Міністерство освіти і науки України

Луцький національний технічний університет

(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій

(повне найменування факультету)

Кафедра комп'ютерної інженерії та безпеки

(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «МАГІСТР»

ДОСЛІДЖЕННЯ ШЛЯХІВ РЕІНЖИНІРИНГУ СЕРВЕРНОЇ КІМНАТИ ДЛЯ ПОКРАЩЕННЯ ЕФЕКТИВНОСТІ ФУНКЦІОНУВАННЯ ІТ-ІНФРАСТРУКТУРИ

RESERCH ON WAYS TO RE-INGINEER THE SERVER ROOM TO IMPROVE THE EFFICIENCY OF THE FUNCTIONING OF THE IT INFRASTRUCTURE

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

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІм-21
Лакодей Олександр Леонідович

(підпис)

Керівник:
к.т.н., доцент
Терлецький Тарас Володимирович

(підпис)

Кваліфікаційну роботу
допущено до захисту
«_____» грудня 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Гринюк Сергій Васильович

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

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

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ доц. Т.ТЕРЛЕЦЬКИЙ
« _____ » _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Лакодею Олександру Леонідовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Дослідження шляхів реінжинірингу серверної кімнати для покращення ефективності функціонування IT-інфраструктури

Керівник роботи к.т.н., доцент Терлецький Тарас Володимирович

затверджені наказом закладу вищої освіти від «17» червня 2025 року № 290/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 9.12.2025р.

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

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Огляд сучасного стану IT-інфраструктури та проблеми функціонування
Аналіз поточного стану серверної кімнати об'єкта дослідження
Розробка та впровадження рішень для реінжинірингу серверної кімнати
Пілотне тестування рішень, аналіз показників
Висновки

5. Перелік графічного (ілюстративного) матеріалу:
Структура IT-інфраструктури
Візуалізація серверної кімнати
Фото серверної кімнати та обладнання
Схема підключення обладнання
Блок-схема поетапності виконання робіт

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз предметної області	Терлецький Т. В., доцент		
Аналіз поточного стану серверних кімнат та ІТ-інфраструктури	Терлецький Т. В., доцент		
Практична реалізація реінжинірингу серверної кімнати	Терлецький Т. В., доцент		
Нормоконтроль	Багнюк Н.В., доцент		
Гарант ОП	Гринюк С.В., доцент		
Показник запозичень тексту	___%		
Академічна доброчесність	Міскевич О.І., ст.викладач		

7. Дата видачі завдання 18.06.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Огляд літератури із досліджуваної проблеми	До 01.08.2025 р.	
2.	Аналіз проблеми за темою роботи та постановка завдань дослідження. Аналіз проблеми за темою роботи та постановка завдань дослідження	До 20.08.2025 р.	
3.	Теоретичне дослідження та практична реалізація	До 25.09.2025 р.	
4.	Практична реалізація об’єкта проектування	До 20.10.2025 р.	
5.	Висновки та пропозиції	До 25.10.2025 р	
6.	Формування списку використаних джерел	До 27.10.2025 р.	
7.	Формування додатків	До 30.10.2025 р.	
8.	Оформлення ілюстративного матеріалу	До 05.11.2025 р.	
9.	Представлення остаточного варіанту кваліфікаційної роботи керівникові	До 11.11.2025 р.	
10.	Нормоконтроль	До 29.11.2025 р.	
11.	Інструментальна перевірка на академічний плагіат	До 02.12.2025 р.	
12.	Здача кваліфікаційної роботи та всіх супровідних документів на кафедру	До 09.12.2025 р.	

Здобувач вищої освіти _____ Лакодей О.Л.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Терлецький Т.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Лакодей О. Л. Дослідження шляхів реінжинірингу серверної кімнати для покращення ефективності функціонування ІТ-інфраструктури. Рукопис.

Кваліфікаційна робота магістра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

Перший розділ присвячено огляду сучасного стану ІТ-інфраструктури та проблем функціонування. Розглянуто роль серверних кімнат у забезпеченні працездатності систем, виділено типові недоліки та проблеми фізичної інфраструктури та сучасні підходи до модернізації серверних приміщень.

В другому розділі здійснено аналіз поточного стану серверної кімнати об'єкта дослідження, проведення аудиту та виявлення вузьких місць та проблем функціонування, оцінку ефективності поточного обладнання.

Третій розділ присвячено опису обгрунтування вибору обладнання, модернізацію фізичного рівня та схемі розробки оптимального мережевого підключення, вибір та налаштування систем автоматизації управління ІТ-інфраструктурою та методикам оцінювання ефективності впроваджених рішень. Описано пілотне тестування рішень, аналіз показників до та після модернізації, оцінка потенціалу масштабування та економічну доцільність впровадження рішень.

Ключові слова: реінжиніринг, ІТ-інфраструктура, серверна кімната, мережева архітектура, продуктивність, відмовостійкість, віртуалізація, автоматизація.

ANNOTATION

Lakodey O. Research on ways to reengineer a server room to improve the efficiency of IT infrastructure. Manuscript.

Qualification work for the master's degree in Computer Engineering, specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three chapters, conclusions, a list of sources used, and appendices.

The first section is devoted to a review of the current state of IT infrastructure and problems of functioning. The role of server rooms in ensuring the operability of systems is considered, typical shortcomings and problems of physical infrastructure and modern approaches to the modernization of server rooms are highlighted.

The second section analyzes the current state of the server room of the research object, conducts an audit and identifies bottlenecks and problems of functioning, and assesses the effectiveness of current equipment.

The third section is devoted to the description of the justification for the choice of equipment, modernization of the physical layer and the scheme for developing optimal network connectivity, selection and configuration of IT infrastructure management automation systems and methods for assessing the effectiveness of implemented solutions. Pilot testing of solutions, analysis of indicators before and after modernization, assessment of scaling potential and economic feasibility of implementing solutions are described.

Keywords: reengineering, IT infrastructure, server room, network architecture, performance, fault tolerance, virtualization, automation.

ЗМІСТ

ВСТУП

Актуальність теми. В умовах стрімкого розвитку цифрових технологій сучасні підприємства дедалі більше залежать від ефективного функціонування своєї IT-інфраструктури. Серверна кімната, як її центральний вузол, відіграє вирішальну роль у стабільності та продуктивності всіх бізнес-процесів. Однак зростання обсягів даних та вимог до відмовостійкості створюють нові виклики. Використання фізично та морально застарілого обладнання призводить до зниження продуктивності, ускладнення масштабування, неефективного використання енергоресурсів та збільшення експлуатаційних витрат. За даними Gartner, до 2025 року понад 80 % підприємств потребуватимуть модернізації інфраструктури для забезпечення стійкості. За таких умов реінжиніринг серверної кімнати стає не просто бажаним, а необхідним кроком для підтримки конкурентоспроможності та подальшого розвитку бізнесу.

Метою роботи є розробка комплексного підходу до реінжинірингу серверної кімнати, спрямованого на покращення ефективності функціонування IT-інфраструктури підприємства шляхом модернізації фізичного рівня, інтеграції сучасних технологій автоматизації та віртуалізації.

Об’єкт дослідження – IT-інфраструктура підприємства.

Предмет дослідження – методи та засоби реінжинірингу серверної кімнати, спрямовані на покращення її продуктивності, надійності та економічної ефективності.

Завдання, які необхідно виконати для досягнення мети:

– дослідити проблеми та «вузькі місця» існуючої IT-інфраструктури на основі проведеного аудиту;

– спроектувати комплексну модель реінжинірингу, що охоплює фізичний, апаратний та програмний рівні;

– розробити модель автоматизації управління інфраструктурою на основі парадигми «Інфраструктура як Код» (IaC);

– запропонувати методику для кількісної оцінки технічної та економічної ефективності впроваджених рішень;

– реалізувати пілотне тестування розроблених рішень для практичної валідації моделі;

– візуалізувати результати порівняльного аналізу ключових показників ефективності до і після модернізації.

Апробація результатів дослідження. Основні теоретичні положення та практичні результати кваліфікаційної роботи були представлені на Міжнародній ноуково-практичній конференції «Наука, освіта і суспільство в умовах змін: виклики та інновації», яка проводилась 10 жовтня 2025 р., м. Кременчук [1]. Крім того, запропонована модель реінжинірингу серверної кімнати наразі проходить тестування в реальних умовах на підприємстві СП ТОВ «Модерн-Експо», що підтверджено відповідним актом впровадження. Після успішного завершення пілотного проєкту очікується повна інтеграція розробленого рішення в ІТ-інфраструктуру підприємства.

РОЗДІЛ 1
ОГЛЯД СУЧАСНОГО СТАНУ ІТ-ІНФРАСТРУКТУРИ ТА ПРОБЛЕМИ ФУНКЦІОНУВАННЯ

1.1 Структура ІТ-інфраструктури підприємства

ІТ-інфраструктура підприємства являє собою складний багатошаровий комплекс взаємопов’язаних апаратних, програмних та мережевих компонентів, які забезпечують функціонування інформаційних систем, підтримку бізнес-процесів та досягнення стратегічних цілей організації. Її структура може варіюватися залежно від розміру підприємства, галузевої специфіки, рівня автоматизації та стратегічних пріоритетів, проте існують загальні ключові елементи та рівні, які можна виділити. Проста ІТ-інфраструктура зображена на рисунку 1.1

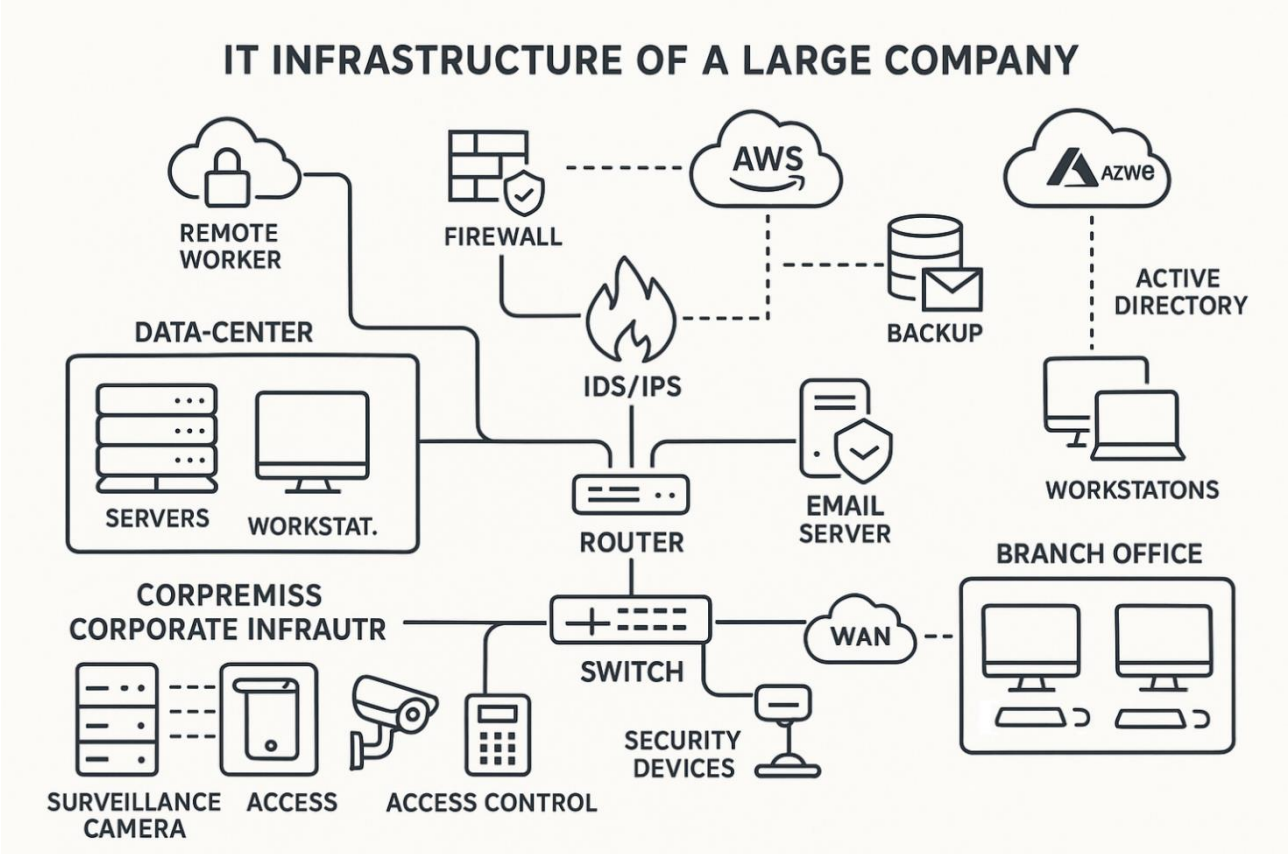

Рисунок 1.1 – Структура ІТ-інфраструктури

На фізичному рівні IT-інфраструктури включає все фізичне обладнання, необхідне для обробки, зберігання та передачі даних. До цього рівня належать:

– серверне обладнання: фізичні сервери (bare metal), які відповідають за обчислювальні потужності підприємства та забезпечують роботу різноманітних сервісів та додатків, різного призначення (файлові сервери, сервери баз даних, веб-сервери, сервери додатків, поштові сервери, сервери віртуалізації тощо), сервери зберігання даних (NAS, SAN, DAS), стрічкові бібліотеки для резервного копіювання та інше спеціалізоване обладнання;

– мережеве обладнання: фізичне обладнання, яке забезпечує зв’язок між компонентами IT-інфраструктури та зовнішнім світом. До нього належать комутатори (switches), маршрутизатори (routers), міжмережеві екрани (firewalls), системи виявлення та запобігання вторгненням (IDS/IPS), точки бездротового доступу (access points), балансувальники навантаження (load balancers), та інше обладнання, що забезпечує передачу даних, сегментацію мережі та безпеку;

– робочі станції та кінцеві пристрої користувачів: ноутбуки, персональні комп’ютери, планшети, смартфони та інші пристрої, які використовуються працівника для виконання своїх функціональних обов’язків та доступу до інформаційних систем;

– кабельна інфраструктура: фізичні кабелі (мідні, оптоволоконні) та роз’єми, що забезпечують з’єднання між усіма апаратними компонентами мережі та серверного обладнання. Сюди також належать патч-панелі та інші елементи організації кабельної системи;

– інфраструктура серверної кімнати (дата-центру): спеціально обладнане приміщення, де розміщується серверне та мережеве обладнання. Для повноцінної роботи дані кімнати обладнані системи електроживлення (резервні джерела, ДБЖ), охолодження (кондиціонери, системи вентиляції), пожежогасіння, контролю доступу та моніторингу.

На логічному рівні IT-інфраструктура охоплює програмне забезпечення та сервіси, які забезпечують функціонування фізичних компонентів та надають

необхідні можливості для роботи користувачів та бізнес-додатків. До цього рівня належать:

– операційні системи (ОС): системне програмне забезпечення, яке керує апаратними ресурсами серверів та робочих станцій. Прикладами таких операційні системи Windows для робочих станцій з різноманіттю версій та Windows Server, для управління серверною частиною. Unix подібні системи, з безліччю рішень для роботи, як кінцевого користувача, так і серверних рішень, macOS та інші;

– системи управління базами даних (СУБД): програмне забезпечення для створення, підтримки та управління базами даних, де зберігаються критично важлива інформація для бізнесу (MySQL, PostgreSQL, Oracle, Firebird, Microsoft SQL Server та ін.);

– мережеві сервіси: служби, що забезпечують функціонування мережі, такі як система доменних імен (DNS), протокол динамічної конфігурації хоста (DHCP), служби каталогів (Active Directory, LDAP), служби авторизації та автентифікації;

– засоби забезпечення інформаційної безпеки: програмні та апаратні рішення, спрямовані на захист IT-інфраструктури та даних від несанкціонованого доступу, шкідливого програмного забезпечення, кібератак та інших загроз. Сюди входять антивірусне програмне забезпечення, міжмережеві екрани (як програмні, так і апаратні рішення), системи виявлення та запобігання вторгненням, засоби шифрування, системи управління ідентифікацією та доступом (AIM);

– системи віртуалізації: технології, що дозволяють запускати декілька віртуальних машин та одному фізичному сервері, що дозволяє оптимізувати використання апаратних ресурсів та підвищувати гнучкість інфраструктури (ESXi, VMware, Proxmox, Hyper-V, Citrix та ін.);

– системи контейнеризації: технології для упаковки додатків та їх залежностей у легкі та портативні контейнери, що спрощує розгортання та управління додатками (Docker, Kubernetes та ін.);

– системи резервного копіювання та відновлення інформації: процеси та програмне забезпечення, для створення резервних копій важливих даних та забезпечення їх швидкого відновлення у випадку збоїв або втрати (Veeam Backup & Replication, Acronis Cyber Protect та ін.);

– системи моніторингу та управління: інструменти, що дозволяють здійснювати центральний моніторинг стану усіх компонентів IT-інфраструктури, виявляти проблеми на ранніх стадіях, керуванням ресурсами (Zabbix, PRTG Network Monitor, Nagios, Netbox, Ansible, Terraform та ін.).

Окрім фізичного та логічного рівнів, дуже важливу роль відіграють людські ресурси для підтримки IT-інфраструктури. Кваліфіковані фахівці, які відповідають за проектування, впровадження, підтримку та розвиток усіх компонентів інфраструктури, знання та досвід яких є критично важливим для забезпечення ефективної, безпечної та безперебійної роботи IT-системи.

Таким чином, структура IT-інфраструктури підприємства є складною екосистемою, що включає різноманітні апаратні засоби, програмне забезпечення, мережеві технології та кваліфікований персонал, які взаємодіють між собою для забезпечення інформаційних потреб організації та підтримки бізнес-процесів. Розуміння цієї структури є ключовим для ефективного управління IT-інфраструктурою, виявлення проблемних зон та планування модернізації, зокрема реінжинірингу серверної кімнати.

1.2 Роль серверної кімнати у забезпеченні працездатності систем

Серверна кімната, часто також названа машинним залом або міні-дата-центр є критично важливою складовою IT-інфраструктури. Візуалізацію серверної кімнати досить добре відображено на рисунку 1.2 [2]. Вона виконує функцію централізованого вузла, в якому фізично розміщені ключові апаратні та інженерні компоненти, що забезпечують стабільне функціонування цифрового середовища компанії. Від її належного проектування, оснащення, організації внутрішніх процесів та обслуговування

напряму залежить безперервність роботи бізнес-систем, збереження даних, швидкодія сервісів та загальна кіберстійкість підприємства.

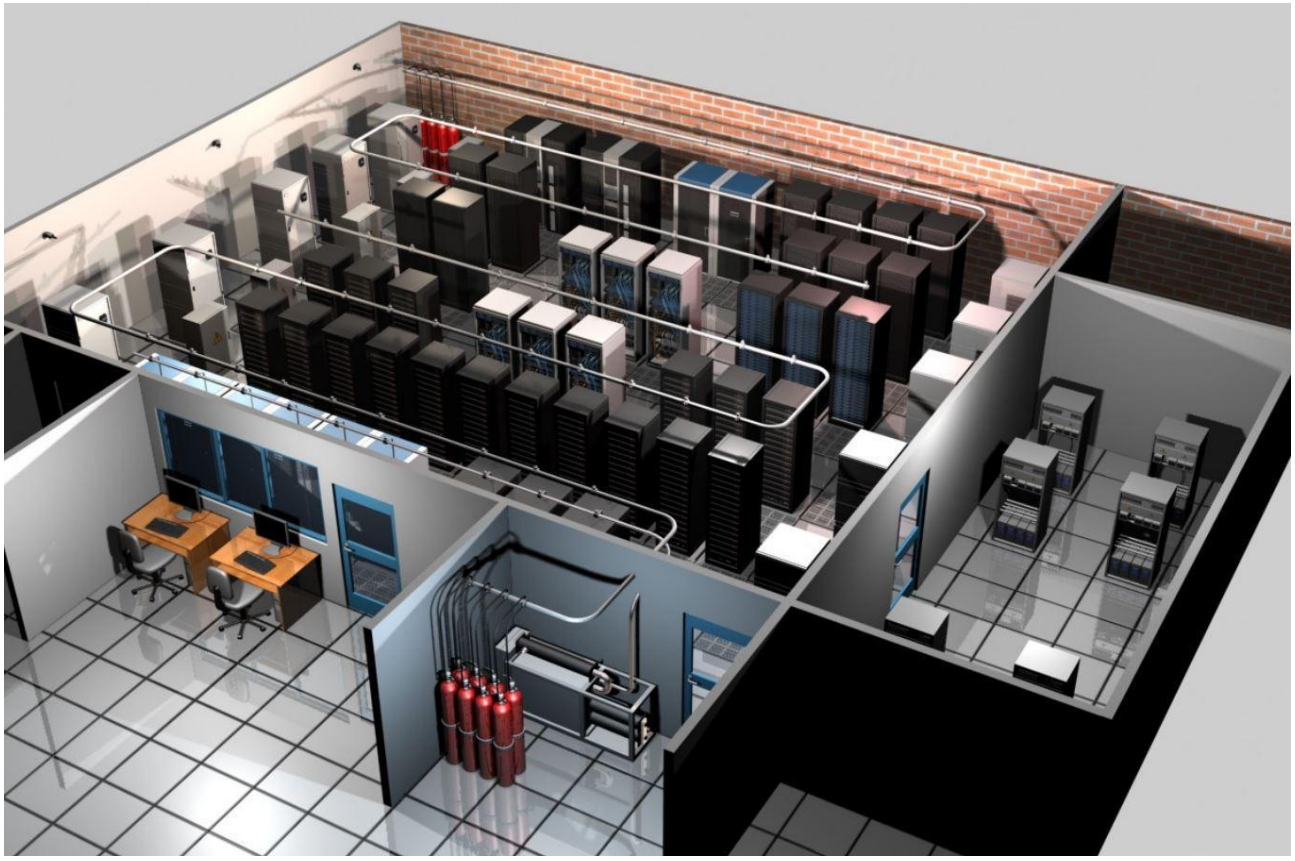

Рисунок 1.2 – Візуалізація серверної кімнати [2]

Типова серверна кімната за своїм призначенням та функціональним навантаженням містить такі ключові елементи, як:

– фізичні сервери – системи, на яких працюють критичні для підприємства сервіси, файлові сховища та ін.;

– мережеве обладнання – комутатори, маршрутизатори, які забезпечуються зв’язок між внутрішніми компонентами IT-інфраструктури, доступ до глобальної мережі інтернет, маршрутизацію трафіку;

– джерела безперебійного живлення – забезпечують стабільне живлення пристроїв у разі зникнення електропостачання, що дозволяє уникнути втрати даних або пошкодження обладнання. У критичних випадках дають можливість перемкнутись на альтернативні джерела живлення;

– системи охолодження – важливий та обов’язковий елемент, для підтримки оптимального температурного режиму в серверній кімнаті. Ідеальною температурою вважається 18-27° С. Перегрів обладнання на 10° С може скоротити термін служби обладнання вдвічі;

– структурована кабельна система – правильно організована мережа кабелів (оптоволокна, витої пари, силових ліній), патч-панелей, кабель-менеджменту, що забезпечує впорядкованість, зручність обслуговування, зменшує ризик помилок під час підключень або модифікацій.

Порушення роботи обладнання серверної кімнати або окремих її елементів (пошкодження мережевої інфраструктури, виходу з ладу ДБЖ, вихід з ладу системи охолодження) може призвести до каскадних збоїв в роботі серверного обладнання, що у свою чергу може зупинити роботу усіх бізнес-додатків.

В умовах сучасного бізнесу важливо не лише забезпечити наявність серверної кімнати, а й перетворити її на локальний дата-центр з наступними характеристиками:

– модульність – розподілення інфраструктури на належні компоненти;

– гібридність – готовність інтеграції з хмарними рішеннями (AWS, Azure, Google Cloud);

– інтелектуальне керування – впровадження BMS (Building Management System), DCIM (Data Center Infrastructure Management);

– автоматизація обслуговування – Ansible, Zabbix, SNMP-моніторинг, автоматичні сповіщення;

– фізична безпека – контроль доступу, пожежна сигналізація та система пожежогасіння, датчики диму, води та руху, відеоспостереження.

Такі перетворення знижують людський фактор, скорочують витрати на обслуговування та збільшуються гнучкість та можливість масштабування ІТ-інфраструктури.

Серверна кімната є «серцем» інформаційної системи підприємства. Її ефективна організація забезпечує надійність, стабільність та продуктивність усіх ключових бізнес-процесів. У зв’язку з цим особливу увагу необхідно приділяти

її проектуванню, модернізації, автоматизації та безпеці. Реформування серверної інфраструктури, згідно з сучасними підходами до реінжинірингу, є одним з основних кроків до побудови ефективної цифрової архітектури підприємства.

1.3 Типові недоліки та проблеми фізичної інфраструктури

Фізична IT-інфраструктура підприємства, особливо в частині серверної кімнати та мережевого обладнання, з часом може накопичувати ряд недоліків та проблем, які негативно впливають на ефективність, надійність та безпеку функціонування всієї інфраструктури. Ці проблеми можуть виникати внаслідок старіння обладнання, неоптимального проектування, недостатнього обслуговування, зростання потреб бізнесу або просто через зміни в технологічному ландшафті.

Розглянемо деякі найпоширеніші недоліки, а саме:

– застаріле обладнання – морально та фізично застаріле, без гарантійного обслуговування обладнання має нижчу продуктивність та вище енергоспоживання, більшу ймовірність відмо, обмежену сумісність з новим програмним забезпеченням та стандартами безпеки;

– відсутність резервного електроживлення – не дає можливості вчасно прийняти міри в ситуаціях зникання або перемикання електроживлення серверної кімнати. Такі ж проблеми може створити низька ємність батарей ДБЖ;

– неефективне охолодження або нераціональне розміщення серверних стійок – може спричинити неефективне або недостатнє охолодження та вентиляцію обладнання;

– безлад в кабельному підключенні – невпорядкована, заплутана або неправильно прокладена кабельна система може створити значні проблеми з вентиляцією обладнання, складність в діагностуванні та пошуку несправностей. Непромаркована кабельна система тільки сприяє помилковому підключенню, збільшує ризик випадкових відключень, може обмежувати пропускну здатність мережі;

– відсутність централізованого моніторингу – за таких умов відслідкувати зміни в серверній кімнати стає складніше, а невчасне реагування на зміни чи проблеми в роботі обладнання може призвести до зупинки роботи обладнання;

– недостатня фізична безпека – може спричинити несанкціонований доступ до серверної кімнати з метою пошкодження, крадіжки або навмисного пошкодження обладнання;

– відсутність належної документації – неповна, недостовірна або застаріла документація на фізичну інфраструктуру ускладнює розуміння загальної структури, проведення діагностики та усунення несправностей, а також плануванню модернізації.

Усі ці фактори підвищують ризик збоїв, погіршують рівень доступності сервісів, збільшують час відновлення після інцидентів, зростання операційних витрат на утримання та обслуговування обладнання та серверної кімнати загалом. Реінжиніринг серверної кімнати спрямований на усунення проблем, модернізацію фізичного рівня та є одним із шляхів вирішення надійної IT-інфраструктури.

1.4 Сучасні підходи до модернізації серверних приміщень

Модернізація серверних приміщень є відповіддю на виклики цифрової трансформації, зростання обсягів даних, потребу у високій доступності та масштабованості. Розглянемо інноваційні технічні рішення, архітектурні практики та стандарти, які забезпечують ефективну, надійну та енергоощадну IT-інфраструктуру.

Одним із ключових напрямів модернізації є орієнтація на міжнародні стандарти. Наприклад, у США прийнято американський (ANSI) стандарт TIA-942, що дає рекомендації як створювати центри даних, і ділить ці центри на типи за ступенем надійності. Фактично, TIA-942 сприймається в усьому світі, як єдиний стандарт для ЦОД (центр обробки даних), однак слід зазначити, що він досить давно не оновлювався. Водночас, жваво розвивається стандарт

BICSI 002 2010 Data Center Design and Implementation Best Practices, котрий з’явився 2010 року і оновлений 2011-го. Кожен із стандартів, здебільшого має власну класифікацію за сукупністю їх параметрів.

Uptime Institute Tier Standard – класифікація дата-центрів за рівнем надійності (Tier I-IV), яка дозволяє оцінити ступінь резервування та відмовостійкості, як це видно на таблиці 1.1. Рівні центрів обробки даних – це визначені рівні стійкості та резервування для інфраструктури IT-об’єктів. Вони широко використовуються в галузях центрів обробки даних, інтернет-провайдерів та хмарних обчислень, як частина інженерного проектування систем високої доступності [3].

Апаратна модернізація інфраструктури включає в себе перехід на високошвидкісні комутатори (10/40/100 Gbps) з підтримкою QoS (quality of service), PoE+ (Power over Ethernet), VLAN (Virtual Local Area Network), SPT (Spanning Tree Protocol). Перехід на оптоволоконні канали (SFP+, QSFP) для магістральних з’єднань [4]. Організація доступу через керовані патч-панелі, які забезпечують стандартизоване, марковане та масштабоване підключення.

Таблиця 1.1 – Класифікація центрів обробки даних

Рівень	Гарантія безвідмовної роботи на рік	Простої на рік	Резервування компонентів
Tier 4	99,995 %	<26,3 хвилини	Відмовостійкий (2N або 2N+1)
Tier 3	99,982 %	<1,6 години	Повний N+1
Tier 2	99,741 %	<22 годин	Часткове резервування живлення та охолодження (часткове N+1)
Tier 1	99,671 %	<28,8 годин	Жоден

Реорганізація структурної кабельної системи (СКС) повинна включати в себе використання кабелю категорії Cat 6a або вище. Оптимальне прокладання кабелю з урахуванням повітряних та підлогових каналів та застосування маркування за стандартом ANSI/TIA-606-B [5].

Для створення гарантованого живлення потрібна інтеграція інтелектуальних UPS-систем із можливістю дистанційного моніторингу та керування, розподілення електроживлення на незалежні лінії, встановлення дизель-генераторів з автоматичним запуском у випадку відключення електроживлення.

Для оптимальної роботи обладнання варто оптимізувати мікроклімат та системи охолодження з використанням інтелектуальних кондиціонерів типу In-Row/In-Rack, які дають можливість охолоджувати локальні гарячі точки [6]. Створення «холодних» та «гарячих» коридорів в серверній кімнаті в свою чергу дасть можливість оптимальній вентиляції та охолодження обладнання і запобігання перегрівання або роботі з високими температурами. Впровадження систем вільного охолодження у відповідних кліматичних зонах.

Сучасні підходи до оптимізації роботи серверних кімнат містять в собі обов’язковий моніторинг обладнання (Zabbix, Grafana, Prometheus), що дає можливість збору даних роботи обладнання, різноманітних датчиків та візуалізації телеметрії. Для зручності та оптимізації конфігурації, оновлення ПЗ варто використати програмні комплекси автоматичним керуванням (Ansible, Puppet, Terraform), системою журналювання (ELK Stack, Graylog). Завдяки цим інструментам досягається проактивне обслуговування, зменшується час виявлення та усунення несправностей.

Для забезпечення фізичної безпеки до серверної кімнати потрібно оновити або встановити СКД (систему контролю доступу), відеоспостереження, датчики руху та відкриття. Визначення відповідальних осіб які будуть мати доступ до серверної кімнати та автоматичну систему сповіщення порушення політик безпеки або фізичного доступу забезпечить зниження ризиків несанкціонованого доступу з метою нанесення шкоди або втручання в роботу обладнання.

Модернізація серверної кімнати це обмежується лише оновленням обладнання. Це комплексний процес, що охоплює фізичну, логічну, безпекову, кліматичну та програмну складові. Актуальні підходи дозволяють створити

ефективну, масштабовану та безпечну IT-інфраструктуру, готову до викликів цифрової трансформації та зростання навантажень.

РОЗДІЛ 2
АНАЛІЗ ПОТОЧНОГО СТАНУ СЕРВЕРНОЇ КІМНАТИ ОБ'ЄКТА ДОСЛІДЖЕННЯ

2.1 Методика проведення аудиту

Аудит серверної кімнати є фундаментальним етапом перед будь-якими роботами з реінжинірингу. Він являє собою систематичний процес збору та аналізу даних про поточний стан фізичної та логічної інфраструктури серверної кімнати, її відповідність встановленим стандартам, найкращим практикам та бізнес-вимогам підприємства. Метою аудиту в контексті даної роботи є не лише констатація фактів, але й виявлення слабких місць, потенційних ризиків та можливостей для оптимізації, що стануть основою для розробки плану реінжинірингу. Ефективний аудит IT-інфраструктури дозволяє об'єктивно оцінити її поточний стан, відповідність бізнес-цілям компанії та визначити напрямки подальшого розвитку [6].

Основними цілями аудиту серверної кімнати в рамках дослідження є:

– оцінка відповідності: визначити, наскільки поточна конфігурація серверної кімнати відповідає галузевим стандартам (наприклад, TIA-942, Uptime Institute), нормативним вимогам та внутрішнім політикам безпеки і експлуатації;

– ідентифікація ризиків: виявити потенційні загрози для безперебійної роботи обладнання, такі як проблеми з електроживленням та охолодженням, фізичною безпекою, пожежною безпекою;

– аналіз ефективності використання ресурсів: оцінити завантаженість серверного обладнання, систем зберігання даних, мережевих каналів, ефективність використання простору та енергоспоживання;

– виявлення «вузьких місць»: локалізувати компоненти інфраструктури, що обмежують загальну продуктивність або масштабованість системи;

– збір вихідних даних для реінжинірингу: сформувати детальну картину поточного стану, яка слугуватиме відправною точкою для планування модернізації;

– документування інфраструктури: створити або актуалізувати детальну документацію щодо всіх аспектів серверної кімнати.

Методика проведення аудиту передбачає послідовне виконання таких етапів: планування та підготовка аудиту, збір даних, аналіз зібраних даних, формування звіту та рекомендації щодо реінжинірингу.

Планування та підготовка аудиту розпочинається з чіткого окреслення меж аудиту – що саме буде перевірятись (фізичне середовище, електроживлення, охолодження, мережева інфраструктура, серверне обладнання, системи безпеки, документація, тощо). Під час планування повинне бути визначені та чітко окреслені часові рамки проведення аудиту. Чітке визначення обсягу аудиту є критично важливим для забезпечення його ефективності та релевантності результатів [6].

Формування аудиторської групи – визначення відповідальних осіб та, за потреби, залучення зовнішніх експертів з досвідом та відповідною сертифікацією проведення об’єктивного аудиту.

Один з основних етапів є розробка плану-графіку аудиту з окресленням часових термінів проведення кожного етапу.

Під час збору попередньої інформації проводиться ознайомлення з наявною документацією, а саме з схемами мережі, планами приміщень, специфікації обладнання, журналу обслуговування, політиками безпеки.

Завершальним етапом підготовки та планування аудиту є підготовка інструментарію – формування чек-листів, опитувальників, підготовки вимірювальних приладів та програмного забезпечення для аналізу.

Другий етап (польовий етап) є основним етапом збору даних.

Фізичне обстеження приміщення включає в себе оцінку розташування, площі, висоти стель, стану стін і підлоги (фальшпідлоги за наявності), стелі. Виявлення та перевірка наявності та стану системи заземлення обладнання, оцінка рівнів освітленості та шуму в серверній кімнаті. Перевірка наявності та відповідності маркування кабелів та обладнання, стійок для серверного обладнання.

Правильне маркування є основою для ефективного управління кабельною системою та швидкого усунення несправностей [7].

Аналіз системи електроживлення надасть можливість перевірки джерел безперебійного живлення, а саме: тип, потужність, час автономної роботи, дата останнього обслуговування або заміни акумуляторів. Проводиться також оцінка стану силових кабелів, розподільчих щитів та розеток. Проводяться заміри напруги, частоти та навантаження на фазах електроживлення, перевірка наявності резервних ліній електроживлення, автоматичного введення резерву (АВР).

Аналіз системи охолодження та вентиляції надає інформацію щодо типу системи кондиціонування, її потужності та резервування, схеми розподілу холодного повітря («холодні» та «гарячі» коридори), проводяться заміри температури та вологості в різних точках серверної кімнати, особливо біля повітрозабірників обладнання та в «гарячих» зонах, проводиться перевірка системи моніторингу кліматичних параметрів. Визначення усіх необхідних параметрів проводиться за допомогою спеціалізованих технічних засобів, як гігрометр (для вимірювання вологості), інфрачервоний термометр або тепловізор (для виявлення точок перегріву), люксметр (для оцінки рівня освітленості), шумомір (для оцінки рівня шуму). «Підтримка оптимального мікроклімату є ключовим фактором для надійності та довговічності IT-обладнання» [8].

Оцінка фізичної безпеки включає в себе збір інформації про доступ до приміщення, використання замків, СКУД, біометрію. Наявність відеоспостереження та системи пожежної сигналізації, автоматичного пожежогасіння (тип, справність, дата останньої перевірки).

Та все ж, основною частиною збору даних є інформація про обладнання, куди входить інвентаризація та аналіз серверного обладнання, а саме: які типи, моделі та конфігурації (CPU, RAM, HDD/SSD) серверів використовується, їхній вік, фізичне розміщення в серверних стійках. Збір інформації про системи зберігання даних, їх типи, наповненість, обсяги зберігання даних, рівні RAID.

Збір даних повинен проводитись як з залученням наявної документації (якщо така є на підприємстві), так і з залученням спеціалізованого програмного забезпечення для інвентаризації (наприклад Spiceworks, Lansweeper, OCS inventory, тощо). Не менш важливою є інформація про мережеве обладнання, куди входять мережеві комутатори, маршрутизатори, міжмережеві екрани (виробники та моделі, конфігурація портів, версії ПЗ) . Стабільність роботи та отримання інформації щодо інцидентів можна отримати за допомогою ПЗ моніторингу систем (наприклад Zabbix, Nagios, PRTG Network Monitor, тощо) для аналізу історичних даних продуктивності. Проведення аудиту кабельної інфраструктури на використання типу кабелю (мідь, оптика), стан патч-панелей та конекторів, організація кабельних трас відбувається візуально та за допомогою технічних засобів (кабельні тестери або аналізатори, мультиметри), може звузити пошук вузьких місць, адже невпорядкована кабельна система може призвести до перегріву, ускладнює обслуговування та підвищує ризик випадкових відключень.

Збір даних про програмне забезпечення та конфігурації, які операційні системи та системи віртуалізації використовуються можна виконати з залучення спеціалізованого програмного забезпечення (наприклад Spiceworks, Lansweeper, OCS inventory, тощо). Наявність та актуальність ліцензій та основні налаштування мережі та безпеки.

Одним з основних аспектів аудиту є проведення інтерв’ювання персоналу. При спілкуванні з IT-спеціалістами, відповідальними за експлуатацію серверної, отримаємо інформацію про типові проблеми, процедури обслуговування та відомі інциденти. Для отримання необхідної інформації також використовуються опитувальники (можливе використання анонімних опитувальників), що дасть можливість отримати значно більшого обсягу інформації для аналізу про інциденти та їх вирішення, регламентне обслуговування обладнання, як фізично, так і на рівні обслуговування операційних систем та програмного забезпечення.

Наступним етапом аудиту є аналіз зібраних даних, який передбачає проведення порівняльного аналізу, тобто зіставлення отриманих даних з вимогами стандартів (наприклад, TIA-942 рівнів I-IV, ISO/IEC 27001 для аспектів безпеки), рекомендаціями виробників обладнання та найкращими практиками (best practices). Проведення оцінки ризиків, класифікація виявлених проблем за ступенем критичності та ймовірності виникнення. Використанням даних моніторингу або проведенням точкових вимірів для оцінки завантаження (CPU, RAM, дискових підсистем та мережевих інтерфейсів) проводиться аналіз продуктивності та завантаженості. Якщо можливо та доцільно, проведення розрахунків показників PUE (Power Usage Effectiveness) для оцінки енергоефективності, що в цілому надасть інформацію про виявлення вузьких місць та точок відмови.

Завершальним етапом аудиту є формування звіту та надання рекомендацій, документ якого повинен містити опис використаної методики, мету та обсяг аудиту, детальний опис поточного стану серверної кімнати з фотофіксацією (за згодою сторін). У звіті повинно бути висвітлено список відповідних невідповідностей, проблем, слабких місць та ризиків, проведено аналіз відповідності стандартам та найкращим практикам. У звіті за результатами аудиту необхідно чітко і структуровано викласти всі знахідки, підкріплюючи їх об’єктивними доказами [9].

Така методика збору та аналізу даних є гнучкою та може бути адаптована та використана під специфіку конкретного підприємства та глибину необхідного аналізу. Важливо пам’ятати, що якість аудиту безпосередньо впливає на успішність подальших етапів реінжинірингу, створення поетапного плану вирішення проблем, впровадження нових технологій та можливості подальшого масштабування IT-інфраструктури.

2.2 Виявлення вузьких місць та проблем функціонування

Після проведення всебічного аудиту серверної кімнати згідно методики, описаною в пункті 2.1, наступним логічним кроком є систематизація та аналіз зібраних даних для ідентифікації конкретних «вузьких місць» (bottlenecks) та проблем функціонування. Вузьким місцем в IT-інфраструктурі називають компоненти системи, продуктивність, або пропускна спроможність якого обмежує загальну продуктивність всієї системи. Проблеми функціонування, в свою чергу, охоплюють ширший спектр недоліків, включаючи ризики безпеки, невідповідність стандартам, неефективне використання ресурсів та труднощі в управлінні. Цей етап є критично важливим, оскільки саме на основі виявлених проблем будуть формуватися завдання для реінжинірингу.

До проблем вузьких місць фізичного середовища та інженерних систем відноситься невідповідність приміщення, а саме недостатня площа для розміщення поточного та майбутнього обладнання, що ускладнює обслуговування та масштабування. Відсутність або неякісна фальшпідлога та/або фальшстеля, що обмежує можливості прокладання кабелів та організації повітряних потоків. Недостатній клас вонестійкості конструкцій, недостатнє або нерівномірне освітлення. Проблеми з герметичністю приміщення, що є причиною потрапляння пилу або вологи, що в свою чергу може бути однією з причин виходу з ладу техніки через перегрівання або виходу з ладу електронних компонентів.

Вузьким місцем системи охолодження та вентиляції є недостатня загальна продуктивність системи кондиціонування для відведення тепла від усього обладнання, особливо в пікові періоди або при підвищенні температури навколишнього середовища. Нерівномірний розподіл холодного повітря, наявність «гарячих точок» біля окремих стійок або одиниць обладнання, відсутність або неефективна організація «холодних» та «гарячих» коридорів можуть призвести до перегрівання обладнання. Застарілі або неефективні кондиціонери з високим енергоспоживанням, відсутність резервування

кондиціонерів, проблема з відведенням конденсату може провокувати появу надмірної вологості в серверній кімнаті, як наслідок виходу з ладу обладнання. Відсутність контролю вологості, що може призвести до статичного розряду (при низькій волості) або корозії (висока вологість). «Оптимальний діапазон відносної волості становить 40-60 %» [9].

Як видно на рисунку 2.1 та рисунку 2.2 в серверних кімнатах підприємства, немає проблем з недостатньою площею кімнати та є можливість масштабування, про що свідчать вільні місця в серверних стійках та вільний простір для встановлення додаткових стійок в разі необхідності.

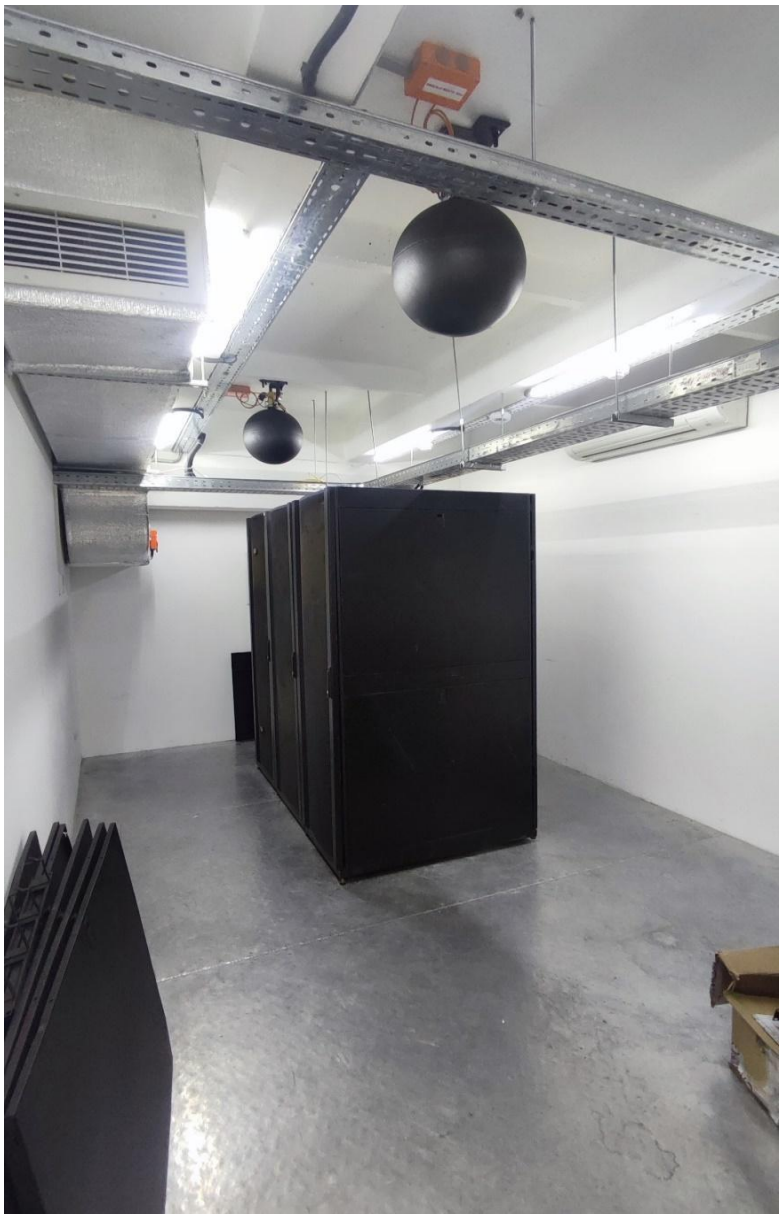

Рисунок 2.1 – Серверна кімната

Рисунок 2.2 – Серверна кімната

При детальному розгляді та перебуваючи безпосередньо в серверній кімнати можна відмітити незначну наявність пилу, що може свідчити про постійне відвідування та нагляд за серверною кімнатою. Під час інтерв’ювання працівниками підприємства було відмічено регламентні роботи по прибиранню та фізичного очищення від пилу. Проте жодних зауважень щодо освітлення або зручності проведення робіт немає, адже доступ до стійок є вільним та добре освітленим.

В даних серверних кімнатах немає фальшпідлоги або фальшстелі, натомість є спроектовані та встановлені кабельні канали з використанням перфорованих лотків для прокладки магістральних кабельних систем, що дає можливість впорядкування кабельної системи та можливість легкого масштабування.

Щодо систем охолодження, то використовуються потужні промислові кондиціонери з запасом потужності, для можливості встановлення додаткового обладнання та/або масштабування, додатково встановлено резервний кондиціонер (з загальною схемою N+1), на випадок виходу з ладу основного блоку охолодження. Добре продумана система вентиляції, при якій «холодні» та «гарячі» коридори мають стабільну температуру. Температурний режим виставлено на рівні 19° С та відносною вологістю 40-60 % згідно норм та рекомендацій ASHRAE. На рисунку 2.2 та рисунку 2.3 добре видно решітки системи кондиціонування та вентилювання.

Рисунок 2.3 – Серверна кімната

Вузьким місцем системи електроживлення є недостатня потужність ДБЖ для забезпечення автономної роботи всього критичного обладнання протягом

необхідного часу або для запуску дизель-генератора. Відсутність резервування ДБЖ, що створює єдину точку відмови, встановлено старі або зношені акумуляторні батареї в ДБЖ, що не забезпечують заявлений час автономії серверної кімнати. Перевантаження окремих ліній живлення, відсутність системи моніторингу параметрів електроживлення в реальному часі. Проблеми із заземленням, що підвищує ризик пошкодження обладнання та ураження струмом персоналу. «Правильне заземлення є критично важливим для безпеки та стабільної роботи чутливого електронного обладнання» [10].

При огляді серверних кімнат бачимо встановлений один з ДБЖ (рис. 2.4).

Рисунок 2.4 – Додатковий блок живлення

Даний ДБЖ встановлено за загальною схемою резервування 2N (дзеркальне резервування), що дає можливість незалежного заживлення обладнання на період запуску дизель-генератора. Дані ДБЖ мають можливість відслідковування навантаження в реальному часі, відслідковування навантаження окремих ліній. При інтерв'юванні персоналу було отримано інформацію, щодо постійного регламентного обслуговування усіх ДБЖ, перевірку та заміну елементів батареї, які втратили свою ємність або не відповідали своїм технічним характеристикам через знос, було проведено оновлення програмного забезпечення під час останнього регламентного обслуговування. Моніторинг параметрів роботи та раннє сповіщення про зміну статусів відбувається за допомогою системи моніторингу Zabbix.

Повернімося до проблем кабельної системи, адже вузьким місцем може стати використання кабелів нижчої категорії (наприклад Cat5 замість Cat6/6A для гігабітних і вищих швидкостей), що обмежує пропускну здатність мережі. Хаотичне прокладання кабелів (так званий «кабельний хаос» або «спагеті») ускладнює доступ до обладнання, погіршує охолодження та підвищує ризик випадкових відключень. «Невпорядкована кабельна система є ознакою поганого управління та може призвести до значних операційних проблем» [5].

Відсутність або неповне маркування кабелів, патч-панелей та портів, що ускладнює пошук несправностей та підключення нового обладнання, пошкоджені кабелі або конектори. Перевищення максимально допустимої довжини кабельних сегментів, недостатня кількість портів на патч-панелях або комутаторах для поточних потреб або майбутнього розширення можуть створити не аби-які проблеми.

Аналізуючи кабельну систему серверних кімнат підприємства Х було виявлено акуратно вкладений кабель в кабельні канали, але нажаль не всі були використані вищої категорії Cat6/6A для магістральних кабелів, натомість використано було оптоволоконні кабелі для підключення обладнання на віддалених точках та до серверів, для пришвидшення передачі даних.

Певні патч-панелі, які встановлено в серверні стійки мають маркування, але більшість кабелів не промарковано взагалі, що створює певний хаос в швидкому пошуку проблеми. На рисинку 2.5 та рисунку 2.6 чітко видно хаос підключення обладнання безпосередньо в серверних стійках, який звисає ніби «спагеті» електронного світу.

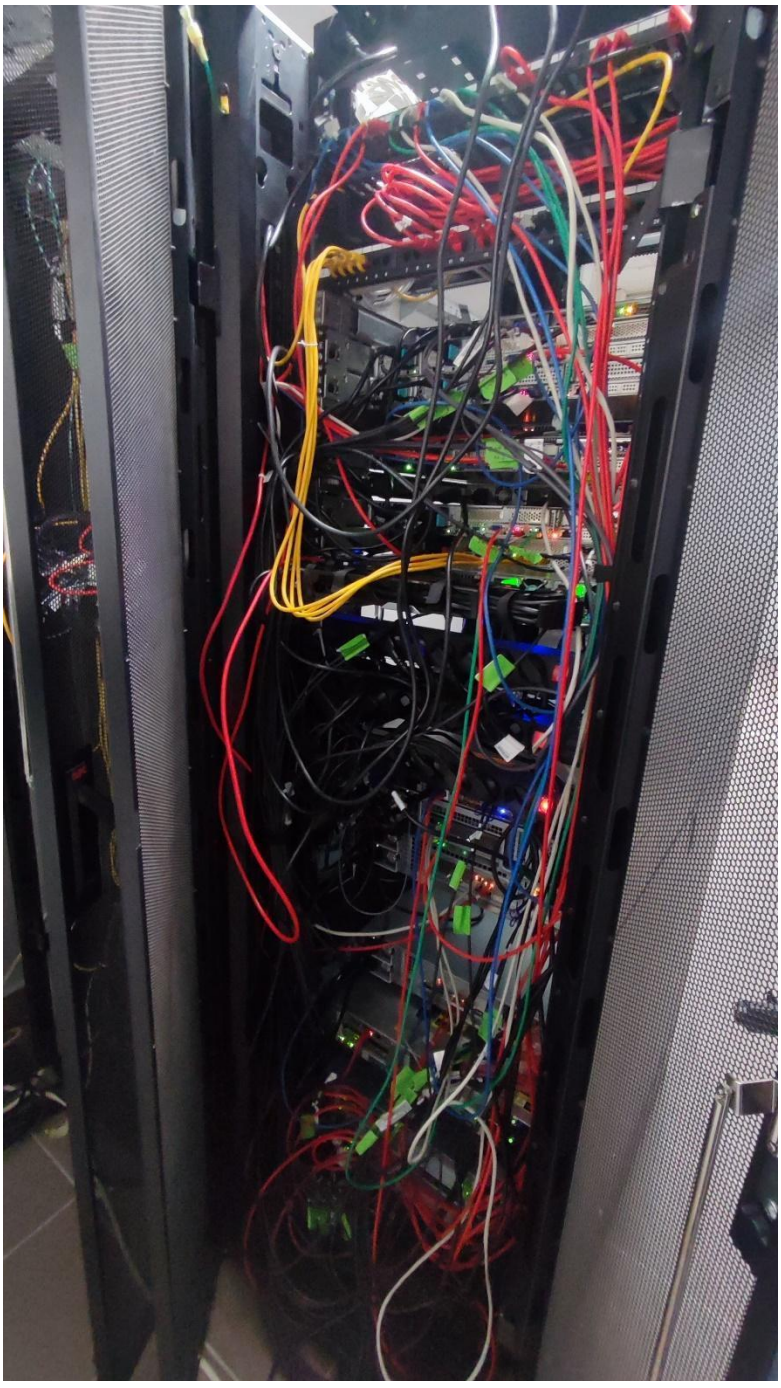

Рисунок 2.5 – Серверна стійка

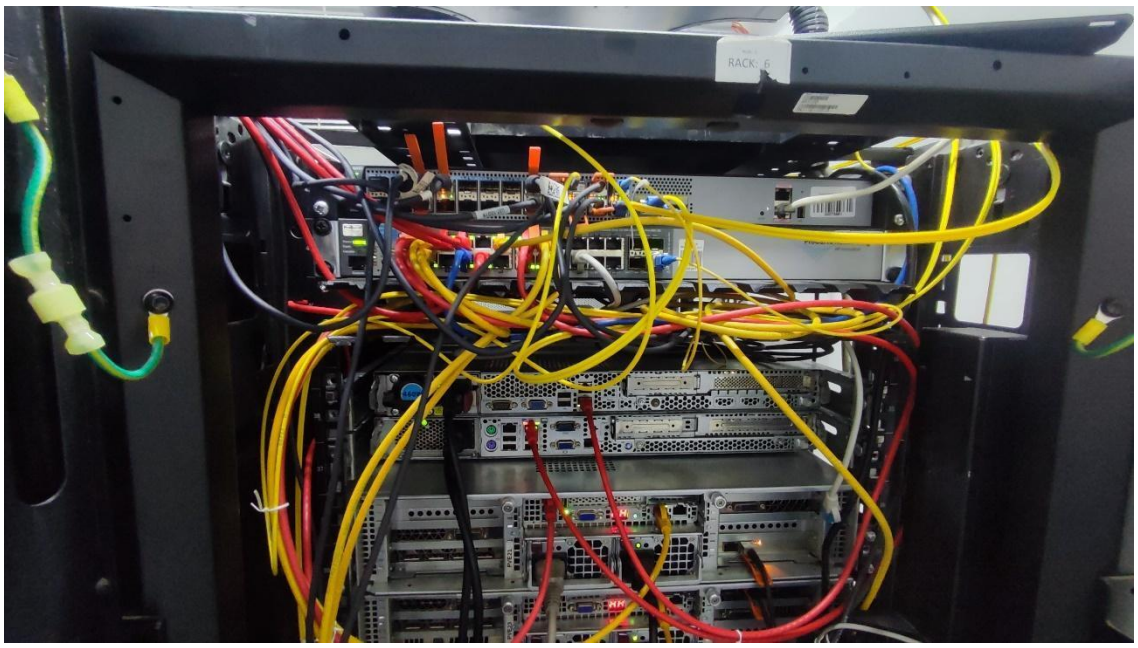

Рисунок 2.6 – Серверна стійка

Щодо перевищення максимально допустимої довжини кабельних сегментів було виявлено та усунено на етапі закладання мережі працівниками підприємства, тому на даному етапі перевищення допустимої довжини кабелю виявлено не було, але було виявлено пошкоджені порти патч-панелей та конекторів кабелів підключення, через що виникали незрозумілі перебої в роботі мережевого обладнання, невідповідність швидкості передачі даних, певні проблеми з підключенням обладнання на кінцевих точках, помилки в роботі комутаторів.

Одним з вузьких місць може бути недостатність вільних портів на комутаторах або патч-панелях для поточних проблем або майбутнього розширення. Однак цієї проблеми на даному етапі в серверних приміщеннях немає, як підтвердження можна побачити вище на фото.

Вузьким місцем серверної кімнати може бути використання застарілого обладнання (сервери, СЗД, комутатори, концентратори) з низькою продуктивністю, високим енергоспоживанням, застарілими консолями управління та відсутністю підтримки з боку виробника (End-of-Life, End-of-Support). Безпосередньо на серверах підприємства може бути недостатність обчислювальних ресурсів (CPU, RAM), що призводить до повільної роботи

додатків. Низька продуктивність дискових підсистем та накопичувачів призводить до затримок та високих значень IOPS (Input/Output Operations Per Second). Особливо критичним може бути недостатня пропускна спроможність мережевих комутаторів (наприклад використання 100 Мбіт/с комутаторів там, де потрібні гігабітні). Відсутність резервування критичних компонентів обладнання (наприклад блоків живлення, мережевих карт в серверах), неефективне використання наявних серверних потужностей (низький рівень утилізації), що вказує на потенціал для віртуалізації або консолідації. Перегрів окремих одиниць обладнання через локальні проблеми з охолодженням або високе власне тепловиділення.

При проведенні аудиту підприємства було виявлено використання комутаторів HPE V1910-48G, ProCurve J4899B Switch 2650, HPE V1910-24G, HPE 1910-48, які мають вже закінчений період підтримки обладнання виробником (End-of-Life), різні в налаштуваннях та досить обмежені можливості керування та контролю. Деякі з них мають несправні порти для підключення, що є одним з найважливіших факторів для заміни обладнання в картині загального реінжинірингу серверної кімнати. Певні сервери, які ще використовуються підприємством мають закінчений період підтримки виробником (End-of-Support), наприклад HP ProLiant DL380p Gen8, ProLiant BL460c Gen8, а деякі з них мають закінчений період життя, наприклад BladeSystem c7000 Enclosure G2, Asus RS500A. Та все ж серед серверів в стійках встановлено більш сучасне обладнання, яке використовується як сервери віртуалізації, зберігання та обробки даних, файлові накопичувачі.

Щодо вузьких місць функціонування проблеми безпеки віднести важко, але це невід’ємний аспект безперебійної роботи серверної кімнати. Недостатність фізичного контролю доступу до серверної кімнати (наприклад використання звичайних замків без журналу доступу) можуть привести до несанкціонованого доступу до серверної кімнати з метою викрадення, нанесення шкоди або несанкціонованого доступу до серверів. Відсутність політик безпеки щодо доступу та роботи в серверній кімнати, або їх ігнорування. Відсутність або

неадекватна система відеоспостереження, відсутність або несправність системи охоронної сигналізації. Невідповідність системи пожежогасіння (наприклад, використання водяного пожежогасіння, яке може нашкодити обладнанню) або її несправність/відсутність регулярних перевірок. «Вибір системи пожежогасіння для серверних приміщень повинен враховувати безпеку для обладнання та персоналу, перевага надається газовим або аерозольним системам» [11].

В серверній, яку розглядаємо вже є встановлена система пожежогасіння, вище на рисунку 2.1, рисунку 2.3 добре видно балони пожежогасіння з використанням газу. Система пожежогасіння має в серверній кімнати датчики диму та вогню, та підключена до загальної системи сповіщення надзвичайних ситуацій підприємства, світлового та звукового сповіщення про надзвичайну ситуацію. З розмови з працівниками було відмічено встановлену СКД (систему контролю доступу) з електромагнітними замками дверей. СКД в своєму комплексі має можливість надавати відповідні дозволи доступу до приміщень з використанням картки-перепустки або RFID-міти, які закріплені за кожним працівником підприємства. СКД також підключена та працює в загальному комплексі охоронної сигналізації підприємства. Варто відмітити відсутність відеоспостереження безпосередньо в серверних кімнатах, що може слугувати відсутністю підтвердження неправомірних дій або недотримання політик безпеки в серверних кімнатах при виконанні робіт працівниками.

Проблемами моніторингу та управління є відсутність централізованої системи моніторингу інженерних систем та параметрів (температура, вологість, електроживлення, протікання) та IT-обладнання (завантаженість, помилки, доступність). Нерегулярне або відсутнє сповіщення відповідальних осіб про критичні події та збої. Складність в управлінні інфраструктурою через відсутність актуальної документації та засобів автоматизації. Підхід до вирішення проблем повинен бути проактивним, а не реактивним, тобто проблеми потрібно попереджати, а не вирішувати після їх виникнення. Як вище було вказано, на підприємстві є встановлена система моніторингу Zabbix, що дає

змогу оперативно реагувати на події та помилки, мати певну історію подій та параметрів обладнання, яке моніториться.

Серед проблем документації та відповідності стандартам є відсутність або неактуальність схем розміщення обладнання, кабельних журналів, схем електроживлення та мережевих діаграм. Відсутність формалізованих процедур обслуговування, резервного копіювання, відновлення після збоїв може привести до невиправних втрат важливих та критично важливих даних та роботи сервісів. Невідповідність реального стану серверної кімнати внутрішнім політикам підприємства або галузевим стандартам (наприклад, часткова відповідність TIA-942 або рекомендаціям Uptime Institute, якщо такі цілі ставилися).

Для кожного виявленого вузького місця чи проблеми необхідно оцінити її на роботи систем чи сервісів. Яка з проблем може привести до простою сервісів та як це вплине на безперебійність бізнес-процесів? Яка проблема знижує продуктивність IT-системи? Які ризики несанкціонованого доступу, втрати чи пошкодження даних створює проблема безпеки даних та інфраструктури? Що може обмежити розвиток IT-інфраструктури в майбутньому? Після ідентифікації та аналізу впливу, проблеми та вузькі місця необхідно пріоритезувати. Критеріями пріоретизації є критичність впливу на бізнес, ймовірності виникнення інцидентів, фінансові збитки, вимоги регуляторів та стандартів, складність та вартість усунення.

2.3 Оцінка ефективності поточного обладнання

Після ідентифікації вузьких місць та проблем функціонування, наступним логічним кроком є глибока оцінка ефективності наявного обладнання. Цей етап не обмежується простою інвентаризацією; його мета – визначити, наскільки поточні апаратні ресурси відповідають сучасним вимогам продуктивності, енергоефективності, надійності та економічній доцільності. Ефективність обладнання – це «комплексний показник, що характеризує здатність апаратного забезпечення виконувати покладені на нього задачі з оптимальним

співвідношенням продуктивності, вартості володіння та споживчих ресурсів» [12]. Результати цієї оцінки стануть обґрунтуванням для прийняття рішень про модернізацію, заміну або залишення в експлуатації окремих компонентів ІТ-інфраструктури в рамках проєкту реінжинірингу.

Оцінку слід проводити за набором чітко визначених критеріїв, що дозволяють отримати об’єктивну та всебічну картину.

Загальну технічну продуктивність (Performance) визначають за такими критеріями, як утилізація ресурсів, а саме: аналіз середніх та пікових значень показників завантаження центральних процесорів (CPU), оперативної пам’яті (RAM), дискових підсистем (IOPS, latency) та мережевих інтерфейсів. Відповідність поточним навантаженням: Чи здатне обладнання обробляти існуючий обсяг даних та транзакцій без суттєвих затримок і збоїв? Порівняння з сучасними аналогами: наскільки технічні характеристики (тактова частота ЦП, швидкість ОЗП, пропускна здатність шини даних) поступаються актуальним моделям на ринку.

Енергоефективність визначають за споживанням електроенергії: прямі заміри або оцінка споживаної потужності в різних режимах роботи. «Витрати на електроенергію складають значну частину операційних витрат сучасного дата-центру, тому енергоефективність обладнання є ключовим фактором» [13]. Одним з аспектів енергоефективності є тепловиділення: оцінка кількості тепла, що генерується обладнанням, оскільки це безпосередньо впливає на навантаження системи охолодження. Співвідношення «продуктивність/ват»: порівняльна оцінка, яка показує, скільки корисної роботи виконує обладнання на одиницю спожитої енергії.

Економічна доцільність та сукупна вартість володіння (Total Cost of Ownership – TCO) дозволяє визначити вартість підтримки, тобто витрати на розширені гарантії та сервісні контракти. Наявність, вартість запасних частин та вартість ремонту. Операційні витрати (OpEx) такі, як: вартість електроенергії, охолодження, місця в стійці. При аналізі потрібно враховувати не лише

капітальні затрати на придбання, але й повні операційні витрати протягом усього життєвого циклу обладнання.

Надійність та життєвий цикл (lifecycle) дає розуміння статусу життєвого циклу. Перевірка на предмет досягнення статусів «Кінець продажу» (End-of-Sale), «Кінець технічної підтримки» (End-of-Support, EoSL) або «Кінець життя» (End-of-Life, EoL). Використання обладнання зі статусом EoL/EoSL несе значні ризики безпеки, оскільки для нього не випускаються оновлення та патчі. Проведення аналізу статистики збоїв та інцидентів, або ж середній час між відмовами (MTBF). Оцінка наявності та працездатності резервних компонентів (блоки живлення, контролери, вентилятори).

Масштабованість та гнучкість надає інформацію про потенціал для модернізації, наприклад: наявність вільних слотів для оперативної пам’яті (ОЗП, RAM), дискових кошиків, портів розширення. Підтримка сучасних технологій, для прикладу: підтримка серверами апаратної віртуалізації або комутаторами мереж 10GbE. Чи не стане дане обладнання перешкодою для зростання бізнесу у найближчі 2-3 роки.

На основі даних, зібраних під час аудиту, та вищезазначених критеріїв, проведемо оцінку ключового обладнання, що використовується в серверній кімнаті:

ProCurve J2899B Switch 2650 – це комутатор рівня доступу з портами 10/100 Мбіт/с та гігабітними аплінками:

– життєвий цикл: статус End-of-Life досягнуто понад 10 років тому (End-of-Sale у 2007 р., End-of-Support у 2012 р.);

– продуктивність: швидкість передачі 100 Мбіт/с є абсолютно недостатньою для підключення сучасних серверів і навіть робочих станцій. Це критичне вузьке місце, що обмежує продуктивність всієї мережі;

– висновок: нерентабельний та небезпечний в експлуатації, є головним кандидатом на негайну заміну.

Серія комутаторів HPE 1910 (V1910-48, V1910-48G, V1910-24G) – це гігабітні комутатори з базовим функціоналом рівня L2+:

– життєвий цикл: статус End-of-Life досягнуто приблизно у 2019-2020 роках. Оновлення безпеки більше не випускаються;

– продуктивність: забезпечують гігабітну швидкість, що може бути достатньо для кінцевих користувачів, але є вузьким місцем для серверних підключень, особливо для СЗД та хостів віртуалізації. Відсутні порти 10 GbE для аплінків, що є досить поширеною причиною низької продуктивності сучасних бізнес-додатків;

– масштабованість: низька. Відсутність підтримки стекування 10 GbE портів обмежує росту інфраструктури;

– висновок: неефективні для серверного сегмента. Можуть бути тимчасово залишені для некритичних підключень, але в рамках реінженірінгу підлягають заміні на моделі з підтримкою 10 GbE.

Сервери HP ProLiant Gen8 (DL380p, BL460c G8) – це сервери, випущені у 2012-2014 роках на базі процесорів Intel Xeon E5-2600 v1/v2:

– життєвий цикл: статус End-of-Service-Life досягнуто приблизно в 2020 році. Отримання офіційної підтримки та оригінальних запчастин ускладнене;

– продуктивність: для свого часу були потужними, але значно поступаються сучасним серверам. Підтримка лише DDR3 пам’яті та PCIe 3.0;

– енергоефективність: дуже низька. Споживають значно більше електроенергії на одиницю обчислень порівняно з сучасними серверами. Сервери 8-го покоління можуть споживати в 2-3 рази більше енергії, ніж сучасні аналоги при виконанні того ж навантаження, що призводить до значних операційних витрат;

– масштабованість: обмежена. Максимальний обсяг ОЗП та кількість ядер не відповідають сучасним вимогам для щільної віртуалізації;

– висновок: економічно та технічно застарілі. Є головними кандидатами на заміну з метою консолідації навантажень на меншій кількості нових, більш ефективних серверів.

Шасі BladeSystem c7000 Enclosure G2:

– життєвий цикл: застаріла модель шасі. Його модулі управління, вентилятори та блоки живлення значно менш ефективні, ніж версії G3 або Platinum;

– продуктивність: пропускна здатність внутрішньої шини та модулів комутації (зазвичай 1Gb Ethernet або старі модулі 10 Gb) є вузьким місцем для сучасних blade-серверів;

– висновок: заміна blade-серверів робить недоцільним подальше використання цього шасі. Підлягає заміні разом з серверами на більш сучасні сервери.

Сервер Asus RS500A-E9-RS4 – це сучасний 1U сервер на базі процесорів AMD Epyc 7001/7002:

– життєвий цикл: актуальний. Повністю підтримується виробником;

– продуктивність: висока. Підтримка великої кількості ядер (до 64 на 2-ге покоління EPYC), пам’яті DDR4 та шини PCIe 4.0 забезпечує відмінну продуктивність для віртуалізації та високопродуктивних обчислень;

– енергоефективність: висока. Сучасна архітектура забезпечує значно кращий показник «продуктивності на ват»;

– масштабованість: висока. Є хороший потенціал для нарощування обсягу ОЗП та встановлення високошвидкісних мережевих адаптерів;

– висновок: ефективне та сучасне обладнання. Є зразком для проведення модернізації та може слугувати основою для нової інфраструктури.

Усе описане вище для зручності оперування та порівняння можна розмістити у зведеній таблиці (табл. 2.1).

Аналіз показав, що значна обладнання, яке використовується на об’єкті дослідження є технічно та морально застарілою. Обладнання HP/HPE покоління Gen8 та серії 1910 досягло свого життєвого циклу, що створює прямі ризики для безпеки та безперебійності системи та бізнес-процесів. Його низька енергоефективність призводить до невиправдано високих операційних витрат на електроенергію та охолодження.

Таблиця 2.1 – Зведена таблиця оцінки ефективності обладнання

Обладнання	Продуктивність	Енерго-ефективність	ТСО (ризики)	Надійність/ Життєвий цикл	Масштабованість	Загальний висновок
Комутатори						
ProCurve J4899B Switch 2650	Низька	Середня	Дуже високий	EoL (2012)	Відсутня	Негайна заміна
HPE 1910 Series (V1910-48G/24G)	Середня	Середня	Високий	EoL (2020)	Низька	Заміна в рамках реінжинірингу
Сервери та шасі						
HP ProLiant DL380p Gen8	Середня	Низька	Високий	EoL/EoSL (2020)	Низька	Заміна, консолідація навантажень
HP ProLiant BL460c Gen8	Середня	Низька	Високий	EoL/EoSL (2020)	Низька	Заміна, консолідація навантажень
BladeSystem c7000 Enclosure G2	Низька	Низька	Дуже високий	Застаріле	Відсутня	Заміна разом із blade-серверами
Asus RS500A-E9-RS4	Висока	Висока	Низький	Актуальне	Висока	Залишити, основа нової інфраструктури

Та все ж наявність сучасного сервера ASUS RS500A демонструє потенціал для значного підвищення ефективності. Таким чином, оцінка чітко вказує на необхідність заміни застарілого обладнання, що є ключовим завданням для наступних етапів реінжинірингу.

РОЗДІЛ 3
РОЗРОБКА ТА ВПРОВАДЖЕННЯ РІШЕНЬ ДЛЯ РЕІНЖИНІРИНГУ СЕРВЕРНОЇ КІМНАТИ

Практична реалізація проєкту реінжинірингу є комплексним, багатоетапним процесом, що вимагає чіткої послідовності дій. Загальна структура та поетапність виконання робіт, від початкового аналізу до фіналізації, представлена на блок-схемі (рис. 3.1).

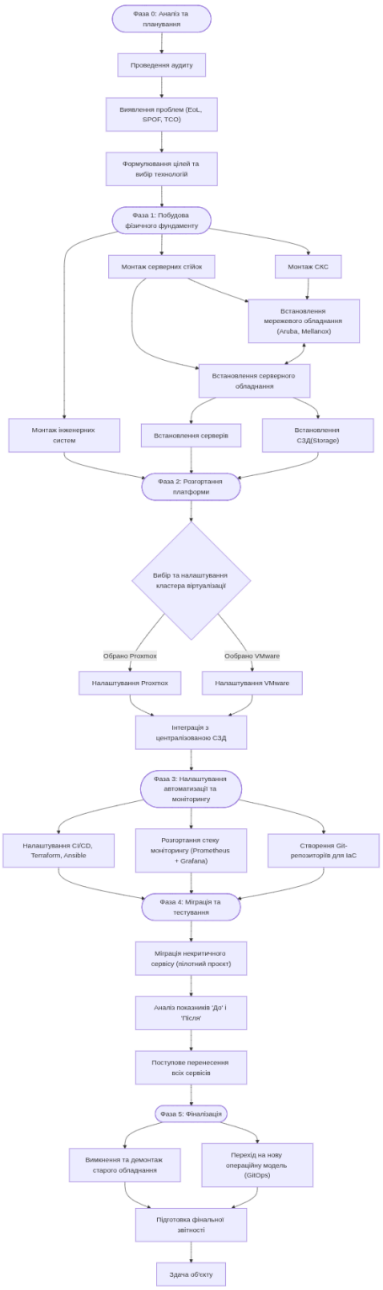

Рисунок 3.1 – Блок-схема поетапності виконання робіт

3.1 Модернізація фізичного рівня: патч-панелі, комутатори, кабельна система та розробка схеми оптимального мережевого підключення

Фізичний рівень мережі є фундаментом усієї IT-інфраструктури. Дослідження, зроблені в розділі 2, чітко продемонстрували, що поточна фізична інфраструктура на об’єкті дослідження, яка включає комутатори ProCurve J4899B та HPE 1910, а також невпорядковану кабельну систему, є головним обмежуючим фактором продуктивності, надійності та безпеки. Метою даного пункту є створення масштабованої, високопродуктивної та легко керованої мережевої основи для всієї IT-інфраструктури підприємства. Перейдемо до розробки комплексного рішення рішення для модернізації фізичного рівня. Така розробка передбачає впровадження гібридної кабельної системи, що поєднує переваги мідних та оптоволоконних технологій, заміну пасивного та активного мережевого обладнання та побудову нової, логічної та ефективної схеми мережевих підключень.

Для побудови надійної та швидкої мережі пропонується гібридний підхід, що використовує як мідні, так і оптоволоконні рішення там, де їх застосування є найбільш доцільним.

До компонентів на основі мідної витої пари віднесемо кабельну продукцію, яка використовується для підключення робочих станцій, принтерів, IP-телефонів та багато іншого обладнання на рівні доступу, а також для серверних з’єднань, де не потрібна швидкість вище 10 Гбіт/с. Рекомендується використовувати екранований кабель «вита пара» категорії 6A (Cat 6A F/UTP). Такий кабель гарантовано підтримує швидкість 10 Гбіт/с (10GBASE-T) і забезпечує відмінний захист від електромагнітних завад, що є критичним для серверної кімнати.

Встановлення 24-портових патч-панелей категорії 6A та горизонтальних або вертикальних кабельних органайзерів є обов’язковим для структурування мідних з’єднань, спрощення адміністрування та забезпечення належного охолодження активного обладнання.

Окрім використання мідних кабельних рішень, де вони досягають своїх меж або є менш ефективними, для найбільш критичних та високошвидкісних з’єднань використовуються оптоволоконні кабелі. «Оптоволокно забезпечує вищу пропускну здатність, повну нечутливість до електромагнітних перешкод та можливість передачі даних на значно більші відстані, що робить його ідеальним вибором для магістральних каналів у сучасних дата-центрах» [14].

Для з’єднань у межах серверної кімнати та будівлі рекомендується використовувати багатомодовий оптоволоконний кабель класу OM4 (Multimode Fiber OM4). Цей вибір є оптимальним за співвідношенням ціна/продуктивність, оскільки він підтримує швидкість 10 Гбіт/с на відстань до 400 метрів та швидкість 40 Гбіт/с та 100 Гбіт/с на відстань до 150 метрів. Такий вибір створює міцну основу для майбітніх модернізацій мережевого ядра без необхідності заміни кабельної інфраструктури.

Для термінування оптоволоконних кабелів встановлюються спеціалізовані стійкові оптоволоконні патч-панелі (Optical Distribution Frame). Вони забезпечують захист крихких волокон та зручну точку для комутації за допомогою оптоволоконних патч-кордів.

Серед видів конекторів оптоволоконних патч-кордів варто виділити такі види:

– SC – пластиковий роз’єм, який використовується в кабельних системах найчастіше. Він забезпечує високу швидкість та щільність з’єднання;

– LC – являє собою точно такий же конектор, що й SC, проте має менші розміри та використовується для підключення до обладнання з високою щільністю портів;

– FC – конектор, виготовлений з металу. Цей тип наконечника відрізняється стійкістю до вібрацій та високою надійністю фіксації внаслідок різьбового з’єднання. Зазвичай, такий наконечник використовується з одномодовими кабелями, використовується для підключення оптичного вимірювального обладнання;

– ST являє собою роз’єм з металевим корпусом та байонетною фіксацією. Найчастіше використоується з багатомодовими кабелями, що містять одне волокно.

Товщина роз’єму LC становить 1.25 мм, у всіх інших – 2.5 мм.

Як стандарт для всіх оптоволоконних з’єднань обирається конектор LC. Цей компактний конектор є де-факто стандартом для сучасного високошвидкісного обладнання завдяки своїй надійності та високій щільності портів.

Впроваджується єдина система кольорового та цифрового маркування для всіх типів кабелів та портів. Наприклад, мідні кабелі маркуються білим кольором, а оптоволоконні патч-корди OM4 – бірюзовим (Aqua), що відповідає галузевим стандартам і дозволяє миттєво візуально розрізняти типи з’єднань.

Пропонується розробка та впровадження сучасної дворівневої ієрархічної архітектури «Ядро-Доступ» (Core-Access), що використовує переваги обох типів кабельних систем.

Рівень ядра (Core Level) – це центральна, високопродуктивна частина мережі, що відповідає за швидку комутацію трафіку між різними сегментами мережі (серверами, СЗД, рівнем доступу). Вимогами до комутаторів ядра є висока продуктивність та неблокуюча архітектура, наявність портів 10GbE/25GbE (SFP+/SFP28) для підключення серверів та інших комутаторів. Підтримка стикування або технологій віртуалізації шасі (наприклад, VSF, IRF) для забезпечення відмовостійкості та спрощення управління, розширений функціонал L3-маршрутизації.

Пропоноване рішення: встановлення двох стикованих L3-комутаторів (наприклад, серії HPE Aruba CX 6300M або аналогів), що працюють у режимі резервування. Це дасть можливість усунути єдину точку відмови (SPOF) і забезпечує безперебійну роботу мережі навіть у разі виходу з ладу одного з пристроїв.

Рівень доступу (Access Layer) – це рівень, який забезпечує підключення кінцевих пристроїв: робочих станцій, принтерів, точок доступу Wi-Fi та менш

критичного обладнання. Вимогами до комутаторів доступу є достатня кількість портів 1GbE (10/100/1000BASE-T) для підключення користувачів, наявність аплінк-портів 10GbE (SFP+) для високошвидкісного з'єднання з ядром мережі. Великою перевагою є підтримка портів PoE/PoE+ (Power over Ethernet) для живлення IP-телефонів, камер відеонагляду та точок доступу, базовий функціонал безпеки (Port Security, ACL).

Пропоноване рішення: Використання керованих L2+ комутаторів (наприклад, серії HPE Aruba CX 6100 або аналогів) з 24 або 48 портами 1GbE та аплінками 10GbE SFP+.

Таким чином можемо розробити схему оптимального мережевого підключення, ключовими принципами якого будуть:

– високошвидкісне підключення серверів, зокрема критично важливі сервери та системи зберігання даних підключаються до комутаторів ядра переважно через оптоволокно з використанням трансиверів SFP+ з швидкістю передачі даних 10 Гбіт/с. Для забезпечення максимальної відмовостійкості та пропускної здатності використовується агрегація каналів (LACP);

– оптоволоконні магістралі, а саме усі з'єднання між рівнем ядра та рівнем доступу (Uplinks) виконуються за допомогою дубльованих оптоволоконних ліній OM4 на швидкості 10 Гбіт/с. Кожен комутатор доступу підключається до обох комутаторів ядра, що забезпечує повне резервування шляху;

– використання мідного з'єднання (кабелю витої пари Cat 6A) на рівні доступу для підключення робочих станції, IP-телефонів та іншого периферійного обладнання з використанням швидкості підключення 1 Гбіт/с;

– сегментація трафіку за допомогою VLAN, що допоможе логічно розділити на віртуальні підмережі (Virtual Local Area Network) незалежно від фізичного середовища передачі. Маршрутизація між віртуальними мережами відбувається на рівні ядра.

Таким чином, очікувані результати від гібридного підходу є – максимальна продуктивність, адже використання оптоволоконних мереж на магістралях та для серверів усуває будь-які мережеві вузькі місця, а мідь

забезпечує економічно ефективне підключення на рівні доступу. Повна нечутливість оптоволоконних ліній до електромагнітних випромінювань робить магістральні канали значно надійнішими. Отримаємо виняткову масштабованість, адже інфраструктура на базі OM4 кабелю готова до переходу на швидкості 40/100 Гбіт/с у майбутньому лише шляхом заміни активного обладнання (комутаторів та трансиверів). Таке поєднання різних фізичних середовищ передачі даних в рамках єдиної архітектури та системи маркування створює прозору та легко керовану інфраструктуру.

Та все ж досконалості немає меж, тому для максимального реінжинірингу пропоную створення та використання виділеної високопродуктивної мережі на базі рішень NVIDIA (Mellanox).

Для забезпечення максимальної продуктивності для критично важливих завдань, таких як доступ до системи зберігання даних (особливо NVMe-oF), міжсерверна комунікація у кластерах віртуалізації та майбутні потреби, пропонується створення окремої, паралельної мережевої фабрики. Цей підхід ізолює надвеликі потоки даних від загальнокорпоративного трафіку, запобігаючи перевантаженням та гарантуючи мінімальну затримку. «сучасні центри обробки даних часто використовують архітектуру з кількома мережевими фабриками (multi-fabric), де загальний трафік і трафік систем зберігання даних фізично розділені для досягнення оптимальної продуктивності та надійності» [15].

В якості серця високопродуктивної мережі пропонується комутатор NVIDIA Specrtum-2 (наприклад, модель SN3700). Цей комутатор забезпечує 32 порти з швидкістю 100/200 GbE, наднизьку затримку та підтримку передових технологій, таких як RDMA over Converged Ethernet (RoCE).

Для серверів, які потребують максимальної продуктивності, такі, як Asus RS500A та майбутні хости віртуалізації, що оснащуються інтелектуальними мережевими адаптерами NVIDIA ConnectX-6 Dx. Ці адаптери підтримують швидкість 100GbE та апаратно розвантажують обробку мережевих протоколів, зокрема RoCE, що дозволяє передавати дані безпосередньо в пам’ять додатків,

минаючи ядро ОС, і таикм чином кардинально знижуючи затримки та навантаження на CPU.

Для коротких з’єднань у межах однієї стіки (до 3 метрів) будуть використовуватись Direct Attach Copper (DAC), що є найбільш економічним рішенням. Для міжстійкових з’єднань будуть використовуватись активні оптичні кабелі (AOC), які являють собою готовий оптоволоконний кабель з інтегрованими трансиверами, що спрощує інсталяцію.

Таким чином фінальна оновлена схема мережевого підключення передбачає дві незалежні мережеві фабрики:

– General Purpose Fabric (загальноцільова мережа): побудована на базі комутаторів HPE Aruba (ядро-доступ). Обслуговує загальний корпоративний трафік, доступ користувачів, управління, інтернет;

– High-Performance Fabric (високопродуктивна мережа): побудована на базі комутатора NVIDIA Spectrum та адаптерів ConnectX. Обслуговує виключно трафік між серверами та СЗД (Storage), а також між вузлами кластерів (Inter-Cluster Communication).

Очікуваними результатами від інтеграції NVIDIA (Mellanox) є екстремальна продуктивність для СЗД, а саме забезпечення наднизьких затримок для доступу до даних, що є критичним для баз даних та систем віртуалізації. Ізоляція та передбачуваність надасть можливість роботи масивних потоків даних (наприклад, резервне копіювання), які ніяк не вплинуть на роботу користувачів у загальноцільовій мережі. Створена інфраструктура повністю готова до впровадження гіперконвергентних рішень (HCI), NVMe over Rabrics та завдань у сфері штучного інтелекту.

Схематично це можна відобразити, як на рисунку 3.1.

3.2 Обґрунтування вибору нового обладнання

Вибір нового обладнання є ключовим етапом реінжинірингу, що безпосередньо впливає на майбутню продуктивність, надійність та сукупну

вартість володіння всієї IT-інфраструктури. Це рішення не може бути довільним, воно базується на глибокому аналізі поточного стану, виявлених проблем (розділ 2) та стратегічних цілях підприємства. Кожен обраний компонент повинен не просто усувати існуючі вузькі місця, але й створювати запас міцності для майбутнього зростання. Нижче наведено детальне обґрунтування для кожної категорії обладнання, обраного для модернізації.

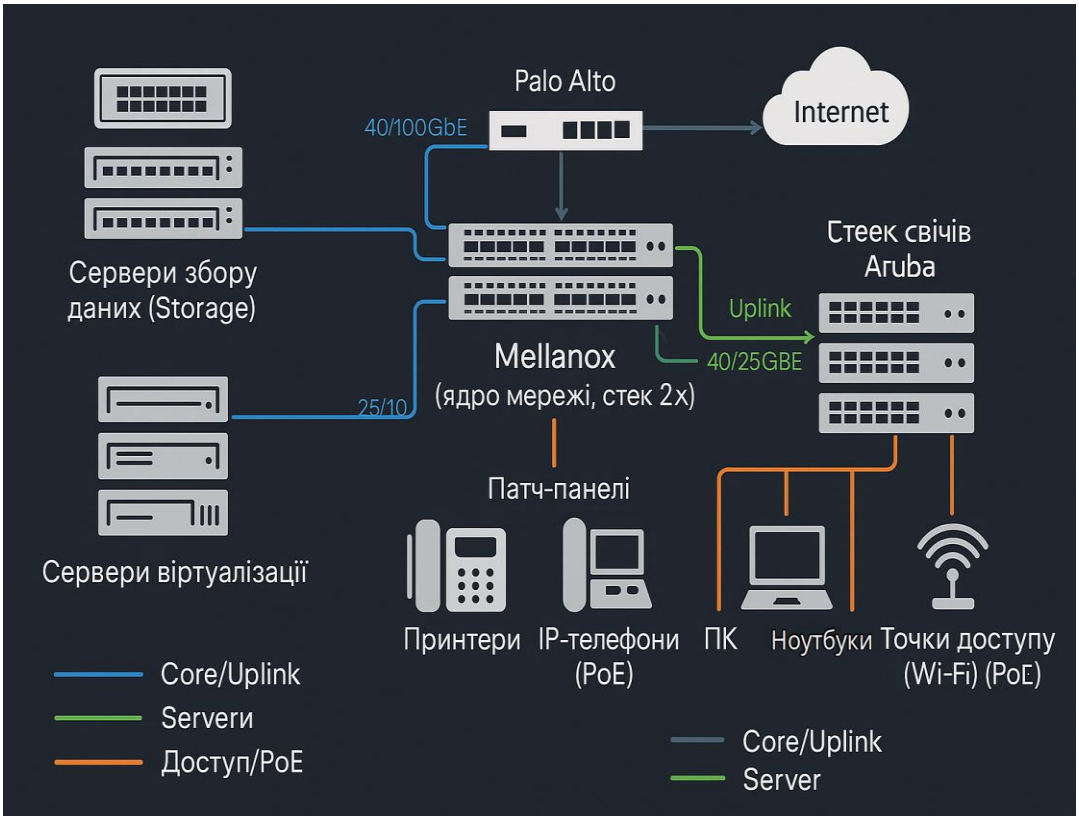

Рисунок 3.1 – Схема підключення обладнання

Виходячи з проблематики, яка була описана в розділі 2, відсутності ядра мережі через використання застарілого обладнання, а саме комутаторів HPE 1910, не мають резервування, не підтримують маршрутизацію L3 та не мають портів 10GbE, що створює критичне вузьке місце. Рішенням є створення відмовостійкого ядра мережі (Core Switches) на базі двох комутаторів HPE Aruba CX 6300M, об’єднаних у віртуальний стек за технологією Aruba VSF (Virtual Switching Framework).

Використання вищевказаних комутаторів надасть нам відмовостійкість, адже технологія VSF дозволяє двом фізичним комутаторам функціонувати як єдиний логічний пристрій. У разі відмови одного з них, другий миттєво перебирає на себе все навантаження, забезпечуючи безперебійну роботу мережі. Це повністю усуває проблему єдиної точки відмови. Комутатори серії 6300M оснащені портами 1/10/25/50GbE (SFP/SFP+/SFP28), що дозволяє реалізувати високошвидкісні оптоволоконні з'єднання з серверами, СЗД та комутаторами доступу, усуваючи існуючі вузькі місця. Наявність повноцінного функціоналу динамічної маршрутизації (OSPF) дозволяє перенести маршрутизацію між VLAN з міжмережевого екрана на ядро мережі, що значно розвантажує екран та прискорює внутрішній трафік. Модульна архітектура та можливісь стекування забезпечують легке нарощування портової ємності та продуктивності в майбутньому.

Проблематикою описаною в розділі 2 використання комутаторів ProCurve J4899B (100 Мбіт/с, EoL) та HPE 1910 (1 Гбіт/с, EoL) для підключення кінцевих користувачів, що обмежує швидкість роботи підключення кінцевих користувачів, несе ризики безпеки та не підтримує сучасні пристрої, наприклад точки доступу Wi-Fi 6 (802.11ax). Рішенням буде заміна усіх комутаторів Рівня доступу (Access Switches) на комутатори моделі HPE Aruba CX 6100.

Вибір маршрутизаторів рівня доступу є використання усіма портами підключення швидкості 1 Гбіт/с, що є стандартом для сучасних робочих місць. Кожен комутатор оснащений портами портами для аплінків 10 GbE SFP+, що дозволяє підключити його до ядра мережі по швидкісних оптоволоконних лініях, усуваючи вузьке місце між ядром та доступом. Підтримка PoE+ дозволяє живити через мережевий кабель IP-телефони, камери відеонагляду та точки доступу Wi-Fi, що спрощує інфраструктуру та зменшує кількість необхідних електричних розеток. Можливість централізованого управління всією лінійкою комутаторів Aruba через єдину платформу (наприклад, Aruba Central) спрощує адміністрування.

Базова мережа, навіть оновлена, не може ефективно впоратись із надвеликими потоками даних, які генерують системи зберігання, кластери віртуалізації та майбутні AI-завдання. Рішенням такої проблеми буде побудова окремої фізичної мережі на базі комутатора NVIDIA Spectrum-2 SN3700 та мережевих адаптерів NVIDIA ConnectX-6 Dx.

Таке рішення забезпечить швидкість підключення 100/200 Гбіт/с між серверами та СЗД, що є абсолютно недосяжним для загальноцільової мережі. Технологія RDMA over Converged Ethernet (RoCE), що підтримується і комутатором, і адаптером, дозволяє серверам обмінюватися даними безпосередньо з пам’яті, минаючи процесор та ядро ОС, що забезпечить наднизькі затримки. Створення окремої фабрики гарантує ізоляцію трафіку, тому процеси резервного копіювання, міграції віртуальних машин чи обробки великих даних ніяк не вплинуть на швидкість роботи користувачів у загальній мережі. Це забезпечує передбачуваність та стабільність роботи всієї IT-системи.

Для побудови гнучкої та ефективної інфраструктури пропонується розділити серверні ресурси на два функціональні пули: обчислювальний (Compute) та для зберігання даних (Storage).

Експлуатація серверів типу HP ProLiant Gen8, які є фізично застарілими, вкрай енергонеефективними через високе споживання електроенергії та великою тепловіддачею, мають обмежену продуктивність та здатні ефективно виконувати сучасні завдання віртуалізації та контейнеризації. Рішенням є повна або часткова заміна старих серверів на сучасні високопродуктивні моделі. В якості референтних моделей для вибору розглядаються HPE PowerEdge DL380 Gen11/Gen12, який є прямим наступником застарілих серверів HP, що забезпечує логічний шлях оновлення. Підтримує новітні процесори Intel Xeon Scalable або AMD EPYC, використовує ОЗП DDR5 та шину PCIe 5.0. Dell PowerEdge R760, один з лідерів ринку, що пропонує аналогічну високу продуктивність, гнучкість конфігурації та розширені засоби віддаленого управління (iDRAC). Asus RS500A-E12 є представником серверів на платформі AMD EPYC, що часто

пропонує краще співвідношення ціни та кількості ядер, що є ідеальним для щільної віртуалізації.

Сучасні сервери пропонують значно більш кількість ядер, підтримують швидшу оперативну пам’ять (DDR5) та новіші шини (PCIe 5.0), що може радикально підвищити продуктивність. Це дозволяє консолідувати навантаження 3-4 старих серверів на один новий, зменшуючи фізичний «слід» в серверній кімнаті та спрощуючи управління.

Нові сервери споживають значно менше електроенергії на одиницю обчислень − це прямо веде до зниження рахунків за електрику та зменшення навантаження на систему кондиціонування, що є однією з головних статей операційних витрат серверної кімнати.

Нові сервери повністю підтримують передові технології віртуалізації (включаючи апаратну підтримку), контейнеризації та безпеки (Secure Boot, TPM 2.0), що є основою для подальших кроків реінжинірингу.

Одним з основних факторів нового обладнання є поставка з повною гарантією від виробника, що мінімізує ризики простоїв та непередбачуваних витрат на ремонт.

Щодо серверів збору даних, то відсутність централізованої системи зберігання даних в конфігурації описаній в розділі 2, де дані зберігаються на локальних дисках серверів є неефективним, негнучким, ускладнює резервне копіювання та не забезпечує належного рівня відмовостійкості.

Рішенням є впровадження централізованої, високопродуктивної системи зберігання даних, яка буде основним клієнтом для високопродуктивної фабрики NVIDIA Mellanox. Розлянемо два основні підходи:

– спеціалізована СЗД (SAN Array): придбання готового рішення, наприклад All-Flash масиву з лінійок Dell PowerStore або HPE Alletra;

– програмно-визначувана СЗД (Software-Defined Storage, SDS): побудова кластера з кількох серверів (наприклад, Dell PowerEdge R7625 або аналогів з великою кількістю дискових відсіків) під управлінням ПЗ, такого як TrueNAS SCALE або Ceph.

Перехід від розрізнених локальних дисків до єдиного пулу зберігання даних значно спрощує управління, моніторинг, розподіл простору та резервне копіювання. Сучасні All-Flash СЗД забезпечують сотні тисяч операцій вводу/виводу на секунду (IOPS) з мікросекундними затримками. Це є критично важливим для баз даних, систем віртуалізації (VDI) та аналітичних додатків. Саме для реалізації цього потенціалу і була спроектована 100 GbE мережа на базі Mellanox з підтримкою RoCE.

Сучасні СЗД «з коробки» пропонують функції, недоступні для локальних дисків: миттєві знімки (Snapshots) (Для швидкого резервного копіювання та відновлення), дедуплікація та компресія (дозволяють значно зменшити фізичний обсяг даних, що зберігаються), асинхронна та синхронна реплікація (для створення катастрофостійких рішень).

Спеціалізовані СЗД мають повне резервування ключових компонентів: два контролери, що працюють в режимі active-active, дубльовані блоки живлення, мережеві порти, що підключаються до різних комутаторів фабрити Mellanox. Це забезпечує безперервність доступу до даних навіть у разі відмови одного з компонентів.

Нарощування ємності відбувається шляхом простого додавання дискових полиць до існуючої системи, без необхідності зупинки її роботи.

Вибір обладнання, розділеного на функціональні пули - обчислювальний та для зберігання даних, у поєднанні з дворівневою мережевою архітектурою є сучасним, збалансованим рішенням. Воно не тільки вирішує всі проблеми, ідентифіковані в розділі 2, але й створює надійну, масштабовану та економічно виправдану платформу, готову до викликів бізнесу на найближчі 5-7 років.

3.3 Інтеграція систем віртуалізації, контейнеризації та моніторингу

Побудована в попередніх пунктах сучасна фізична та мережева інфраструктура є лише фундаментом. Справжня ефективність, гнучкість та керованість досягаються на програмному рівні через впровадження сучасних

платформних технологій. Цей етам реінжинірингу знаменує перехід від застарілої моделі «один фізичний сервер – один додаток» до динамічного консолідованого та автоматизованого середовища. Інтеграція віртуалізації, контейнеризації та моніторингу дозволить перетворити набір апаратного забезпечення на єдиний, керований пул ресурсів, що є основою для побудови приватного хмарного середовища.

Віртуалізація є першим і найважливішим кроком у підвищенні ефективності використання апаратних ресурсів. Вона дозволяє абстрагувати обчислювальні ресурси (CPU, RAM, Storage, Network) від фізичного обладнання.

В попередньому розділі при проведенні аудиту було виявлено вкрай низький коефіцієнт утилізації застарілих серверів. Більшість серверів було завантажено на 10-15 %, споживаючи при цьому 70-80 % від своєї максимальної потужності. Це призводило до невиправданих витрат на електроенергію, охолодження та обслуговування великої кількості фізичних машин.

Рішенням даної проблеми є розгортання кластера віртуалізації на базі нових потужних серверів (HPE, Dell, Asus). В рамках дослідження розглядаються дві провідні платформи: VMware vSphere як галузевий стандарт для великих підприємств, та Proxmox Virtual Environment (VE) як потужна open-source альтернатива.

У варіанті з VMware vSphere (ESXi + vCenter) – це зріла та надійна платформа, що є де-факто стандартом у корпоративному сегменті.

Ключовими перевагами цієї системи віртуалізації є:

– висока доступність (High Availability, HA) – автоматичний перезапуск віртуальних машин на іншому справному хості у разі апаратного збою;

– «жива» міграція (vMotion) – переміщення працюючих ВМ між фізичними хостами без жодної секунди простою для проведення технічного обслуговування;

– динамічне управління ресурсами (DRS) – автоматичне балансування навантаження між хостами для забезпечення оптимальної продуктивності;

– екосистема та підтримка – найширша підтримка з боку виробників обладнання та програмного забезпечення.

Серед недоліків можна виділити високу вартість ліцензії та щорічної підтримки підтримки, що значно збільшує вартість обслуговування.

Варто розглянути систему віртуалізації Proxmox Virtual Environment – це комплексна open-source платформа, що поєднує два типи віртуалізації (KVM для повноцінних віртуальних машин та LXC для легковагих контейнерів).

Ключовими перевагами цієї системи віртуалізації є:

– нульова вартість ліцензії – продукт є безкоштовним, оплачується лише опціональна комерційна підтримка. Це радикально знижує вартість обслуговування;

– гнучкість – вбудована підтримка віртуальних машин і контейнерів в єдиному веб-інтерфейсі. Це дозволяє обирати оптимальний тип віртуалізації для кожного конкретного завдання;

– вбудовані функції – Proxmox «з коробки» надає функціонал кластеризації, високої доступності та живої міграції, що є аналогом Vmware;

– програмно-визначуване сховище – глибока інтеграція з файловою системою ZFS та розподіленим сховищем Ceph дозволяє будувати гнучкі та відмовостійкі системи зберігання даних без дорогого спеціалізованого обладнання.

Серед недоліків варто відмітити поріг входження, адже вимагає від адміністраторів глибших знань Linix та open-source технологій; екосистема, яка швидко зростає, та все ж ще менша ніж у VMware.

Обидві платформи дозволяють вирішити поставлене завдання консолідації. Вибір VMware vSphere є виправданим для організацій з великим бюджетом та існуючою експертизою. Вибір Proxmox VE є оптимальним для компаній, що прагнуть максимально знизити витрати та готові інвестувати у розвиток компетенцій своїх співробітників в open-source технологіях.

Незалежно від вибору гіпервізора, для сучасних додатків рекомендується впровадження платформи Kubernetes (K8s). Вона буде розгорнута на групі віртуальних машин, створених на попередньому етапі.

Контейнеризація є наступним еволюційним кроком, що доповнює віртуалізацію та надає ще більшу гнучкість для розробки і розгортання додатків. Традиційний підхід до розгортання додатків (один додаток на одну ВМ) все ще лишається неефективним для мікросервісної архітектури та сучасних DevOps-практик. Він повільний, вимагає багато ресурсів та ускладнює автоматизацію. Вибір розгортання платформи оркестрації контейнерів Kubernetes (K8s) є універсальним і не залежить від обраного гіпервізора. Наприклад, при розгортанні кластера Kubernetes розгортається на групі віртуальних машин, створених у кластері vSphere. Це класичний та надійний підхід. При використання Proxmox VE, кластер Kubernetes також розгортається на віртуальних машинах (KVM). Додатково, Proxmox надає унікальну можливість запускати робочі вузли Kubernetes у легковагих LXC-контейнерах, що може ще більше підвищити щільність розміщення та зменшити накладні витрати.

Перевагами інтеграції Kubernetes є ефективність використання ресурсів, адже контейнери значно «легші» за віртуальні машини. На одній віртуальній машині можна запустити десятки контейнерів, до що дозволяє досягти максимальної щільності розміщення додатків. Розгортання, оновлення та масштабування додатків у контейнерах займає секунди, а не хвилини чи години, як у випадку з ВМ. Контейнер з додатком буде однаково працювати на ноутбуці розробника, на тестовому середовищі та і продуктивному кластері. Архітектура Kubernetes не залежить від платформи віртуалізації, що забезпечує гнучкість та уникнення прив’язки до одного вендора.

Керувати сучасною, динамічною інфраструктурою без всеохоплюючого моніторингу неможливо. Система моніторингу є «нервовою системою» всієї інфраструктури.

На старому обладнанні моніторинг був відсутній або фрагментарний, тому проблеми виявлялись реактивно, вже після скарг користувачів.

Рішенням проблеми моніторингу є впровадження сучасного стеку моніторингу на базі Prometheus для збору метрик та Grafana для візуалізації. Цей стек є гнучким і може збирати дані з будь-якої інфраструктури. Стек Prometheus + Grafana дозволяє збирати метрики з усіх рівнів інфораструктури в єдину систему, незалежно від вибору гіпервізора. Через IPMI або SNMP Exporters можна проводити моніторинг серверів та комутаторів, через що можна відслідковувати роботу фізичного обладнання. Prometheus легко інтегрується з обома системами гіпервізора за допомогою спеціалізованих «експортерів» – vSphere VM Exporter та Proxmox VE Exporter відповідно. Обидва експортери надають детальні метрики про стан хостів, віртуальних машин, сховищ та кластера в цілому. Моніторинг кластера Kubernetes та додатків є нативним та абсолютно ідентичним для обох сценаріїв.

Система сповіщення Prometheus дозволяє налаштувати гнучкі правила для сповіщень, попереджаючи про проблеми до того, як вони вплинуть на користувачів.

Grafana може одночасно підключатись до різних джерел даних, дозволяючи створювати єдині інформаційні панелі, які відображатимуть стан всієї інфраструктури (наприклад, стан Proxmox-кластера та метрики Kubernetes на одному екрані).

Послідовна інтеграція систем віртуалізації, контейнеризації та моніторингу перетворює оновлену серверну кімнату на єдиний, узгоджений організм. Це створює гнучку, відмовостійку, ефективну та прозору платформу, яка не тільки вирішує поточні проблеми бізнесу, але й закладає міцний технологічний фундамент для майбутніх інновацій.

3.4 Вибір та налаштування систем автоматизації управління IT-інфраструктурою

Створення сучасної інфраструктури на базі віртуалізації та контейнеризації неминуче призводить до зростання складності. Ручне

управління десятками віртуальних машин, сотнями контейнерів та мережевими конфігураціями стає неефективним, повільним та джерелом людських помилок. У даному пункті розглянемо перехід від ручного, імперативного підходу до сучасної парадигми «Інфраструктура як Код» (Infrastructure as Code, IaC).

IaC – це підхід до управління та виділення ресурсів інфраструктури через файли конфігурації, які читаються машиною, а не через ручне налаштування чи інтерактивні інструменти. Проблеми ручного налаштування призводять до «дрейфу конфігурацій», коли середовища розробки, тестування та експлуатації починають відрізнятись одне від одного. Це спричиняє помилки при розгортанні та ускладнює діагностику. Процес розгортання нового сервера є повільним та погано документованим.

Рішенням такої проблеми є впровадження стеку інструментів автоматизації, які дозволяють описати всю інфраструктуру – від віртуальних машин до правил брандмауера – у вигляді коду. Цей код зберігається в системі контролю версій (наприклад, Git) разом із кодом додатків.

Ключовими перевагами IaC є відтворюваність та консистентність, як гарантія того, що кожне середовище, розгорнуте за одним і тим же кодом, буде абсолютно ідентичним. Автоматичне розгортання десятків ВМ та контейнерів за лічені хвилини замість годин ручної роботи надасть швидкість та ефективність виконання завдань. За контролем версій та аудит відповідає зберігання коду інфраструктури в Git та дає повну історію змін: хто, коли і що саме змінив. Це спрощує відкат до попередніх версій та забезпечує прозорий аудит. Код сам по собі є точною та завжди актуальною документацією інфраструктури.

Для реалізації IaC пропонується використовувати дворівневий стек інструментів, де кожен інструмент вирішує своє специфічне завдання.

Рівень 1 – виділення ресурсів (Provisioning).

Terraform – це інструмент для безпечного та ефективного створення, зміни та версіювання інфраструктури. Завданням для цього інструменту є створення «сирих» ресурсів: віртуальних машин у кластері VMware або Proxmox, мережевих VLAN на комутаторах Aruba, DNC-записів, правил брандмауера

тощо.

Вибір Terraform обгрунтований декларативним підходом, адже ви описуєте бажаний кінцевий стан інфраструктури, а Terraform сам визначає, які дії (створити, змінити, видалити) потрібно виконати, щоб досягти цього стану. Мультиплатформність Terraform працює через «провайдерів» і має підтримку практично будь-якого обладнання та ПЗ, включаючи VMware vSphere, Proxmox VE, мережеве обладнання, хмарні сервіси. Це забезпечує гнучкість та унеможливлює прив’язку до одного вендора. Terraform веде файл стану (state file), в якому зберігає інформацію про створені ресурси. Це дозволяє йому планувати та безпечно застосовувати інкрементальні зміни.

Рівень 2 – управління конфігурацією (Configuration Management).

Після того, як Terraform створив віртуальну машину, Ansible «входить всередину» і налаштовує її. Завданням Ansible є встановлення та налаштування ПЗ (веб-сервери, бази даних), управління конфігураційними файлами, застосування оновлень безпеки, створення користувачів, управління сервісами.

Вибором в користь Ansible є безагентна архітектура, адже не потребує встановлення клієнтського ПЗ на керовані сервери. Ansible працює через стандартні протоколи SSH (для Linux) та WinRM (для Windows), що значно спрощує розгортання та обслуговування. Сценарії автоматизації (playbooks) пишуться на мові YAML, яка є легкою для читання та вивчення навіть для непрограмістів. Фундаментальною властивістю Ansible є ідемпотентність, тобто запуск одного і того є сценарію кілька разів призведе до того ж самого результату, що і перший запуск. Якщо пакет вже встановлено, Ansible не буде його встановлювати знову. Це робить операції безпечними та передбачуваними. Велика кількість готових модулів та шаблонів автоматизації на порталі Ansible Galaxy дозволяє не «винаходити велосипед» для типових завдань.

Кінцевою метою є повна автоматизація процесу внесення змін до інфраструктури за допомогою конвеєра безперервної інтеграції та доставки (CI/CD).

Налаштування та інтеграція процесів управління інфраструктурою

здійснюється на основі створення конвеєра CI/CD із використанням принципів GitOps. Кінцевою метою такого підходу є повна автоматизація внесення змін до інфраструктури за допомогою інструментів безперервної інтеграції та доставки, що забезпечує стабільність, повторюваність і передбачуваність усіх операцій. Для реалізації цього завдання можуть застосовуватися популярні системи CI/CD, зокрема GitLab CI/CD або Jenkins.

GitOps-підхід передбачає, що інженери не взаємодіють безпосередньо з віртуалізаційними платформами, такими як vCenter чи Proxmox. Усі зміни виконуються шляхом редагування коду інфраструктури, написаного за допомогою Terraform або Ansible, у локальній копії Git-репозиторію. Після цього формується Merge Request, який запускає відповідний конвеєр CI/CD.

На початковому етапі конвеєр автоматично виконує валідацію коду. Цей процес включає перевірку синтаксичних помилок та аналіз відповідності коду визначеним стандартам, що дозволяє уникнути помилок ще до виконання змін у середовищі. Якщо перевірка пройшла успішно, система переходить до етапу планування, де виконується команда «terraform plan». Результатом є детальний опис майбутніх змін в інфраструктурі, який автоматично додається у вигляді коментаря до Merge Request.

Після цього зміни проходять командне рецензування. Інші члени команди аналізують як сам код, так і запропонований план його виконання. Такий механізм ґрунтується на принципі «чотирьох очей» і дозволяє виявляти можливі помилки або небажані наслідки ще до фактичного внесення змін у систему.

Заключним етапом є застосування змін. Після схвалення та злиття Merge Request у головну гілку репозиторію CI/CD-конвеєр автоматично виконує команду «terraform apply», що реалізує внесені зміни у реальну інфраструктуру. Одразу після цього запускається сценарій Ansible, який здійснює налаштування та конфігурацію компонентів, забезпечуючи повну готовність середовища до роботи.

3.5 Методика оцінювання ефективності впроваджених рішень

Після розробки та імплементації комплексних рішень з реінжинірингу серверної кімнати, ключовим етапом є об’єктивна та вимірювана оцінка їх ефективності. Цей процес не може базуватися на суб’єктивних відчуттях; він вимагає чіткої методики, як дозволить кількісно порівняти показники функціонування інфраструктури «до» та «після» модернізації. Мета даної методики – визначити, наскільки були досягнуті цілі реінжинірингу, та надати дані для розрахунку економічної доцільності проєкту. Оцінка буде проводитись за чотирма ключовими напрямками: технічна продуктивність, економічна ефективність, надійність та операційна ефективність.

Оцінка технічної продуктивності та швидкодії є одним із ключових етапів аналізу ефективності модернізованої IT-інфраструктури. Основна мета цього блоку полягає у визначенні того, наскільки швидшою, стабільнішою та чутливішою стала система після впровадження змін. Для цього застосовуються ключові показники ефективності (KPI), які дозволяють здійснити комплексну оцінку роботи інфраструктури на різних рівнях.

До основних показників відноситься пропускна здатність мережі, що визначається як середня та пікова швидкість передачі даних між ключовими вузлами: сервер-сервер, сервер-система зберігання даних, ядро-доступ. Важливим параметром також є затримка мережі (latency), яка характеризує час проходження пакету між серверами. Особливу увагу приділяється вимірюванню цього показника у високопродуктивній мережевій фабриці Mellanox, що є критичною для ефективності обробки даних.

Окремо оцінюється продуктивність системи зберігання даних. Для цього визначається кількість операцій вводу/виводу на секунду (IOPS), а також середній час відгуку системи зберігання у мілісекундах. Такі показники дозволяють оцінити, наскільки швидко система здатна обробляти запити користувачів і бізнес-додатків.

Ще одним важливим аспектом є час розгортання віртуальної машини. Він

вимірюється від моменту запуску автоматизованого скрипта Terraform до повної готовності віртуальної інфраструктури до експлуатації. Це дає можливість визначити ефективність використання інструментів інфраструктури як коду (IaC) та їхню роль у прискоренні бізнес-процесів.

Не менш важливим є показник часу відгуку бізнес-додатків. Він характеризує швидкість завантаження та доступність критично важливих програмних рішень для кінцевого користувача, що безпосередньо впливає на якість роботи співробітників та ефективність бізнес-процесів.

Для збору даних та проведення вимірювань використовуються спеціалізовані інструменти. У сфері оцінки роботи мережі застосовується утиліта iperf3 для вимірювання пропускної здатності, а також ping і mtr для визначення затримок. Додатково показники збираються з системи моніторингу Prometheus за допомогою SNMP Exporter, який інтегрується з мережевим обладнанням.

Продуктивність систем зберігання аналізується за допомогою вбудованих засобів моніторингу СЗД, а також спеціалізованих утиліт тестування дискової підсистеми, таких як fio або CrystalDiskMark. У сфері віртуалізації та моніторингу бізнес-додатків дані отримуються з журналу подій системи автоматизації, зокрема GitLab CI/CD, а також з комплексів моніторингу Prometheus та Grafana.

Оцінка економічної ефективності та сукупної вартості володіння (TCO) є важливим етапом аналізу результатів модернізації IT-інфраструктури. Метою цього блоку є визначення прямого фінансового ефекту від впроваджених змін, а також виявлення факторів, які впливають на зменшення витрат, оптимізацію ресурсів і підвищення рентабельності експлуатації серверної інфраструктури.

Одним із ключових показників ефективності є загальне енергоспоживання серверної кімнати, що вимірюється в кВт/год за певний період (зазвичай за місяць). Оптимізація цього параметра дозволяє зменшити витрати на електроенергію, що безпосередньо впливає на загальну вартість володіння інфраструктурою.

Ще одним важливим показником є PUE (Power Usage Effectiveness) – коефіцієнт ефективності використання енергії. Він визначається як співвідношення загальної кількості спожитої енергії до обсягу електроенергії, що безпосередньо використовується IT-обладнанням. Зменшення значення PUE свідчить про підвищення енергоефективності, особливо у частині роботи системи охолодження та допоміжної інфраструктури серверної кімнати.

Крім того, аналізується коефіцієнт консолідації, який визначає співвідношення кількості віртуальних машин до кількості фізичних серверів. Вищий показник свідчить про ефективніше використання апаратних ресурсів та зменшення витрат на придбання, обслуговування й утримання фізичного обладнання.

Важливим критерієм також є використання площі в серверній кімнаті, яке вимірюється за кількістю зайнятих юнітів (U) у серверних стійках. Оптимізація цього параметра дозволяє ефективніше використовувати фізичний простір, знижуючи потребу у додаткових стійках і витратах на розширення інфраструктури.

Для отримання достовірних даних застосовуються спеціалізовані методи та інструменти. Вимірювання енергоспоживання здійснюється за допомогою інтелектуальних блоків розподілу живлення (Smart PDU), даних із лічильників електроенергії та рахунків від постачальника. Коефіцієнт консолідації та показники використання площі визначаються на основі інформації, отриманої з систем віртуалізації vCenter або Proxmox, а також результатів фізичної інвентаризації обладнання.

Оцінка надійності та доступності є важливим етапом аналізу ефективності модернізованої IT-інфраструктури. Основна мета цього блоку полягає у визначенні того, наскільки стабільнішою, безперервнішою та відмовостійкішою стала система після впровадження змін. Оцінка проводиться на основі ключових показників ефективності (KPI), що дозволяють комплексно дослідити працездатність сервісів та їхню готовність до використання кінцевими користувачами.

Одним із головних показників є час безвідмовної роботи (Uptime), який визначає відсоток часу, протягом якого критично важливі сервіси були доступні для користувачів. Цільовий рівень доступності складає 99,9 % і вище, що відповідає високим стандартам безперервності бізнес-процесів.

Uptime відображає відсоток часу, протягом якого система або критично важливі сервіси залишаються доступними для користувачів.

Формула розрахунку (3.1):

$$\text{Uptime (\%)} = (1 - T_{downtime} / T_{total}) \times 100, \quad (3.1)$$

де Tdowntime – сумарний час простою системи за визначений період, год;

Ttotal – загальний час спостереження за системою, год;

Uptime показує відсоток часу, протягом якого система або сервіс були доступними для користувачів. Чим вищий показник, тим стабільніше функціонує інфраструктура. У сучасних корпоративних середовищах прийнятним вважається рівень доступності 99,9 % і вище.

Наведемо приклад розрахунку.

Згідно з формулою (3.1) протягом місяця (Ttotal = 720 годин) сервер був недоступний протягом 2 годин (Tdowntime = 2): Uptime = (1 − 2 / 720) × 100 = 99,72 %.

Це означає, що за місяць система працювала стабільно протягом 99,72 % часу, що відповідає високим стандартам доступності.

Іншим ключовим показником є середній час між відмовами (MTBF – Mean Time Between Failures), який визначає середній проміжок часу між інцидентами, що потребують втручання спеціалістів. Чим вищий показник MTBF, тим стабільніше функціонує інфраструктура.

Формула розрахунку (3.2):

$$MTBF = T_{operational} / N_{failures}, \quad (3.2)$$

де Toperational − загальний час роботи системи, год;

Nfailures − кількість зареєстрованих інцидентів або відмов за аналізований період;

MTBF характеризує середній проміжок часу між критичними відмовами системи. Високий показник свідчить про стабільність роботи інфраструктури та меншу ймовірність виникнення інцидентів.

Наведемо приклад розрахунку згідно формули (3.2).

За квартал серверна інфраструктура працювала 1800 годин (Toperational = 1800), за цей час було зафіксовано 3 відмови (Nfailures = 3): MTBF = 1800 / 3 = 600 годин.

Це означає, що система в середньому працювала 600 годин без збоїв, що є показником високої надійності.

Також важливим є середній час відновлення (MTTR – Mean Time To Recovery), який характеризує швидкість відновлення працездатності системи після збою. Завдяки впровадженню механізмів автоматичного перемикання у режим високої доступності (HA) та покращеним інструментам діагностики, цей показник можна суттєво знизити, що позитивно впливає на загальний рівень доступності сервісів.

Формула розрахунку (3.3):

$$MTTR = \Sigma Trepair / Nfailures, \quad (3.3)$$

де ΣTrepair – сумарний час, витрачений на усунення відмов, год;

Nfailures – кількість зареєстрованих інцидентів за період;

MTTR показує середній час, необхідний для відновлення працездатності системи після збою. Зменшення цього показника є критичним для забезпечення високої доступності сервісів та мінімізації негативного впливу на бізнес-процеси.

Приклад розрахунку згідно з формулою (3.3) наступний: за три місяці виникало 3 інциденти, на усунення яких було витрачено 4, 3 та 5 годин

відповідно: MTTR = (4 + 3 + 5) / 3 = 12 / 3 = 4 години.

Це означає, що середній час відновлення сервісів після збою становить 4 години, що є прийнятним показником для більшості корпоративних середовищ.

Для збору даних та оцінки показників використовуються сучасні інструменти моніторингу. Основним джерелом є система Prometheus у поєднанні з Grafana, які надають детальні дашборди доступності та історію сповіщень про інциденти. Крім того, проводиться аналіз журналів інцидентів, що дозволяє визначити частоту виникнення збоїв, час реагування та ефективність заходів щодо усунення проблем.

Оцінка операційної ефективності та автоматизації є важливим етапом аналізу впливу модернізації IT-інфраструктури на роботу технічного персоналу та швидкість виконання повсякденних завдань. Мета цього блоку полягає у визначенні того, наскільки знизилося навантаження на IT-фахівців, покращилась якість процесів і прискорилось виконання типових операцій завдяки впровадженню автоматизації.

Одним із основних показників ефективності є час виконання типових завдань. Він характеризує тривалість операцій, необхідних для розгортання нових сервісів, застосування патчів безпеки, створення тестових середовищ та інших рутинних дій. Зменшення цього показника є свідченням підвищення продуктивності та ефективності роботи IT-команди.

Ще одним важливим критерієм є кількість ручних операцій. Для оцінки цього параметра використовується співвідношення між кількістю завдань, виконаних автоматично за допомогою конвеєрів CI/CD, та завдань, що потребували ручного втручання фахівців. Зростання рівня автоматизації дозволяє знизити ризик помилок, оптимізувати робочий час персоналу та підвищити надійність виконання завдань.

Окремо оцінюється показник кількості помилок, пов’язаних із людським фактором. Його зменшення свідчить про підвищення стабільності інфраструктури, оскільки автоматизація процесів, зокрема впровадження принципів Infrastructure as Code (IaC), значно скорочує кількість інцидентів,

викликаних неправильною конфігурацією або некоректними діями персоналу.

Для збору та аналізу даних використовуються спеціалізовані інструменти. Журнали систем автоматизації, таких як GitLab CI/CD або Jenkins, дозволяють визначити час виконання завдань і ефективність роботи конвеєрів. Система контролю версій Git використовується для аналізу історії комітів і підтвердження виконання змін через підхід IaC. Додатково оцінюється статистика із внутрішньої системи запитів, що дозволяє порівняти кількість і типи заявок на технічну підтримку до та після модернізації інфраструктури.

Запропонована методика створює прозору та комплексну систему для вимірювання успішності проєкту реінжинірингу. Вона дозволяє перейти від загальних фраз «стало краще» до конкретних цифр, які демонструють покращення в продуктивності, зниження витрат та підвищення стабільності. Дані, зібрані згідно з цією методикою, стануть основою для наступних етапів аналізу, включаючи розрахунок економічної доцільності та оцінку потенціалу для подальшого масштабування інфраструктури.

3.6 Пілотне тестування рішень, аналіз показників до і після модернізації та оцінка потенціалу масштабування

Теоретичне обґрунтування та розробка технічних рішень є лише першою частиною комплексного проєкту модернізації IT-інфраструктури. Для підтвердження ефективності обраних підходів, перевірки їхньої працездатності та виявлення можливих недоліків доцільним є проведення етапу пілотного тестування. Такий підхід дозволяє застосувати розроблену методику оцінювання (п. 3.5) у реальних умовах, отримати фактичні результати роботи системи, порівняти їх із показниками старої інфраструктури та об’єктивно оцінити потенційні переваги нової архітектури.

Мета пілотного проєкту полягає у перевірці працездатності, продуктивності та керованості оновленої IT-інфраструктури на прикладі реального бізнес-додатку у контрольованому середовищі. Такий підхід дозволяє

мінімізувати ризики, забезпечити передбачуваність результатів та виявити можливі проблеми ще до повномасштабного впровадження.

Для тестування було обрано додаток, який відповідає ключовим критеріям:

– некритичність для бізнесу – тимчасова недоступність сервісу під час проведення міграції не спричиняє значних фінансових втрат або зупинки бізнес-процесів;

– репрезентативність – обраний додаток має типову архітектуру, наприклад, поєднання веб-сервера та бази даних, що забезпечує реалістичне моделювання навантаження, подібного до інших корпоративних систем;

– можливість вимірювання продуктивності – показники роботи додатку можуть бути легко зафіксовані, зокрема, час завантаження веб-сторінок, кількість оброблених транзакцій або швидкість обміну даними.

В якості прикладу було обрано внутрішній корпоративний портал компанії, який використовується для тестування, розробки та внутрішньої взаємодії між підрозділами.

На початковому етапі здійснюється збір базових показників продуктивності пілотного додатку на існуючій інфраструктурі. Ці дані формують контрольні значення для подальшого порівняння результатів, згідно з методикою, описаною у п. 3.5.

Для створення інфраструктури нового середовища використовується платформа віртуалізації VMware або Proxmox. Розгортання віртуальних машин, налаштування мережевої взаємодії та конфігурація серверів виконуються за допомогою інструментів Terraform та Ansible, що забезпечує високу швидкість і передбачуваність процесу.

На етапі «міграція даних та конфігурацій» виконується перенесення баз даних, файлів і налаштувань додатку з попередньої інфраструктури на нове середовище. Забезпечується цілісність даних та коректність бізнес-логіки.

Після розгортання додаток запускається в тестовий продуктивний режим на визначений період, зазвичай від двох до чотирьох тижнів. Протягом цього часу здійснюється активний збір метрик за допомогою системи моніторингу

Prometheus у поєднанні з дашбордами Grafana. Відстежуються ключові показники продуктивності, стабільності та доступності сервісу.

По завершенню тестового періоду результати аналізуються та порівнюються з вихідними значеннями. На основі отриманих даних робиться висновок про доцільність масштабного впровадження нової інфраструктури.

На основі даних, зібраних до початку реінжинірингу та під час пілотного тестування, формується порівняльна таблиця (табл. 3.1), що наочно демонструє ефект від впроваджених рішень.

Таблиця 3.1 – Порівняльна таблиця реінжинірингу

Напрямок / Показник	Стан «До» (стара інфраструктура)	Стан «Після» (нова інфраструктура)	Зміна (%)
Технічна продуктивність			
Час відгуку додатку	850 мс	150 мс	↓ 82 %
IOPS СЗД (пікове)	~ 1,200 IOPS (локальні HDD)	> 50,000 IOPS (All-Flash СЗД)	↑ >4000 %
Пропускна здатність (сервер-СЗД)	1 Гбіт/с	100 Гбіт/с (Mellanox Fabric)	↑ 9900 %
Економічна ефективність			
Енергоспоживання (3 сервери)	~ 1.5 кВт·год	~ 0.6 кВт·год (1 новий сервер)	↓ 60 %
Зайнятий простір у стійці	6U (3 сервери по 2U)	2U (1 сервер)	↓ 67 %
Час відновлення після збою хоста	2-4 години (ручне відновлення)	< 5 хвилин (автоматичне HA)	↓ 98 %
Операційна ефективність			
Час розгортання нового сервера	1-2 дні (ручне налаштування)	~ 15 хвилин (Terraform + Ansible)	↓ >99 %
Кількість ручних втручань	Постійно	Мінімально (через GitOps)	↓

Дані з таблиці беззаперечно свідчать про досягнення поставлених цілей. Нова інфраструктура демонструє кардинальне зростання продуктивності, значне зниження операційних витрат та підвищення надійності. Автоматизація практично повністю виключає ручну роботу при виконанні типових завдань.

Оцінка потенціалу масштабування інфраструктури є одним із ключових

аспектів реінжинірингу, оскільки головна мета модернізації полягає не лише у підвищенні продуктивності, але й у створенні гнучкої системи, здатної ефективно реагувати на зростання потреб бізнесу. Нова архітектура забезпечує підтримку масштабування на кількох рівнях, що дозволяє оптимально використовувати наявні ресурси та швидко адаптуватися до зміни навантажень.

Першим напрямком є вертикальне масштабування (Scale-Up). Завдяки використанню сучасних платформ віртуалізації, таких як vCenter або Proxmox, збільшення обчислювальних ресурсів (CPU, RAM) для існуючої віртуальної машини здійснюється в кілька кліків у вебінтерфейсі. У більшості випадків така операція не потребує перезавантаження віртуальної машини, що значно підвищує зручність та швидкість виконання змін. Для порівняння, у старій інфраструктурі розширення ресурсів вимагало фізичної зупинки сервера, встановлення додаткового обладнання та виконання тривалих налаштувань. Крім того, нова архітектура надає можливість не лише додавати, а й вилучати ресурси, повертаючи їх у загальний пул для повторного використання іншими сервісами.

Другим ключовим напрямком є горизонтальне масштабування (Scale-Out). Додавання нового фізичного сервера до кластера віртуалізації VMware або Proxmox виконується за стандартизованою процедурою, що не потребує складної інтеграції. Новий хост автоматично стає частиною загального пулу ресурсів, підвищуючи сумарну продуктивність інфраструктури та рівень її відмовостійкості. Для додатків використовується платформа Kubernetes, яка забезпечує автоматичне горизонтальне масштабування контейнеризованих сервісів за допомогою механізму Horizontal Pod Autoscaler. Це дозволяє системі динамічно створювати додаткові копії контейнерів під час зростання навантаження та автоматично скорочувати їх кількість, коли потреба у ресурсах зменшується. Такий підхід гарантує високу ефективність використання обчислювальних потужностей.

Окрему увагу приділено можливостям масштабування мережевої інфраструктури та системи зберігання даних (СЗД). Завдяки архітектурі типу

«Ядро-Доступ» інтеграція нових комутаторів доступу виконується швидко та без ускладнень, оскільки вони підключаються безпосередньо до наявного ядра мережі. Крім того, високопродуктивна комутаційна фабрика Mellanox проєктувалася з урахуванням можливості подальшого розширення, що дозволяє збільшувати пропускну здатність мережі без суттєвої перебудови інфраструктури. У системі зберігання даних реалізовано концепцію «масштабування на льоту»: додавання нових дискових полиць або розширення наявних сховищ виконується без зупинки роботи, що забезпечує безперервність бізнес-процесів та швидке реагування на зростання обсягу даних.

Нова інфраструктура перетворює статичний та обмежений набір серверів на динамічну, еластичну платформу, подібну до публічної хмари. Вона здатна гнучко та швидко адаптуватися до будь-яких змін у потребах бізнесу, будь то запуск нового проєкту чи сезонне зростання навантаження, що було абсолютно неможливо на старому обладнанні.

3.7 Економічна доцільність впровадження

Будь-який інфраструктурний проєкт, незалежно від його технічної досконалості, повинен бути економічно виправданим. Цей пункт присвячений фінансовому аналізу проєкту реінжинірингу, метою якого є довести, що запропоновані інвестиції не є просто витратами, а є вигідним вкладенням, яке принесе пряму та непряму економічну вигоду для підприємства. Аналіз буде базуватися на розрахунку ключових фінансових показників: сукупної вартості володіння (Total Cost of Ownership, TCO) та повернення інвестицій (Return on Investment, ROI).

Капітальні витрати (CapEx) являють собою одноразові інвестиції, спрямовані на придбання апаратного забезпечення, програмних ліцензій та послуг, необхідних для реалізації проєкту модернізації IT-інфраструктури. Вони формують основний обсяг фінансування, що забезпечує створення оновленої серверної архітектури, мережевої інфраструктури та системи зберігання даних.

Основна частина витрат була спрямована на оновлення серверного обладнання, системи зберігання даних та мережевих компонентів. Для побудови високопродуктивного середовища віртуалізації було закуплено три обчислювальні сервери корпоративного класу (Dell, HPE або Asus) орієнтовною вартістю ~30 000 USD. Додатково було інвестовано ~25 000 USD у впровадження сучасної системи зберігання даних (СЗД) типу All-Flash, що забезпечує високу швидкість обробки та доступу до даних.

Для побудови продуктивної мережевої інфраструктури передбачено оновлення мережевого ядра за допомогою двох комутаторів Aruba CX 6300M, що становить ~15 000 USD, а також розширення мережі доступу шляхом встановлення чотирьох комутаторів Aruba CX 6100 із загальною вартістю ~8 000 USD.

Додатково було інвестовано у створення високошвидкісної мережевої фабрики Mellanox, що складається з одного центрального комутатора NVIDIA Spectrum та чотирьох адаптерів ConnectX-6. Загальні витрати на цей компонент становили ~20 000 USD. До капітальних витрат також включено придбання пасивного мережевого обладнання – патч-панелей, органайзерів та кабелів – на суму ~5 000 USD.

Таким чином, загальні витрати на апаратне забезпечення склали приблизно 103 000 USD.

Для забезпечення роботи віртуалізаційного середовища передбачено придбання ліцензій VMware vSphere Essentials Plus Kit на три сервери-хости загальною вартістю ~6 000 USD. Водночас, у разі вибору альтернативної платформи Proxmox VE, вартість ліцензій може бути нульовою. Однак у такому випадку необхідно врахувати витрати на щорічну підписку на технічну підтримку, що орієнтовно становить ~3 000 USD на рік.

Загальні витрати на програмне забезпечення склали близько 6 000 USD.

Якщо для реалізації проєкту залучаються сторонні підрядники, до капітальних витрат включаються послуги з монтажу, налаштування та міграції даних. Орієнтовна вартість таких робіт становить ~5 000 USD.

Загальні капітальні витрати на реалізацію проєкту становлять:

CapEx = 103 000 USD (апаратне забезпечення) + 6 000 USD (програмне забезпечення) + 5 000 USD (послуги) = 114 000 USD.

Ці інвестиції дозволяють забезпечити надійну основу для побудови сучасної, масштабованої та високопродуктивної IT-інфраструктури, яка здатна підтримувати подальший розвиток підприємства.

OpEx – це регулярні витрати, необхідні для підтримки та функціонування інфраструктури. Тут ми спостерігаємо основний ефект економії (табл. 3.2).

Таблиця 3.2 – Таблиця порівняння регулярних витрат

Стаття витрат	«До» (стара інфраструктура, 10 серверів Gen8)	«Після» (нова інфраструктура, 3 сервери + СЗД)	Річна економія
Електроенергія	(10 серверів * 0.5 кВт * 24 год * 365 днів) * $0.15/кВт·год = $6,570	(3 сервери * 0.3 кВт + 0.6 кВт СЗД) * 24 * 365 * $0.15 = $1,971	$4,599
Охолодження (прибл. 40 % від вартості енергії IT)	$6,570 * 0.4 = $2,628	$1,971 * 0.4 = $788	$1,840
Підтримка та ризики (вартість простоїв, пошук EoL запчастин)	Оціночно ~ $10,000 / рік	Гарантійна підтримка включена у вартість (перші 3 роки) ~ $0	$10,000
Адміністративні витрати (час персоналу на ручне керування)	0.5 FTE * $30,000/рік = $15,000	0.1 FTE * $30,000/рік = $3,000 (завдяки автоматизації)	$12,000
Разом річні OpEx	$34,198	$5,759	$28,439

Нова інфраструктура дозволяє досягти щорічної економії операційних витрат у розмірі ~$28,500.

Для оцінки економічної ефективності проєкту реінжинірингу IT-інфраструктури було проведено розрахунок показників окупності та рентабельності інвестицій. Ключовим фактором є сукупна економія витрат підприємства протягом п’ятирічного періоду експлуатації нової інфраструктури. Розрахунки показують, що прогнозована економія становить приблизно $28,439 на рік, а за п’ять років – $142,195.

Чистий прибуток від реалізації проєкту визначається як різниця між сумарною економією та загальними інвестиціями. Формула розрахунку має вигляд (3.4):

$$\text{Net Profit} = \text{Загальна економія} - \text{Загальні інвестиції}. \quad (3.4)$$

Підставивши відповідні значення згідно формули (3.4), отримаємо: Net Profit = \$142,195 – \$114,000 = \$28,195.

Рентабельність інвестицій (ROI) відображає ефективність вкладених коштів та розраховується за формулою (3.5):

$$\text{ROI} = (\text{Net Profit} / \text{Загальні інвестиції}) * 100\ \%. \quad (3.5)$$

Виконуючи розрахунок за формулою (3.5), отримуємо: ROI = (\$28,195 / \$114,000) * 100 % = 24,7 %.

Таким чином, за п’ятирічний період впровадження нового рішення проєкт демонструє рентабельність майже 25 %, що є позитивним показником для IT-інвестицій.

Крім того, було визначено термін окупності інвестицій (Payback Period), який показує, за який період проєкт компенсує початкові витрати. Формула розрахунку має вигляд (3.6):

$$\text{Payback Period} = \text{Загальні інвестиції} / \text{Річна економія}. \quad (3.6)$$

Отже, термін окупності, згідно формули (3.6), становить: Payback Period = \$114,000 / \$28,439 ≈ 4,0 роки.

Слід зазначити, що отриманий показник окупності є консервативним, оскільки не враховує непрямі вигоди, такі як підвищення продуктивності бізнес-процесів, зниження ризиків простоїв, скорочення витрат на підтримку застарілої інфраструктури та уникнення потенційних репутаційних втрат.

Попри значні початкові інвестиції, загальна вартість володіння (TCO) новою IT-інфраструктурою протягом п’ятирічного періоду є суттєво нижчою, ніж витрати на підтримку існуючої застарілої системи. Різниця становить близько $28,000 на користь модернізованої інфраструктури. Це свідчить про ефективність переходу на оновлену архітектуру та підтверджує довгострокову економічну вигоду від впровадження проєкту.

Результати розрахунків демонструють, що проєкт реінжинірингу серверної кімнати є економічно доцільним та фінансово обґрунтованим. Модернізація не лише суттєво підвищує надійність, масштабованість та ефективність IT-інфраструктури, але й забезпечує відчутну фінансову вигоду за рахунок зниження операційних витрат.

Отримані показники ROI та скорочення TCO підтверджують, що реалізація проєкту – це не просто витрати на IT, а стратегічна інвестиція у підвищення безперервності бізнес-процесів, мінімізацію ризиків та створення фундаменту для подальшого розвитку компанії.

ВИСНОВКИ

Проведене дослідження шляхів реінжинірингу серверної кімнати дозволило розробити комплексну, технічно обґрунтовану та економічно доцільну модель модернізації, яка вирішує ключові проблеми застарілих IT-інфраструктур та створює фундамент для подальшого цифрового розвитку підприємства.

У ході виконання роботи було вирішено поставлені завдання та отримано такі основні наукові й практичні результати:

– досліджено та діагностовано критичні проблеми типової застарілої IT-інфраструктури, серед яких: апаратна застарілість обладнання (End-of-Life), що створює загрози безпеці; відсутність відмовостійкості через наявність єдиних точок відмови (SPOF); високі операційні витрати через низьку енергоефективність; та обмежена продуктивність, що гальмує роботу бізнес-додатків;

– спроектовано комплексну, багаторівневу модель реінжинірингу. На фізичному рівні вона включає гібридну інфраструктуру з дворівневою мережевою архітектурою (General Purpose та High-Performance Fabric) та спеціалізованими пулами серверів. На логічному рівні – гнучку програмно-визначувану платформу, що трансформує фізичні ресурси в єдиний керований пул;

– розроблено модель повної автоматизації управління на основі парадигми «Інфраструктура як Код» (IaC). Запропоновано використання дворівневого стеку інструментів (Terraform та Ansible), інтегрованого у GitOps-процес на основі CI/CD-конвеєра, що перетворює будь-які зміни в інфраструктурі на прозорий, контрольований та документований процес;

– запропоновано та застосовано методику кількісної оцінки ефективності, що дозволила об’єктивно порівняти показники до і після модернізації за технічними, економічними та операційними критеріями;

– реалізовано практичну валідацію запропонованої моделі через пілотне

тестування, яке підтвердило дієвість розроблених рішень;

– візуалізовано та проаналізовано результати, які кількісно підтвердили успішність проєкту. Аналіз показав кардинальне зростання технічної продуктивності (скорочення часу відгуку на 82 %, зростання IOPS у 40 разів), економічну доцільність (зниження витрат на електроенергію на 60 %, нижчий ТСО) та операційну ефективність (скорочення часу розгортання сервера з днів до хвилин).

Практична значущість отриманих результатів полягає в тому, що розроблена модель є універсальною дорожньою картою для підприємств, що прагнуть модернізувати свою ІТ-інфраструктуру. Її впровадження дозволяє трансформувати застарілу серверну кімнату з ризикованого центру витрат на надійний, гнучкий та ефективний бізнес-актив, що забезпечує стабільність, знижує операційні витрати та створює основу для впровадження інновацій.

Рекомендації щодо впровадження полягають у необхідності розглядати ІТ-інфраструктуру як стратегічний актив, формувати довгостроковий план її розвитку та інвестувати у навчання персоналу. Ключовими технічними рекомендаціями є стандартизація платформи віртуалізації, використання Kubernetes для нових додатків та, найголовніше, обов’язкове застосування підходу «Інфраструктура як Код» для всіх операцій. Для успішного переходу пропонується поетапний підхід, що забезпечує керований та мінімально ризикований процес модернізації.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Терлецький Т. В., Угрин Д. І., Багнюк Н. В., Кайдик О. Л., Лакодей О. Л. Дослідження рішень та модернізація інфраструктури домашніх серверів. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. Луцьк, 2025. № 61, с. 206-212.

2. SaaS та хмарні рішення в автоматизації ArtSoft. 2024. URL: https://artsoft.mk.ua/articles/saas-ta-hmarni-rishennya-v-avtomatyzacziyi/ (дата звернення: 27.06.2025).

3. Центр даних Вікіпедія. 2024. URL: https://uk.wikipedia.org/wiki/Центр_даних (дата звернення: 29.06.2025).

4. Odom W. CCNA 200-301 Official Cert Guide, Volume 1. 2nd ed. Cisco Press, 2024. URL: https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-1-9780138229634 (дата звернення: 13.07.2025).

5. ANSI/TIA-942-C: Telecommunications Infrastructure Standard for Data Centers, Telecommunications Industry Association. 2024. URL: https://www.tiafotc.org/tia-standards-update/tia-942-c/ (дата звернення: 20.07.2025).

6. ASHRAE TC 9.9 Datacom Encyclopedia / ASHRAE Technical Committee 9.9. 2024. URL: https://tpc.ashrae.org/?cmtKey=fd4a4ee6-96a3-4f61-8b85-43418dfa988d (дата звернення: 16.07.2025).

7. ANSI/TIA-942-C: Telecommunications Infrastructure Standard for Data Centers / Telecommunications Industry Association. 2024. URL: https://www.tiafotc.org/tia-standards-update/tia-942-c/ (дата звернення: 14.08.2025).

8. ASHRAE TC 9.9 Datacom Encyclopedia / ASHRAE Technical Committee 9.9. 2024. URL: https://tpc.ashrae.org/?cmtKey=fd4a4ee6-96a3-4f61-8b85-43418dfa988d (дата звернення: 3.09.2025).

9. CISA Review Manual. 28th ed. / ISACA. 2024. URL: https://www.gettextbooks.com/search/?isbn=ISACA (дата звернення: 13.09.2025).

10. Правила улаштування електроустановок: ПУЕ:2017: Наказ Міністерства енергетики та вугільної промисловості України від 21.07.2017 № 476. URL:

https://zakon.isu.net.ua/sites/default/files/normdocs/pau_rozdil_1.pdf (дата звернення: 15.09.2025).

11. NFPA 75: Standard for the Fire Protection of Information Technology Equipment. 2024 ed. National Fire Protection Association. 2024. URL: https://webstore.ansi.org/standards/nfpa/nfpa752024 (дата звернення: 17.09.2025).

12. The CFO’s Guide to IT Asset Management / InvGate. 2024. URL: https://invgate.com/resources/cfo-guide-to-itam (дата звернення: 27.09.2025).

13. Google Data Center Efficiency / Google. 2025. URL: https://datacenters.google/efficiency (дата звернення: 16.10.2025).

14. Sterling D. J. Technician’s Guide to Fiber Optics. 4th ed. Cengage Learning, c. 2020. URL: https://www.mscdirect.com/product/36477073 (дата звернення: 21.10.2025).

15. Mellanox Spectrum – The RoCE-Ready Switch / NVIDIA. 2020. URL: https://network.nvidia.com/pdf/solutions/SB_Mellanox_Spectrum_RoCE-Ready-Switch.pdf (дата звернення: 27.10.2025).