DOI: https://doi.org/10.36910/6775-2524-0560-2025-61-29
УДК 004.72
Терлецький Тарас Володимирович[1], к.т.н., доцент
https://orcid.org/0000-0002-4114-0734
Угрин Дмитро Ілліч[2], д.т.н., професор
https://orcid.org/0000-0003-4858-4511
Багнюк Наталія Володимирівна[1], к.т.н., доцент
https://orcid.org/0000-0002-7120-5455
Пугач Сергій Олександрович[3], доктор географічних наук, професор
https://orcid.org/0000-0002-3738-7961
Лакодей Олександр Леонідович[1], магістрант
[1]Луцький національний технічний університет, м. Луцьк, Україна
[2] Чернівецький національний університет імені Юрія Федьковича, м. Чернівці, Україна
[3] Волинський національний університет імені Лесі Українки, м. Луцьк, Україна

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

Терлецький Т. В., Угрин Д. І., Багнюк Н. В., Пугач С. О., Лакодей О. Л. Дослідження шляхів реінжинірингу серверної кімнати для покращення ефективності функціонування ІТ-інфраструктури. У статті розглядається комплексна модель реінжинірингу застарілої серверної кімнати для підвищення ефективності функціонування ІТ-інфраструктури підприємства. Проведено аудит типової інфраструктури, виявлено ключові проблеми, а саме: апаратна застарілість, відсутність відмовостійкості, високі операційні витрати та низька продуктивність. Розроблено багаторівневу модель модернізації, що включає проєктування гібридної фізичної інфраструктури з дворівневою мережевою архітектурою (General Purpose та High-Performance Fabric) та спеціалізованими пулами серверів. Обґрунтовано перехід на програмно-визначувану платформу на базі систем віртуалізації та контейнеризації з використанням гіпервізорів. Запропоновано модель повної автоматизації управління на основі парадигми «Інфраструктура як Код» (IaC) з використанням стеку інструментів Terraform та Ansible. Проведено порівняльний аналіз показників до і після модернізації, який підтвердив значне зростання технічної продуктивності (скорочення часу відгуку на 82%), підвищення надійності та суттєве зниження операційних витрат (на 60% на електроенергію), що доводить економічну доцільність запропонованих рішень.
Ключові слова: реінжиніринг, серверна кімната, ІТ-інфраструктура, віртуалізація, Infrastructure as Code, відмовостійкість.

Terletskyi T., Uhryn D., Bahniuk N., Pugach S., Lakodei O. Research on ways to reengineer a server room to improve the efficiency of IT infrastructure. The article considers a comprehensive re-engineering model for an outdated server room to improve the efficiency of an enterprise's IT infrastructure. An audit of a typical legacy infrastructure was conducted, identifying key issues: hardware obsolescence, lack of fault tolerance, high operational costs, and low performance. A multi-level modernization model has been developed, which includes the design of a hybrid physical infrastructure with a dual-fabric network architecture (General Purpose and High-Performance Fabric) and specialized server pools. The transition to a software-defined platform based on virtualization and containerization systems is justified. A model for full management automation based on the "Infrastructure as Code" (IaC) paradigm using a stack of Terraform and Ansible tools is proposed. A comparative analysis of "before" and "after" metrics was carried out, which confirmed a significant increase in technical performance (response time reduction by 82%), improved reliability, and a substantial decrease in operational costs (60% reduction in electricity), proving the economic feasibility of the proposed solutions.
Keywords: re-engineering, server room, IT infrastructure, virtualization, Infrastructure as Code, fault tolerance.

Постановка наукової проблеми. В умовах цифрової трансформації ІТ-інфраструктура перестає бути допоміжним інструментом і стає ключовим бізнес-активом, що напряму впливає на конкурентоспроможність компанії. Проте багато підприємств продовжують експлуатувати застарілі серверні кімнати, спроєктовані 10-15 років тому. Така інфраструктура несе в собі значний технологічний борг – вона нездатна ефективно справлятися з сучасними навантаженнями (аналітика великих даних, машинне навчання, мікросервісні додатки), є надзвичайно дорогою в утриманні через високе енергоспоживання та часті збої, а також гальмує впровадження сучасних практик розробки, таких як DevOps. Відсутність автоматизації та гнучкості робить будь-які зміни повільними, ризикованими та трудомісткими. Таким чином, виникає потреба розробки універсальної, комплексної моделі реінжинірингу, яка б дозволила не просто замінити старе обладнання, а фундаментально трансформувати ІТ-інфраструктуру в гнучку, автоматизовану, безпечну та економічно ефективну платформу, готову до викликів майбутнього та завдань бізнесу.

Аналіз останніх досліджень і публікацій. Тематика модернізації центрів обробки даних (ЦОД) [1] є предметом численних досліджень. Сучасні підходи до архітектури та дизайну ЦОД

детально описані в роботі Дж. Бель [2], де наголошується на важливості програмно-визначуваних рішень. Технічні та інженерні аспекти функціонування інфраструктури регламентуються визнаними галузевими стандартами. Так, стандарт ANSI/TIA-942-C [3] визначає вимоги до надійності та структури телекомунікаційної інфраструктури, а рекомендації ASHRAE TC 9.9 [4] встановлюють норми для мікроклімату та систем охолодження, що є критичним для енергоефективності та відмовостійкості апаратного забезпечення.

Сучасні мережеві архітектури, що відходять від пласких топологій до ієрархічних моделей «ядро-доступ», детально розглядаються в посібниках від провідних вендорів, таких як Cisco [5]. Окремий напрямок досліджень присвячений високопродуктивним мережам для систем зберігання даних та обчислювальних кластерів. Робота Е. Коена та М. Кагана [6] глибоко аналізує переваги технології RDMA over Converged Ethernet (RoCE), яка дозволяє досягти наднизьких затримок, недосяжних для традиційного Ethernet. Важливість стратегічного підходу до управління IT як бізнес-активом та ключовим елементом цифрової трансформації підкреслюється в роботах українських науковців [7].

Виділення невирішених раніше частин загальної проблеми. Попри велику кількість досліджень, більшість з них фокусується на окремих аспектах модернізації (наприклад, лише на віртуалізації мережевої частини або на автоматизації). Залишається недостатньо дослідженою проблема створення єдиної, комплексної та цілісної моделі, яка б поєднувала модернізацію фізичного рівня (мережі, сервери), впровадження програмно-визначуваної платформи (віртуалізація, контейнери) та повну автоматизацію процесів управління (IaC, GitOps). Особливо гостро ця проблема стоїть для підприємств, які потребують не просто теоретичних рекомендацій, а практичної, поетапної дорожньої карти з детальним розрахунком економічної доцільності.

Враховуючи вищесказане, актуальним є розробка комплексної, багаторівневої моделі реінжинірингу застарілої серверної кімнати та доведення її технічної й економічної ефективності на основі порівняльного аналізу ключових показників. Основними завданнями дослідження є: провести аудит типової застарілої інфраструктури та ідентифікувати ключові проблеми, спроєктувати сучасну гібридну фізичну та логічну архітектуру, розробити модель автоматизації управління на основі парадигми IaC, провести порівняльний аналіз технічних та економічних показників до і після модернізації.

Основна частина дослідження. Дослідження структуровано за трьома послідовними етапами: по-перше, глибока діагностика існуючої інфраструктури для точного визначення проблем; по-друге, розробка комплексної, багаторівневої моделі реінжинірингу; і по-третє, практична валідація запропонованих рішень через пілотне тестування та порівняльний аналіз ключових показників ефективності.

Практична реалізація проєкту реінжинірингу є комплексним, багатоетапним процесом. Загальна послідовність виконання робіт, від початкового аналізу до фіналізації, представлена на блок-схемі (рис.1).

Етап 1: аудит та діагностика об'єкта дослідження.

На першому етапі проведено комплексний аудит інфраструктури об'єкта дослідження згідно з розробленою методикою [8], яка базується на провідних галузевих стандартах, таких як TIA-942-C [3, 6] для телекомунікаційної інфраструктури та ASHRAE TC 9.9 [4] для інженерних систем. Аналіз виявив низку критичних проблем, що унеможливлювали подальший розвиток та створювали прямі ризики для бізнес-процесів:

– апаратна застарілість та ризики безпеці: встановлено, що понад 80% серверного та мережевого обладнання досягло статусу End-of-Life (EoL). Це означає не лише відсутність гарантійної підтримки від виробника, але й, що більш критично, припинення випуску оновлень безпеки, що робило всю інфраструктуру вразливою до сучасних кіберзагроз;

– відсутність відмовостійкості: архітектура системи характеризувалася наявністю численних єдиних точок відмови (SPOF). Відсутність резервування на рівні комутаторів, блоків живлення та систем зберігання даних означала, що збій будь-якого з цих компонентів призвів би до повної зупинки залежних сервісів на невизначений час;

– енергетична та економічна неефективність: заміри показали, що рівень завантаженості старих серверів не перевищував 15-20%, тоді як їхнє енергоспоживання становило 70-80% від максимального. Це, у поєднанні з неефективною системою охолодження, генерувало надлишкові

операційні витрати та непропорційно збільшувало сукупну вартість володіння інфраструктурою, що робило її утримання фінансово обтяжливим для підприємства;

– обмежена продуктивність: пропускна здатність мережі на рівні 1 Гбіт/с та використання повільних HDD-дисків у серверах створювали критичні «вузькі місця», що значно уповільнювало роботу баз даних, файлових сховищ та інших бізнес-додатків.

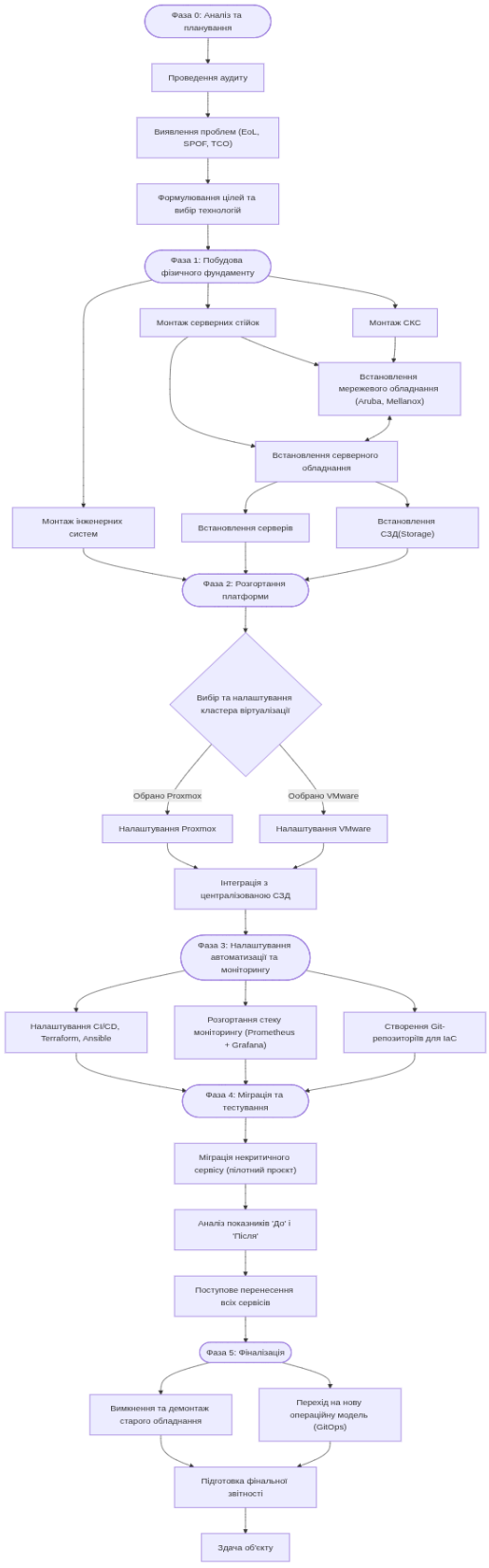

Рис.1. Блок-схема поетапного виконання реінжинірингу серверної кімнати

Окремої уваги заслуговує аналіз бізнес-впливу виявлених проблем. Застаріла інфраструктура є не просто технічним недоліком, а джерелом прямих фінансових та репутаційних ризиків. Наприклад, відсутність відмовостійкості (SPOF) означає, що вихід з ладу єдиного центрального комутатора чи сервера може призвести до повної зупинки всіх бізнес-процесів на кілька годин. Прямі збитки від такого простою включають втрачену виручку та штрафи за невиконання зобов'язань, а непрямі – втрату довіри клієнтів та зниження продуктивності співробітників.

Статус End-of-Life для обладнання створює критичні ризики безпеці. Відсутність оновлень від виробника робить інфраструктуру вразливою до нових видів кібератак, таких як програми-вимагачі (ransomware). Успішна атака може призвести не лише до фінансових втрат, але й до повної втрати критичних бізнес-даних. Таким чином, продовження експлуатації застарілого обладнання є економічно невиправданим ризиком, вартість якого значно перевищує інвестиції в модернізацію.

Етап 2: розроблена модель реінжинірингу.

На основі результатів аудиту розроблена цілісна модель модернізації, що охоплює фізичний, апаратний, програмний та процесний рівні.

Фізичний та апаратний рівні (рис. 2): в основі нової архітектури лежить дворівнева мережева фабрика, що фізично розділяє потоки даних. Для загального корпоративного трафіку спроєктовано відмовостійкий стек комутаторів HPE Aruba (General Purpose Fabric). Для надшвидкісного обміну даними між серверами та системами зберігання даних створено окрему High-Performance Fabric на базі обладнання NVIDIA Mellanox зі швидкістю 100 Гбіт/с та підтримкою технології RoCE, яка мінімізує мережеві затримки [6]. Серверні ресурси розділені на спеціалізовані пули: обчислювальні сервери (Compute) для віртуальних машин та контейнерів, та системи зберігання даних (Storage) на базі All-Flash масивів для максимальної продуктивності дискових операцій. Надійність фізичних з'єднань забезпечується структурованою кабельною системою з використанням мідних кабелів Cat 6A та оптоволокна OM4 [9].

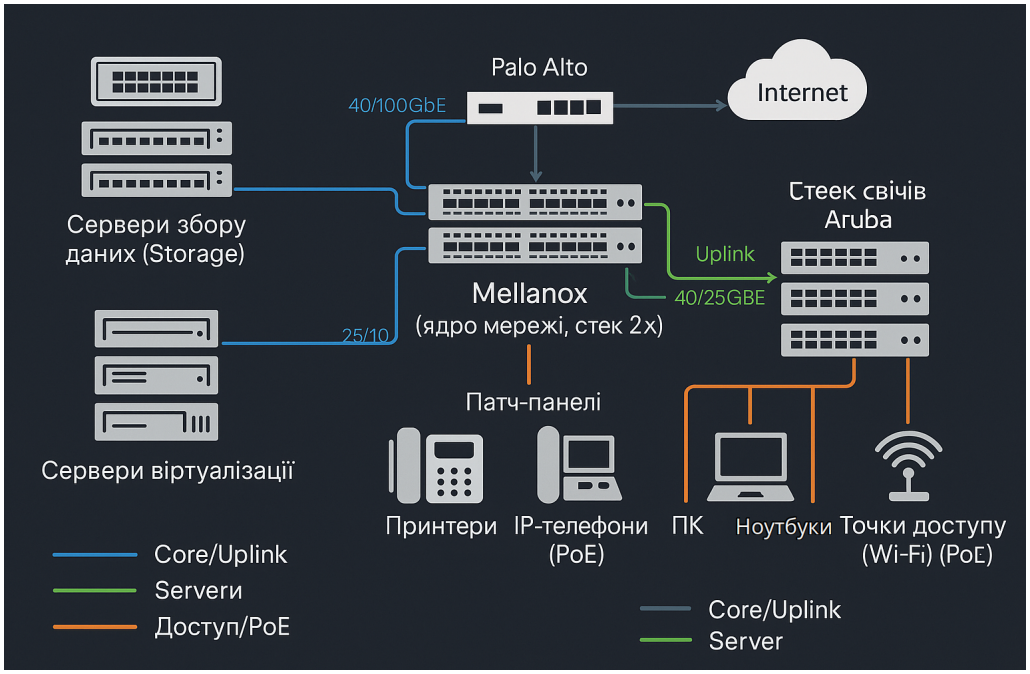

Рис.2. Архітектура дворівневої мережевої фабрики

Програмно-визначувана платформа та автоматизація: на новому обладнанні розгортається гнучка програмно-визначувана платформа. За допомогою систем віртуалізації (VMware vSphere або Proxmox VE) проводиться консолідація фізичних серверів у єдиний пул ресурсів. Це дозволяє досягти високий рівень завантаженості обладнання та надає такі інструменти, як висока доступність (HA) та «жива» міграція (vMotion). Поверх віртуального середовища інтегрується платформа оркестрації контейнерів Kubernetes, що стає стандартним середовищем для розгортання та масштабування сучасних мікросервісних додатків.

Ключовим елементом моделі є перехід до парадигми «Інфраструктура як Код» (IaC). Управління всією інфраструктурою здійснюється за допомогою дворівневого стеку інструментів: Terraform використовується для декларативного опису та виділення базових ресурсів (ВМ, мережі, сховища), а Ansible − для їх подальшої детальної конфігурації (встановлення ПЗ, налаштування сервісів). Усі зміни вносяться через GitOps конвеєр, що робить процес прозорим, контрольованим та відтворюваним. Повний контроль над станом усіх компонентів забезпечує система моніторингу на базі Prometheus + Grafana.

Окрім продуктивності та відмовостійкості, при проєктуванні нової архітектури значну увагу приділено фундаментальним принципам безпеки, що реалізовані на кількох рівнях:

– мережева безпека та сегментація: нова архітектура на базі комутаторів HPE Aruba дозволяє реалізувати глибоку сегментацію трафіку за допомогою віртуальних локальних мереж (VLAN) та списків контролю доступу (ACL). Створено окремі ізольовані сегменти для серверів, користувачів, IP-телефонії та, що найважливіше, для управління інфраструктурою. Це означає, що навіть у разі компрометації пристрою в користувацькому сегменті, зловмисник не матиме прямого доступу до серверного сегмента чи інтерфейсів управління обладнанням;

– безпека площини управління (Management Plane): для доступу до інтерфейсів управління гіпервізорами (vCenter/Proxmox), комутаторами та серверних консолей (iDRAC/iLO) створено окремий, суворо ізольований управлінський VLAN. Доступ до цього сегмента дозволено лише з обмеженої кількості робочих місць адміністраторів, що значно знижує поверхню атаки на найкритичніші компоненти інфраструктури;

– безпека на рівні хостів та даних забезпечується централізованим управлінням конфігураціями за допомогою Ansible, що дозволяє автоматично застосовувати єдині політики безпеки до всіх серверів. Це включає налаштування брандмауера, відключення непотрібних сервісів, регулярне встановлення оновлень безпеки та забезпечення відповідності внутрішнім стандартам («hardening»). Крім того, сучасні системи зберігання даних (СЗД), що обрані для проєкту, підтримують шифрування даних у стані спокою (Data-at-Rest Encryption), що гарантує конфіденційність інформації навіть у випадку фізичної крадіжки дисків.

Такий багаторівневий підхід до безпеки дозволяє створити надійний захищений периметр і мінімізувати ризики, пов'язані як із зовнішніми, так і з внутрішніми загрозами.

Етап 3: валідація та аналіз ефективності.

Для підтвердження дієвості розробленої моделі проведено пілотне тестування, що полягало в міграції репрезентативного додатку на нову інфраструктуру. Протягом тестового періоду проводився збір та порівняльний аналіз ключових показників ефективності (таблиця 1).

Табл. 1. Порівняльний аналіз ключових показників ефективності

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%
Рівень доступності (SLA)	99,0% (без резервування)	99,95% (з HA кластером)	↑ 0,95%
Час відновлення після	2-4 години (ручне	< 5 хвилин	↓ 98%

збою хоста	відновлення)	(автоматичне HA)	
Операційна ефективність			
Час розгортання нового сервера	1-2 дні (ручне налаштування)	~ 15 хвилин (Terraform + Ansible)	↓ >99%
Кількість ручних втручань	Постійно	Мінімально (через GitOps)	↓

Результати тестування продемонстрували кардинальне зростання за всіма напрямками. Час відгуку сервісів скоротився більш ніж у 5 разів, продуктивність дискових операцій зросла в десятки разів, що було підтверджено даними системи моніторингу та результатами стрес-тестування, а час розгортання нової інфраструктури скоротився з днів до хвилин, що наочно демонструє переваги автоматизації.

Економічна доцільність проєкту [10, 7] підтверджена аналізом операційних витрат. Завдяки консолідації та переходу на сучасне енергоефективне обладнання, загальне енергоспоживання вдалося скоротити на 60%. Розрахунок сукупної вартості володіння (TCO) за 5-річний період показав, що, незважаючи на значні початкові капітальні вкладення, нова інфраструктура є значно вигіднішою в утриманні, ніж подальша експлуатація застарілої системи (таблиця 2).

Табл. 2. Порівняльний аналіз ключових показників економічної доцільності

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

Висновки та перспективи подальшого дослідження. Проведене дослідження довело, що комплексний реінжиніринг серверної кімнати дозволяє трансформувати її з ризикованого центру витрат на ефективний та гнучкий бізнес-актив. Розроблена модель, що поєднує модернізацію фізичного рівня, впровадження програмно-визначуваних технологій та повну автоматизацію, є універсальною дорожньою картою для підприємств, що прагнуть модернізувати свою IT-інфраструктуру.

Перспективи подальшого дослідження лежать у площині впровадження на базі створеної платформи більш «просунутих» парадигм: архітектура нульової довіри (Zero Trust): впровадження мікросегментації та посиленого контролю доступу між усіма компонентами системи; AIOps (AI for IT Operations) − застосування штучного інтелекту для предиктивного аналізу стану інфраструктури та автоматичного усунення проблем; гібридна хмара: інтеграція локальної інфраструктури з публічними хмарними провайдерами для реалізації сценаріїв аварійного відновлення та «хмарних сплесків».

Особливо перспективним напрямком є побудова гібридної хмарної інфраструктури. Створена локальна платформа може бути інтегрована з публічними хмарними провайдерами (AWS, Azure, Google Cloud) для реалізації двох ключових сценаріїв. Перший – «хмарні сплески» (Cloud Bursting), коли при пікових навантаженнях, що перевищують потужність локальних серверів,

система автоматично розгортає додаткові обчислювальні вузли в публічній хмарі. Це дозволяє гнучко та економічно ефективно справлятися з тимчасовими стрибками навантаження.

Другий сценарій – катастрофостійкість як сервіс (Disaster Recovery as a Service, DRaaS). Замість побудови дорогої резервної серверної кімнати, можна налаштувати постійну реплікацію критичних віртуальних машин та даних у хмарне середовище. У разі повної відмови основного майданчика (наприклад, через пожежу чи тривале відключення електроенергії), бізнес-процеси можуть бути швидко відновлені на базі хмарних ресурсів, що забезпечує високий рівень безперервності бізнесу (Business Continuity). Дослідження та впровадження цих підходів є логічним наступним кроком після успішного завершення реінжинірингу.

Список бібліографічного опису:

1. Центр даних. Вікіпедія. 2024. URL: https://uk.wikipedia.org/wiki/Центр_даних (дата звернення: 26.07.2025).
2. Belle J. Modern Data Center Architecture and Design: A Practical Guide. O'Reilly Media, 2022. 450 p.
3. ANSI/TIA-942-C:2023. Telecommunications Infrastructure Standard for Data Centers. Telecommunications Industry Association, 2023.
4. ASHRAE TC 9.9. Thermal Guidelines for Data Processing Environments. 5th ed. Atlanta : ASHRAE, 2021.
5. Odom W. Official Cert Guide: CCNA 200-301. Cisco Press, 2022. 1600 p.
6. Cohen E., Kagan M. Ethernet-Based High-Performance Networks: A Deep Dive into RoCE and 100GbE. Berkeley : Apress, 2021. 240 p.
7. Литвин І. В., Олексів І. Б. Стратегічне управління цифровою трансформацією підприємства : монографія. Львів : Видавництво Львівської політехніки, 2021. 340 с. URL: https://www.google.com/search?q=https://ena.lpnu.ua/handle/ntb/53842 Text (дата звернення: 02.09.2025).
8. Davis D. C., Schiller M., Wheeler K. IT Auditing Using Controls to Protect Information Assets, Third Edition. https://public.ebookcentral.proquest.com/choice/PublicFullRecord.aspx?p=6254685. Sterling D. J. Technician's Guide to Fiber Optics. 6th ed. Boston : Cengage Learning, 2020. 608 p. (дата звернення: 05.09.2025).
9. Правила улаштування електроустановок (ПУЕ). URL: https://zakon.isu.net.ua/sites/default/files/normdocs/pue.pdf (дата звернення: 05.09.2025).
10. ANSI/TIA-942-C:2023. Telecommunications Infrastructure Standard for Data Centers. Telecommunications Industry Association, 2023.

References:

1. Data center. Wikipedia. 2024. URL: https://en.wikipedia.org/wiki/Data_center (date of access: 26.07.2025).
2. Belle J. Modern Data Center Architecture and Design: A Practical Guide. O'Reilly Media, 2022. 450 p.
3. ANSI/TIA-942-C:2023. Telecommunications Infrastructure Standard for Data Centers. Telecommunications Industry Association, 2023.
4. ASHRAE TC 9.9. Thermal Guidelines for Data Processing Environments. 5th ed. Atlanta : ASHRAE, 2021.
5. Odom W. Official Cert Guide: CCNA 200-301. Cisco Press, 2022. 1600 p.
6. Cohen E., Kagan M. Ethernet-Based High-Performance Networks: A Deep Dive into RoCE and 100GbE. Berkeley : Apress, 2021. 240 p.
7. Lytvyn I. V., Oleksiv I. B. Strategic Management of Enterprise Digital Transformation : monograph. Lviv : Lviv Polytechnic Publishing House, 2021. 340 p. (date of access: 02.09.2025).
8. Davis D. C., Schiller M., Wheeler K. IT Auditing Using Controls to Protect Information Assets, Third Edition. https://public.ebookcentral.proquest.com/choice/PublicFullRecord.aspx?p=6254685. Sterling D. J. Technician's Guide to Fiber Optics. 6th ed. Boston : Cengage Learning, 2020. 608 p. (date of access: 05.09.2025).
9. Electrical Installation Rules (PUE). URL: https://zakon.rada.gov.ua/laws/show/z0571-18#Text (date of access: 05.09.2025).
10. ANSI/TIA-942-C:2023. Telecommunications Infrastructure Standard for Data Centers. Telecommunications Industry Association, 2023.