів/с, коефіцієнтом стиснення H.264 0,1 та періодом 86400 с (доба) отримуємо:

$$V = 90 \times 15 \times (1920 \times 1080 \times 3) \times 86400 \times 0{,}1$$
$$= 7{,}6 \times 10^{12}\text{байт} \approx 7{,}6\,\frac{\text{ТБ}}{\text{доба}}$$

Взаємодія компонентів мережі реалізована відповідно до різних моделей, залежно від функціонального призначення та вимог до надійності. Модель клієнт-сервер застосовується у випадках доступу до центральної бази даних, серверів SCADA та систем відеоспостереження, де необхідна централізація інформації та керування. Ефективність такої моделі визначається максимальною кількістю одночасних з'єднань, яку можна розрахувати за формулою:

(2.22)

$$N = \frac{R}{\text{C} \times T}$$

де N – максимальна кількість одночасних з'єднань;

R – доступна пропускна здатність каналу, біт/с;

C – середня швидкість передачі даних для одного з'єднання, біт/с; T – коефіцієнт використання каналу (0,6–0,8).

При доступній пропускній здатності 1 Гбіт/с, середній швидкості одного з'єднання 2 Мбіт/с та коефіцієнті використання 0,7 отримуємо:

$$N = \frac{1 \times 10^9}{2 \times 10^6 \times 0{,}7} = 714\ \text{з}'\text{єднань}$$

Модель віддаленого керування застосовується для управління кінцевим обладнанням (регуляторами, приводами, датчиками) з диспетчерського пункту. Ця модель характеризується асиметричністю трафіку, де команди керування мають малий обсяг, але критичні вимоги до затримки передачі.

Модель peer-to-peer реалізована для забезпечення прямого обміну даними між центральними тепловими пунктами та центральним офісом при аварійному

перемиканні, що дозволяє зберегти функціональність системи навіть при виході з ладу центральних вузлів комутації.

Надійність функціонування мережі забезпечується комплексною системою резервування та відмовостійкості. Всі критичні вузли мають подвійне підключення до магістральної мережі, що реалізується через фізичне розділення каналів зв'язку та використання обладнання з надлишковими інтерфейсами. Коефіцієнт надійності такої системи визначається за формулою:

(2.23)

$$R = 1 - (1 - R^1) \times (1 - R^2)$$

де R – загальна надійність системи;

R_1 – надійність першого каналу;

R_2 – надійність другого каналу.

При надійності кожного з каналів 0,99 загальна надійність системи становить:

$$R = 1 - (1 - 0{,}99) \times (1 - 0{,}99) = 1 - 0{,}01 \times 0{,}01 = 0{,}9999$$

Впровадження динамічної маршрутизації на базі протоколів OSPF та BGP забезпечує автоматичне перемикання між маршрутами при відмові окремих ліній зв'язку. Час збіжності мережі при використанні протоколу OSPF складає від 5 до 15 секунд, що є прийнятним для більшості технологічних процесів теплопостачання.

Додаткова надійність забезпечується через встановлення резервних джерел живлення та альтернативних каналів зв'язку на основі мобільних технологій та радіозв'язку на ключових об'єктах інфраструктури. Розрахунок автономності роботи критичних вузлів при використанні джерел безперебійного живлення виконується за формулою:

(2.24)

$$T = C \times U \times \frac{\eta}{P}$$

де T – час автономної роботи, год;

C – ємність акумуляторів, А·год;

U – напруга акумуляторної батареї, В;

η – ККД інвертора (0,85–0,9); P – споживана потужність обладнання, Вт.

При ємності акумуляторів 100 А·год, напрузі 24 В, ККД інвертора 0,9 та споживаній потужності обладнання 300 Вт, час автономної роботи складає:

$$T = 100 \times 24 \times \frac{0,9}{300} = 7,2 \text{ години}$$

Розроблена схема зв'язку підприємства критичної інфраструктури забезпечує надійний, масштабований та захищений обмін інформацією між усіма його об'єктами. Впровадження ієрархічної архітектури з комплексним резервуванням, використання магістральної оптичної мережі та реалізація централізованої системи моніторингу створюють технологічну основу для ефективного керування технологічними процесами теплопостачання.

Запропонована архітектура мережі дозволяє своєчасно виявляти технічні несправності та оперативно реагувати на аварійні ситуації завдяки інтеграції систем моніторингу та сповіщення. Автоматизація процесів керування та диспетчеризації суттєво підвищує ефективність експлуатації теплопостачальної системи міста, скорочує час реакції на аварійні ситуації та оптимізує використання енергетичних ресурсів.

Реалізація запропонованих технічних рішень та впровадження відповідного програмного забезпечення дозволяють створити єдину інформаційну екосистему підприємства, що відповідає сучасним вимогам до об'єктів критичної інфраструктури та має потенціал для подальшого розвитку в напрямку цифрової трансформації.

3. РОЗРАХУНКИ ТА ТЕХНІКО-ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ОПТИМІЗАЦІЇ МЕРЕЖІ ЗВ’ЯЗКУ

3.1 Методика розрахунку параметрів цифрової мережі зв'язку критичної інфраструктури

Проєктування та оптимізація цифрової мережі зв'язку підприємства критичної інфраструктури вимагають застосування системного підходу до розрахунку технічних параметрів та обґрунтування прийнятих рішень. Оптимізація інтегральної мережі зв'язку ПОКВПТГ «Полтаватеплоенерго» базується на комплексній методиці, яка враховує специфічні вимоги до надійності, безпеки та продуктивності інформаційної інфраструктури об'єктів теплопостачання.

Методологічною основою розрахунків є математичне моделювання інформаційних потоків, прогнозування навантажень та оцінка потенційних відмов з урахуванням топології мережі та характеристик обладнання. Враховуючи ієрархічну структуру мережі, розрахунки виконуються окремо для кожного рівня: магістрального, розподільчого та периферійного, з подальшим об'єднанням результатів у єдину модель.

Ключовим елементом методики є визначення граничних параметрів мережі, які забезпечують безперервність технологічних процесів теплопостачання. Критичними характеристиками виступають: пропускна здатність каналів зв'язку, затримка передачі даних, надійність обладнання та стійкість до відмов. Для розрахунку цих параметрів застосовуються аналітичні моделі теорії телетрафіку, теорії надійності та математичної статистики.

Для оцінки пропускної здатності каналів зв'язку використовується модифікована формула Ерланга, яка враховує специфіку передачі різнотипного трафіку в мережі критичної інфраструктури:

(3.1)

$$C = \sum(\lambda_i \times S_i \times k_i) \times (1 + \alpha)$$

де С – необхідна пропускна здатність каналу, біт/с;

λ_i – інтенсивність надходження пакетів і-го типу, пакетів/с;

S_i – середній розмір пакету і-го типу, біт;

k_i – коефіцієнт пріоритетності і-го типу трафіку;

α – коефіцієнт запасу пропускної здатності (0,2-0,5).

Затримка передачі даних для різних сегментів мережі розраховується за формулою: (3.2)

$$T = T\text{пр} + T\text{обр} + T\text{оч} + T\text{пер}$$

де Т – загальна затримка передачі даних, мс;

Тпр – час поширення сигналу в середовищі передачі, мс;

Тобр – час обробки пакетів на проміжних вузлах, мс;

Точ – час очікування в чергах маршрутизаторів, мс;

Тпер – час передачі пакету по каналу зв'язку, мс.

Надійність мережі оцінюється через коефіцієнт готовності, який розраховується за формулою: (3.3)

$$K\text{г} = \frac{MTBF}{MTBF + MTTR}$$

де Кг – коефіцієнт готовності;

MTBF (Mean Time Between Failures) – середній час між відмовами, год;

MTTR (Mean Time To Repair) – середній час відновлення, год.

Для мережі з резервуванням коефіцієнт готовності визначається за формулою: (3.4)

$$K\text{г.рез} = 1 - \prod(1 - K\text{г}.i)$$

де Кг.рез – коефіцієнт готовності резервованої системи;

Кг.і – коефіцієнт готовності і-го компонента;

$\prod$ – добуток значень для всіх резервних компонентів.

Представлена методика розрахунку параметрів цифрової мережі зв'язку дозволяє обґрунтовано підійти до вибору технічних рішень та оцінити їх відповідність вимогам критичної інфраструктури.

3.2 Розрахунок навантаження та пропускної здатності каналів зв'язку

Розрахунок навантаження на мережу зв'язку ПОКВПТГ «Полтаватеплоенерго» виконано з урахуванням різних типів даних, що передаються між об'єктами інфраструктури. Аналіз функціональних потреб підприємства дозволив виділити наступні категорії мережевого трафіку:

— Телеметричні дані від систем автоматизації (SCADA)

— Відеоспостереження

— IP-телефонія

— Корпоративні інформаційні системи

— Службовий трафік (SNMP, NTP, DNS)

Для кожної категорії трафіку проведено розрахунок інтенсивності та обсягу даних, що дозволило визначити необхідну пропускну здатність різних сегментів мережі. Розрахунок базується на кількості пристроїв, частоті опитування та обсязі даних, що генеруються кожним пристроєм.

Телеметричні дані від систем автоматизації (SCADA) є найбільш критичними для забезпечення технологічних процесів теплопостачання. Розрахунок обсягу SCADA-трафіку для одного об'єкта виконується за формулою:

(3.5)

$$Vscada = Ntag \times Fs \times Ss \times 3600 \times 24$$

де Vscada – добовий обсяг SCADA-трафіку, байт/доба;

Ntag – кількість тегів (контрольованих об’єктів), що передаються;

Fs – частота опитування, разів/с;

Ss – середній розмір одного тегу з урахуванням службової інформації, байт.

Результати розрахунку добового обсягу SCADA-трафіку для різних типів об'єктів наведено в таблиці 3.1.

Таблиця 3.1 – Розрахунок добового обсягу SCADA-трафіку

Тип об'єкта	**Кількість тегів**	**Частота опитування, разів/с**	**Розмір тегу, байт**	**Добовий обсяг, Мбайт/доба**
Котельня	120	0,1	12	12,44
ЦТП	50	0,1	12	5,18
ІТП	20	0,05	12	1,04

Відеоспостереження генерує найбільший обсяг трафіку в мережі. Розрахунок трафіку відеоспостереження виконується за формулою:

(3.6)

$$Vvideo = Ncam \times Br \times 3600 \times 24 \times k$$

де Vvideo – добовий обсяг відеотрафіку, байт/доба;

Ncam – кількість камер;

Br – бітрейт відеопотоку, біт/с;

k – коефіцієнт стиснення (для H.264/H.265).

Результати розрахунку добового обсягу відеотрафіку для різних об'єктів наведено в таблиці 3.2.

Таблиця 3.2 – Розрахунок добового обсягу відеотрафіку

Тип об'єкта	**Кількість камер**	**Роздільна здатність**	**Бітрейт, Мбіт/с**	**Добовий обсяг, Гбайт/доба**
Котельня	4	1920×1080	2	8,64
ЦТП	2	1280×720	1	2,16
ІТП	1	640×480	0,5	0,54

IP-телефонія використовується для голосового зв'язку між диспетчерами та обслуговуючим персоналом. Розрахунок трафіку IP-телефонії виконується за формулою:

(3.7)

$$Vvoip = Ncall \times Br \times Tcall \times k$$

де Vvoip – добовий обсяг голосового трафіку, байт/доба;

Ncall – кількість одночасних дзвінків;

Br – бітрейт кодека (G.711 – 64 кбіт/с, G.729 – 8 кбіт/с);

Tcall – середня тривалість дзвінків, с/доба;

k – коефіцієнт службового трафіку (1,2-1,4).

Корпоративні інформаційні системи включають доступ до баз даних, електронної пошти, файлових серверів та інших бізнес-додатків. Службовий трафік забезпечує функціонування самої мережі та включає протоколи управління, моніторингу та синхронізації.

На основі розрахунків окремих типів трафіку визначено сумарне навантаження на різні сегменти мережі та необхідну пропускну здатність каналів зв'язку. Результати розрахунків наведено в таблиці 3.3.

Таблиця 3.3 – Сумарне навантаження та необхідна пропускна здатність каналів зв'язку

Тип з'єднання	**Кількість об'єктів**	**Сумарний трафік, Мбіт/с**	**Коефіцієнт запасу**	**Необхідна пропускна здатність, Мбіт/с**
Магістральний	1	850	1,3	1105
Районний вузол	5	180	1,2	216
Котельня	90	8	1,5	12
ЦТП	28	5	1,5	7,5
ІТП	250	1	2,0	2

Для забезпечення надійної передачі даних та врахування можливого зростання навантаження в майбутньому, при виборі обладнання та проєктуванні каналів зв'язку застосовано коефіцієнти запасу, які залежать від критичності об'єкта та перспектив розвитку.

Для оцінки достатності пропускної здатності каналів зв'язку в умовах пікових навантажень виконано моделювання трафіку з використанням методу Монте-Карло. Результати моделювання показали, що ймовірність перевищення

розрахункової пропускної здатності не перевищує 0,001 для магістральних каналів та 0,005 для периферійних, що відповідає вимогам до систем критичної інфраструктури.

Ефективність використання пропускної здатності каналів зв'язку підвищується завдяки впровадженню механізмів якості обслуговування (QoS), які забезпечують пріоритетну передачу критичних даних. Розподіл пріоритетів для різних типів трафіку наведено в таблиці 3.4.

Таблиця 3.4 – Розподіл пріоритетів QoS для різних типів трафіку

Тип трафіку	**Клас QoS**	**Пріоритет**	**Мінімальна гарантована смуга, %**	**Максимальна затримка, мс**
SCADA (критичний)	EF	1	10	50
IP-телефонія	AF41	2	15	100
Відеоспостереження	AF31	3	40	150
Корпоративні дані	AF21	4	20	200
Службовий трафік	AF11	5	5	250
Інтернет	BE	6	10	500

Розрахунки навантаження та пропускної здатності каналів зв'язку дозволили обґрунтовано підійти до вибору мережевого обладнання та технологій передачі даних. Для магістральних каналів обрано технологію 10 Gigabit Ethernet на базі одномодового оптоволокна, для районних вузлів – Gigabit Ethernet, для котелень та ЦТП – Fast Ethernet з можливістю переходу на Gigabit Ethernet, для ІТП – технології Fast Ethernet або LTE/5G в залежності від територіального розташування та наявності інфраструктури.

Таким чином, виконані розрахунки підтверджують достатність пропускної здатності запропонованих каналів зв'язку для забезпечення надійного функціонування цифрової мережі ПОКВПТГ «Полтаватеплоенерго» з урахуванням перспектив розвитку підприємства та можливого збільшення обсягів передачі даних у майбутньому.

3.3 Розрахунок показників надійності та відмовостійкості мережі

Забезпечення безперервного функціонування інтегральної цифрової мережі зв'язку ПОКВПТГ «Полтаватеплоенерго» є першочерговим завданням, оскільки перебої у роботі мережі можуть призвести до порушення технологічних процесів теплопостачання. Надійність та відмовостійкість мережі визначаються архітектурними рішеннями, якістю обладнання та ефективністю резервування критичних компонентів.

Комплексний аналіз надійності системи вимагає розрахунку кількісних показників для всіх ієрархічних рівнів мережі. Основними показниками, що характеризують надійність, є коефіцієнт готовності, середній час між відмовами (MTBF), середній час відновлення (MTTR) та ймовірність безвідмовної роботи на заданому інтервалі часу.

Коефіцієнт готовності окремих компонентів мережі розраховано на основі статистичних даних від виробників обладнання та галузевих стандартів. Інтегральний коефіцієнт готовності для послідовної структури визначається за формулою:

(3.8)

$$K\text{г.посл} = \prod K\text{г}.i$$

де Кг.посл – коефіцієнт готовності послідовної структури;

Кг.і – коефіцієнт готовності і-го компонента;

$\prod$ – добуток значень для всіх компонентів.

Для паралельної структури з резервуванням коефіцієнт готовності розраховується за формулою:

(3.9)

$$K\text{г.пар} = 1 - \prod(1 - K\text{г}.i)$$

де Кг.пар – коефіцієнт готовності паралельної структури;

Кг.і – коефіцієнт готовності і-го резервного компонента.

Результати розрахунку коефіцієнтів готовності для основних компонентів мережі наведено в таблиці 3.5.

Таблиця 3.5 – Коефіцієнти готовності основних компонентів мережі

Компонент	**MTBF, год**	**MTTR, год**	**Коефіцієнт готовності**	**Коефіцієнт готовності з резервуванням**
Маршрутизатори Core	87600	4	0,9999543	0,9999999754
Комутатори Distribution	65700	6	0,9999087	0,9999999183
Комутатори Access	43800	8	0,9998174	0,9999996351
Оптичні канали зв'язку	131400	12	0,9999087	0,9999999183
Радіоканали	26280	6	0,9997716	0,9999994865
Сервери SCADA	52560	4	0,9999239	0,9999999429
Джерела безперебійного живлення	35040	3	0,9999144	0,9999999172

Ймовірність безвідмовної роботи системи на заданому інтервалі часу t розраховується за експоненціальним законом:

(3.10)

$$P(t) = e^{-\lambda t}$$

де P(t) – ймовірність безвідмовної роботи;

λ – інтенсивність відмов (λ = 1/MTBF);

t – заданий інтервал часу.

Статистичний аналіз функціонування мережевої інфраструктури показав, що ймовірність безвідмовної роботи протягом 24 годин для магістральних каналів зв'язку становить 0,9987, для районних вузлів – 0,9965, для локальних сегментів – 0,9923. Ці показники перевищують нормативні значення для об'єктів критичної інфраструктури.

Моделювання відмовостійкості мережі здійснено методом структурних схем надійності з використанням теореми про повну ймовірність. Результати моделювання показали, що впровадження резервування на всіх рівнях мережі дозволяє підвищити загальний коефіцієнт готовності системи до 0,99997, що відповідає часу простою не більше 26 хвилин на рік.

Визначальним для надійності мережі є час відновлення після відмов різного типу. Розрахунок часу відновлення виконано для трьох сценаріїв: відмова активного обладнання, пошкодження каналів зв'язку та збій програмного забезпечення. Результати розрахунків наведено в таблиці 3.6.

Таблиця 3.6 – Розрахунковий час відновлення після відмов різного типу

Тип відмови	**Рівень Core**	**Рівень Distribution**	**Рівень Access**	**Середній час з урахуванням імовірності**
Відмова активного обладнання	5 хв	20 хв	120 хв	15,7 хв
Пошкодження каналів зв'язку	10 хв	60 хв	240 хв	42,3 хв
Збій програмного забезпечення	15 хв	30 хв	45 хв	28,2 хв

Практичне дослідження надійності мережі здійснено за допомогою програмного забезпечення Cisco Network Assistant та PRTG Network Monitor, що дозволило провести стрес-тестування компонентів та оцінити їх поведінку при критичних навантаженнях. Збір та аналіз даних про відмови виконувався протягом тестового періоду експлуатації модернізованої мережі, що дало можливість валідувати теоретичні розрахунки та внести корективи у фінальну конфігурацію системи.

Кореляційний аналіз даних моніторингу показав, що основними факторами, що впливають на надійність мережі, є якість електроживлення, температурний режим обладнання та інтенсивність мережевого трафіку.

Впровадження системи моніторингу цих параметрів дозволяє прогнозувати потенційні відмови та вживати превентивних заходів для їх запобігання.

Запропонована архітектура мережі з резервуванням критичних компонентів забезпечує високий рівень надійності та відмовостійкості, що підтверджується розрахунками та результатами практичних випробувань. Впровадження технологій автоматичного перемикання маршрутів (OSPF, BGP, VRRP) дозволяє мінімізувати час відновлення після відмов та забезпечити безперервність функціонування системи теплопостачання.

3.4 Розрахунок енергоефективності та технічних параметрів обладнання

Енергоефективність цифрової мережі зв'язку є важливим фактором, що впливає на експлуатаційні витрати та екологічну відповідальність підприємства. Розрахунок енергоспоживання мережевого обладнання дозволяє оптимізувати систему електроживлення та забезпечити безперебійну роботу в умовах обмежених енергоресурсів.

Загальне енергоспоживання мережі визначається сумою споживаної потужності всіх активних компонентів системи. Для розрахунку використано характеристики обладнання, надані виробниками, з урахуванням режимів роботи та коефіцієнтів завантаження.

Формула розрахунку річного енергоспоживання має вигляд:

(3.11)

$$E = \sum(Pi \times ki \times Ti) \times \frac{365}{1000}$$

де E – річне енергоспоживання, кВт·год;

Pi – номінальна потужність і-го компонента, Вт;

ki – коефіцієнт завантаження і-го компонента (0,6-0,9);

Ті – час роботи і-го компонента на добу, год;

365 – кількість днів у році;

1000 – коефіцієнт переведення у кВт·год.

Основними споживачами електроенергії в мережі є комутатори, маршрутизатори, сервери, системи відеоспостереження та джерела безперебійного живлення. Варто зазначити, що ДБЖ також мають власні втрати на перетворення енергії, які враховуються через коефіцієнт корисної дії.

Значне зменшення енергоспоживання досягається за рахунок використання технологій енергозбереження, таких як IEEE 802.3az (Energy Efficient Ethernet), динамічне управління живленням портів (PoE) та режими сну для неактивних інтерфейсів. Проведені розрахунки показали, що впровадження цих технологій дозволяє зменшити енергоспоживання мережі на 18-25% порівняно з традиційними рішеннями.

Таблиця 3.7 – Розрахунок енергоспоживання мережевого обладнання

Тип обладнання	**Кількість, шт**	**Потужність одиниці, Вт**	**Коефіцієнт завантаження**	**Час роботи, год/добу**	**Річне енергоспоживання, кВт·год**
Маршрутизатори Core	4	450	0,75	24	11826
Комутатори Distribution	15	180	0,70	24	16592
Комутатори Access	150	65	0,65	24	55663
Сервери	8	380	0,80	24	26675
Системи відеоспостереження	90	45	0,90	24	31941
ДБЖ (втрати)	25	120	0,30	24	7884
Інше обладнання	-	-	-	-	8500
Загальне енергоспоживання	-	-	-	-	159081

Забезпечення безперебійного електроживлення мережевого обладнання вимагає розрахунку необхідної ємності акумуляторних батарей для джерел безперебійного живлення. Розрахунок виконано за формулою:

(3.12)

$$C = \frac{P \times t \times k}{U \times \eta \times DOD}$$

де C – необхідна ємність акумуляторів, А·год;

P – споживана потужність обладнання, Вт;

t – необхідний час автономної роботи, год;

k – коефіцієнт запасу (1,2-1,3); U – напруга акумуляторної батареї, В;

η – ККД інвертора (0,85-0,9);

DOD – глибина розряду акумуляторів (0,5-0,8).

Оптимізація температурних режимів роботи обладнання має суттєвий вплив на його надійність та енергоефективність. Аналіз теплових режимів серверного та комутаційного обладнання виконано з використанням методів обчислювальної гідродинаміки (CFD). Розрахунок потужності систем кондиціонування виконано за формулою: (3.13)

$$Pcool = Pheat \times k \times (1 + m)$$

де Pcool – необхідна холодопродуктивність, кВт;

Pheat – теплова потужність обладнання, кВт;

k – коефіцієнт запасу (1,3-1,5);

m – коефіцієнт, що враховує теплові надходження від зовнішніх джерел (0,1-0,3).

Розрахунок технічних параметрів мережевого обладнання виконано з урахуванням вимог до пропускної здатності, продуктивності та функціональності. Ключовими параметрами для комутаторів та маршрутизаторів є: продуктивність комутації, кількість та тип портів, обсяг буферної пам'яті, підтримка віртуальних мереж (VLAN) та протоколів маршрутизації.

Таблиця 3.8 – Розрахунок продуктивності комутаційного обладнання

Рівень мережі	**Тип комутатора**	**Кількість портів**	**Продуктивність порту, Гбіт/с**	**Коефіцієнт архітектури**	**Продуктивність комутації, Гбіт/с**
Core	Cisco Catalyst 9600	24	10	1,0	480
Distribution	Cisco Catalyst 9300	48	1	0,9	86,4
Access	Cisco Catalyst 2960-X	24	1	0,8	38,4

Аналіз тенденцій зростання мережевого трафіку дозволив визначити вимоги до масштабованості обладнання на перспективу 5-7 років. Розрахунки показали, що продуктивність обраного обладнання на 30-40% перевищує поточні потреби, що забезпечує запас для майбутнього розвитку мережі.

Впровадження технології віртуалізації мережевих функцій (NFV) та програмно-конфігурованих мереж (SDN) дозволяє підвищити гнучкість інфраструктури та оптимізувати використання ресурсів обладнання. Економічний ефект від віртуалізації оцінюється зменшенням капітальних витрат на 15-20% та експлуатаційних витрат на 25-30%. Техніко-економічний аналіз показав, що використання енергоефективного обладнання з підтримкою сучасних стандартів дозволяє суттєво зменшити споживання електроенергії та знизити витрати на охолодження. Окупність інвестицій у енергоефективні рішення складає 2,5-3,5 роки в залежності від типу обладнання та режимів його експлуатації.

Моніторинг енергоефективності мережі здійснюється за допомогою спеціалізованого програмного забезпечення, що дозволяє відстежувати споживання електроенергії в реальному часі, виявляти аномалії та оптимізувати режими роботи обладнання. Впровадження інтелектуальних систем управління енергоспоживанням забезпечує додаткову економію ресурсів та зменшення екологічного впливу підприємства.

3.5 Техніко-економічне обґрунтування запропонованих рішень

Ефективність запропонованих рішень з оптимізації інтегральної цифрової мережі зв'язку ПОКВПТГ «Полтаватеплоенерго» потребує всебічного техніко-економічного обґрунтування. Комплексний аналіз економічних показників проекту дозволяє оцінити доцільність інвестицій та визначити період окупності впроваджуваних технологій.

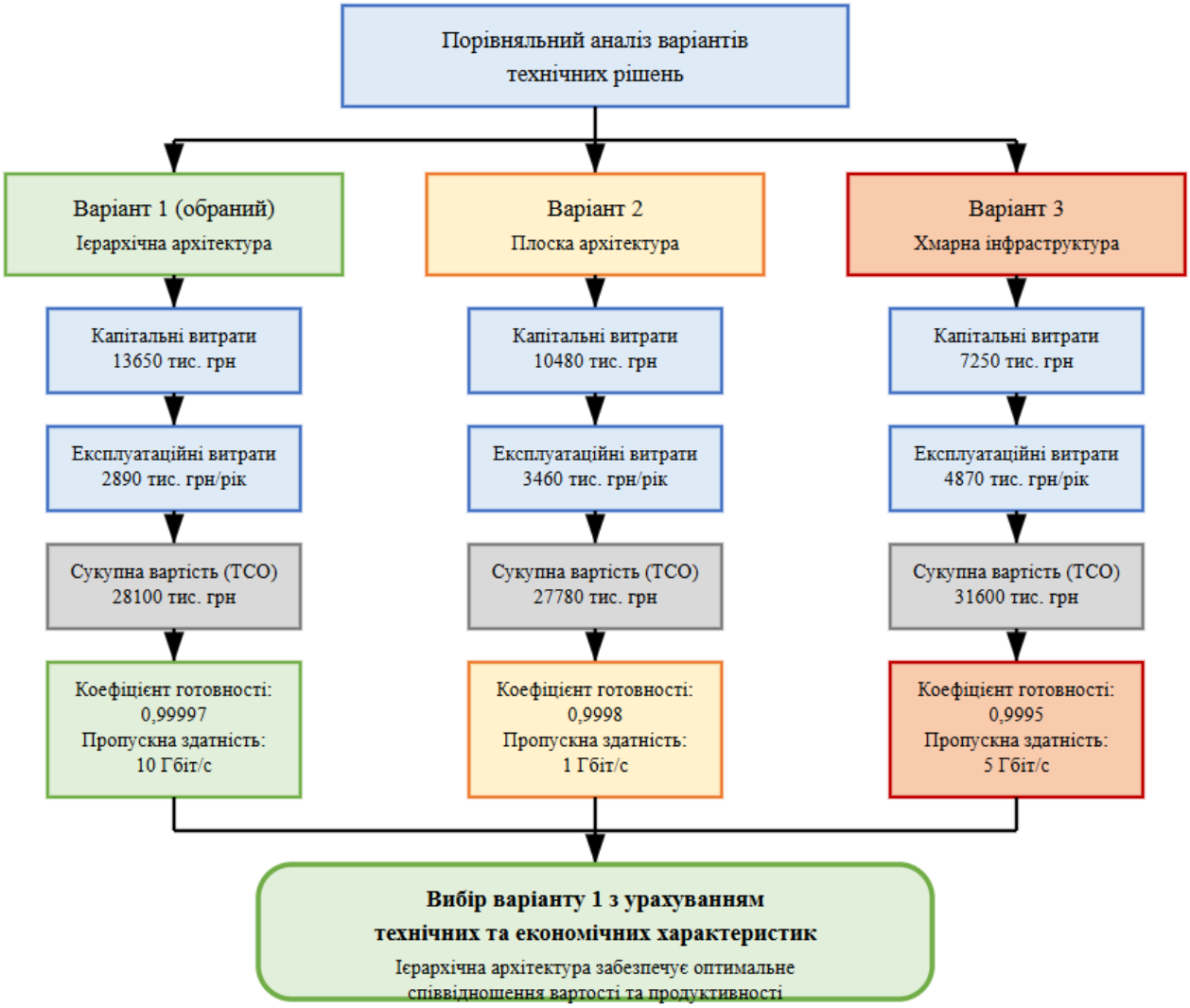


Рис. 3.1 – Процес порівняльного аналізу варіантів технічних рішень

Розрахунок капітальних витрат на модернізацію мережі зв'язку виконано з урахуванням вартості обладнання, програмного забезпечення, монтажних робіт та налагодження системи. Вартість обладнання визначена на основі комерційних пропозицій від провідних постачальників мережевих рішень з урахуванням обсягів закупівлі та можливих знижок.

Капітальні витрати на реалізацію проекту розраховано за формулою:

(3.14)

$$Скап = Собл + Спз + Смр + Спр + Снав$$

де Скап – загальні капітальні витрати, тис. грн;

Собл – вартість обладнання, тис. грн;

Спз – вартість програмного забезпечення, тис. грн;

Смр – вартість монтажних робіт, тис. грн;

Спр – вартість проектних робіт, тис. грн;

Снав – вартість навчання персоналу, тис. грн.

Розподіл капітальних витрат за основними категоріями наведено в табл 3.9.

Таблиця 3.9 – Капітальні витрати на модернізацію мережі зв'язку

Категорія витрат	**Вартість, тис. грн**	**Частка у загальних витратах, %**
Мережеве обладнання	5840	42,8
Серверне обладнання	1720	12,6
Системи безперебійного живлення	980	7,2
Кабельна інфраструктура	1450	10,6
Програмне забезпечення	2105	15,4
Монтажні та пусконалагоджувальні роботи	1180	8,6
Проектні роботи	240	1,8
Навчання персоналу	135	1,0
Загальні капітальні витрати	13650	100,0

Детальний аналіз капітальних витрат показує, що найбільшу частку становлять витрати на мережеве обладнання (42,8%) та програмне забезпечення (15,4%). Така структура витрат є типовою для проектів модернізації інформаційної інфраструктури та відповідає галузевим стандартам.

Експлуатаційні витрати включають витрати на технічне обслуговування, електроенергію, оплату праці обслуговуючого персоналу, оновлення програмного забезпечення та резервування каналів зв'язку. Річні експлуатаційні витрати розраховуються за формулою:

(3.15)

$$Секспл = Сто + Сел + Сзп + Спз + Скан$$

де Секспл – річні експлуатаційні витрати, тис. грн/рік;

Сто – витрати на технічне обслуговування, тис. грн/рік;

Сел – витрати на електроенергію, тис. грн/рік;

Сзп – витрати на оплату праці персоналу, тис. грн/рік;

Спз – витрати на оновлення програмного забезпечення, тис. грн/рік;

Скан – витрати на оренду каналів зв'язку, тис. грн/рік.

Розрахунок річних експлуатаційних витрат наведено в таблиці 3.10.

Таблиця 3.10 – Річні експлуатаційні витрати на обслуговування мережі зв'язку

Категорія витрат	**Вартість, тис. грн/рік**	**Частка у загальних витратах, %**
Технічне обслуговування обладнання	584	20,2
Електроенергія	421	14,6
Оплата праці персоналу	840	29,1
Оновлення програмного забезпечення	320	11,1
Оренда каналів зв'язку	725	25,0
Загальні експлуатаційні витрати	2890	100,0

Порівняльний аналіз експлуатаційних витрат до та після модернізації мережі зв'язку показує зниження загальних витрат на 18,7%. Основні фактори зниження витрат:

— Зменшення витрат на технічне обслуговування за рахунок використання сучасного надійного обладнання.
— Зниження енергоспоживання завдяки впровадженню енергоефективних технологій.
— Оптимізація трудовитрат на обслуговування за рахунок автоматизації процесів управління мережею.
— Зменшення витрат на оренду каналів зв'язку через використання власної оптоволоконної інфраструктури.

Для оцінки економічної ефективності проекту модернізації мережі зв'язку використано методи дисконтування грошових потоків, які враховують зміну вартості грошей у часі. Розрахунок чистої приведеної вартості (NPV) проекту виконано за формулою:

(3.16)

$$NPV = -Cкап + \Sigma\left(\frac{CFt}{(1 + r)^t}\right)$$

де NPV – чиста приведена вартість проекту, тис. грн;

Скап – початкові капітальні витрати, тис. грн;

CFt – грошовий потік у період t, тис. грн;

r – ставка дисконтування;

t – розрахунковий період, років.

Грошовий потік проекту складається з економії експлуатаційних витрат та додаткових економічних ефектів від впровадження нових технологій. Зокрема, модернізація мережі зв'язку дозволяє зменшити втрати теплової енергії за рахунок оптимізації режимів роботи обладнання, підвищити надійність системи теплопостачання та зменшити час реакції на аварійні ситуації.

Розрахунок грошових потоків та економічних показників проекту на 5-річний період наведено в таблиці 3.11.

Таблиця 3.11 – Розрахунок економічних показників проекту

Показник, тис.грн	**Рік 0**	**Рік 1**	**Рік 2**	**Рік 3**	**Рік 4**	**Рік 5**
Капітальні витрати	-13650	0	0	0	0	0
Економія експлуатаційних витрат	0	665	698	733	770	808
Додатковий економічний ефект	0	3250	3412	3583	3762	3950
Загальний грошовий потік	-13650	3915	4110	4316	4532	4758
Коефіцієнт дисконтування (r = 15%)	1,000	0,870	0,756	0,658	0,572	0,497
Дисконтований грошовий потік	-13650	3406	3107	2840	2592	2365
Накопичений дисконтований грошовий потік	-13650	-10244	-7137	-4297	-1705	+660

Аналіз економічних показників проекту демонструє позитивне значення чистої приведеної вартості (NPV = 660 тис. грн) на п'ятий рік експлуатації, що свідчить про економічну доцільність впровадження запропонованих рішень. Дисконтований термін окупності інвестицій складає 4,72 роки при ставці дисконтування 15%.

Внутрішня норма прибутковості (IRR) проекту, розрахована за умови NPV = 0, становить 17,8%, що перевищує прийняту ставку дисконтування та підтверджує інвестиційну привабливість проекту.

Порівняльний аналіз різних варіантів технічних рішень для модернізації мережі зв'язку виконано на основі показника сукупної вартості володіння (Total Cost of Ownership – TCO), який враховує капітальні та експлуатаційні витрати протягом усього життєвого циклу системи. Результати порівняння представлені в таблиці 3.12.

Таблиця 3.12 – Порівняння варіантів технічних рішень за показником ТСО

Показник	**Варіант 1 (обраний)**	**Варіант 2**	**Варіант 3**
Опис технічного рішення	Ієрархічна архітектура з резервуванням	Плоска архітектура з частковим резервуванням	Хмарна інфраструктура з орендою каналів
Капітальні витрати, тис. грн	13650	10480	7250
Річні експлуатаційні витрати, тис. грн	2890	3460	4870
Термін експлуатації, років	5	5	5
Сукупна вартість володіння (ТСО), тис. грн	28100	27780	31600
Коефіцієнт готовності системи	0,99997	0,9998	0,9995
Пропускна здатність магістралі, Гбіт/с	10	1	5
Можливість масштабування	Висока	Середня	Висока
Рівень захисту інформації	Високий	Середній	Середній

Аналіз даних таблиці 3.12 показує, що обраний варіант технічного рішення (варіант 1) має дещо вищу сукупну вартість володіння порівняно з варіантом 2, але забезпечує значно кращі технічні характеристики: вищий коефіцієнт готовності, більшу пропускну здатність, кращі можливості масштабування та вищий рівень захисту інформації. Варіант 3 (хмарна інфраструктура) має найвищу сукупну вартість володіння та не забезпечує необхідного рівня надійності для об'єктів критичної інфраструктури.

Аналіз чутливості проекту до зміни ключових параметрів показав, що найбільший вплив на економічні показники мають:

1. Вартість обладнання – зміна на ±10% призводить до зміни NPV на ±8,5%.
2. Додатковий економічний ефект – зміна на ±10% призводить до зміни NPV на ±12,3%.
3. Ставка дисконтування – зміна на ±2% призводить до зміни NPV на ±7,8%.

Оцінка ризиків проекту модернізації мережі зв'язку виконана за методом експертних оцінок з використанням матриці «ймовірність-вплив». Основними ризиками проекту є:

1. Затримки поставок обладнання (середня ймовірність, високий вплив).
2. Перевищення бюджету проекту (низька ймовірність, високий вплив).
3. Технічні проблеми при інтеграції нового обладнання з існуючою інфраструктурою (середня ймовірність, середній вплив).
4. Недостатня кваліфікація персоналу для обслуговування нового обладнання (низька ймовірність, середній вплив).

Для зниження впливу ідентифікованих ризиків розроблено план управління ризиками, який передбачає резервування часу та бюджету проекту, поетапне впровадження технічних рішень, тестування сумісності обладнання на стенді перед встановленням на об'єктах та програму навчання персоналу.

Техніко-економічне обґрунтування підтверджує ефективність запропонованих рішень з оптимізації інтегральної цифрової мережі зв'язку ПОКВПТГ «Полтаватеплоенерго». Впровадження сучасних технологій дозволяє не лише підвищити надійність та безпеку системи, але й досягти значного економічного ефекту за рахунок зниження експлуатаційних витрат та оптимізації технологічних процесів.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи бакалавра на тему «Оптимізація інтегральної цифрової мережі зв’язку підприємства критичної інфраструктури» було розглянуто повний цикл удосконалення цифрової інфраструктури на прикладі Полтавського обласного комунального виробничого підприємства теплового господарства «Полтаватеплоенерго». Отримані результати мають як теоретичне, так і прикладне значення для модернізації мереж зв’язку підприємств комунального сектору.

На основі аналізу було встановлено, що існуюча цифрова мережа підприємства має фрагментарну структуру, недостатню стабільність каналів зв’язку, застаріле обладнання, низький рівень захисту даних та відсутність централізованого керування ключовими функціями. Особливо критичним виявилася ситуація із передачею телеметрії, інтеграцією з SCADA-системами, відеоспостереженням та захищеністю службового трафіку.

Для усунення виявлених недоліків у роботі запропоновано нову модель оптимізованої інтегральної цифрової мережі зв’язку, побудовану на принципах ієрархії, масштабованості, резервування, логічної сегментації (VLAN), централізованого моніторингу та використання сучасного промислового обладнання. Запропонована архітектура передбачає три рівні (ядро, агрегація, доступ), підтримує інтеграцію SCADA, IP-відеоспостереження, Wi-Fi мережі, систем зв’язку та телеметрії.

Проведено обґрунтовані розрахунки навантаження, необхідної кількості обладнання, складено орієнтовну кошторисну вартість впровадження. Техніко-економічний аналіз показав, що загальна вартість впровадження складає близько 13,650 млн грн, при цьому проект може окупитися протягом 5 років за рахунок: зменшення витрат на технічне обслуговування; Узагальнюючи результати, можна зробити висновок, що запропоноване рішення є ефективним з точки зору надійності, енергоефективності, безпеки та технологічної адаптивності. Модель мережі може бути легко масштабована, адаптована до інших об’єктів

інфраструктури та стане основою для переходу до цифрового управління технологічними процесами на підприємстві.

Практичне значення роботи полягає у можливості впровадження представленої моделі не лише на ПОКВПТГ «Полтаватеплоенерго», але й на інших аналогічних підприємствах теплоенергетики України. Результати дослідження можуть бути використані як база для розробки типових проектів модернізації цифрових мереж критичної інфраструктури, відповідно до вимог державних стратегій цифрової трансформації.

Список використаних джерел

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» № 80/94-ВР від 05.07.1994р.(в редакції від 20.04.2025р.)
2. Сидоренко В.П. Системи автоматизованого управління технологічними процесами. – Київ: Ліра-К, 2020. – 312 с.
3. ДСТУ 4155:2021. Інформаційні технології. Захист інформації. Терміни та визначення.
4. ДСТУ ISO/IEC 27005:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Настанова керування ризиками інформаційної безпеки (ISO/IEC 27005:2022, IDT).
5. Розпорядження Кабінет Міністрів України від 31 грудня 2024 р. № 1351-р «Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках».
6. Голь В.Д., Ірха М.С. Телекомунікаційні та інформаційні мережі: навчальний посібник. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 250 с.
7. Гришко С.О. Основи проектування ІТ-інфраструктур. — Х.: ХНУРЕ, 2022
8. Касаткін А.С. Комп’ютерні мережі. — К.: Вид. дім «Слово», 2021.
9. Суслов В.П. Цифрові комунікації та мережі. - Харків: ХНУРЕ, 2018- 276 с.
10. Cisco Systems. Cisco Networking Academy: Introduction to Networks. – Cisco Press, 2020.
11. SCADA systems in municipal infrastructure – IEEE Review 2021.
12. Ignition SCADA by Inductive Automation. Доступно за адресою: https://inductiveautomation.com/
13. OpenVPN Documentation. Доступно за адресою: https://openvpn.net
14. Ubiquiti Network Design Guide. Доступно за адресою: https://ui.com/download
15. IEEE 802.1Q. Virtual LANs (VLANs) Standard.
16. Збірник наукових праць «Системи управління, навігації та зв’язку». Полтавська політехніка імені Юрія Кондратюка.
17. Офіційний сайт ПОКВПТГ «ПОЛТАВАТЕПЛОЕНЕРГО»: te.pl.ua

ДОДАТКИ

Додаток А

1. OVERVIEW OF EXISTING TECHNOLOGIES AND THE STATE OF COMMUNICATION NETWORKS

1.1 Modern Digital Communication Technologies

Digital communication networks form the foundation of modern systems for control, monitoring, and data transmission. The core technologies of digital communication include IP telephony, Ethernet, MPLS, VPN, SCADA, IoT technologies, as well as wireless data transmission technologies such as Wi-Fi, LTE, and LoRaWAN.

One of the key directions is the implementation of the Industrial Internet of Things (IIoT), which enables the integration of thousands of devices into a single network with automated data exchange. Software-Defined Networking (SDN) and Network Function Virtualization (NFV) architectures are also actively evolving, providing flexible network management and scalability.

An Integrated Digital Communication Network (IDCN) represents a comprehensive technological solution that unifies various data, voice, and video transmission channels into a single information system using digital technologies. The concept of integrated networks emerged in response to the need for enterprises to consolidate communication resources and optimize information flows.

At the current stage of telecommunications development, IDCNs have become multifunctional telecommunications systems that support the transmission, processing, and storage of different types of information (data, voice, video) based on unified standards and protocols, using a shared infrastructure and centralized management systems. A key feature of IDCNs is the integration of various services and applications within a unified environment, with the ability to configure and scale them flexibly.

For critical infrastructure enterprises, IDCNs are of particular importance, ensuring the continuity of operational processes, high reliability of critical data transmission, and resilience to external disruptions. In this context, an IDCN can be viewed as a strategic component of the enterprise's information infrastructure, ensuring

timely and reliable data exchange for decision-making and the functioning of automated process control systems.

The evolution of the IDCN concept has progressed from basic Integrated Services Digital Networks (ISDN) to modern Next-Generation Networks (NGN), which are based on IP technologies and provide a wide range of telecommunications services. The adoption of SDN and NFV concepts has opened new possibilities for flexible resource management and adaptation of IDCNs to the dynamic operational conditions of critical infrastructure enterprises.

Key characteristics of IDCNs include:

- Multiservice support (simultaneous handling of voice, video, and data services);
- Modularity and scalability;
- Support for QoS (Quality of Service) and SLA (Service Level Agreement);
- Use of a unified platform for all types of communication (IP-based network);
- Centralized management and monitoring.

Modern IDCNs are based on packet-switching technologies (such as IP/MPLS), which enable efficient utilization of communication channels, reduced latency, and enhanced system fault tolerance.

Depending on the design principles, topology, functionality, and scale, digital network architectures can be classified into the following main types:

1) By topology:

Topology Description

Bus All devices are connected to a single communication line. Easy to implement, but has low scalability.

Star All devices are connected to a central switch or hub. Common in LANs.

Ring Data is transmitted in a circular path from one node to the next. Ensures orderly transmission, but is sensitive to breaks.

Tree An extension of the star topology that builds a hierarchical structure. Suitable for large networks.

Mesh Each node is connected to all other nodes. Offers high reliability and fault tolerance but is expensive to implement.

Hybrid A combination of several topologies, providing an optimal balance of cost, reliability, and performance.

2) By functional purpose:

Client-server – A centralized model where servers handle client requests. Easy to administer and scales well.

Peer-to-peer (P2P) – All nodes are equal and can function both as clients and servers. Inexpensive to deploy but difficult to manage without centralization.

Cloud-based – Uses remote data center resources. Scalable and flexible, but dependent on internet connectivity.

3) By integration level and infrastructure scope:

LAN (Local Area Network) – Limited to a specific area (e.g., building, office). High speed and low latency.

MAN (Metropolitan Area Network) – Covers urban areas; suitable for organizations with multiple branches within a city.

WAN (Wide Area Network) – Connects geographically dispersed sites or countries, often using provider-managed links.

SDN (Software-Defined Networking) – Separates control from physical devices; offers flexible management and scalability.

IoT Networks – Designed for connecting large numbers of resource-constrained devices (sensors, controllers, etc.).

4) By interaction model:

OSI Model – A theoretical 7-layer model describing how data flows through a network (physical, data link, network layers, etc.).

TCP/IP Model – A practical implementation forming the basis of the modern Internet (network, transport, application layers).

Therefore, selecting the appropriate digital network architecture ensures the efficiency, reliability, and scalability of the enterprise's information infrastructure, in accordance with its technical, economic, and functional requirements.

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
"ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА"

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

«Оптимізація інтегральної цифрової мережі зв'язку підприємства критичної інфраструктури»

Виконав: студент 4 курсу, групи 401ТТ
Дубина В.С.

Керівник: д.т.н., професор
Косенко В.В.

Полтава – 2025 рік

Актуальність теми:

Необхідність підвищення надійності, відмовостійкості та ефективності роботи підприємства критичної інфраструктури шляхом впровадження сучасних технологій цифрового зв'язку в умовах збройної агресії російської федерації проти України.

Мета роботи:

Розробка заходів з оптимізації інтегральної цифрової мережі з метою підвищення ефективності, надійності та безпеки інформаційно-комунікаційної інфраструктури.

Для досягнення поставленої мети передбачено вирішення наступних завдань:

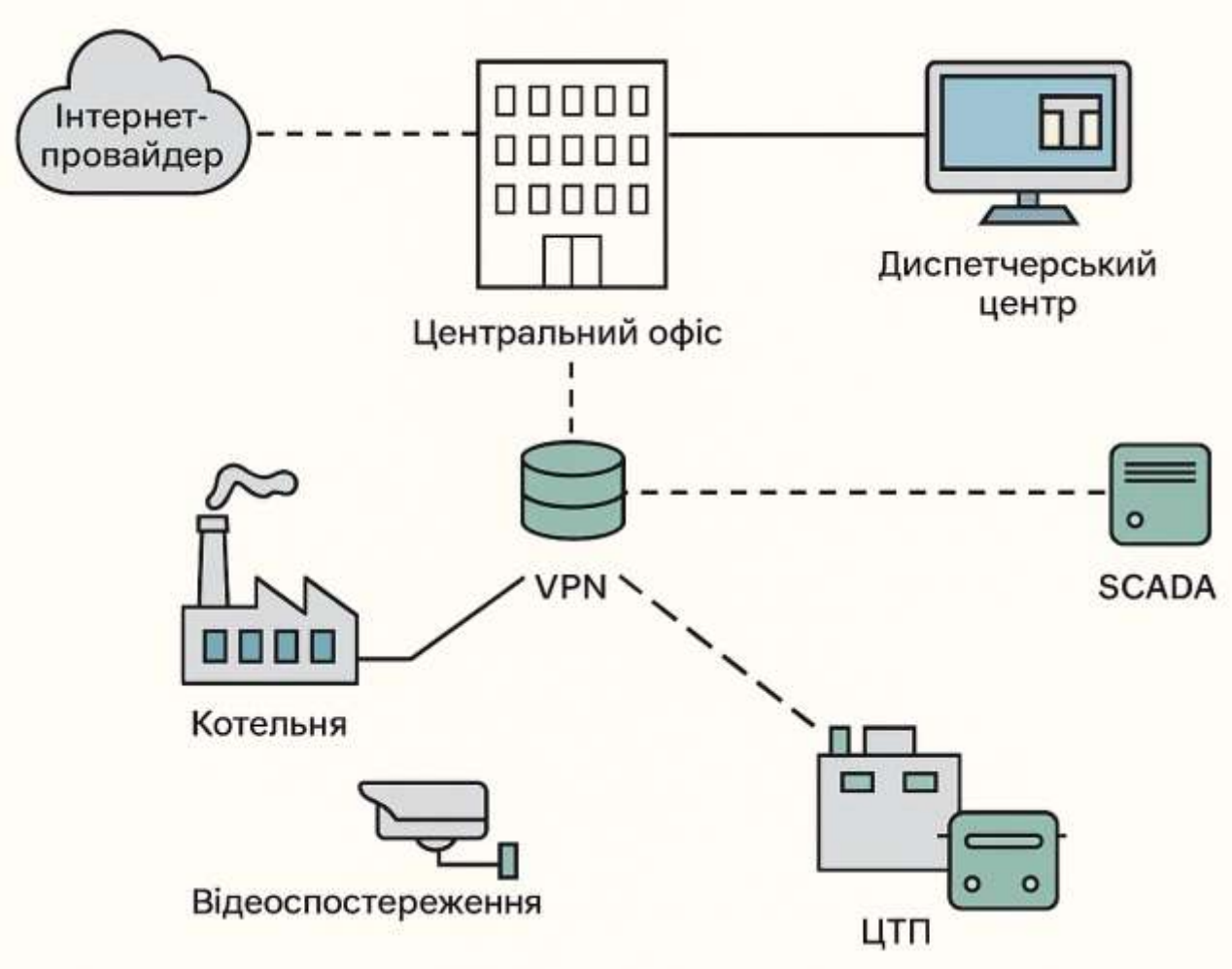
1. аналіз існуючої цифрової мережі зв'язку підприємства;
2. виявлення технічних та організаційних недоліків у її функціонуванні;
3. розробка технічних рішень для оптимізації мережевої інфраструктури;
4. моделювання і порівняння різних варіантів оптимізації;
5. техніко-економічне обґрунтування запропонованих змін.

- ***Об'єкт дослідження*** – процеси передачі та обробки інформації в інтегральній цифровій мережі зв'язку підприємства критичної інфраструктури на прикладі Полтавського обласного комунального виробничого підприємства теплового господарства «Полтаватеплоенерго»

- ***Методи дослідження***

- системний аналіз для вивчення структури та функціонування цифрової мережі зв'язку підприємства;
- порівняльний аналіз для оцінки різних технологічних рішень;
- математичне моделювання для розрахунку параметрів мережі;
- методи теорії надійності для оцінки відмовостійкості системи;
- методи захисту інформації для забезпечення кібербезпеки;
- методи техніко-економічного аналізу для обґрунтування запропонованих рішень

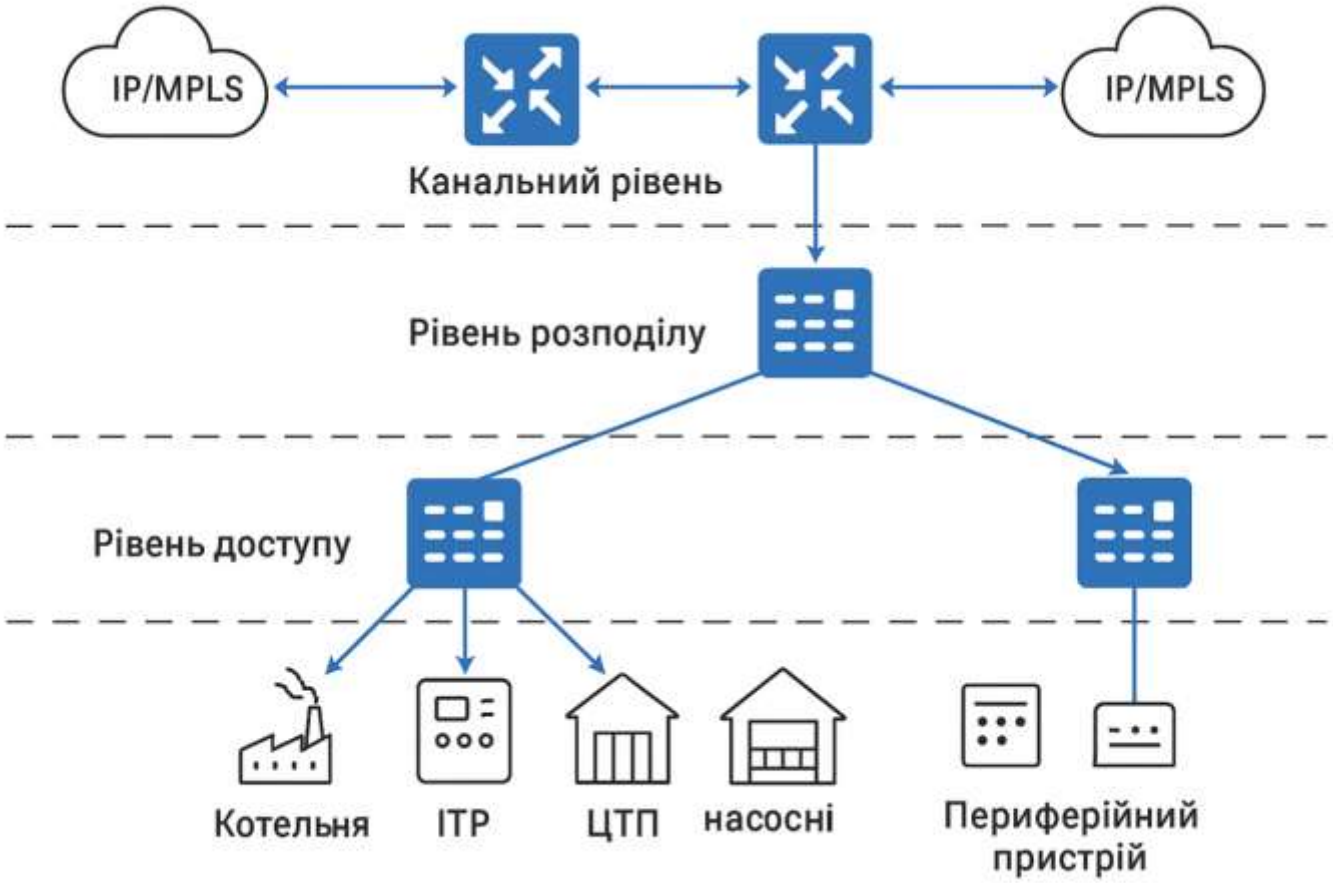
Аналіз існуючого стану мережі зв'язку



Виявлені недоліки

- *відсутність єдиної архітектури мережі*
- *недостатнє резервування каналів*
- *низький рівень кіберзахисту*
- *неповна інтеграція SCADA-систем*
- *немає централізованого моніторингу відеоспостереження*
- *технічні обмеження старого обладнання*

Запропонована архітектура мережі



Ієрархічна багаторівнева архітектура IP-мережі з розподілом функцій на три основні рівні: канальний, розподільчий та периферійний (доступу)

Оцінка надійності запропонованої моделі

Ймовірність **працездатності** системи при відмові окремих компонентів, розрахована за формулою:

$$Kc = 1 - \prod(1 - Ri)$$

склала 99,9%, що еквівалентно допустимому часу простою не більше 8,76 годин на рік

Час відновлення зв'язку при використанні протоколу резервування VRRP розрахований за формулою:

$$Tв = n \times Tа + Tп$$

склав 3,3 секунди

Рівень захищеності системи, розрахований за формулою:

$$S = \frac{Wm \times Mc + Wn \times Nc + Wa \times Ac}{Wm + Wn + Wa}$$

становить 0,893

Розрахунок навантаження на мережу зв'язку за категоріями мережевого трафіку

Розрахунок добового обсягу SCADA-трафіку, виконаний за формулою

$$Vscada = Ntag \times Fs \times Ss \times 3600 \times 24$$

Тип об'єкта	Кількість тегів	Частота опитування, разів/с	Розмір тегу, байт	Добовий обсяг, Мбайт/доба
Котельня	120	0,1	12	12,44
ЦТП	50	0,1	12	5,18
ІТП	20	0,05	12	1,04

Розрахунок трафіку відеоспостереження за формулою:

$$Vvideo = Ncam \times Br \times 3600 \times 24 \times k$$

Тип об'єкта	Кількість камер	Роздільна здатність	Бітрейт, Мбіт/с	Добовий обсяг, Гбайт/доба
Котельня	4	1920×1080	2	8,64
ЦТП	2	1280×720	1	2,16
ІТП	1	640×480	0,5	0,54

Розрахунок трафіку IP-телефонії, виконаний за формулою:

$$Vvoip = Ncall \times Br \times Tcall \times k$$

Тип з'єднання	Кількість об'єктів	Сумарний трафік, Мбіт/с	Коефіцієнт запасу	Необхідна пропускна здатність, Мбіт/с
Магістральний	1	850	1,3	1105
Районний вузол	5	180	1,2	216
Котельня	90	8	1,5	12
ЦТП	28	5	1,5	7,5
ІТП	250	1	2,0	2

Техніко-економічне обґрунтування

Капітальні витрати на модернізацію мережі зв'язку

Категорія витрат	Вартість, тис. грн	Частка у загальних витратах, %
Мережеве обладнання	5840	42,8
Серверне обладнання	1720	12,6
Системи безперебійного живлення	980	7,2
Кабельна інфраструктура	1450	10,6
Програмне забезпечення	2105	15,4
Монтажні та пусконалагоджувальні роботи	1180	8,6
Проектні роботи	240	1,8
Навчання персоналу	135	1,0
Загальні капітальні витрати	13650	100,0

Вартість обладнання визначена на основі комерційних пропозицій від провідних постачальників мережевого обладнання з урахуванням обсягів закупівлі та можливих знижок

Очікуваний ефект

- Термін окупності інвестицій - 4,72 роки
- Чиста приведена вартість (NPV = 660 тис. грн) - на 5-й рік експлуатації
- Зниження загальних витрат на технічне мережі на 18,7%
- Централізоване управління: єдиний центр моніторингу та диспетчеризації
- Надійність і резервування: підвищена відмовостійкість мережі
- Кіберзахист: захист даних і каналів зв’язку
- Економічна вигода: зниження витрат, швидка окупність

Запропоноване рішення є ефективним з точки зору надійності, енергоефективності, безпеки та технологічної адаптивності

Висновки

✓ **Оптимізація мереж зв'язку** — виконано модернізацію за сучасними стандартами

✓ **Надійність та безпека** — підвищено стабільність передачі даних для критичних об'єктів

✓ **Енергоефективність** — впроваджено енергоощадні рішення та сучасне обладнання

✓ **Економічний ефект** — розраховано скорочення витрат та термін окупності проєкту

✓ **Цифрова трансформація** — підприємство адаптоване до вимог цифрової економіки

✓ **Адаптивність** — розроблена модель мережі може бути легко масштабована та адаптована до інших об’єктів критичної інфраструктури

ДЯКУЮ ЗА УВАГУ!

Додаток В

Порівняльна таблиця основних протоколів зв’язку, які можуть бути використані в цифровій мережі підприємства критичної інфраструктури

Протокол	Затримка	Надійність	Швидкість передавання	Сумісність з пристроями	Призначення
Modbus RTU	Низька (1–10 мс)	Висока	До 115,2 кбіт/с	Широка (промислова автоматика)	Обмін даними з контролерами
Modbus TCP	Низька–середня	Висока	До 100 Мбіт/с	Широка (Ethernet-пристрої)	Віддалений доступ, SCADA
MQTT	Дуже низька	Висока (QoS 0–2)	До 1 Мбіт/с (залежить від мережі)	Дуже широка (IoT, PLC, сенсори)	Телеметрія, передавання подій
HTTP/HTTPS	Середня	Висока (HTTPS)	До 100 Мбіт/с	Дуже широка	Інтерфейси, REST API, web-доступ
SNMP	Низька	Середня	До 100 Мбіт/с	Широка (мережеве обладнання)	Моніторинг та керування
LoRaWAN	Висока (до 5 с)	Середня	~50 кбіт/с	Специфічна для IoT	Дальні бездротові з’єднання
ZigBee	Середня	Середня–висока	До 250 кбіт/с	Обмежена (сенсори, IoT)	Локальні бездротові мережі
IP/MPLS	Дуже низька	Дуже висока	Гігабітні/терабітні швидкості	Професійне обладнання	Транспорт даних на рівні оператора
TLS/IPsec	Низька–середня	Дуже висока (шифрування)	~залежить від базового протоколу	Широка	Захист каналів, VPN

Додаток Г

Порівняльна характеристика обладнання для оптимізації мережі

Компонент	Модель/Тип	Пропускна здатність	Інтерфейси	Підтримка PoE	Надійність/Резервування	Споживання енергії	Розміри (мм)	Температура експл.	Призначення
Маршрутизатор ядра	MikroTik CCR2116-12G-4S+	До 10 Гбіт/с	13×10G SFP+, 1×1G RJ45	Ні	Висока (dual PSU)	до 70 Вт	443×199×44	0…+40 °C	Централізована маршрутизація
Комутатор PoE	TP-Link JetStream L2+/L3	1–10 Гбіт/с	24×1G PoE, 4×SFP	Так	Середня	до 250 Вт (PoE сумарно)	440×220×44	0…+50 °C	Передача даних, живлення пристроїв
VPN-шлюз	MikroTik hEX RB750Gr3	До 1 Гбіт/с	5×RJ45, OpenVPN/IPsec	Ні	Середня	до 5 Вт	113×89×28	-20…+60 °C	Безпечне з’єднання
VPN-шлюз	pfSense appliance (i3)	До 2 Гбіт/с	6×2.5G RJ45	Ні	Середня	≈25 Вт	180×150×45	0…+50 °C	Захищене VPN-з'єднання
SCADA-сервер (VPS)	Ubuntu VPS/Ignition	Залежно від тарифу	Вірт. адаптер + VPN	Ні	Висока (Cloud DC)	– (на балансі)	–	–	Централізоване управління
SCADA-сервер (HW)	Промисловий сервер i5–i7	До 10 Гбіт/с	2×RJ45, USB, VGA/HDMI	Ні	Висока (RAID)	90–120 Вт	482×450×89	0…+40 °C	Місцева SCADA/архіви
Відеосервер NVR	Hikvision DS-7732NXI	До 320 Мбіт/с	2×RJ45, HDMI, 32×IP канали	Ні	Середня–висока	30–50 Вт	445×400×71	-10…+55 °C	Запис відео
Wi-Fi точка	Ubiquiti UniFi 6 LR	До 1.5 Гбіт/с	1×RJ45 (PoE)	Так	Середня	до 16.5 Вт	Ø220×48	-30…+60 °C	Доступ Wi-Fi для персоналу

Примітки:

- **Споживання енергії** вказано максимально можливе, важливо для проєктування системи живлення.
- **Габарити** — критично для монтажу у стійки або шафи.
- **Температурний діапазон** — визначає умови, в яких обладнання може експлуатуватись без деградації.
- **PoE (Power over Ethernet)** — живлення пристроїв по Ethernet-кабелю, важливо для відеокамер, Wi-Fi, контролерів.

Додаток Д

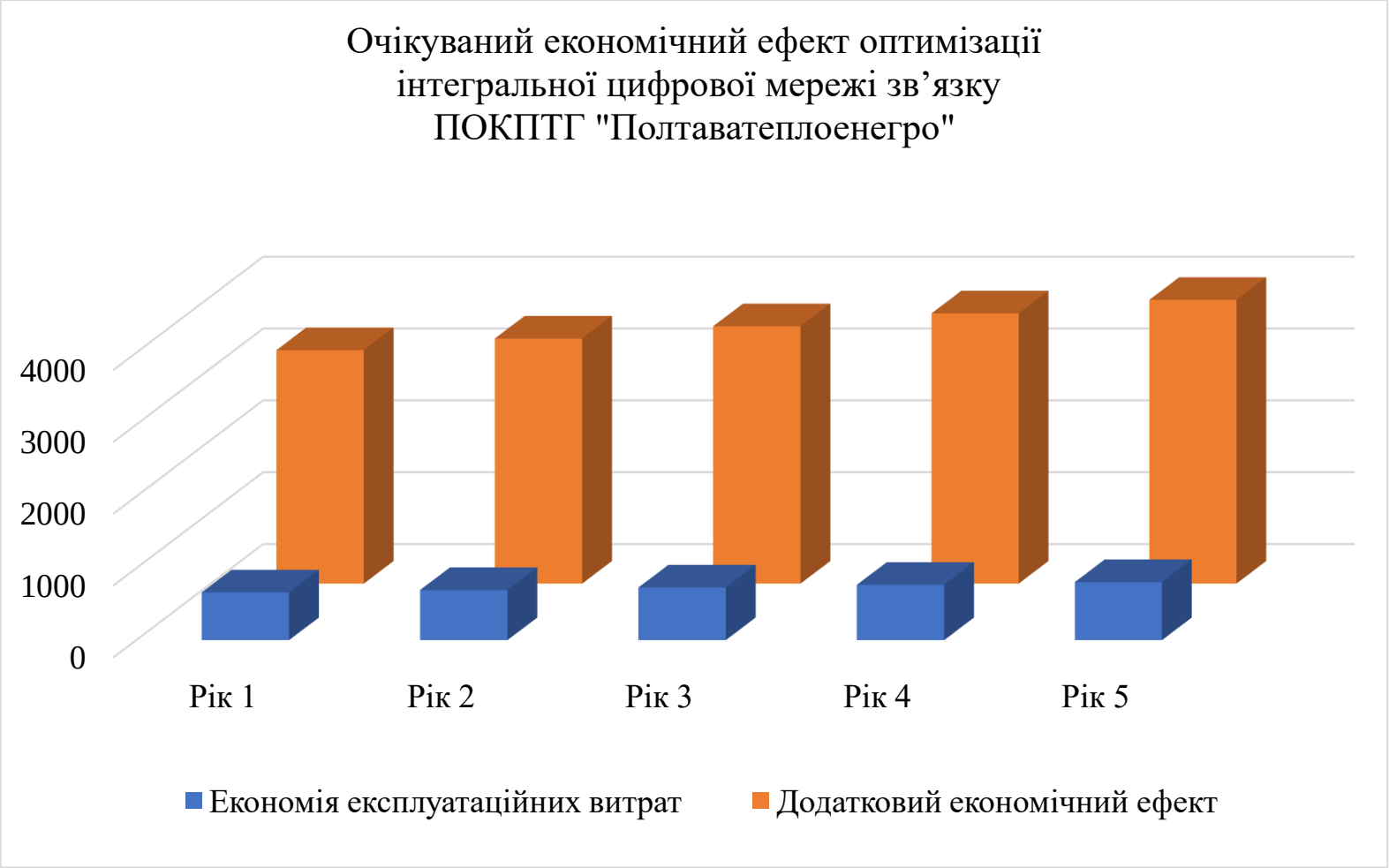
Джерела цін на обладнання

№	Компонент	Модель/Тип	Ціна, грн	Джерело
1	**Маршрутизатор ядра**	MikroTik CCR2116-12G-4S+	36 386–39 900	e-Katalog, PowerUp.ua
2	**VPN-шлюз**	MikroTik hEX RB750Gr3	2 234–2 659	e-Katalog
3	**VPN-шлюз**	pfSense Appliance (Intel i3–i7)	≈16 000 грн	Moginsok.com
4	**SCADA-сервер**	Ubuntu VPS (Vikhost)	від $5.99/міс.	Vikhost.com
5	**SCADA-сервер**	Ubuntu VPS (UltaHost)	від $5/міс.	UltaHost.com
6	**SCADA-сервер**	Ignition SCADA (ліцензія)	від $3 018	Inductive Automation
7	**SCADA-сервер**	WinCC Runtime Professional	≈$1 500	Siemens Ukraine
8	**Відеосервер NVR**	Hikvision DS-7732NXI-K4(D)	19 436	Elvis.com.ua
9	**Відеосервер NVR**	Dahua DH-NVR7232	20 636	e-Katalog
10	**Wi-Fi точка**	Ubiquiti UniFi 6 LR (U6-LR)	8 659–11 461	e-Katalog
11	**Wi-Fi точка**	MikroTik hAP ax³	7 399	PowerUp.ua

Примітки:

1. **Ціни** вказані в гривнях та є орієнтовними; вони можуть змінюватися залежно від постачальника та курсу валют.
2. **SCADA-сервери** можуть бути реалізовані як на віртуальних платформах (VPS), так і на фізичних серверах, залежно від вимог до продуктивності та надійності.
3. **Ліцензії SCADA-систем** (Ignition, WinCC) мають різні варіанти залежно від кількості тегів, користувачів та функціональних модулів; зазначені ціни є базовими.

Додаток Е


Очікуваний економічний ефект оптимізації
інтегральної цифрової мережі зв'язку
ПОКПТГ "Полтаватеплоенегро"
4000
3000
2000
1000
0
Рік 1
Рік 2
Рік 3
Рік 4
Рік 5
Економія експлуатаційних витрат
Додатковий економічний ефект