Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Галузь знань 12 – Інформаційні технології

Спеціальність 123 –Комп'ютерна інженерія

на тему «Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників»

КвРКІ. 2301145.22.02.38 ПЗ

Виконав: студент 2 курсу, група КІ2м-23-1 _____ Дмитро АНДРЄЄВ
Підпис Ім'я, прізвище

Керівник канд. екон. наук, доцент _____ Світлана САЧЕНКО
Науковий ступінь, вчене звання Підпис Ім'я, прізвище

До захисту допускаю:
Зав. кафедри КІІС, д.ф., доц.
Ольга ПАВЛОВА
01 05 2025 р.

Хмельницький, 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень МАГІСТР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма ОСВІТНЬО-НАУКОВА ПРОГРАМА «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Ольга ПАВЛОВА

" 01 " 09 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Дмитру АНДРСЄВУ

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників

Керівник проекту (роботи) Саченко С.І., к.е.н., доцент

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

Затверджена наказом ректора університету від 08.01.2025 р. № 1

2. Строк подання студентом проекту (роботи) на кафедру 01.05.2025 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників; виділити ключові особливості оптимізації та моделювання критичної IT інфраструктури цифровими двійниками, а також розглянути цільову функцію та алгоритми оптимізації критичної IT інфраструктури цифровими двійниками; розробити метод оптимізації критичної IT інфраструктури цифровими двійниками та дослідити практичне застосування цифрових двійників у критичній інфраструктурі.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

6. Консультанти розділів кваліфікаційної роботи магістра

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Сергій ЛИСЕНКО, професор кафедри КІС		
Антиплагіат	Андрій НІЧЕПОРУК, доцент кафедри КІС		

7. Дата видачі завдання « 01 » 09 2024р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) кваліфікаційної роботи магістра	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики КвРМ з керівником	01.09.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.10.2024	виконано
3	Робота над розділом 1 – аналіз відомих моделей, методів за темою; постановка задачі	01.11.2024	виконано
4	Робота над розділом 2 – розробка моделей для вирішення поставленої задачі	01.12.2024	виконано
5	Робота над науковою статтею	01.02.2025	виконано
6	Робота над розділом 3 – розробка методів для вирішення поставленої задачі	15.02.2025	виконано
7	Робота над розділом 4 – проектування засобів для вирішення поставленої задачі, експериментальна частина	01.04.2026	виконано
8	Оформлення пояснювальної записки згідно вимог	18.04.2025	виконано
9	Попередній захист КРМ	29.04.2025	виконано
10	Захист КРМ на засіданні ЕК	До 25.05.2025	

Студент _____ Дмитро АНДРЄЄВ
Підпис Ініціали, прізвище

Керівник роботи _____ Світлана САЧЕНКО
Підпис Ініціали, прізвище

РЕФЕРАТ

Тема кваліфікаційної роботи магістра: «Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників»

Автор роботи: Андрєєв Дмитро Леонідович

Керівник роботи: Саченко С.І.

Пояснювальна записка: 77 с., 10 рис., 0 табл., 3 дод., 81 джерела.

КРИТИЧНА ІНФРАСТРУКТУРА, ЦИФРОВІ ДВІЙНИКИ, ОПТИМІЗАЦІЯ МОДЕЛЮВАННЯ, ЦІЛЬОВА ФУНКЦІЯ.

Об’єктом дослідження є процес моніторингу об'єктів критичної інфраструктури на основі цифрових двійників.

Предметом дослідження є процес оптимізації та моделювання об'єктів критичної інфраструктури на основі цифрових двійників.

Метою кваліфікаційної роботи магістра є покращення ефективності оптимізації критичної IT інфраструктури цифровими двійниками.

Для розв’язання поставлених задач використовувалися метод оптимізації та моделювання критичної IT інфраструктури цифровими двійниками.

Наукова новизна отриманих результатів:

- розроблено метод для забезпечення безперебійного працювання критичної інфраструктури, особливістю яких є використання цифрових двійників на практиці.

На основі проведених досліджень розроблено метод оптимізації критичної IT інфраструктури цифровими двійниками.

Практична значимість отриманих результатів полягає у розробленні проєкту «Цифровий двійник IT-інфраструктури НЕК «Укренерго».

У вступі подано об’єкт та предмет дослідження, мету, наукову новизну та практичну цінність роботи, а також характеристику структури роботи.

У першому розділі розглянуто питання моніторингу об'єктів критичної інфраструктури, а також проведено аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників .

У другому розділі розглянуто та виділено ключові особливості оптимізації та моделювання критичної ІТ інфраструктури цифровими двійниками .

У третьому розділі було опрацьовано процес оптимізації об'єктів критичної інфраструктури на основі цифрових двійників, а саме його цільову функцію та алгоритми оптимізації критичної ІТ інфраструктури цифровими двійниками.

У четвертому розділі розглянуто ефективність методу оптимізації критичної ІТ інфраструктури цифровими двійниками, а також проведено дослідження експериментів та досліджень методу оптимізації критичної ІТ інфраструктури цифровими двійниками.

У висновках підведено підсумки досягнення результатів з розв’язання завдань дослідження.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

IoT	Інтернет речей
IT	Інформаційні технології
ОС	Операційні системи
КІ	Критична інфраструктура

ВСТУП

У сучасному світі стабільне функціонування об’єктів критичної інфраструктури (КІ) - таких як енергетичні системи, об’єкти зв’язку, транспортні вузли, системи водопостачання та водовідведення, об’єкти охорони здоров’я, банківська система, а також ІТ-інфраструктури - є ключовим фактором національної безпеки, соціальної стабільності та економічної стійкості. Будь-які порушення в роботі таких систем, спричинені технічними збоями, зовнішніми атаками, людським фактором або стихійними лихами, можуть призвести до серйозних наслідків: масштабних відключень, паралічу логістичних ланцюгів, порушення доступу до життєво важливих послуг, економічних втрат і навіть загроз життю та здоров’ю громадян.

У зв’язку з цим зростає потреба у впровадженні ефективних рішень, що дозволяють здійснювати цілодобовий моніторинг, вчасне виявлення аномалій, швидке реагування на інциденти, а також прогнозування потенційних відмов до моменту їхнього виникнення. Сучасні підходи, засновані на традиційних засобах моніторингу, вже не завжди здатні забезпечити належний рівень адаптивності, точності та швидкості аналізу.

Інноваційним та перспективним напрямом у цьому контексті є використання технології цифрових двійників (Digital Twins). Цифровий двійник - це динамічна віртуальна копія фізичного об’єкта, системи або процесу, яка створюється на основі реальних технічних характеристик та актуальних даних. Цей підхід забезпечує двосторонній зв’язок між фізичною і цифровою моделлю, що дозволяє не лише візуалізувати поточний стан об’єкта, але й аналізувати історичні дані, виявляти тренди, виконувати моделювання аварійних сценаріїв, а також автоматизовано приймати рішення щодо оптимізації та усунення вразливостей.

Отже, завдяки інтеграції телеметричних даних, логів, показників сенсорів та систем штучного інтелекту, цифрові двійники перетворюються на потужний інструмент прогнозної аналітики, стратегічного планування та адаптивного управління ІТ-інфраструктурою в режимі реального часу. Таким чином, ця

технологія відкриває нові можливості для забезпечення високої надійності, гнучкості, безпеки та енергоефективності критичних систем, що є особливо важливим у контексті зростаючих кіберзагроз, глобальної нестабільності та потреби в цифровій трансформації ключових секторів.

Метою даної дипломної роботи є дослідження системи моніторингу об’єктів критичної інфраструктури, а також покращення ефективності оптимізації критичної IT інфраструктури цифровими двійниками, яка здатна в режимі реального часу збирати дані, аналізувати їх, прогнозувати відмови та візуалізувати поточний стан IT-активів.

Поставлена мета досягається розв’язанням таких основних завдань:

- аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників;
- виділити ключові особливості оптимізації та моделювання критичної IT інфраструктури цифровими двійниками;
- розглянути цільову функцію та алгоритми оптимізації критичної IT інфраструктури цифровими двійниками;
- розробити метод оптимізації критичної IT інфраструктури цифровими двійниками та дослідити практичне застосування цифрових двійників у критичній інфраструктурі.

Об’єктом дослідження є процес моніторингу об'єктів критичної інфраструктури на основі цифрових двійників.

Предметом дослідження є процес оптимізації та моделювання об'єктів критичної інфраструктури на основі цифрових двійників.

Наукова новизна отриманих результатів:

- розроблено метод для забезпечення безперебійного працювання критичної інфраструктури, особливістю яких є використання цифрових двійників на практиці.

На основі проведених досліджень розроблено метод оптимізації критичної IT інфраструктури цифровими двійниками.

Практична значимість отриманих результатів полягає у розробленні проєкту «Цифровий двійник IT-інфраструктури НЕК «Укренерго».

Для розв’язання поставлених задач використовувалися метод оптимізації та моделювання критичної ІТ інфраструктури цифровими двійниками.

1 АНАЛІЗ ВІДОМИХ МЕТОДІВ І ТЕХНОЛОГІЙ МОНІТОРИНГУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ЦИФРОВИХ ДВІЙНИКІВ

1.1 Моніторинг обєктів критичної інфраструктури

Об'єкти критичної інфраструктури [1, 2] (КІ) є основою сучасного суспільства, охоплюючи такі сектори, як енергетика, транспорт, водопостачання, зв'язок та охорона здоров'я. Їх безперебійна робота має першорядне значення для національної безпеки, економічної стабільності та громадської безпеки. Однак ці об'єкти стикаються з безліччю загроз - від стихійних лих і кібератак до людських помилок і навмисного саботажу. Тому ефективний моніторинг має вирішальне значення для зменшення ризиків і забезпечення стійкості.

Постійний моніторинг об'єктів критичної інфраструктури є ключовим елементом забезпечення їхньої безпеки, стійкості та ефективності функціонування. Одним із основних результатів впровадження таких систем є можливість раннього виявлення загроз, оскільки моніторинг у режимі реального часу [3, 4] дає змогу своєчасно виявляти аномальні процеси, ознаки потенційних порушень та нові загрози, що створює передумови для оперативного реагування та мінімізації негативних наслідків. Важливою перевагою є також підтримка процесів профілактичного обслуговування, що базується на аналізі отриманих даних з метою прогнозування можливих відмов обладнання, оптимізації технічних графіків обслуговування та скорочення часу простою виробничих систем.

Крім того, безперервний моніторинг сприяє істотному підвищенню рівня ситуаційної обізнаності операторів та відповідальних осіб завдяки наданню інтегрованого уявлення про функціонування об'єкта [5, 6], що охоплює поточні виробничі параметри, характеристики середовища та рівень потенційних ризиків, а також попереджень щодо виникнення небезпечних ситуацій. Комплексне спостереження забезпечує не лише виявлення загроз, а й формує підґрунтя для прийняття обґрунтованих стратегічних і тактичних рішень.

Суттєвий внесок безперервного моніторингу полягає і в підвищенні загального

рівня безпеки об'єктів критичної інфраструктури, зокрема шляхом використання інтегрованих систем відеоспостереження, контролю доступу та систем виявлення вторгнень, що дозволяє ефективно запобігати несанкціонованим втручанням. Водночас постійний моніторинг виступає інструментом забезпечення відповідності чинним нормативно-правовим вимогам у сфері безпеки, де передбачено обов'язкове документування, контроль і регулярну звітність.

Особливу роль моніторингові системи відіграють у процесах реагування на надзвичайні ситуації та аварії. Зокрема, у випадку стихійних лих або техногенних катастроф, моніторингові дані стають базою для оперативної оцінки ступеня пошкоджень об'єкта, визначення пріоритетних заходів щодо ліквідації наслідків та координації процесів відновлення [7], що в цілому сприяє зниженню соціально-економічних втрат та підвищенню швидкості реабілітаційних заходів.

Система моніторингу об'єктів критичної інфраструктури складається з низки ключових компонентів, кожен із яких виконує важливу функцію у забезпеченні надійного збору, передачі, аналізу та захисту даних. Основу таких систем формують датчики та засоби збору даних [8, 9], що здійснюють безперервне вимірювання різноманітних параметрів, серед яких температура, тиск, швидкість потоку, рівень вібрацій, а також фіксація подій, пов’язаних із забезпеченням безпеки.

Надійні комунікаційні мережі забезпечують оперативну та захищену передачу інформації від датчиків до центральних станцій моніторингу, що є необхідною умовою для підтримки актуальності та достовірності даних. На наступному етапі здійснюється обробка та аналіз даних за допомогою сучасних аналітичних інструментів, які дозволяють виявляти закономірності, вчасно розпізнавати аномальні ситуації та ідентифікувати потенційні загрози для об'єкта.

Інформація, отримана в результаті аналітичної обробки, візуалізується через інтегровані інформаційні панелі та системи звітності, що забезпечують оперативне відображення стану об’єкта в режимі реального часу, а також генерування сповіщень про критичні події для оперативного реагування. Важливою складовою системи є інтегровані засоби фізичної безпеки, серед яких системи відеоспостереження, контролю доступу та виявлення вторгнень, що підвищують загальний рівень

захищеності об'єктів критичної інфраструктури.

Крім того, одним із визначальних елементів ефективності систем моніторингу є реалізація заходів кібербезпеки, що включають застосування брандмауерів, систем виявлення вторгнень та технологій шифрування даних. Ці заходи спрямовані на захист системи від потенційних кібератак та несанкціонованого доступу, що є надзвичайно важливим в умовах зростаючої кіберзагрози.

Сучасні технології суттєво змінюють підходи до моніторингу об'єктів критичної інфраструктури. Інтернет речей (IoT) [10] відкриває можливість розгортання розгалужених мереж датчиків, що забезпечують надходження даних про різні параметри в режимі реального часу. Застосування штучного інтелекту (AI) та машинного навчання (ML) дає змогу обробляти великі масиви даних, виявляти приховані закономірності та здійснювати прогнозування можливих відмов обладнання. Використання хмарних обчислень [11] забезпечує масштабованість і економічну ефективність у питаннях зберігання, обробки та аналізу даних, що надходять із систем моніторингу. Значну роль відіграють також цифрові двійники, які являють собою віртуальні копії фізичних об'єктів і дають змогу моделювати експлуатаційні процеси та передбачати потреби у технічному обслуговуванні. Впровадження технологій 5G та периферійних обчислень забезпечує значне пришвидшення передачі й обробки даних, що суттєво підвищує ефективність моніторингу та оперативного управління в реальному часі.

Розвиток новітніх технологій істотно змінює концепцію моніторингу об'єктів критичної інфраструктури. Інтернет речей (IoT) [10] сприяє створенню розгалужених мереж сенсорів, які забезпечують безперервний збір даних про широкий спектр параметрів в режимі реального часу, що є необхідною умовою для оперативного реагування на зміни стану об'єкта. Використання технологій штучного інтелекту (AI) та машинного навчання (ML) відкриває можливості для обробки великих обсягів інформації, виявлення складних закономірностей у даних та прогнозування потенційних відмов обладнання або появи критичних ситуацій.

Хмарні обчислення [11] забезпечують масштабовані, гнучкі та економічно доцільні рішення для зберігання, обробки та аналізу даних, що дозволяє значно

зменшити витрати на підтримку інфраструктури моніторингу. Важливим інструментом сучасних систем управління є цифрові двійники, які являють собою віртуальні копії фізичних об'єктів і дозволяють моделювати реальні процеси, прогнозувати поведінку систем та планувати технічне обслуговування на основі отриманих результатів.

Впровадження технологій 5G та периферійних обчислень забезпечує надзвичайно високу швидкість передачі даних та мінімізацію затримок обробки інформації, що значно підвищує ефективність моніторингу і оперативного управління об'єктами критичної інфраструктури в реальному часі. Таким чином, інтеграція сучасних технологічних рішень створює нові можливості для забезпечення безпеки, надійності та стійкості важливих об'єктів у різних галузях економіки.

Останніми роками цифрові близнюки стають все більш популярними, особливо в сфері критичної інфраструктури. Цифровий двійник[13, 14] - це віртуальна копія фізичного активу або системи, яка використовує дані для моделювання своєї продуктивності та поведінки. У випадку критичної інфраструктури цифрові двійники можуть забезпечити точне представлення поточного стану системи та потенційних майбутніх сценаріїв, дозволяючи операторам оптимізувати роботу та зменшити ризики. У цьому блозі ми розглянемо використання цифрових двійників у критичній інфраструктурі.

Проблема проведення тестів на кібербезпеку [15] для існуючих промислових систем управління добре відома. Після розгортання критично важливу систему неможливо зробити недоступною для імітації кібератаки, а отже, важко запровадити коригувальні заходи на основі фактичних результатів тестування. З іншого боку, для об'єктів критичної інфраструктури необхідний високий рівень безпеки, а для нових проектів обов'язковим є забезпечення безпеки за замовчуванням. Такі вимоги вимагають архітектурного підходу до впровадження безпеки вже на ранніх етапах розробки. Однак застосування системного підходу до проектування[15, 16] не гарантує економічної ефективності аналізу заходів безпеки, що є надзвичайно обтяжливим завданням, оскільки створення фізичної моделі часто є дорогим або

неможливим. Для вирішення цих проблем ми пропонуємо запровадити в архітектурному плані системи особливе уявлення, яке називається «Цифровий двійник кібербезпеки» (Cybersecurity Digital Twin) [19]. Це модель архітектури системи, спеціально розроблена для забезпечення надійної основи для симуляцій з метою розробки належних контрзаходів без виведення з ладу фізичної інфраструктури. Також об'єкти критичної інфраструктури, такі як заклади охорони здоров'я та транспорту, є життєво важливими для функціонування громади, особливо під час масштабних надзвичайних ситуацій. У цій роботі ми досліджуємо потенційне застосування цифрових двійників для моніторингу стану об'єктів критичної інфраструктури, що постраждали від стихійних лих, на основі інформації, поширеної в соціальних мережах. Для цього ми проаналізували дані соціальних мереж, отримані під час двох стихійних лих у двох різних країнах, щоб виявити повідомлення про вплив на об'єкти критичної інфраструктури, а також ступінь тяжкості цього впливу та їхній оперативний стан. Це дослідження має на меті вивчити використання цифрових двійників у критичній інфраструктурі за допомогою огляду літератури, а також бібліометричного та наукового картографічного аналізу. Згідно з результатами дослідження, цифрові двійники відіграють важливу роль у критичній інфраструктурі, оскільки вони можуть покращити безпеку, стійкість, надійність, технічне обслуговування, безперервність та функціонування критичної інфраструктури в усіх секторах. Інтелектуальне та автономне [19, 20] прийняття рішень, оптимізація процесів, розширене відстеження, інтерактивна візуалізація та моніторинг, аналіз і прогнозування в режимі реального часу - ось деякі з переваг, які можуть дати цифрові двійники. Нарешті, результати дослідження показали здатність цифрових двійників долати розрив між фізичним і віртуальним середовищами, використовуватися в поєднанні з іншими технологіями та інтегруватися в різні середовища і домени. Критична інфраструктура може складатися з віртуальних та/або фізичних активів, систем та процесів і спирається на технологічні досягнення та додатки для безперешкодної інтеграції та функціонування в різних сферах; отже, вона є невід'ємним компонентом сучасних суспільств, які все більше залежать від них [21,22]. Критична інфраструктура та її

визначення розвиваються разом зі змінами, які відбуваються для забезпечення надійного, безпечного та ефективного функціонування громад, а також економічного добробуту та соціального благополуччя [23]. Оскільки критична інфраструктура має важливе значення для сталого майбутнього [24], забезпечення її стійкості та безперервного функціонування, навіть за складних обставин та загроз, має вирішальне значення. Питання кібербезпеки, ризики та вразливості є ще однією серйозною проблемою критичної інфраструктури, оскільки вона є однією з основних цілей для різноманітних кібератак. Тому підвищення безпеки, доступності, стійкості, безперервності та продуктивності критичної інфраструктури є нагальним національним пріоритетом для багатьох країн [25].

Цей факт не є несподіванкою, оскільки критична інфраструктура суттєво впливає на повсякденне життя завдяки комунальним послугам, які вона надає [10]. Транспортні системи та системи громадського транспорту, енергетичні мережі, мережі зв'язку, аптеки та медичні клініки - це лише деякі приклади. Крім того, вона розглядається як величезна державна інвестиція, порушення роботи якої може мати серйозні наслідки [26, 27]. Оскільки критична інфраструктура включає як фізичні, так і віртуальні системи та активи, забезпечення її кібер- та фізичної безпеки і стійкості є обов'язковим. У контексті критичної інфраструктури стійкість означає здатність конкретної системи виявляти, протистояти, адаптуватися, реагувати та відновлюватися після руйнівних подій і надзвичайних ситуацій, а також внутрішніх і зовнішніх загроз, і безпосередньо впливає на надійність системи [28].

Існує 16 широких секторів критичної інфраструктури, в яких руйнування або несправність їхніх фізичних або віртуальних систем, активів та мереж матиме руйнівні наслідки [29]. А саме, ці сектори включають хімічну промисловість, комерційні об'єкти, комунікації, критичне виробництво, греблі, оборонну промислову базу, аварійні служби, енергетику, фінансові послуги, продовольство і сільське господарство, урядові об'єкти, охорону здоров'я і громадське здоров'я, інформаційні технології, ядерні реактори, матеріали і відходи, транспортні системи, а також системи водопостачання і водовідведення [29]. Однак геополітичні події та економічні зміни можуть змінити цей перелік секторів . Варто зазначити, що

критична інфраструктура в різних секторах не є незалежною, а взаємопов'язаною та взаємозалежною. Типи взаємозалежності критичної інфраструктури можуть бути описані з різних вимірів. Таким чином, згідно з, різні дослідження представляють різні типи взаємозалежності критичної інфраструктури, такі як (i) фізична, кібернетична, географічна або логічна, (ii) функціональна або просторова [30], (iii) фізична, геопросторова, політична або інформаційна, (iv) вхідна, взаємна, спільна, ексклюзивна або спільна та (v) функціональна, фізична, бюджетна або ринково-економічна. Оскільки цифрові двійники є керованими даними і точними віртуальними копіями об'єктів реального світу, вони можуть допомогти подолати розрив між фізичним і віртуальним середовищами і використовуватися в різних умовах і сферах [23,24,25]. Отримуючи вхідні дані від фізичного об'єкта [26] і завдяки своїм різноманітним вимірам і можливостям, цифрові двійники дозволяють оптимізувати послуги, продукти і пристрої та покращити кібербезпеку [9] завдяки постійному моніторингу в режимі реального часу і використанню переваг як горизонтального, так і вертикального підходів [27]. У контексті цифрових двійників горизонтальні підходи стосуються впровадження та застосування цифрових двійників у різних секторах та сферах використання, тоді як вертикальні підходи стосуються глибокої інтеграції цифрових двійників та їх оптимізації в конкретних сферах або сферах використання. Основними властивостями цифрових двійників є залежність від домену, синхронізація, автономність та саморозвиток [28]. Крім того, комунікаційні можливості, унікальні ідентифікатори, приводи і датчики, штучний інтелект, безпека і конфіденційність, довіра і віртуальне представництво є одними з основних характеристик цифрових двійників [29]. Ці властивості та характеристики роблять цифрових двійників можливими для інтеграції в різні сфери. Технології розширеної реальності, робототехніка, тактильні пристрої, моделювання на основі даних, машинний зір, хмарні обчислення, тактильний інтернет, мережі 5G, штучний інтелект та інтернет речей - це лише деякі з різних технологій, які дозволяють реалізувати цифрових двійників [24, 30]. Цифрові двійники мають потенціал для подальшого підвищення безпеки, стійкості, безперервності та функціонування критичної інфраструктури в усіх секторах. Оскільки ця тема розвивається, важливо

представити її еволюцію. Кілька систематичних оглядів літератури вивчали роль цифрових двійників в інфраструктурі [31,32]. Хоча були проведені дослідження, які вивчали впровадження, використання та роль цифрових двійників у різних сферах, наприклад, у транспорті, енергетиці, транспорт, енергетика, інфраструктура [37], інтелектуальні промислові системи, виробництво [39], інтелектуальні будівлі, охорона здоров'я [41], транспорт, енергетика, наскільки нам відомо, не було жодного іншого дослідження, яке б представляло поточний стан справ щодо впровадження та інтеграції цифрових двійників у контексті критичної інфраструктури, беручи до уваги всі сфери критичної інфраструктури за допомогою бібліометричного та картографічного аналізу. Щоб заповнити цю прогалину в літературі, це дослідження має на меті вивчити використання цифрових двійників у критичній інфраструктурі за допомогою огляду, бібліометричного аналізу та наукового картографування існуючої літератури. Основними дослідницькими питаннями, які необхідно було дослідити, були: яка роль цифрових двійників у критичній інфраструктурі та який поточний стан справ у цій галузі на основі існуючих літературних джерел. Таким чином, основним внеском дослідження можна вважати представлення існуючої літератури, бібліометричний та картографічний аналіз відповідних документів, виявлення еволюції теми та нових тем, а також рекомендації щодо подальших напрямків дослідження. Цифрові двійники складаються з програмних сервісів і моделей, які використовують різні аспекти обробки даних [36] і являють собою віртуальну копію фізичного об'єкта або системи, фокусуючись при цьому на взаємодії між фізичними і цифровими об'єктами [37,38]. Тому, оскільки цифрові двійники можуть підтримувати моніторинг та оптимізацію в режимі реального часу, а також прийняття рішень на основі моделювання, їх можна впроваджувати протягом усього життєвого циклу продукту за необхідності [42]. Цифрові двійники працюють в унісон зі своїми фізичними аналогами [41]. Отже, вони змінюються та розвиваються одночасно з розвитком життєвого циклу продукту, що, в свою чергу, призводить до підвищення зручності використання, керованості та точності [24]. Цифрові двійники можна розглядати як живі цифрові моделі фізичних об'єктів, представлені в деталях від мікро до макрорівня, вони постійно поповнюються

новими даними та інформацією про статус фізичного об'єкта і здатні прогнозувати майбутні стани, а також підвищувати загальну безпеку і продуктивність фізичного об'єкта [22]. Отже, цифрові двійники використовують дані, процеси, інтегроване моделювання, когнітивні послуги та машиночитані подання, щоб забезпечити офіційне індивідуальне віртуальне представлення фізичних об'єктів та їх станів, поведінки, ресурсів, взаємодій, характеристик та комунікаційних можливостей [24,31,22,23,33]. Завдяки передбачуваним сферам застосування, модульності вмісту, інтеграції даних, технологіям, стандартам та метамоделям цифрові двійники можуть розробляти двонаправлені динамічні процеси відображення та високоточні цифрові представлення [68,69], які забезпечують конструктивний зворотний зв'язок та розуміння за допомогою моделювання та прогнозування стану, поведінки та інтерактивності об'єктів у режимі реального часу. фізичні особи [48]. Більш того, Цифрові двійники забезпечують розширене і автономне прийняття рішень, моніторинг і аналіз в режимі реального часу, а також інтерактивну візуалізацію, які дозволяють організаціям оптимізувати свої процеси і операції, ефективно оцінювати, як будуть розвиватися їхні активи в майбутньому, підвищувати їх безпеку і надійність і вирішувати найважливіші проблеми [38]. Цифрові двійники можуть бути впроваджені в різні сфери та випадки використання, приносячи переваги та покращуючи процеси [23]. Наприклад, у побудованих середовищах цифрові двійники можуть використовуватися для надання допомоги у плануванні, будівництві, експлуатації та обслуговуванні побудованих об'єктів. Щоб забезпечити ефективну інтеграцію, необхідно ретельно розглянути завдання, питання безпеки та збереження даних, а також питання, пов'язані з часом. Це особливо актуально в разі критично важливої інфраструктури. Ефективний моніторинг об’єктів критичної інфраструктури має важливе значення для забезпечення стійкості в складному світі, що постійно змінюється. Використовуючи передові технології та впроваджуючи надійні заходи безпеки, організації можуть зменшити ризики, підвищити обізнаність про ситуацію та захистити ці життєво важливі активи. Оскільки загрози розвиваються [40], постійна адаптація та інновації є вирішальними для підтримки безпеки та надійності критичної інфраструктури.

1.2 Аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників

Цифрові двійники, широко відомі як digital twins [41], - це віртуальні копії фізичних активів або систем, які відображають умови реального часу завдяки безперервним потокам даних із сенсорних мереж та інших джерел даних. Ці динамічні моделі призначені не тільки для представлення геометрії об'єкта, але й для імітації його експлуатаційної поведінки та взаємодії з навколишнім середовищем. Спочатку з'явившись у таких галузях, як аерокосмічна та обробна промисловість, цифрові двійники розширилися, щоб стати важливими інструментами моніторингу та управління інфраструктурою, включаючи Мости, електромережі, Системи водопостачання та міські об'єкти. Їх еволюція зумовлена досягненнями в області пристроїв Інтернету речей, сенсорних технологій та аналізу даних, які дозволяють цим цифровим поданням постійно оновлюватися та імітувати умови реального світу.

В основі технології digital twins [42] лежить інтеграція трьох фундаментальних компонентів. По-перше, фізичний об'єкт - реальний компонент інфраструктури, такий як міст або електростанція-оснащений датчиками, які реєструють ключові параметри, такі як температура, деформація, вібрація та тиск. По-друге, високодеталізована віртуальна модель створюється за допомогою програмного забезпечення для моделювання та фізичних методів моделювання, таких як аналіз кінцевих елементів. По-третє, надійні канали передачі даних забезпечують безперебійну передачу даних з датчиків в режимі реального часу в цифрову модель. Крім того, передові аналітичні системи та алгоритми машинного навчання обробляють ці потоки даних, щоб передбачити майбутню поведінку, виявити аномалії та виявити потенційні збої до їх виникнення.

Одним з основних методів моніторингу критичної інфраструктури за допомогою цифрових двійників є використання великих сенсорних мереж та інтеграція з IoT [43]. Ці датчики збирають оперативні дані в режимі реального часу, які потім вводяться в цифрову модель, що дозволяє здійснювати безперервний моніторинг та аналіз. Наприклад, у цивільних спорудах акселерометри,

тензометричні датчики та волоконно-оптичні датчики можуть бути встановлені на мостах та будівлях для постійного відстеження стану їх конструкцій. Аналогічно, в енергетичних системах інтелектуальні лічильники та системи SCADA надають дані, які можна використовувати для моніторингу роботи енергосистеми та прогнозування несправностей роботи [44]. Поєднання цих технологій дозволяє отримувати оперативні дані в режимі реального часу, які допомагають інженерам і особам, які приймають рішення, оперативно виявляти і усувати проблеми.

Окрім збору даних, імітаційне та прогностичне моделювання є важливою частиною впровадження цифрових двійників [45, 46]. Цифрові двійники використовують передові інструменти моделювання для відтворення поточного стану активу та прогнозування майбутніх умов за різних сценаріїв. Моделі, засновані на фізиці, які часто використовують метод скінченних елементів, передбачають розподіл напружень, втому та потенційні точки руйнування конструкцій. При інтеграції з машинним навчанням це моделювання стає ще більш ефективним, оскільки Історичні дані та дані в режимі реального часу об'єднуються для прогнозування продуктивності, планування технічного обслуговування та оптимізації операцій. Ця можливість [47] не тільки підвищує надійність обладнання, але і продовжує термін його служби і скорочує незаплановані простої.

Візуалізація та аналіз даних [47] також є важливими елементами систем digital twin. Сучасні платформи пропонують інтерактивні інформаційні панелі та захоплюючі 3D-інтерфейси, часто доповнені віртуальною реальністю, які надають операторам інтуїтивно зрозумілий доступ до складних даних. За допомогою цих інтерфейсів особи, які приймають рішення, можуть спостерігати за роботою системи в режимі реального часу, аналізувати історичні тенденції та отримувати попередження про аномалії. Такі інструменти дозволяють [48] вживати превентивних заходів, що вкрай важливо в умовах, коли будь-яка затримка з реагуванням може призвести до значних наслідків для безпеки або економіки.

Що стосується технологій, цифрові двійники покладаються на ряд сучасних рішень для зв'язку та управління даними. Передові обчислювальні та хмарні платформи працюють в тандемі для обробки, зберігання та аналізу безперервного

потоку даних. Хоча периферійні обчислення мінімізують затримку за допомогою локальної обробки даних, Хмарні обчислення забезпечують масштабованість, необхідну для складного моделювання та широкого історичного аналізу. Безпека залишається головним пріоритетом, оскільки цифрові двійники залежать від безпечної передачі конфіденційних даних. Для захисту цих систем від кіберзагроз використовуються протоколи шифрування, стандарти безпечної передачі даних і перевірки цілісності в режимі реального часу.

Багато галузей промисловості використовують технологію цифрового двійника через її трансформаційний потенціал. Наприклад, в моніторингу мостів цифрові двійники дозволяють на ранній стадії виявляти конструктивні проблеми за допомогою даних датчиків в режимі реального часу і моделювання. Один помітний випадок був пов'язаний із залізничним мостом у Норвегії, де дані з волоконних датчиків бреггівської решітки [49] дозволили інженерам своєчасно виявляти дефекти для планування технічного обслуговування, хоча і не змогли повністю запобігти інциденту. В енергетичному секторі цифрові двійники використовуються для управління електромережами, балансуючи попит і пропозицію, прогнозуючи перебої в роботі і оптимізуючи графіки технічного обслуговування критично важливих компонентів, таких як трансформатори. Містобудування також виграє від цифрових моделей-близнюків; такі міста, як Сінгапур, розробили комплексні віртуальні копії, які імітують транспортні потоки, використання комунальних послуг та сценарії реагування на надзвичайні ситуації, що значно допомагає в управлінні ресурсами та готовності до стихійних лих.

Промисловий та обробний сектори [50] використовують цифрові аналоги для підвищення операційної ефективності та впровадження інновацій. На виробництві віртуальні копії виробничого обладнання дозволяють проводити профілактичне технічне обслуговування та оптимізацію процесів, скорочуючи час простою і підвищуючи якість продукції. Керуючи ланцюгами поставок, цифрові двійники допомагають відстежувати та моделювати логістичні операції [50], забезпечуючи оптимальний розподіл ресурсів та своєчасне обслуговування.

Незважаючи на їх значні переваги, впровадження цифрових двійників

пов'язане з певними труднощами. Питання якості даних та інтеграції залишаються основними проблемами, оскільки неточності датчиків або некалібровані пристрої можуть призвести до спотворення моделей. Крім того, величезні обсяги даних, необхідні для створення точних цифрових двійників, вимагають передових методів об'єднання даних і високоякісних історичних даних, які не завжди можуть бути легко доступні. Кібербезпека являє собою ще одну серйозну проблему [51]; завдяки безперервним потокам даних і взаємопов'язаності цифрові двійники вразливі до кібератак, таких як програми-вимагачі або витік даних. Дотримання законів про конфіденційність та забезпечення безпечної передачі та зберігання даних є важливими, як і необхідність стандартизованих протоколів для забезпечення взаємодії між різними системами.

Заглядаючи в майбутнє, ми очікуємо, що майбутні розробки в області технології цифрового двійника дозволять вирішити ці проблеми за рахунок інтеграції новітніх технологій. Досягнення передових обчислень та впровадження мереж 5G обіцяють ще більше скоротити час очікування та розширити можливості обробки даних у режимі реального часу. Впровадження технології блокчейн [52] може забезпечити засоби для забезпечення цілісності даних і створення незмінних записів про зміни, в той час як більш просунутий штучний інтелект і алгоритми глибокого навчання поліпшать прогнозну аналітику і виявлення аномалій. Очікується більш широке впровадження в галузі, оскільки зусилля зі стандартизації, здійснені такими організаціями, як ISO та різними консорціумами digital twin, продовжують розвиватися. У міру розвитку нормативно-правової бази та етичних норм [53], вони будуть сприяти безпечному і відповідальному впровадженню технології digital twin.

Методи моніторингу критичної інфраструктури з використанням цифрових двійників. Сенсорні мережі та інтеграція Інтернету речей. В основі цифрових двійників лежить велика мережа датчиків і пристроїв Інтернету речей, які фіксують такі важливі параметри, як температура, деформація, тиск, вібрація і швидкість потоку. Наприклад:

- моніторинг структурного стану [54] (SHM): акселерометри, тензометричні

датчики та волоконно - оптичні датчики встановлюються на мостах та будівлях для постійного контролю цілісності;

- енергетичні системи: інтелектуальні лічильники і системи SCADA (диспетчерського управління і збору даних) відстежують споживання енергії в режимі реального часу і продуктивність мережі;

- екологічні датчики [55]: встановлюються в системах водопостачання та міських умовах для відстеження погодних умов, якості повітря та інших факторів навколишнього середовища;

- дані, зібрані цими датчиками, передаються в режимі реального часу в digital double, де вони використовуються для оновлення моделі та виявлення відхилень від очікуваної поведінки; імітаційне та прогностичне моделювання.

Цифрові двійники активно застосовують інструменти моделювання [56, 78], які використовують вхідні дані з датчиків для формування моделей поточного стану об’єкта в режимі реального часу. Серед основних підходів виділяють моделювання на основі фізичних принципів, що передбачає використання методу кінцевих елементів (FEA) або статистичних методів кінцевих елементів (State farm) для прогнозування розподілу напружень, втомних процесів та потенційних зон руйнування, що має особливу цінність для конструкцій у сфері цивільного будівництва. Інший важливий напрямок передбачає використання методів машинного навчання та штучного інтелекту [73, 78], де вдосконалені алгоритми аналізують історичні дані й дані в реальному часі для прогнозування майбутнього стану об'єкта, оптимізації операційних процесів та планування технічного обслуговування. Завдяки машинному навчанню стає можливим виявлення тонких закономірностей у потоках даних із сенсорів, що дозволяє ідентифікувати ранні ознаки погіршення стану об’єкта або потенційних кіберзагроз.

Сучасні платформи digital twins, включають в себе надійні механізми [57, 72] аналізу даних і інструменти візуалізації, які дозволяють операторам переглядати поточний стан і показники роботи інфраструктури за минулі періоди. Наприклад, інтерфейси інформаційних панелей - інформаційні панелі в режимі реального часу, які відображають ключові показники ефективності (KPI) і попереджають операторів

про аномалії; інтерфейси 3D і віртуальної реальності (VR) [58] - імерсивні моделі, які дозволяють інженерам "пройтися" по цифровому поданню об'єкта, підвищуючи ситуаційну обізнаність; прогнозовані звіти про технічне обслуговування - аналітичні дані для прогнозування необхідності технічного обслуговування допомагають запобігти незапланованим простоям та продовжити термін служби обладнання.

Ефективна, безпечна та надійна передача даних є критично важливою для успішної роботи цифрових двійників. Для цього застосовується широкий спектр технологій таких, як периферійні та хмарні обчислення [59, 71] та захищені протоколи передачі даних [70].

Периферійні обчислення здійснюють обробку даних безпосередньо на місці їх збору, що дозволяє мінімізувати затримки та підвищити швидкість реакції системи. Водночас хмарні платформи забезпечують централізоване зберігання великих обсягів інформації та виконання потужного аналітичного оброблення даних, включно з моделюванням складних сценаріїв та аналізом довгострокових тенденцій. Також для гарантування безпеки інформаційних потоків у цифрових двійниках використовуються сучасні методи шифрування даних, а також спеціалізовані захищені протоколи обміну, такі як DNP3, FTP і передача CSV-файлів через HTTPS. Крім того, впроваджуються механізми перевірки цілісності даних, що дозволяє запобігати підробкам, втратам або пошкодженню інформації під час її передачі.

Програмне забезпечення для моделювання та інструменти моделювання охоплюють широкий спектр технологічних рішень, що активно застосовуються під час створення цифрових двійників. Інформаційне моделювання будівель (BIM) широко використовується в цивільній інфраструктурі, адже інтегрує геометричні характеристики об'єктів із даними про їх експлуатаційні властивості для побудови детальних тривимірних моделей [74, 75]. Програмне забезпечення для аналізу кінцевих елементів [60] (FEA), таке як ANSYS та Abaqus, дозволяє моделювати поведінку конструкцій під дією різноманітних навантажень і сприяє прогнозуванню їхньої міцності та надійності. Крім того, у багатьох галузях промисловості створюються власні користувальницькі платформи моделювання, які поєднують можливості штучного інтелекту, машинного навчання та імітаційних моделей,

пристосованих до специфічних потреб конкретних сфер діяльності.

Штучний інтелект та машинне навчання [78] відіграють визначальну роль в обробці великих обсягів даних, що збираються цифровими двійниками. Алгоритми штучного інтелекту здійснюють виявлення аномалій шляхом аналізу потоків даних із сенсорів для виявлення закономірностей, які можуть свідчити про потенційні збої або кіберзагрози. Інтелектуальна аналітика [76, 77], що базується на моделях машинного навчання, дозволяє прогнозувати майбутній стан інфраструктурних об’єктів на основі даних про їхню минулу продуктивність та інформації, що надходить у режимі реального часу. Крім того, системи, керовані штучним інтелектом, активно підтримують процес прийняття рішень, формуючи рекомендації щодо технічного обслуговування та оптимізації експлуатаційних процесів, що сприяє підвищенню загальної стійкості систем.

Управління енергосистемою [61, 67] суттєво виграє від впровадження технології цифрових двійників. Цифрові копії електромереж забезпечують моніторинг енергосистеми в режимі реального часу, інтегруючи дані з інтелектуальних лічильників та SCADA-систем для ефективного балансування навантаження, прогнозування можливих перебоїв у роботі та оптимізації розподілу енергії. Прогнозоване технічне обслуговування [62] стає можливим завдяки моделюванню поведінки трансформаторів та інших ключових елементів інфраструктури, що дозволяє операторам своєчасно виявляти потенційні несправності та планувати ремонтні роботи до виникнення критичних поломок.

Міська інфраструктура та концепція "розумних міст" активно трансформуються під впливом технологій цифрових двійників. Моделі віртуальних міст [66], розроблені, зокрема, у таких мегаполісах, як Сінгапур, об'єднують дані транспортних систем, інженерних мереж та екологічних сенсорів, що дозволяє містобудівникам моделювати транспортні потоки, оптимізувати розподіл ресурсів і розробляти плани реагування на надзвичайні ситуації. Цифрові моделі-двійники [63, 79] також використовуються для підвищення готовності до стихійних лих, забезпечуючи можливість імітації таких подій, як повені чи землетруси, оцінки їхнього впливу на міську інфраструктуру та планування ефективних маршрутів

евакуації й стратегій використання ресурсів.

Промислова та обробна галузі також активно використовують можливості цифрових двійників, що дозволяє підприємствам суттєво підвищувати ефективність своїх процесів. На виробничих об'єктах цифрові двійники забезпечують постійний моніторинг технічного стану та прогнозну аналітику, що сприяє скороченню часу простою й підвищенню загальної продуктивності. Крім того, цифрові двійники відіграють важливу роль в оптимізації ланцюгів поставок [64, 68], дозволяючи ефективно відстежувати та управляти логістичними процесами, контролювати рівень запасів і планувати графіки виробництва, що в результаті підвищує стійкість і гнучкість виробничих систем.

Якість та інтеграція даних [65, 80] є фундаментальними аспектами для успішного створення та функціонування цифрових двійників. Надійність моделювання та точність прогнозів значною мірою залежать від того, наскільки дані, що надходять у систему, є повними, точними та узгодженими. Одним із критичних завдань на цьому етапі є калібрування датчиків та об'єднання даних [69], оскільки неточні, некалібровані або спотворені дані можуть суттєво знизити точність цифрового двійника, спричиняючи хибні висновки або неправильні рішення в реальному середовищі. Інтеграція даних, що надходять із різнорідних джерел - таких як сенсори, SCADA-системи, корпоративні бази даних або зовнішні інформаційні потоки, - вимагає застосування високонадійних методів обробки, які дозволяють зберігати узгодженість і актуальність інформації в режимі реального часу.

1.3 Постановка задачі

Поставлена мета досягається розв’язанням таких основних завдань:

1. аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників;
2. дослідити ключові особливості оптимізації та моделювання критичної IT інфраструктури цифровими двійниками;
3. покращити цільовою функцію та алгоритм оптимізації критичної IT інфраструктури цифровими двійниками;

4. розробити метод оптимізації критичної IT інфраструктури цифровими двійниками та дослідити практичне застосування цифрових двійників у критичній інфраструктурі.

1.4 Висновки до першого розділу

Досліджено потенційне застосування цифрових двійників для моніторингу стану об'єктів критичної інфраструктури, а також його ефективності, що має важливе значення для забезпечення стійкості в складному світі, що постійно змінюється. Проаналізовано відомі методи та технології моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників, які значно розширюють можливості управління інфраструктурними системами: від раннього виявлення потенційних відмов і дефектів до оптимізації обслуговування та стратегічного планування. Застосування таких технологій особливо актуальне для об’єктів з підвищеним рівнем ризику, де важлива кожна секунда реагування.

2 КЛЮЧОВІ ОСОБЛИВОСТІ ОПТИМІЗАЦІЇ ТА МОДЕЛЮВАННЯ КРИТИЧНОЇ ІТ ІНФРАСТРУКТУРИ ЦИФРОВИМИ ДВІЙНИКАМИ

2.1 Оптимізація критичної ІТ інфраструктури цифровими двійниками

В сучасному світі, де технології стрімко розвиваються, підтримка та модернізація ІТ-інфраструктури стають ключовими факторами успіху для будь-якої компанії. Оптимізація інфраструктури дозволяє підвищити продуктивність, знизити витрати та забезпечити надійність у роботі систем.

Цифрові двійники відіграють важливу роль в оптимізації критичної ІТ-інфраструктури, забезпечуючи віртуальне моделювання фізичних систем для покращення їхньої ефективності, надійності та безпеки. Вони дозволяють організаціям створювати точні віртуальні копії фізичних активів, що сприяє оптимізації використання ресурсів, підвищенню енергоефективності та зниженню витрат.

Використання цифрових двійників у критичній ІТ-інфраструктурі відкриває нові можливості для ефективного управління, аналізу та вдосконалення технологічних процесів. Ми виділили ряд переваг застосування цифрових двійників у критичній ІТ-інфраструктурі, які розглянемо нижче.

Першою перевагою є покращений моніторинг та глибока діагностика систем
Цифрові двійники дають змогу у режимі реального часу відстежувати всі параметри та показники роботи ІТ-систем, серверів та мереж. Це дозволяє оперативно реагувати на відхилення, швидко локалізувати джерело проблеми та приймати рішення щодо її усунення ще до виникнення критичної ситуації. Таким чином, зменшується ризик збоїв і підвищується загальна надійність інфраструктури.

Наступною перевага - реалізація прогнозного технічного обслуговування
Завдяки глибокому аналізу накопичених даних та машинному навчанню цифрові двійники можуть передбачити потенційні поломки або збої обладнання. Це дозволяє заздалегідь планувати обслуговування і модернізацію, мінімізувати незаплановані простої та суттєво зменшити витрати на аварійне реагування.

Ще одна з переваг - енергоефективність та ресурсна оптимізація. Віртуальне

моделювання роботи ІТ-систем допомагає оптимізувати споживання електроенергії та інших ресурсів. Аналізуючи різні сценарії навантаження, цифровий двійник пропонує конфігурації, які зменшують енергоспоживання без шкоди для продуктивності. Це особливо актуально для дата-центрів, де витрати на електроенергію є одними з найвищих.

Підвищення кібербезпеки та стійкості до зовнішніх загроз це остання, але не менш важлива перевага використання цифрових двійників у критичній ІТ-інфраструктурі. Завдяки можливості моделювати потенційні атаки та аномалії, цифрові двійники дозволяють виявляти вразливі місця у системах безпеки ще до того, як ними скористається зловмисник. Вони також використовуються для тестування різних сценаріїв реагування, що підвищує загальний рівень готовності ІТ-інфраструктури до надзвичайних ситуацій.

Оптимізація критичної ІТ-інфраструктури є стратегічно важливим процесом, що спрямований на забезпечення стабільної, ефективної та безпечної роботи всіх інформаційно-технологічних компонентів, які підтримують ключові бізнес-процеси, особливо в умовах зростання загроз і складності систем. Оптимізація охоплює низку послідовних етапів, кожен з яких має вирішальне значення для досягнення високого рівня продуктивності, масштабованості та надійності.

Перший етап - аналіз та планування. На цьому етапі проводиться глибоке вивчення поточного стану ІТ-інфраструктури: ідентифікуються всі компоненти (сервери, сховища, мережеве обладнання, ПЗ, служби безпеки); визначаються ключові показники ефективності (KPI), критичні точки відмови, рівень навантаження та потенційні вразливості.; формулюються вимоги до продуктивності, безпеки та відмовостійкості; проводиться SWOT-аналіз, формується дорожня карта змін із урахуванням цілей організації та бюджету.

Наступним етапом є проектування. Цей етап включає розробку оптимальної архітектури: обираються сучасні апаратні та програмні рішення (сервери, системи віртуалізації, хмарні сервіси, системи зберігання даних, засоби безпеки); проектується мережева топологія з урахуванням сегментації, балансування навантаження та резервування; розробляється концепція кіберзахисту (Zero Trust,

багаторівневий захист, SIEM, SOC); враховуються вимоги до масштабування, інтеграції з існуючими системами та відповідності стандартам (наприклад, ISO/IEC 27001, NIST).

Третій етап - впровадження. Цей етап передбачає практичну реалізацію проекту: проводиться налаштування серверів, мереж, віртуальних машин, програмного забезпечення; інтегруються нові компоненти у вже існуючу IT-екосистему з мінімальним впливом на безперервність роботи; реалізується резервне копіювання, аварійне відновлення, налаштовуються політики доступу; проводиться тестування всіх систем на сумісність, продуктивність і безпеку.

Ще один етап називається моніторинг та підтримка. Для підтримки стабільної роботи систем впроваджуються засоби моніторингу: використовуються інструменти для реального часу спостереження за навантаженням, затримками, логами, аномаліями; виявляються і оперативно усуваються збої та інциденти; впроваджуються автоматизовані сценарії реагування на критичні події; забезпечується регулярне оновлення систем, патч-менеджмент і аудит безпеки.

Оптимізація - заключний етап оптимізації. На основі зібраних даних проводиться глибокий аналіз ефективності IT-інфраструктури: ідентифікуються «вузькі місця», неефективні або застарілі компоненти; впроваджуються сучасні технології (контейнери, мікросервіси, SDN, автоматизація через IaC); оновлюється програмне забезпечення та апаратна база відповідно до сучасних вимог; застосовуються алгоритми оптимізації (ML, евристика, генетичні алгоритми) для автоматичного управління ресурсами; визначаються сценарії масштабування та адаптації до нових навантажень або кіберзагроз.

У підсумку, така комплексна оптимізація не лише покращує технічні показники, а й сприяє зниженню витрат, підвищенню бізнес-гнучкості та стійкості до зовнішніх впливів. У критичній IT-інфраструктурі, особливо в таких секторах, як енергетика, фінанси або транспорт, це є запорукою національної безпеки та стійкого розвитку.

Щоб ефективно оптимізувати IT-інфраструктуру, необхідно регулярно проводити аудит, виявляти слабкі місця та усувати потенційні загрози. Застарілі

системи можуть негативно впливати на продуктивність і безпеку, тому їх варто своєчасно оновлювати або замінювати.

Управління ризиками, пов’язаними з критичними IT-системами, може потребувати залучення зовнішніх фахівців або IT-аутсорсингових компаній, що допоможе підтримувати стабільність роботи бізнес-процесів.

Використання хмарних технологій сприяє підвищенню гнучкості та масштабованості інфраструктури, дозволяючи швидко адаптувати ресурси до змін у вимогах компанії.

Загалом, оптимізація критичної IT-інфраструктури потребує комплексного підходу, включаючи ретельне планування, постійний моніторинг і своєчасне оновлення для забезпечення її стабільності та безпеки.

Оптимізація критичної IT-інфраструктури - це стратегічно важливий процес, спрямований на забезпечення стабільної, надійної та безпечної роботи цифрових систем підприємства. Вона охоплює не лише технічне вдосконалення, а й організаційні заходи, що впливають на загальну ефективність IT-екосистеми. На додаток до основних етапів, варто розглянути такі ключові аспекти, як: ідентифікація та управління ризиками, технічне документування систем, автоматизація операційних процесів, безпечне управління доступом та інтеграція інноваційних технологій.

Ідентифікація та управління ризиками полягає у важливості своєчасного виявлення можливих загроз, які можуть вплинути на функціонування IT-інфраструктури, а також розробці превентивних заходів, сценаріїв реагування на критичні інциденти і тестування відновлення після збоїв сприяє підвищенню кіберстійкості та зменшенню тривалості простоїв.

В основі технічного документування систем лежить формування повної та актуальної технічної документації щодо структурної побудови, конфігурацій, мережевих залежностей та політик управління системами, що значно полегшує масштабування, аудит, обслуговування та модернізацію інфраструктури;

Автоматизація операційних процесів грунтується на застосуванні спеціалізованих програмних засобів для автоматичного моніторингу стану систем,

запуску резервного копіювання, встановлення оновлень, управління навантаженням тощо. Автоматизація підвищує швидкість реакції на зміни в середовищі, скорочує витрати часу й ресурсів, а також мінімізує вплив людського чинника.

Безпечне управління доступом здійснює впровадження сучасних механізмів ідентифікації та авторизації користувачів, регулярний аудит привілеїв, а також застосування політик мінімального доступу. Такі заходи дозволяють захистити критичні дані від внутрішніх та зовнішніх загроз і підвищити загальний рівень кібербезпеки.

Інтеграція інноваційних технологій включає використання інструментів штучного інтелекту, машинного навчання та цифрових двійників дозволяє здійснювати глибший аналіз продуктивності систем, прогнозувати навантаження та виявляти аномалії в режимі реального часу. Це відкриває нові можливості для гнучкої адаптації та інтелектуального управління ресурсами.

Цей підхід до оптимізації дозволяє створити гнучку, масштабовану та захищену IT-інфраструктуру, здатну ефективно реагувати на динамічні виклики цифрового середовища.

Розглянемо на конкретному прикладі впровадження оптимізації в роботу дата-центру великої фінансової установи.

Фінансова установа має великий дата-центр, який обслуговує мільйони транзакцій щодня. Через зростання навантаження почали виникати періодичні збої, а енергоспоживання значно перевищувало норми. Була прийнята стратегія впровадження цифрового двійника IT-інфраструктури для оптимізації процесів.

Етапи впровадження цифрового двійника для оптимізації процесів у дата-центрі великої фінансової установи охоплювали кілька ключових кроків. На першому етапі було створено віртуальну модель, яка базувалася на реальній конфігурації серверного обладнання, мережевих пристроїв та систем охолодження. До цифрового двійника інтегрували дані з фізичних датчиків температури, навантаження на процесори, обсягів трафіку та показників енергоспоживання, що забезпечило достовірне відображення поточного стану інфраструктури.

На другому етапі здійснювався аналіз отриманих у реальному часі даних.

Модель дозволяла виявляти вузькі місця у функціонуванні систем, такі як перенавантаження певних кластерів серверів чи неефективність роботи охолоджувальних установок у окремих зонах дата-центру.

Далі проводилася оптимізація розподілу навантаження. За допомогою симуляцій цифровий двійник випробував різні стратегії балансування ресурсів між серверами. На основі результатів тестування було обрано найефективніший варіант, що дозволив знизити затримку в обробці запитів на 30% і суттєво підвищити продуктивність систем у години пікового навантаження.

На четвертому етапі реалізували заходи з енергетичної оптимізації. Моделювання впливу зміни температурних режимів на продуктивність обладнання дало можливість удосконалити роботу систем кондиціонування, внаслідок чого споживання електроенергії вдалося скоротити на 15%, без негативного впливу на стабільність функціонування дата-центру.

Завершальним етапом стало впровадження механізмів прогнозування відмов. Завдяки аналізу історичних даних цифровий двійник набув здатності передбачати потенційні відмови серверного обладнання за кілька днів до можливого інциденту, що дозволило своєчасно здійснювати профілактичне технічне обслуговування та суттєво підвищити надійність роботи IT-інфраструктури.

В результаті впровадження заходів з оптимізації функціонування дата-центру великої фінансової установи були досягнуті суттєві покращення. Зокрема, постійний моніторинг у режимі реального часу із застосуванням цифрового двійника забезпечив своєчасне виявлення аномалій та потенційних точок відмови, що дозволило зменшити тривалість простоїв на 40%. Прогнозування поведінки системи під навантаженням сприяло завчасному усуненню ризиків виникнення збоїв, унаслідок чого середній час простою сервісів скоротився майже вдвічі, підвищуючи доступність ключових фінансових послуг для користувачів.

Оптимізація розподілу обчислювальних ресурсів на основі аналітики цифрового двійника дозволила підвищити загальну продуктивність системи на 25%. Застосування алгоритмів адаптивного управління забезпечило оперативний перерозподіл навантаження між серверами, що призвело до мінімізації затримок і

покращення швидкості обробки запитів, особливо в періоди пікової активності, що позитивно позначилося на функціонуванні критично важливих бізнес-додатків.

Оптимізація сценаріїв енергоспоживання шляхом моделювання дозволила досягти зниження споживання електроенергії на 15%. Удосконалення роботи систем охолодження, живлення та балансування навантаження сприяло зменшенню витрат енергоресурсів без втрати продуктивності, що, у свою чергу, призвело до скорочення експлуатаційних витрат та зниження екологічного навантаження на довкілля.

Інтеграція цифрового двійника з системами забезпечення інформаційної безпеки дозволила моделювати та тестувати різноманітні сценарії кібератак без ризику для реальної інфраструктури. Це сприяло своєчасному виявленню потенційних загроз і вдосконаленню заходів кібербезпеки, що підвищило рівень захисту даних і зміцнило довіру до IT-інфраструктури з боку партнерів, клієнтів і регуляторних органів.

Крім того, впровадження цифрового двійника дозволило оптимізувати витрати на IT-обслуговування. Прогнозування технічного стану обладнання, автоматизація рутинних процесів обслуговування, а також планування закупівлі запчастин сприяли скороченню кількості позапланових виїздів інженерного персоналу та зменшенню обсягів ручних перевірок, що у підсумку дозволило суттєво знизити загальні витрати на експлуатацію дата-центру.

Отже, впровадження цифрового двійника дозволило не тільки оптимізувати існуючу інфраструктуру, а й надало можливість прогнозувати подальші дії, гнучко реагувати на зміни навантаження та підвищити стійкість критично важливої IT-системи.

Розглянемо приклад впровадження цифрового двійника в критичній інфраструктурі АЕС (рис. 2.1)

Впровадження цифрового двійника для системи охолодження реакторного відділення АЕС

Мета впровадження - підвищення безпеки, оптимізація енергоспоживання та забезпечення прогнозного обслуговування системи охолодження ядерного реактора.

Функціональність цифрового двійника

Рисунок 2.1 - Приклад впровадження цифрового двійника в критичній інфраструктурі АЕС

Реальний моніторинг: отримання даних у режимі реального часу з датчиків температури, тиску, швидкості потоку охолоджувального середовища; порівняння показників з історичними даними для виявлення відхилень або потенційних збоїв.

Симуляції сценаріїв: моделювання поведінки системи при різних аварійних ситуаціях (наприклад, зниження тиску, збій насоса, перегрів); випробування нових параметрів без ризику для реального об’єкта.

Прогнозування відмов: на основі зібраних даних і машинного навчання прогнозуються терміни зносу обладнання; формуються графіки технічного обслуговування з урахуванням ризиків і пріоритетів.

Оптимізація процесів: розрахунок оптимального режиму роботи насосів і вентиляторів для економії енергії; зменшення теплових втрат і навантаження на систему без шкоди для безпеки.

Результати впровадження цифрового двійника для системи охолодження реакторного відділення атомної електростанції засвідчили низку істотних покращень. Завдяки моделюванню теплових і гідравлічних процесів у реальному

часі вдалося підвищити ефективність використання обладнання на 12–18%. Цифровий двійник забезпечував точне відстеження робочих параметрів насосів, теплообмінників та інших ключових компонентів, що дозволило операторам приймати обґрунтовані рішення щодо режимів експлуатації, зменшити простої та підвищити коефіцієнт корисної дії систем, одночасно продовжуючи ресурс їхньої роботи.

Оптимізація роботи вентиляторів, насосів і контурів циркуляції охолоджувальної рідини сприяла зниженню енергоспоживання на 10–15%. Використання алгоритмів машинного навчання дозволило виявити такі режими роботи обладнання, які забезпечували належний рівень охолодження з мінімальними витратами енергії. Це призвело до суттєвого економічного ефекту та водночас зменшило екологічне навантаження на довкілля.

Крім того, завдяки можливості моделювати поведінку системи в умовах змін навантаження, зовнішніх чинників та внутрішніх збоїв, вдалося скоротити кількість нештатних ситуацій на 20%. Цифровий двійник дозволив своєчасно виявляти потенційні відхилення у роботі системи охолодження та застосовувати проактивні заходи, що запобігало виникненню критичних інцидентів, таких як перегрів або відмова контурів охолодження.

Важливим досягненням стало впровадження переходу до планового обслуговування на основі фактичного стану обладнання замість жорстких графіків або аварійних зупинок. Дані цифрового двійника дозволяли прогнозувати знос ключових компонентів, що допомогло мінімізувати кількість аварійних робіт, знизити навантаження на технічний персонал та загалом підвищити надійність експлуатації реакторного відділення.

Нарешті, використання цифрового двійника сприяло підвищенню рівня загальної безпеки об’єкта та забезпеченню відповідності міжнародним стандартам, зокрема нормам МАГАТЕ (IAEA Safety Standards). Завдяки можливості документувати та контролювати критичні параметри в реальному часі процеси аудитів і перевірок стали значно простішими, що позитивно позначилося на довірі до безпеки експлуатації ядерної установки як з боку внутрішніх структур, так і

міжнародних регулюючих органів.

Отже, впровадження цифрового двійника в критичній інфраструктурі, зокрема на АЕС, забезпечує підвищення безпеки, ефективності та надійності систем за рахунок точного моделювання, моніторингу в реальному часі та прогнозування потенційних загроз. Це дозволяє оперативно реагувати на відхилення, оптимізувати технічне обслуговування й приймати обґрунтовані рішення протягом усього життєвого циклу об’єкта.

Щоб ефективно оптимізувати ІТ-інфраструктуру, необхідно регулярно проводити аудит, виявляти слабкі місця та усувати потенційні загрози. Застарілі системи можуть негативно впливати на продуктивність і безпеку, тому їх варто своєчасно оновлювати або замінювати.

Управління ризиками, пов’язаними з критичними ІТ-системами, може потребувати залучення зовнішніх фахівців або ІТ-аутсорсингових компаній, що допоможе підтримувати стабільність роботи бізнес-процесів.

Використання хмарних технологій сприяє підвищенню гнучкості та масштабованості інфраструктури, дозволяючи швидко адаптувати ресурси до змін у вимогах компанії.

Загалом, оптимізація критичної ІТ-інфраструктури потребує комплексного підходу, включаючи ретельне планування, постійний моніторинг і своєчасне оновлення для забезпечення її стабільності та безпеки.

2.2 Моделювання критичної ІТ інфраструктури цифровими двійниками

Цифрові двійники – це віртуальні копії фізичних об'єктів або систем, що дають змогу в реальному часі відстежувати їхній стан, аналізувати роботу та прогнозувати можливі зміни. Вони допомагають покращити керування інфраструктурою, підвищити її ефективність і знизити ризики.

Застосування цифрових двійників у сфері критичної інфраструктури демонструє значний потенціал для підвищення ефективності, безпеки та надійності її роботи. Зокрема, в енергетичному секторі компанії ETAP і Schneider Electric

впровадили цифровий двійник для аналізу енергоспоживання дата-центрів, що працюють із використанням технологій штучного інтелекту. Завдяки цій розробці стало можливим у режимі реального часу здійснювати моніторинг електроспоживання, прогнозувати зміни навантаження та оптимізувати розподіл ресурсів, що сприяє підвищенню енергоефективності об'єктів.

У галузі ядерної енергетики прикладом ефективного використання цифрових двійників є Чорнобильська атомна електростанція, де створено тривимірні моделі інфраструктури. Ці цифрові копії допомагають безпечно планувати виконання робіт, обирати оптимальні маршрути пересування персоналу та мінімізувати ризики радіаційного впливу, що є критично важливим для охорони здоров'я працівників та довкілля.

У телекомунікаційній сфері цифрові двійники використовуються для випробування нових технічних рішень у віртуальному середовищі. Це дозволяє знижувати ймовірність виникнення технічних помилок під час реального впровадження змін, а також модернізувати мережеву інфраструктуру без порушення безперервності її роботи. Таким чином, технологія цифрових двійників поступово стає невід'ємною складовою розвитку та удосконалення критичних секторів інфраструктури.

Завдяки можливості моделювати поведінку систем, аналізувати різні сценарії розвитку подій та оптимізувати ресурси, цифрові двійники відкривають нові горизонти для підвищення надійності, ефективності та безпеки критичної інфраструктури. Нижче розглянуто ключові переваги моделювання критичної IT інфраструктури цифровими двійниками, що зумовлюють його стрімке впровадження у стратегічно важливих галузях.

Збільшення ефективності це перша з переваг моделювання критичної IT інфраструктури цифровими двійниками**.** Цифрові двійники дозволяють моделювати роботу IT-інфраструктури або інженерних систем у реальному часі, аналізувати продуктивність та завантаження окремих компонентів. Це дає змогу: оптимізувати розподіл ресурсів (серверних потужностей, енергоспоживання, трафіку), зменшити кількість ручних операцій шляхом автоматизації, підвищити загальний коефіцієнт

використання обладнання (OEE), скоротити витрати на обслуговування та експлуатацію.

Попередження аварій і збоїв - наступна перевага. Модель цифрового двійника дозволяє постійно аналізувати стан системи на основі телеметрії, логів та показників з сенсорів. Це дає можливість: прогнозувати потенційні несправності за допомогою методів предиктивної аналітики; здійснювати технічне обслуговування за потребою (condition-based maintenance), а не за графіком; вчасно виявляти перегріви, перевантаження, відмови в логіці або апаратному забезпеченні; запобігати серйозним аваріям та скоротити час простою.

Ще одна з переваг - підвищення рівня безпеки**.** Цифровий двійник створює безпечне середовище для: тестування нових налаштувань, оновлень або змін у конфігурації без ризику для реальної системи;моделювання впливу потенційних кібератак або фізичних загроз; тренування персоналу в умовах симуляції надзвичайних ситуацій; перевірки відповідності нормативним вимогам без зупинки реального обладнання.

Черговою перевагою є покращене управління прийняттям рішень**.** Моделі цифрових двійників можуть використовуватися для багатосценарного аналізу («що-якщо»), що дає змогу: оцінювати наслідки управлінських рішень до їх впровадження, порівнювати ефективність різних стратегій модернізації, оптимізувати інвестиції у розвиток інфраструктури, формувати дані для підтримки рішень у кризових ситуаціях.

Безперервна адаптація та масштабування це заключна перевага, яку ми виділили. Завдяки здатності оновлюватися в режимі реального часу, цифрові двійники: відображають актуальний стан системи з мінімальною затримкою, легко адаптуються до змін у конфігурації або умовах експлуатації, забезпечують швидкий перехід до нових архітектур або навантажень без втрат стабільності.

Загалом, цифрові двійники стають потужним інструментом для управління критичною інфраструктурою, допомагаючи компаніям знижувати ризики, покращувати безпеку та ефективніше використовувати ресурси.

Цифрові двійники є потужним інструментом для моделювання та управління

критичною інфраструктурою. Вони створюють віртуальні копії фізичних об'єктів або систем, що дозволяє відстежувати їхній стан у реальному часі, аналізувати роботу та прогнозувати можливі зміни. Це сприяє підвищенню ефективності, зниженню ризиків і оптимізації процесів.

Цифрові двійники та традиційне моделювання є потужними інструментами для аналізу та прогнозування поведінки систем. Попри використання цифрових моделей в обох підходах, між ними існують суттєві відмінності.

Розглянемо масштаб та рівень охоплення. Традиційне моделювання зазвичай орієнтоване на окремі елементи або процеси в межах певної системи. Воно дозволяє глибоко аналізувати окремі аспекти роботи, але при цьому часто не враховує взаємозв’язки між різними компонентами, що може призводити до фрагментарного бачення ситуації.

Цифрові двійники, навпаки, охоплюють всю систему в комплексі. Вони забезпечують наскрізне бачення функціонування об'єкта або інфраструктури, дозволяючи моделювати складні сценарії взаємодії всіх її частин. Це включає паралельне відтворення багатьох процесів, що взаємно впливають один на одного, і дозволяє краще розуміти поведінку системи у динамічному середовищі.

Розглянемо інтерактивність, гнучкість і динамічне оновлення. У традиційних моделях зміни параметрів здійснюються вручну, а оновлення моделей потребує повторного запуску або навіть повного переналаштування. Дані, як правило, не надходять автоматично, що обмежує адаптивність таких моделей до змін у реальному часі.

Цифрові двійники, натомість, забезпечують повну інтерактивність та оперативне оновлення завдяки постійному потоку даних з фізичних об’єктів через сенсори, IoT-пристрої або інші канали збору інформації. Модель автоматично синхронізується з реальною системою, дозволяючи проводити симуляції в режимі реального часу, тестувати різні сценарії розвитку подій та приймати обґрунтовані рішення на основі актуальних даних.

Розглянемо постійну взаємодію з фізичним об’єктом. Традиційне моделювання зазвичай базується на фіксованих вихідних даних, які збираються на момент

проєктування або дослідження. Модель не має постійного з’єднання з об'єктом у реальному світі, що обмежує її актуальність у процесі експлуатації.

Цифрові двійники, натомість, функціонують у тісному зв’язку з фізичною системою завдяки двонаправленому обміну інформацією. Через мережі датчиків, IoT-пристрої та системи телеметрії цифровий двійник отримує оновлені дані в режимі реального часу й може впливати на об'єкт, пропонуючи оптимальні рішення або навіть автоматично ініціюючи дії.

Розглянемо універсальність протягом усього життєвого циклу. Традиційне моделювання переважно зосереджується на ранніх етапах життєвого циклу системи – таких як проєктування, планування або верифікація. Після впровадження системи модель часто втрачає свою актуальність.

Цифровий двійник супроводжує систему на всіх етапах її існування - від початкового проєктування до експлуатації, обслуговування і навіть виведення з експлуатації. Це дозволяє постійно вдосконалювати архітектуру, знижувати витрати, прогнозувати потенційні збої та забезпечувати ефективне управління протягом усього життєвого циклу.

Розглянемо технологічну складність та вимоги до інфраструктури. Традиційні моделі можуть бути реалізовані за допомогою простих програмних рішень, без необхідності в складній апаратній інфраструктурі. Це робить їх доступними, але водночас обмежує можливості реалістичної симуляції складних та динамічних систем.

Цифрові двійники, у свою чергу, вимагають високого рівня технологічної підготовки. Для їх ефективної роботи потрібна інтеграція великої кількості датчиків, систем збирання й обробки даних, аналітичних платформ (наприклад, AI/ML), хмарних сервісів, інструментів візуалізації та потужних обчислювальних ресурсів. Такий підхід забезпечує точне, гнучке й масштабоване моделювання реального світу у цифровому середовищі.

Загалом, цифрові двійники надають більш глибоке та динамічне розуміння системи, дозволяючи не лише прогнозувати її поведінку, але й активно впливати на процеси в реальному часі. Традиційне моделювання залишається корисним

інструментом для аналізу окремих аспектів системи, проте цифрові двійники відкривають ширші можливості для комплексного управління та оптимізації.

Впровадження цифрових двійників у критичну інфраструктуру відіграє важливу роль у підвищенні ефективності, безпеки та надійності складних систем. Особливості їхнього моделювання визначаються необхідністю роботи з реальними об'єктами, високими вимогами до безпеки та інтеграцією передових технологій.

Особливості моделювання цифрових двійників в критичній інфраструктурі:

1) глибока інтеграція з фізичними системами - цифрові двійники є не просто віртуальними моделями, а динамічними копіями реальних об'єктів або систем; вони синхронізуються з фізичними елементами за допомогою сенсорів, що дозволяє відстежувати поточний стан інфраструктури та прогнозувати зміни в режимі реального часу;

2) використання складних математичних моделей - моделювання критичної інфраструктури вимагає застосування складних алгоритмів, що базуються на методах штучного інтелекту, машинного навчання та фізичних симуляціях; це дозволяє точно аналізувати взаємозв’язки між елементами системи та передбачати потенційні загрози чи відмови;

3) постійне оновлення та адаптація - на відміну від традиційного моделювання, цифрові двійники не є статичними; вони постійно оновлюються завдяки даним, що надходять із датчиків та інших джерел, забезпечуючи актуальність інформації та можливість оперативного прийняття рішень;

4) забезпечення кібербезпеки - критична інфраструктура є основною мішенню для кіберзагроз, тому цифрові двійники повинні бути захищені від несанкціонованого доступу; використання шифрування, блокчейн-технологій та спеціалізованих алгоритмів захисту допомагає запобігти витоку даних і можливим атакам на систему;

5) візуалізація та 3D-моделювання - цифрові двійники дозволяють створювати реалістичні 3D-моделі фізичних об'єктів, що полегшує їх моніторинг, аналіз та управління; це особливо корисно для складних інженерних систем, таких як енергетичні мережі, транспортна інфраструктура або промислові об’єкти;

6) інтеграція з Інтернетом речей (IoT) - цифрові двійники критичної інфраструктури працюють у тісному зв’язку з IoT-пристроями, що дозволяє збирати великі обсяги даних у режимі реального часу; завдяки цьому можна проводити точний аналіз та прогнозувати можливі сценарії розвитку подій;

7) моделювання сценаріїв та прогнозування ризиків - однією з основних переваг цифрових двійників є можливість тестування різних сценаріїв та аналізу їхніх наслідків; це дозволяє прораховувати потенційні ризики, запобігати критичним збоям та оптимізувати процеси управління інфраструктурою;

8) підвищення надійності та оптимізація ресурсів - завдяки цифровим двійникам можна виявляти неефективні ділянки в роботі інфраструктури та покращувати використання ресурсів; це сприяє зменшенню витрат, підвищенню продуктивності та запобіганню аварійним ситуаціям.

Цифрові двійники змінюють підхід до управління критичною інфраструктурою, забезпечуючи її стійкість, безпеку та ефективність. Вони дозволяють не лише відстежувати стан систем у режимі реального часу, але й передбачати можливі загрози, що робить їх ключовим інструментом у сучасних технологічних екосистемах.

Розглянемо приклад цифрового двійника енергетичної підстанції. Енергетична підстанція є критичним об'єктом, що відповідає за передачу та розподіл електроенергії в регіоні. Будь-який збій у її роботі може призвести до відключення енергопостачання, економічних втрат і навіть загроз для життя.

Цифровий двійник енергетичної підстанції - це віртуальна модель, що інтегрує фізичні об’єкти, дані в реальному часі та алгоритми аналітики для забезпечення безперервного моніторингу, моделювання, прогнозування та оптимізації роботи об’єкта критичної інфраструктури.

Мета моделювання: створення цифрового двійника підстанції з метою забезпечення моніторингу в реальному часі, прогнозування відмов обладнання та оптимізації технічного обслуговування.

Кроки моделювання цифрового двійника:

1) збір та агрегування даних - встановлення IoT-сенсорів на ключових

елементах обладнання: трансформаторах, автоматичних вимикачах, шинопроводах, кабельних каналах, системах охолодження; збір історичних даних (SCADA, OPC, журналів обслуговування) щодо режимів навантаження, температури, вологості, частоти збоїв, циклів вмикання/вимикання; оцифрування технічної документації, схем, специфікацій та стандартів для інтеграції в цифрову модель;

2) створення 3D-моделі підстанції - використання BIM (Building Information Modeling), CAD або лазерного 3D-сканування для побудови точного геометричного зображення об'єкта; візуалізація структурних і функціональних елементів підстанції: трансформаторних відсіків, кабельних трас, шаф керування, заземлення, охоронних зон; анімація потоку енергії, руху персоналу, зон обслуговування тощо;

3) побудова фізико-математичної моделі обладнання - створення моделей електричних, теплових, механічних процесів на основі відповідних законів (Ома, Кірхгофа, Фур'є, Ньютона); моделювання динаміки роботи автоматики, релейного захисту, АСКТП; інтеграція методів штучного інтелекту (ML/DL) для виявлення аномалій, прогнозування відмов, оптимізації роботи обладнання;

4) інтеграція цифрового двійника з фізичною системою - надсилання даних у реальному часі з сенсорів до цифрової моделі через MQTT, OPC UA, REST API; виведення інтерактивних дашбордів: температурний профіль, графіки навантаження, енергоспоживання, технічний стан компонентів; сигналізація аварійних ситуацій, запуск сценаріїв реагування;

5) аналіз сценаріїв роботи та відмов - віртуальна симуляція різних подій: коротке замикання, відмова трансформатора, перевантаження фідерів; аналіз сценаріїв безперебійного живлення, балансування навантаження в мережі при часткових збоях; тестування алгоритмів релейного захисту, запуск резервного живлення, оцінка часу реагування системи;

6) прогнозування та динамічне планування технічного обслуговування - на основі зібраних телеметричних даних аналізується стан компонентів: трансформаторної оливи, з'єднань, вентиляційних систем; визначаються критичні пороги зносу, будується графік обслуговування, заснований на реальному технічному стані обладнання; уникається надмірне або запізніле обслуговування -

зменшуються витрати, підвищується надійність;

7) розширення функціоналу та інтелектуальне управління - впровадження елементів автоматизованого управління навантаженням, температурними режимами, вентиляцією на основі аналізу цифрового двійника; створення моделей для навчання персоналу в симульованому середовищі; підключення до загального енергетичного цифрового близнюка регіону/мережі для оптимізації глобальних процесів передачі електроенергії.

Нижче розглянемо структуру коду для простої Python-емуляції цифрового двійника. Це демо цифрового двійника, що отримує “дані” з сенсорів (емульовані); аналізує стан трансформатора (перегрів, перевантаження) та прогнозує несправності.

Проєктна структура подано на рисунку 2.2.

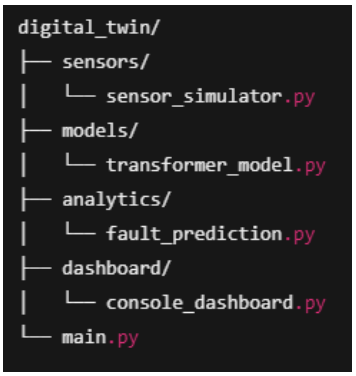

Рисунок 2.2 - Проєктна структура

На рисунку 2.3 показано імітацію роботи датчика.

```
import random

def read_sensor_data():
    return {
        "temperature": random.uniform(60, 110),  # °C
        "load": random.uniform(0.5, 1.5),         # Відносне навантаження
        "vibration": random.uniform(0.2, 0.8),    # Умовні одиниці
    }
```

Рисунок 2.3 - Імітація роботи датчика

На рисунку 2.4 зображено перевірки стану датчика.

```python
def is_overheated(temp):
    return temp > 95

def is_overloaded(load):
    return load > 1.2

def is_vibration_excessive(vibration):
    return vibration > 0.6
```

Рисунок 2.4 - Перевірки стану датчика

На рисунку 2.5 показано прогнозування ризиків на основі даних що зібрав датчик.

```python
def predict_failure(sensor_data):
    score = 0
    if sensor_data["temperature"] > 100:
        score += 0.4
    if sensor_data["load"] > 1.3:
        score += 0.4
    if sensor_data["vibration"] > 0.7:
        score += 0.2

    if score > 0.6:
        return "Ймовірна відмова найближчим часом"
    elif score > 0.3:
        return "Підвищений ризик — потрібна діагностика"
    else:
        return "Стан стабільний"
```

Рисунок 2.5 - Прогнозування ризиків

На рисунку 2.6 зображено вивід інформації по датчику та прогнозовані ризики.

```python
def display_status(data, prediction):
    print("📡 Дані сенсорів:")
    print(f"Температура: {data['temperature']:.2f}°C")
    print(f"Навантаження: {data['load']:.2f}")
    print(f"Вібрації: {data['vibration']:.2f}")
    print("\n🧠 Прогноз:")
    print(f"📈 {prediction}")
    print("-" * 40)
```

Рисунок 2.6 - Вивід інформації

На рисунку 2.7 зображено запуск цифрового двійника для тестування системи.

```
import time
from sensors.sensor_simulator import read_sensor_data
from models.transformer_model import is_overheated, is_overloaded, is_vibration_excessive
from analytics.fault_prediction import predict_failure
from dashboard.console_dashboard import display_status

if __name__ == "__main__":
    while True:
        sensor_data = read_sensor_data()
        prediction = predict_failure(sensor_data)
        display_status(sensor_data, prediction)
        time.sleep(2)
```

Рисунок 2.7 - Запуск цифрового двійника

Очікуваними результатами впровадження цифрового двійника енергетичної підстанції є суттєве скорочення аварійних відключень завдяки безперервному моніторингу стану обладнання та ранньому виявленню відхилень, що дозволяє знизити кількість аварій до 40% і позитивно впливає на стабільність електропостачання. Також - оптимізація витрат на технічне обслуговування шляхом переходу від планово-профілактичного до умовно-профілактичного обслуговування на основі предиктивної аналітики, що веде до зменшення експлуатаційних витрат на 25%. Завдяки можливості швидкої діагностики і локалізації несправностей у режимі реального часу, що значно скорочує час простою обладнання та забезпечує оперативне усунення проблем,що являє собою прискорене виявлення технічних дефектів. Підвищення рівня енергетичної безпеки регіону завдяки проактивному управлінню інфраструктурою та моделюванню критичних сценаріїв - знижує ризик масових відключень і зміцнює надійність енергосистеми в умовах надзвичайних ситуацій або кіберзагроз, а також покращення прозорості та керованості процесів. Це покращення досягається шляхом інтеграції даних з різних джерел в єдину цифрову модель, що забезпечує повну видимість технічного стану об’єкта для операторів, інженерного персоналу та керівництва.

Отже, моделювання критичної інфраструктури за допомогою цифрових двійників дозволяє створити точну віртуальну копію фізичної системи для її глибокого аналізу, моніторингу та оптимізації в реальному часі. Завдяки інтеграції з

датчиками та аналітичними алгоритмами, цифрові двійники підвищують надійність, ефективність і стійкість критичних ІТ-систем, забезпечуючи своєчасне реагування на ризики та підтримку безперервності операцій.

2.3 Висновки до другого розділу

Встановлено, що оптимізація критичної ІТ-інфраструктури за допомогою цифрових двійників дозволяє підвищити ефективність управління ресурсами, мінімізувати ризики збоїв і забезпечити безперервність роботи систем у режимі реального часу.

А також досліджено, що моделювання критичної ІТ-інфраструктури за допомогою цифрових двійників забезпечує глибоке розуміння роботи систем, підвищує надійність та сприяє прийняттю обґрунтованих рішень для їх оптимального функціонування.

3 ПРОЦЕС ОПТИМІЗАЦІЇ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ЦИФРОВИХ ДВІЙНИКІВ

3.1 Цільова функція оптимізації критичної IT інфраструктури цифровими двійниками

У контексті цифрової трансформації критичних IT-систем цифрові двійники стають потужним інструментом для досягнення максимальної ефективності, надійності та стійкості інфраструктури. Вони дозволяють моделювати, аналізувати та оптимізувати реальні процеси без прямого втручання в фізичну систему. Центральним елементом такого підходу є цільова функція - узагальнений критерій або сукупність критеріїв, які система прагне оптимізувати.

Основними складовими цільової функції оптимізації критичної IT-інфраструктури є підвищення продуктивності, надійність і безперебійність роботи, оптимізація витрат, енергоефективність, кібербезпека та адаптивність до змін.

Розглянемо детальніше кожну складову цільової функції оптимізації критичної інфраструктури.

Підвищення продуктивності полягає в оптимізації використання ресурсів, безперервності сервісів та зменшення часу відповіді систем. Завдяки цифровому двійнику можливе моделювання оптимальних конфігурацій роботи мережевих та обчислювальних систем із врахуванням динамічних змін навантаження. Система може передбачити пікові періоди та автоматично перерозподіляти потужності, забезпечуючи стабільну роботу критичних додатків та сервісів, а також здійснює зменшення латентності між компонентами за рахунок аналізу потоків даних у віртуальному середовищі.

Надійність і безперебійність роботи включає зниження частоти аварій, покращене резервування та failover-моделювання. Моделювання фізичного зносу компонентів дозволяє заздалегідь виявити критичні елементи, що можуть призвести до збоїв. Цифровий двійник дозволяє протестувати сценарії відмов у режимі симуляції та підібрати найкращу стратегію відновлення і віртуальне тестування

автоматичного перемикання на резервні системи у разі відмови основної інфраструктури.

Оптимізація витрат охоплює зниження OPEX (операційних витрат), прогнозне бюджетування та автоматизацію рутинних процесів. Прогнозне обслуговування дозволяє проводити ремонт лише тоді, коли це справді необхідно, зменшуючи витрати на непотрібне обслуговування. Завдяки аналітиці цифрового двійника можна точніше планувати закупівлі, модернізацію та заміну компонентів. Автоматизація рутинних процесів призводить до зниження навантаження на IT-персонал і скорочення витрат на ручну роботу.

Енергоефективність грунтується на інтелектуальному керуванні енергоспоживанням, застосуванні “зелених” технологій та управлінні тепловими режимами. Моделі дозволяють аналізувати в реальному часі, які компоненти споживають найбільше електроенергії, та оптимізувати їхню роботу, а також виявляють можливості для інтеграції альтернативних джерел енергії (наприклад, резервне живлення від сонячних панелей) і запобігають перегріву за допомогою прогнозної оптимізації охолодження, що водночас знижує енергоспоживання.

Кібербезпека складається зі сценарного моделювання атак, оптимізації розміщення захисних засобів та підтримку стандартів інформаційної безпеки віртуальні моделі яких допомагають тестувати відповідність ISO/IEC 27001, NIST CSF тощо. Цифровий двійник дозволяє симулювати DDoS-атаки, проникнення у систему, або вразливість до експлойтів без шкоди для реального середовища. На основі результатів симуляцій можна краще розподілити мережеві екрани, системи виявлення вторгнень (IDS/IPS), сегментацію.

Адаптивність до змін зводиться до гнучкого масштабування, аварійної готовності та самоадаптації. Це дає можливість швидко додавати або відключати віртуальні машини, служби або обчислювальні ресурси без потреби у фізичній модернізації. Цифровий двійник може моделювати природні катастрофи або техногенні події (наприклад, затоплення дата-центру) і допомагати сформувати план аварійного реагування (DRP). Також інтеграція з ML-модулями дозволяє системі самостійно коригувати параметри, реагуючи на зміну вхідних даних і середовища.

Цільова функція є ключовим елементом процесу оптимізації, що визначає мету, до якої прагне система при прийнятті рішень. У контексті цифрових двійників критичної IT-інфраструктури ця функція дозволяє не лише ефективно управляти ресурсами, а й забезпечити високу надійність, продуктивність і стійкість до збоїв.

Основні властивості цільової функції:

1. багатокритеріальність - у реальних умовах неможливо зосередитися лише на одному аспекті (наприклад, продуктивності), оскільки це може спричинити небажані наслідки в інших сферах (наприклад, зростання витрат чи зниження безпеки); формується багатокритеріальна функція, що охоплює: мінімізацію експлуатаційних витрат; максимізацію пропускної здатності та продуктивності; гарантування інформаційної безпеки; оптимальне енергоспоживання та екологічність; вона реалізується через: зважене середнє (weighted sum); pareto-оптимізацію (без шкоди для одних критеріїв покращити інші); компромісне програмування;

2. динамічність - IT-середовище постійно змінюється: з’являються нові сервіси, користувачі, загрози, оновлення; змінюються політики кібербезпеки, юридичні вимоги (наприклад, GDPR, NIS2); у зв'язку з цим цільова функція повинна: адаптуватися в реальному часі; автоматично оновлювати параметри відповідно до нових подій чи змін; цифровий двійник виступає “живим” середовищем, яке постійно синхронізується з фізичною системою і адаптує цільову функцію до змін конфігурації;

3. чутливість до контексту - одне й те саме рішення може бути ефективним для одного типу інфраструктури й неефективним для іншого; цільова функція має враховувати: тип IT-інфраструктури: дата-центр, IoT-мережа, енергетичний вузол, транспортна платформа; форму та пріоритетність навантажень: обчислення, передача даних, зберігання; фокус на цільовій меті: час реакції, надійність, відповідність SLA; саме це дозволяє створити контекстно-орієнтовану оптимізацію, що враховує умови експлуатації, критичність ресурсів, час доби, навантаження;

4. оцінюваність і вимірюваність - ефективність оптимізації не можна довести без вимірюваних показників; для кожного критерію цільової функції повинні бути чіткі метрики та KPI, наприклад: час відповіді системи (response time), рівень

енергоспоживання (kWh/од. часу), середній час простою (MTTR, MTBF), коефіцієнт ризику відмови (Failure Risk Index), індекс захищеності системи (Security Score); завдяки цифровому двійнику ці параметри можна моніторити в реальному часі та агрегувати для прогнозної аналітики;

5. прогнозна здатність - цільова функція має не тільки оцінювати поточний стан, але й формувати сценарії майбутнього: прогнозування навантаження на мережу чи систему; оцінка ймовірності збоїв чи кібератак; розрахунок строку до наступного технічного обслуговування; для цього застосовуються: машинне навчання (ML) та штучний інтелект (AI); імітаційне моделювання; аналіз часових рядів; це дозволяє перейти від реактивного управління до проактивного, зменшуючи ризики та оптимізуючи ресурси заздалегідь;

6. гнучкість у налаштуванні - в умовах різних галузей або середовищ, структура цільової функції може відрізнятися: у фінансових установах - фокус на безпеці, транзакційній цілісності та резервуванні; у хмарних платформах - пріоритет масштабованості та автоматичного балансування; у енергетичних об'єктах - стабільність, точність передбачення та інтеграція з SCADA; необхідна модульність цільової функції дозволяє: додавати/видаляти критерії, налаштовувати ваги або пріоритети, швидко адаптувати модель під нові сценарії використання.

Цільова функція у сфері оптимізації критичної IT-інфраструктури повинна поєднувати аналітичну чіткість, адаптивну гнучкість і операційну реалізованість. Вона має бути водночас вимірюваною, динамічною, гнучкою та здатною до прогнозування - а цифрові двійники виступають ключовим інструментом для її практичного втілення.

Оптимізація із застосуванням цифрових двійників дозволяє автоматизувати прийняття рішень, виконувати моделювання "що, якби" (what-if analysis), тестувати нові конфігурації без ризику для реальної системи, а також покращувати обслуговування інфраструктури.

Розглянемо приклад цільової функції для оптимізації навантаження на серверну мережу критичної інфраструктури.

Мета: мінімізувати загальне навантаження на серверну мережу таким чином,

щоб уникнути перевантаження окремих вузлів, забезпечити безперебійне обслуговування користувачів та мінімізувати затримки при обробці запитів.

Опис системи:

Мережа складається з n серверів з різною обчислювальною потужністю;

Кожен сервер обробляє запити від клієнтів або підсистем;

Навантаження змінюється динамічно залежно від часу доби, кількості користувачів, типу запитів.

Формалізація цільової функції:

Нехай:

L_i - навантаження на і-тий сервер (у % від максимально допустимого);

R_i - ресурсна ємність (CPU, RAM, диск) і-того сервера;

T_i - середній час відповіді сервера і;

P_i - споживання енергії сервером і;

λ_i - коефіцієнт запитів на сервер і (інтенсивність трафіку);

x_i - змінна, що показує частку запитів, направлених на сервер і.

Цільова функція:

$$Minimize\ Z = \alpha * max(Li) + \beta * \Sigma(Ti * xi) + \gamma * \Sigma(Pi * xi)$$

$$Minimize\ Z = \alpha * max(L\_i) + \beta * \Sigma(T\_i * x\_i) + \gamma * \Sigma(P\_i * x\_i)$$

$$Minimize\ Z = \alpha * max(Li) + \beta * \Sigma(Ti * xi) + \gamma * \Sigma(Pi * xi)$$

де:

α - ваговий коефіцієнт важливості рівномірності навантаження;

β - ваговий коефіцієнт мінімізації часу відповіді;

γ - ваговий коефіцієнт енергоефективності.

Обмеження:

1. Навантаження не може перевищувати межу:

$$Li \leq Lmax \forall i L\_i \leq L\_max\ \forall\ i\ Li \leq Lmax \forall i$$

2. Кількість оброблених запитів дорівнює загальному потоку:

$$\Sigma(xi) = 1 \Sigma(x\_i) = 1\ \Sigma(xi) = 1$$

3. Навантаження враховує ресурсну ємність:

$$Li = (\lambda i * xi)/RiL\_i = (\lambda\_i * x\_i) / R\_i\, Li = (\lambda i * xi)/Ri$$

Важливість цифрового двійника серверної мережі: збирає в реальному часі метрики з усіх серверів; моделює розподіл навантаження при зміні конфігурацій; імітує поведінку системи при сплесках активності; прогнозує точки перевантаження або вихід з ладу; запускає оптимізаційні алгоритми (наприклад, генетичні, градієнтні або евристичні) для мінімізації функції Z.

Збір метрик у реальному часі полягає в тому, що цифровий двійник постійно отримує дані від усіх фізичних серверів системи: навантаження процесора (CPU), використання оперативної пам’яті (RAM), мережевий трафік, температурні показники, показники споживання енергії, часи відповіді тощо. Ці метрики дозволяють отримати повну картину стану серверної інфраструктури та швидко реагувати на зміни.

Моделювання розподілу навантаження при зміні конфігурацій грунтується на тому, що цифровий двійник надає можливість тестувати різні варіанти конфігурацій мережі, балансування навантаження, оновлення програмного забезпечення або апаратної частини - без ризику для реальної інфраструктури. Це дозволяє: обрати найбільш ефективну стратегію балансування запитів, уникнути несподіваних збоїв при переході на нову архітектуру, швидше впроваджувати інновації без шкоди для стабільності.

Імітація поведінки системи при пікових навантаженнях дозволяє за допомогою цифрового двійника імітувати екстремальні сценарії, зокрема: різке зростання кількості користувачів, атаки типу DDoS, аварійне вимкнення вузлів або сегментів мережі. Таке тестування дозволяє оцінити, наскільки система готова до нестандартних ситуацій та наскільки ефективно працює існуюча політика аварійного реагування.

Прогнозування перевантажень або збоїв виражається в тому, що завдяки алгоритмам машинного навчання та історичним даним цифровий двійник може передбачати майбутні точки перевантаження, потенційні збої або деградацію сервісу. Це дає змогу: заздалегідь планувати масштабування інфраструктури, попереджати аварії, впроваджувати проактивне обслуговування.

Запуск оптимізаційних алгоритмів для мінімізації цільової функції показує, що цифровий двійник є ідеальним середовищем для використання алгоритмів оптимізації. Наприклад: генетичні алгоритми допомагають знаходити найкращий розподіл навантаження з урахуванням багатьох параметрів; градієнтні методи забезпечують швидке зближення до локального або глобального оптимуму; евристичні підходи дозволяють ефективно шукати рішення в складних або нечітко визначених ситуаціях. Усі ці алгоритми працюють із цільовою функцією (наприклад, мінімізацією Z, що включає навантаження, час відповіді та енергоспоживання) та забезпечують постійне самонавчання системи.

Оптимізація серверної мережі з використанням цифрового двійника дала змогу досягти суттєвих результатів у підвищенні ефективності та стійкості інфраструктури. Одним із ключових досягнень стало забезпечення балансованого розподілу навантаження між серверами. Завдяки аналітичним можливостям цифрового двійника система змогла автоматично відстежувати стан кожного вузла й оперативно перерозподіляти вхідні запити, запобігаючи перевантаженням. Це дозволило рівномірно використовувати обчислювальні ресурси мережі, мінімізуючи ризики зниження якості сервісів і забезпечуючи загальну стабільність роботи.

Іншим важливим результатом стало суттєве зменшення кількості простоїв. Завдяки постійній віртуальній симуляції інфраструктури в реальному часі цифровий двійник виявляв потенційні вузькі місця та можливі точки відмов ще до фактичного виникнення проблем. Це забезпечувало своєчасне перенаправлення потоків або динамічне коригування конфігурацій, що дозволило скоротити кількість аварійних зупинок і прискорити процес відновлення після збоїв.

Крім того, була суттєво покращена загальна продуктивність мережі. Завдяки оптимізованому розподілу запитів зменшився час відповіді серверів, підвищилася швидкість обробки даних і покращилася ефективність використання обладнання. Цифровий двійник дозволяв системі динамічно адаптуватися до змін навантаження, особливо в періоди пікової активності, забезпечуючи стабільно високий рівень обслуговування користувачів.

Оптимізація також позитивно вплинула на енергоспоживання інфраструктури.

Завдяки зменшенню перенавантаження серверів обладнання функціонувало в більш енергоефективному режимі. Крім того, цифровий двійник прогнозував сценарії надлишкового енергоспоживання й пропонував рішення щодо тимчасового вимкнення або зниження потужності окремих вузлів без втрати продуктивності, що сприяло скороченню експлуатаційних витрат і зменшенню вуглецевого сліду.

Нарешті, застосування цифрового двійника сприяло підвищенню надійності та стійкості серверної мережі. Моделювання критичних сценаріїв, таких як вихід з ладу окремих компонентів або кіберзагрози, дозволило виявити вразливі місця в архітектурі й підготувати заходи для забезпечення безперервності надання послуг навіть у кризових ситуаціях. Таким чином, цифровий двійник став важливим інструментом для комплексного підвищення ефективності, безпеки та стійкості серверної інфраструктури.

Отже, цифровий двійник виконує не лише роль «дзеркала» фізичної інфраструктури, а й активного інтелектуального інструмента, що дозволяє забезпечити прогнозоване, ефективне та безпечне управління IT-ресурсами. Його можливості виходять далеко за межі простого моніторингу, адже він: оптимізує роботу серверної мережі: автоматично аналізує навантаження та пропонує найефективніші сценарії розподілу ресурсів; дозволяє протестувати нові конфігурації або оновлення без ризику для реального середовища; підтримує безперервну роботу навіть у разі пікових навантажень чи збоїв; підвищує надійність і масштабованість системи: завдяки прогнозній аналітиці визначає потенційні точки відмови до їх виникнення; створює сценарії аварійного реагування та забезпечує швидке відновлення; дозволяє масштабувати ресурси віртуально, прогнозуючи потреби бізнесу наперед; зменшує витрати на обслуговування: замість реактивного обслуговування застосовує predictive maintenance - обслуговування за реальним станом компонентів; автоматизує рутинні процеси та знижує потребу в постійному втручанні інженерів; підвищує ефективність використання обладнання, подовжуючи його життєвий цикл; покращує якість надання IT-послуг: забезпечує стабільну роботу сервісів з мінімальними затримками та високою доступністю; дає змогу швидко адаптуватися до змін у попиті, впроваджувати нові сервіси без збоїв;

забезпечує прозорість, контроль та звітність завдяки інтегрованим аналітичним панелям та візуалізаціям; виступає як цифровий радник для IT-фахівців: генерує рекомендації на основі машинного навчання та великих даних; підтримує прийняття рішень у реальному часі: від оптимізації конфігурацій до управління кризовими ситуаціями; забезпечує віртуальне середовище для симуляції будь-яких сценаріїв без впливу на реальну систему; результаті впровадження цифрового двійника організація отримує: більш гнучку й стійку до ризиків IT-інфраструктуру, прозору та контрольовану систему управління ресурсами, і, що найважливіше, конкурентну перевагу завдяки технологічній передбачуваності та економічній ефективності.

3.2 Алгоритми оптимізації критичної IT інфраструктури цифровими двійниками

Цифрові двійники відкривають нові можливості в управлінні критичною IT-інфраструктурою, адже вони не лише відображають поточний стан системи, а й стають основою для глибокого інтелектуального аналізу та ухвалення обґрунтованих рішень. У цьому процесі ключову роль відіграють алгоритми оптимізації, які дозволяють адаптувати роботу системи до змінних умов і знаходити найефективніші конфігурації. Одним із підходів до розв'язання складних оптимізаційних задач є використання евристичних та метаевристичних алгоритмів. У ситуаціях, коли кількість змінних і обмежень є надзвичайно великою, традиційні методи часто виявляються малоефективними. Зокрема, генетичні алгоритми імітують процеси природної еволюції та використовуються для пошуку оптимальних рішень, наприклад, під час балансування навантаження або вибору найбільш продуктивних серверів. Алгоритм рою частинок (Particle Swarm Optimization) ефективно застосовується для налаштування параметрів мережевої інфраструктури, а метод симульованого відпалу (Simulated Annealing) дозволяє знаходити глобальні оптимальні рішення у великих просторах варіантів. Використання цих підходів дає змогу ефективно вирішувати задачі розподілу ресурсів, оптимізації навантаження та мінімізації затримок у роботі систем. Ще одним потужним інструментом є

алгоритми машинного навчання та методи глибокого підкріплення. Завдяки великому обсягу даних, які накопичуються у процесі роботи цифрового двійника, можна реалізувати навчання з підкріпленням для автоматичного адаптивного керування навантаженням на сервери, прогнозування трафіку в години пікового навантаження та підвищення стійкості системи до перевантажень і атак типу DDoS. Використання методів глибокого підкріплювального навчання (Deep Reinforcement Learning) дозволяє моделювати поведінку складних динамічних систем і приймати оптимальні рішення в реальному часі. Наприклад, спеціалізовані агенти здатні змінювати конфігурацію віртуальних машин у хмарних середовищах для досягнення оптимального балансу між продуктивністю й енергоефективністю.

Додатково суттєво розширює можливості цифрового двійника інтеграція із генеративними моделями штучного інтелекту (Generative AI). Таке поєднання дозволяє створювати моделі для проведення сценарного аналізу «що, якщо», тестувати нові архітектурні рішення, моделювати поведінку систем у разі аварійних ситуацій або кіберзагроз, а також автоматично генерувати оптимізовані конфігурації IT-інфраструктури на основі історичних даних і прогнозів розвитку подій. Завдяки цьому система отримує можливість не лише реагувати на зміни, а й проактивно розробляти найбільш ефективні стратегії дій, що мінімізує ризик людських помилок і підвищує якість обслуговування критичних цифрових систем.

Цифрові двійники (Digital Twins) у сфері критичної IT-інфраструктури забезпечують не просто візуалізацію або моніторинг реальних об'єктів і систем, а й створюють можливість глибокого аналітичного аналізу та оптимізації їх роботи в реальному часі. Алгоритми оптимізації є основним інструментом, що забезпечує цю функціональність.Застосування алгоритмів оптимізації в цифрових двійниках критичної IT-інфраструктури забезпечує низку важливих переваг, які суттєво підвищують ефективність управління системами.

Насамперед, оптимізаційні алгоритми сприяють автоматизації процесів управління ресурсами. Завдяки їм цифрові двійники можуть самостійно перерозподіляти навантаження між серверами або мережевими вузлами відповідно до поточного стану інфраструктури, оптимізувати використання віртуальних машин,

процесорних ядер, оперативної пам'яті, сховищ даних та мережевих каналів. Вони також дозволяють оперативно виявляти "вузькі місця" в системі й пропонувати ефективні варіанти їх усунення. Наприклад, у періоди пікового навантаження оптимізаційні механізми перенаправляють трафік на менш завантажені сервери, що сприяє зниженню часу відгуку і підтримці стабільної роботи.

Ще однією важливою перевагою є оптимізація енергоспоживання. Для дата-центрів мінімізація витрат на електроенергію є критично важливою задачею. Алгоритми оптимізації допомагають визначати мінімально необхідну кількість активних серверів для обслуговування поточних запитів, переводити неактивні ресурси в сплячий режим або вимикати їх, а також знаходити найенергоефективніші маршрути для передавання даних. Завдяки цьому знижуються експлуатаційні витрати без негативного впливу на продуктивність системи.

Цифрові двійники також активно використовуються для прогнозування відмов і планування превентивного обслуговування. Збираючи телеметричні дані з усіх компонентів системи, цифрові моделі за допомогою прогнозних та оптимізаційних алгоритмів здатні передбачати ймовірність виникнення збоїв або критичного падіння продуктивності. Вони допомагають формувати оптимальні графіки технічного обслуговування та моделювати вплив можливих інцидентів на функціонування інфраструктури, що значно зменшує кількість аварійних ситуацій та час простоїв.

Крім того, цифрові двійники дозволяють ефективно планувати масштабування й розвиток IT-інфраструктури. Завдяки можливості моделювання різних сценаріїв розширення - таких як додавання нових серверів або впровадження сучасних технологій - можна оцінювати їхній вплив на загальну ефективність системи та обирати найбільш доцільні варіанти за допомогою багатокритеріальних оптимізаційних підходів. Це забезпечує раціональне використання ресурсів та обґрунтовані інвестиції у розвиток.

Окрему увагу слід приділити питанню кібербезпеки. Оптимізаційні алгоритми дають змогу цифровим двійникам оперативно виявляти вразливі елементи інфраструктури, динамічно адаптувати політики безпеки та конфігурації мережі, а також імітувати кіберінциденти для оцінки стійкості системи. Це підвищує

готовність до потенційних загроз і зміцнює здатність системи до самовідновлення в разі атак.

Таким чином, впровадження алгоритмів оптимізації в цифрові двійники критичної IT-інфраструктури сприяє створенню більш ефективних, надійних та адаптивних систем, що відповідають сучасним вимогам до продуктивності, безпеки та енергоефективності.

Отже, алгоритми оптимізації в поєднанні з цифровими двійниками перетворюють традиційне адміністрування IT-інфраструктури в інтелектуальне, передбачуване та адаптивне управління. Це особливо важливо в критичних системах, де будь-який збій може мати серйозні наслідки - від фінансових втрат до загроз національній безпеці.

Розглянемо схему алгоритму оптимізації критичної IT інфраструктури цифровими двійниками (рис. 3.2)

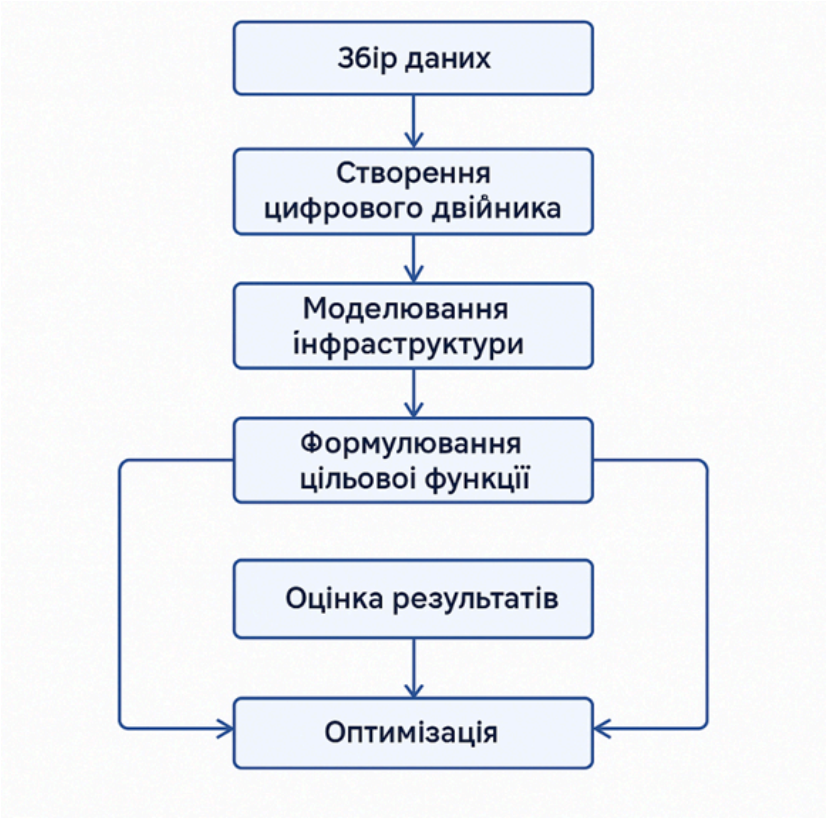

Рисунок 3.2 – Схема алгоритму оптимізації критичної IT інфраструктури цифровими двійниками

Процес функціонування цифрового двійника критичної IT-інфраструктури

охоплює кілька взаємопов’язаних етапів, що забезпечують безперервний моніторинг, оптимізацію й адаптивне управління системою.

На першому етапі здійснюється збір даних у реальному часі. Цифровий двійник інтегрується з основними компонентами IT-інфраструктури: фізичними та віртуальними серверами, мережевим обладнанням (маршрутизаторами, комутаторами, балансувальниками навантаження), системами зберігання даних (NAS, SAN, SSD-масивами) та енергетичними системами (ДБЖ, генераторами, електромережами). Збираються ключові показники, зокрема системні метрики (CPU, RAM, I/O, uptime), мережеві характеристики (пропускна здатність, втрата пакетів, затримки), фізичні параметри (температура, вологість, енергоспоживання), сигнали подій (логи систем, SIEM-сповіщення) та дані щодо безпеки (IDS/IPS-алерти, активність фаєрволів, спроби вторгнень). Збір даних здійснюється за допомогою агентів, SNMP-протоколу, телеметрії, syslog-повідомлень та API хмарних платформ.

Далі відбувається аналіз поточного стану інфраструктури. Дані проходять стадії очищення та нормалізації, що забезпечує їх узгодженість і достовірність. На основі обробленої інформації виконується класифікація стану кожного вузла, визначаючи категорії "норма", "підвищене навантаження" або "ризик відмови". Також виявляються кореляції між подіями, наприклад, зв'язок між зростанням трафіку, підвищенням температури обладнання та деградацією продуктивності. Результатом є динамічна карта здоров'я всієї IT-інфраструктури.

Третім етапом є моделювання різних сценаріїв. Цифровий двійник створює віртуальні копії систем для тестування поведінки під час високих навантажень (наприклад, у період розпродажів або DDoS-атак), аварійних подій (вихід з ладу вузлів або втрата енергопостачання), інфраструктурних змін (міграція віртуальних машин, введення нових дата-центрів) або зовнішніх впливів (стихійні лиха, електромагнітні завади). Імітація таких ситуацій відбувається в контрольованому середовищі з урахуванням фізичних, логічних і бізнес-параметрів.

На основі змодельованих сценаріїв здійснюється запуск алгоритмів оптимізації. Для пошуку найкращих рішень застосовуються генетичні алгоритми, що імітують еволюційні процеси, градієнтні методи мінімізації функцій втрат,

евристичні підходи для роботи у складних багатоваріантних середовищах, а також методи глибокого підкріплювального навчання (Deep RL), де агенти самостійно удосконалюють стратегії керування. Під час оптимізації враховуються існуючі обмеження, такі як ліцензійні вимоги, умови SLA, топологія мережі та політики безпеки. Після чисельного моделювання виконується вибір оптимального рішення. Система ранжує стратегії відповідно до їхнього впливу на продуктивність, енергоефективність і вартість впровадження. Додатково оцінюється рівень відмовостійкості та відповідність угодам про рівень обслуговування (SLA). На основі цих критеріїв обирається кілька найкращих варіантів, які можуть бути затверджені як автоматично, так і вручну. Основними показниками ефективності виступають зниження споживання ресурсів, підвищення надійності системи та мінімізація ризиків. Реалізація обраних рішень у реальному середовищі відбувається за допомогою автоматичної оркестрації (із застосуванням інструментів Kubernetes, Ansible, Terraform), балансування навантаження, міграції сервісів між вузлами та дата-центрами, оновлення політик безпеки або якості обслуговування (QoS), активації резервних компонентів та відключення проблемних елементів. Перед безпосереднім впровадженням можливий попередній перегляд змін за допомогою дашбордів або 3D-візуалізацій.

На завершальному етапі реалізується механізм зворотного зв'язку та самонавчання. Цифровий двійник фіксує фактичні результати у вигляді KPI та логів, порівнює прогнозовані значення з реальними та на основі цього коригує свої моделі. Вдосконалення стосується як параметричних моделей, так і гіперпараметрів алгоритмів машинного навчання та шаблонів сценаріїв. Завдяки накопиченню досвіду цифровий двійник підвищує точність прогнозування навіть для рідкісних або складних ситуацій.

У разі потреби результати оптимізації можуть бути інтегровані в загальну систему управління підприємством. Дані передаються до CMDB, DCIM, систем керування SLA/DevOps, ERP або BI-систем для формування звітності та аналітики. Це забезпечує прозорість керування інфраструктурою, покращує стратегічне планування та дозволяє напряму впливати на ключові бізнес-метрики. Алгоритм

працює циклічно - після кожної оптимізації двійник збирає нові дані й покращує наступний цикл. Це забезпечує адаптивну, самооптимізовану ІТ-інфраструктуру, стійку до змін та загроз.

Визначено сім основних результатів оптимізації критичної ІТ-інфраструктури за допомогою цифрових двійників, які забезпечують значні переваги у всіх аспектах функціонування інфраструктури.

Першим результатом є раціоналізація використання ресурсів. Цифрові двійники дозволяють здійснювати збалансоване і динамічне розподілення обчислювальних потужностей, мережевого трафіку, обсягу зберігання та оперативної пам'яті. Це дозволяє уникнути перевантажень окремих компонентів, зменшує час простоїв і дає змогу ефективно використовувати наявні ресурси, без необхідності у додаткових інвестиціях в апаратне забезпечення.

Другим важливим результатом є зменшення ймовірності критичних збоїв. Завдяки постійному моніторингу, реальному аналізу даних та прогнозуванню потенційних несправностей система може своєчасно виявляти аномалії. Це дозволяє застосовувати проактивну стратегію реагування, що полягає у локалізації проблем до того, як вони призведуть до серйозних збоїв або відмов сервісів, що критично важливо для підтримки безперервності бізнес-процесів.

Третім результатом є зростання продуктивності систем. Інтелектуальний аналіз навантажень, оптимізація маршрутизації запитів і розподілу завдань дозволяє суттєво прискорити виконання операцій, що безпосередньо впливає на покращення швидкодії додатків і зменшення часу відгуку систем. Це створює умови для масштабування без втрати продуктивності.

Четвертим результатом є оптимізація енергоспоживання. Цифрові двійники дають змогу детально відслідковувати енергоспоживання кожного компонента інфраструктури, що дозволяє виявляти неефективне використання електроенергії та «гарячі точки». Результатом цього є впровадження стратегій енергоефективного навантаження, автоматичне вимкнення неактивних вузлів та використання профілів економії енергії, що знижує витрати на електроживлення та охолодження.

П’ятим результатом є інтелектуальне управління інфраструктурою в режимі

реального часу. Інтеграція цифрових двійників із системами автоматизації (наприклад, DevOps, NetOps, CloudOps) дозволяє оперативно адаптувати інфраструктуру до змін навантаження, автоматично перемикати систему на резервні вузли при збої та застосовувати оптимальні сценарії реагування на інциденти без втручання оператора. Це забезпечує гнучкість, стійкість та автономність інфраструктури.

Шостим результатом є покращення кіберстійкості. Завдяки можливості моделювати та тестувати різноманітні кібератаки у віртуальному середовищі, цифровий двійник дає змогу оцінювати вразливості системи, перевіряти ефективність існуючих заходів безпеки та формувати превентивні політики для захисту критичних елементів інфраструктури. Це підвищує здатність системи виявляти, протистояти та швидко відновлюватися після кіберінцидентів.

Сьомим результатом є підвищення економічної ефективності. Зниження часу простоїв, автоматизація рутинних процесів, енергозбереження та покращення продуктивності в цілому призводять до зменшення загальних витрат на експлуатацію IT-інфраструктури. Це дозволяє підприємствам підвищувати рентабельність та досягати більшої операційної ефективності.

Отже, алгоритми оптимізації критичної IT-інфраструктури за допомогою цифрових двійників відкривають нові можливості для забезпечення стабільності, ефективності та безпеки IT-систем. Завдяки моделюванню в реальному часі, прогнозуванню збоїв та інтелектуальному управлінню ресурсами, цифрові двійники дозволяють знизити операційні ризики, оптимізувати енергоспоживання та підвищити загальну продуктивність інфраструктури. Це робить їх потужним інструментом у забезпеченні безперервності бізнес-процесів в умовах зростаючих кіберзагроз і технологічних викликів.

3.3 Висновки до третього розділу

Для реалізації аналітичної оцінки було розроблено цільову функцію для процесу оптимізації об'єктів критичної IT інфраструктури цифровими двійниками,

яка дозволяє не лише ефективно управляти ресурсами, а й забезпечити високу надійність, продуктивність і стійкість до збоїв.

Розроблено алгоритми оптимізації критичної IT інфраструктури цифровими двійниками, застосування яких дозволяє знаходити найкращі конфігурації роботи систем у змінних умовах.

4 МЕТОД ОПТИМІЗАЦІЇ КРИТИЧНОЇ ІТ ІНФРАСТРУКТУРИ ЦИФРОВИМИ ДВІЙНИКАМИ

4.1 Метод оптимізації критичної ІТ інфраструктури цифровими двійниками

Цифровий двійник - це віртуальна модель фізичної ІТ-системи, яка точно відображає її структуру, поведінку та динаміку в режимі реального часу. Він функціонує як інтерактивна цифрова копія серверів, мереж, систем зберігання даних та інших ключових компонентів, дозволяючи проводити експерименти, моделювання та оптимізацію без впливу на реальне середовище.

Основна мета застосування цифрових двійників - оптимізація.

До основних властивостей методу оптимізації критичної ІТ інфраструктури цифровими двійниками належать: забезпечення високої надійності та відмовостійкості, оптимізація управління ресурсами, прогнозування та планування технічного обслуговування та підтримка прийняття рішень.

Забезпечення високої надійності та відмовостійкості полягає в тому, що цифровий двійник може імітувати різноманітні аварійні сценарії, допомагаючи виявити слабкі місця системи та вчасно вжити заходів щодо їх усунення. Використання цифрової моделі дозволяє тестувати стратегії безперервності бізнесу (Business Continuity) та сценарії відновлення після збоїв.

В основі оптимізації управління ресурсами лежать системи, що працюють із цифровими двійниками, які можуть автоматично визначати перевантажені вузли (сервери, сховища, мережі) та пропонувати найкращі шляхи балансування навантаження. Це призводить до економії енергії, зменшення перегріву обладнання та продовження його терміну служби.

Прогнозування та планування технічного обслуговування грунтується на аналізі історичних і реальних даних, що дозволяє цифровому двійнику визначити, коли саме обладнання може вийти з ладу. Це дає змогу переходити від реактивного до прогнозного обслуговування, що значно скорочує час простоїв і знижує витрати.

Підтримка прийняття рішень базується на тому, що цифрові двійники використовуються як симуляційне середовище для тестування змін у конфігураціях,

розгортання нових сервісів або масштабування ресурсів. Алгоритми оптимізації (генетичні, градієнтні, нейромережеві) дозволяють цифровому двійнику обирати найефективніші рішення з тисяч можливих варіантів.

Приклади алгоритмів оптимізації, які можуть застосовуватись у цифрових двійниках критичної IT-інфраструктури: генетичні алгоритми (GA), градієнтні методи (Gradient Descent, Newton-Raphson тощо), машинне навчання (ML) та глибоке навчання (DL), евристичні алгоритми, алгоритми рою частинок (Particle Swarm Optimization, PSO) та мурашиної колонії (Ant Colony Optimization, ACO), стохастичні методи оптимізації (Simulated Annealing, Monte Carlo) та підкріплювальне навчання (Reinforcement Learning, RL).

Генетичні алгоритми (GA) це методи еволюційного моделювання, які імітують процес природного добору. Вони ефективно застосовуються для вирішення задач із великою кількістю змінних, таких як балансування навантаження між серверами, вибір оптимального шляху передачі даних у мережі або розподіл обчислювальних ресурсів у хмарних середовищах. Генетичні алгоритми забезпечують гнучкість у моделюванні змін середовища в цифровому двійнику та пошук оптимальних сценаріїв розвитку подій.

Градієнтні методи (Gradient Descent, Newton-Raphson тощо) використовуються для точного налаштування параметрів у системах із визначеними математичними моделями, наприклад, оптимізація температурного режиму дата-центрів або мінімізація часу обробки запитів у хмарній IT-архітектурі. У цифрових двійниках вони дозволяють створити адаптивну модель, що реагує на зміну параметрів у реальному часі, з метою досягнення мінімальних витрат або максимальної продуктивності.

Машинне навчання (ML) та глибоке навчання (DL) це ключові технології для цифрових двійників, які дозволяють здійснювати передбачення (predictive analytics), класифікацію подій, виявлення аномалій та адаптивне керування процесами. Наприклад, алгоритми на основі нейронних мереж можуть аналізувати лог-файли, сенсорні дані та показники продуктивності, щоб прогнозувати поломки або навантаження на IT-інфраструктуру. У випадках великомасштабної системи

(наприклад, обчислювального кластера) DL дозволяє будувати моделі з високим рівнем деталізації.

Евристичні алгоритми застосовуються для швидкого прийняття рішень у ситуаціях із частковою або неповною інформацією. Наприклад, при виникненні аварійної ситуації цифровий двійник може за допомогою евристичних методів оперативно запропонувати набір дій для мінімізації втрат. Такі алгоритми часто комбінуються з експертними системами або правилами прийняття рішень (rule-based systems).

Алгоритми рою частинок (Particle Swarm Optimization, PSO) та мурашиної колонії (Ant Colony Optimization, ACO) це біоінспіровані методи, які імітують поведінку колективного інтелекту (рою птахів, мурах тощо). Використовуються для задач маршрутизації, планування ресурсів або енергетичної ефективності. Наприклад, ACO може моделювати найкращі маршрути для передачі даних з найменшою затримкою та найменшим навантаженням.

Стохастичні методи оптимізації (Simulated Annealing, Monte Carlo) ідеально підходять для складних топологічних задач, де необхідно уникати локальних мінімумів. У цифрових двійниках їх можна використовувати для моделювання розподілу навантаження в змінному середовищі або для пошуку найкращої конфігурації систем резервування.

Підкріплювальне навчання (Reinforcement Learning, RL) дозволяє цифровим двійникам навчатися на основі зворотного зв’язку від середовища. RL особливо корисне для динамічних систем, де цифровий двійник взаємодіє з реальним світом і поступово вчиться приймати оптимальні рішення - наприклад, автоматичне регулювання потужності в ЦОД або реагування на збої в мережі.

Переваги використання таких алгоритмів у цифрових двійниках:

- постійна адаптація до змін у системі та навколишньому середовищі;
- автоматизоване прийняття рішень без участі оператора;
- прогнозування відмов і зниження ризиків завдяки аналітиці;
- оптимізація енерговитрат, часу реакції, продуктивності та витрат;
- можливість тестування сценаріїв віртуально без шкоди для фізичної

інфраструктури.

Завдяки застосуванню різних класів алгоритмів цифрові двійники перетворюються на ефективні інструменти інтелектуального управління IT-інфраструктурою нового покоління.

Загальний метод оптимізації цифровим двійником включає такі етапи:

1. збір телеметричних даних з усіх вузлів системи;
2. аналіз поточного стану та виявлення «вузьких місць»;
3. моделювання сценаріїв поведінки при зміні навантаження або відмові компонентів;
4. оптимізація параметрів роботи системи;
5. реалізація змін у реальному середовищі або на рівні рекомендацій;
6. зворотній зв’язок - оцінка ефективності змін та самонавчання.

Використання цифрових двійників для оптимізації критичної IT-інфраструктури стає все більш затребуваним у великих дата-центрах, телеком-компаніях, банківських структурах та урядових організаціях. Вони дозволяють забезпечити: безперебійну роботу; ефективне використання ресурсів; зниження витрат; підвищення стійкості до збоїв та атак.

Етапи методу оптимізації цифровим двійником в критичній інфркаструктурі (рис.4.1).

Розглянемо етап збору і обробки даних з фізичної інфраструктури. Мета - отримати повну, актуальну і деталізовану картину стану всіх компонентів IT-системи. Що включає: збір телеметричних даних з усіх джерел: серверів, маршрутизаторів, комутаторів, систем зберігання даних (СГД), джерел живлення, систем охолодження. Моніторинг основних метрик: CPU, RAM, дискових I/O, використання пропускної здатності, температури компонентів, електроспоживання, часів затримки. Виявлення шаблонів навантаження, аномалій, частоти інцидентів, сезонних коливань. Інструменти системи моніторингу: Zabbix, Prometheus, Grafana. Агенти збору даних: Telegraf, Collectd. Системи обробки логів: ELK Stack, Graylog. Протоколи доступу до даних: SNMP, IPMI, Redfish, REST API. Результат - формування структурованого потоку даних для побудови точного цифрового

відображення.

Наступний етап - побудова та оновлення цифрової моделі. Мета - створити актуальну цифрову копію (Digital Twin), яка відображає фізичну інфраструктуру з максимальною точністю. Що включає: віртуалізація всіх фізичних та логічних компонентів: серверів, VM, сховищ, мережевої топології, систем керування. Врахування специфікацій кожного елемента: частоти відмов, обмежень по температурі, ліній затримки, залежностей між модулями. Постійна синхронізація цифрової моделі з фізичною мережею: через API, агенти або прямі підключення до керуючих систем. Інструменти: платформи цифрових двійників: Siemens NX, AnyLogic, Azure Digital Twins, IBM Maximo. CAD/CAE-моделі, емулятори та емуляційні середовища (GNS3, EVE-NG - для мережевої частини). Засоби інтеграції: OPC UA, MQTT, REST.

Далі розглянемо аналіз поточного стану системи. Мета - виявити проблемні зони та оцінити ефективність поточного функціонування. Що включає: побудова ключових метрик: середнє завантаження, пікова активність, коефіцієнт доступності (availability), середній час відповіді (latency), коефіцієнт використання ресурсів. Виявлення вузьких місць (bottlenecks) - сегменти системи, які обмежують загальну продуктивність. Візуалізація зони ризику, надмірного резервування або навпаки - критичного недовантаження. Результат - створення інформованої бази для моделювання сценаріїв та вибору напрямків оптимізації.

Моделювання сценаріїв - ще один етап. Мета - передбачити, як інфраструктура поводитиметься за різних умов. Що включає: проведення сценаріїв типу What-if (що буде, якщо…): відмова комутатора, сплеск трафіку, кіберінцидент, модернізація серверного обладнання. Симуляція стрес-навантажень: симуляція DDoS, підвищення запитів на 500% за короткий проміжок часу, відключення обраних кластерів. Перевірка впливу змін: наприклад, як вплине переміщення віртуальних машин між датацентрами на затримку. Результат - перевірені гіпотези щодо поведінки системи в критичних ситуаціях без шкоди для реального середовища.

Дослідимо етап застосування алгоритмів оптимізації. Мета - знайти найкращу архітектуру і параметри системи відповідно до обраних критеріїв ефективності. Що

включає: визначення цільової функції. Наприклад: $Z = \alpha * \text{Час\_відгуку} + \beta * \text{Споживання\_ресурсів} + \gamma * \text{Ймовірність\_відмови}$. Застосування сучасних алгоритмів оптимізації: генетичні - еволюційний пошук найкращих комбінацій; градієнтні методи - локальна оптимізація параметрів; евристики/метаевристики - швидкий пошук в умовах неповної інформації; методи машинного навчання (Supervised, Reinforcement Learning). Інструменти: SciPy, TensorFlow, PyTorch, DEAP (генетичні алгоритми), Optuna, RayTune.

Важливим етапом також є валідація результатів на цифровій моделі. Мета - перевірити на моделі, чи запропоновані зміни дійсно покращують ситуацію. Що включає: проведення симуляції в оптимізованій конфігурації. Порівняння KPI до та після: час відповіді, рівень завантаження, енергоспоживання, доступність. Оцінка нових ризиків: створення нових конфліктів, зростання навантаження на сусідні компоненти. Результат - підтвердження, що вибране рішення стабільне та ефективне.

Проаналізуємо етап реалізацію змін у реальному середовищі. Мета - інтегрувати оптимізовану модель в реальну інфраструктуру. Що включає: втілення змін через системи автоматизації: *Ansible, Puppet, Chef, Terraform*. Виконання міграції, балансування навантаження, зміна пріоритетів обслуговування. Контроль за тим, як зміни впливають на живе середовище в режимі реального часу. Безпека: зміни можуть бути спочатку реалізовані в тестовому або staging-середовищі, після чого розгортаються поступово (canary deployment).

Заключним етапом є самонавчання та адаптація. Мета - перетворити цифрового двійника на систему, що самостійно адаптується до змін середовища. Що включає: накопичення історичних даних для аналізу тенденцій. Навчання моделей прогнозування: прогноз навантажень, ймовірності відмов, оптимального часу для технічного обслуговування. Використання підкріплювального навчання (Reinforcement Learning) для автоматичного прийняття рішень на основі попереднього досвіду. Постійне оновлення цифрової моделі в залежності від зовнішніх і внутрішніх змін. Результат - система стає адаптивною, здатною до автономного самовдосконалення.

Рисунок 4.1 - Етапи методу оптимізації цифровим двійником в критичній інфркаструктурі

Метод оптимізації критичної IT-інфраструктури за допомогою цифрових двійників є сучасним підходом, що поєднує віртуальне моделювання, аналітику в реальному часі та алгоритми штучного інтелекту для досягнення максимальної ефективності, надійності та адаптивності системи. Цифрові двійники дають змогу:

- безпечно тестувати сценарії без втручання в реальне середовище;
- оперативно виявляти проблеми та перевантаження;
- прогнозувати майбутні ризики й точки відмов;
- обирати оптимальні конфігурації за допомогою інтелектуальних алгоритмів.

Завдяки цьому підходу організації можуть зменшити ризики простоїв, оптимізувати витрати на ресурси, підвищити відмовостійкість та покращити загальну продуктивність критичних цифрових систем.

Таким чином, цифрові двійники перетворюються на ключовий інструмент

стратегічного управління IT-інфраструктурою, особливо у сферах, де стабільність і безперервність є критично важливими.

4.2 Експерименти та дослідження методу оптимізації критичної IT інфраструктури цифровими двійниками

Дослідження та експерименти з використання цифрових двійників у критичній IT-інфраструктурі спрямовані на підвищення безпеки, надійності та ефективності систем.

Цифрові двійники активно впроваджуються в різні галузі критичної інфраструктури, і результати експериментальних досліджень підтверджують їх ефективність у забезпеченні безперервної роботи, надійності та безпеки систем. Нижче наведено низку прикладів досліджень та практичних реалізацій. Комплексний бібліометричний аналіз наукової літератури.

У журналі Information опубліковано дослідження, де було здійснено ґрунтовний бібліометричний аналіз понад 3400 наукових публікацій з баз даних Scopus і Web of Science. Основною метою дослідження було виявлення ключових напрямів застосування цифрових двійників у сфері критичної інфраструктури. Аналіз охоплював публікації за останнє десятиріччя, що дало змогу простежити динаміку наукових інтересів, географію досліджень та міждисциплінарні зв’язки.

Дослідники дійшли висновку, що цифрові двійники відіграють все більш важливу роль у модернізації критичних систем завдяки своїй здатності інтегрувати віртуальне моделювання з даними з фізичних об’єктів у режимі реального часу. Такі технології мають великий потенціал у покращенні стійкості до зовнішніх загроз, забезпеченні кібербезпеки, ефективному управлінні технічним обслуговуванням, а також в оптимізації загальної роботи систем.

Зокрема, значну увагу в літературі приділено використанню цифрових двійників у таких галузях, як: енергетичні мережі, де вони сприяють балансуванню навантаження, прогнозуванню споживання та виявленню відмов; транспортна інфраструктура, для моніторингу стану доріг, мостів, рейкових систем та

прогнозування їхнього зносу; водопостачання та очисні споруди, де цифрові моделі дозволяють виявляти витоки, покращувати якість обслуговування та зменшувати втрати води.

Також було відзначено стрімке зростання кількості досліджень у сфері застосування цифрових двійників у поєднанні з такими технологіями, як штучний інтелект, Інтернет речей (IoT) та великі дані, що ще більше розширює можливості адаптивного управління критично важливою інфраструктурою.

Дослідження моделювання насосних станцій. У журналі Buildings описано високоточний підхід до створення цифрового двійника для насосної станції. У цьому дослідженні було реалізовано комплексну модель, яка враховує не лише фізичні характеристики обладнання, такі як геометрія, гідравлічні параметри та технічні обмеження, але й операційні процеси в режимі реального часу завдяки інтеграції з датчиками та SCADA-системами.

Завдяки впровадженню цифрового двійника вдалося досягти кількох важливих переваг. По-перше, було оптимізовано графіки технічного обслуговування, що дало змогу скоротити кількість незапланованих зупинок і зменшити експлуатаційні витрати. По-друге, модель забезпечила автоматизоване виявлення несправностей на основі аналізу відхилень у даних сенсорів, що дозволяє вчасно виявляти аномалії та запобігати аварійним ситуаціям.

Крім того, цифровий двійник дозволив точно прогнозувати споживання енергії, що стало основою для розробки стратегій енергоефективного управління. Це особливо актуально для великих інфраструктурних об’єктів, де споживання енергії є одним з основних витратних факторів. В перспективі, така модель може бути масштабована для управління кількома об’єктами в рамках єдиної платформи, забезпечуючи централізований моніторинг та аналіз на рівні всієї системи водопостачання.

Розгялнемо станційний цифровий двійник гідроакумулюючої електростанції (Ірландія). Компанія Akselos реалізувала цифрового двійника для однієї з ключових гідроакумулюючих станцій в Ірландії, що є критичним об’єктом національної енергетичної інфраструктури. У проєкті була створена високоточна структурна

модель, яка поєднує в собі фізичні параметри будівельних конструкцій, гідромеханічного обладнання та геотехнічні характеристики.

Особливістю цієї реалізації стало використання даних у режимі реального часу, які надходять із розгалуженої мережі датчиків, вмонтованих у конструктивні елементи станції. Завдяки цьому цифровий двійник забезпечує неперервний моніторинг технічного стану об’єкта та динамічне оновлення інженерних розрахунків, враховуючи зміну навантажень, температури, вологості та інших критичних факторів.

Це дозволило інженерам не лише точно виявляти потенційні пошкодження чи зони напруження до появи візуальних дефектів, а й оптимізувати графіки технічного обслуговування, уникаючи зайвих простоїв. Крім того, така система підвищила рівень безпеки експлуатації, зменшила ризики аварій та надала аналітичну підтримку для прийняття стратегічних рішень щодо модернізації інфраструктури.

Впровадження цифрового двійника Akselos продемонструвало, як сучасні моделювальні технології здатні підвищити надійність та довговічність критичних енергетичних об’єктів, зменшуючи витрати та екологічні ризики.

Цифровий двійник мосту для інфраструктурного моніторингу. У журналі Automation in Construction представлено комплексне дослідження, присвячене створенню цифрового двійника мостової конструкції, який поєднує фізичні, кіберфізичні, інтеграційні та сервісні компоненти. Цей багаторівневий підхід дозволив не лише змоделювати геометрію та матеріальні характеристики моста, а й включити до системи дані з численних сенсорів, таких як тензодатчики, акселерометри та температурні датчики, що забезпечують безперервний моніторинг у режимі реального часу.

Завдяки інтеграції з системами інтернету речей (IoT) та інтелектуального аналізу даних, цифровий двійник дозволив відстежувати зміну навантаження, вібрації, деформації та інші показники, що свідчать про зношування або можливі пошкодження. Це значно покращило точність прогнозування технічного стану конструкції, а також дозволило оптимізувати планування ремонтних робіт, зменшуючи витрати на обслуговування та підвищуючи безпеку експлуатації.

Окрім цього, цифровий двійник став основою для розробки сценаріїв управління ризиками, симуляції аварійних ситуацій і розробки превентивних заходів, що є надзвичайно важливим для критичних інфраструктурних об’єктів. Такий підхід також відкрив можливості для інтеграції з міськими системами управління інфраструктурою та довгострокового стратегічного планування.

Тестування кіберзахисту енергетичних систем за допомогою цифрових двійників. У публікації на arXiv запропоновано інноваційну модель цифрового двійника фізичного лабораторного стенду, призначеного для симуляції сценаріїв кіберзагроз у розумних енергетичних мережах (smart grids). Модель охоплює як апаратну, так і програмну інфраструктуру, дозволяючи у режимі реального часу відтворювати складні атаки, зокрема DDoS, втручання у протоколи зв’язку та маніпуляції з даними датчиків.

Цифровий двійник не лише імітує поведінку системи під час атак, а й дозволяє тестувати ефективність різних захисних стратегій, зокрема систем виявлення вторгнень, механізмів відновлення та адаптивного керування. Таким чином, він виступає як платформа для навчання, дослідження та вдосконалення політик кіберзахисту, сприяючи підвищенню рівня готовності до реальних інцидентів.

Крім того, завдяки відкритому доступу та масштабованій архітектурі, ця модель може бути адаптована до різних конфігурацій енергетичних систем, що робить її цінним інструментом як для дослідників, так і для практиків у сфері критичної інфраструктури.

Ці приклади підтверджують, що цифрові двійники стають потужним інструментом для оптимізації функціонування критичної інфраструктури. Вони дозволяють не лише виявляти потенційні проблеми до їх фактичного виникнення, а й проводити моделювання різних сценаріїв в безпечному віртуальному середовищі. Це значно зменшує витрати на обслуговування, підвищує надійність і продуктивність систем, а також забезпечує сталу роботу інфраструктури в умовах зростаючих технологічних викликів та кіберзагроз.

Крім того, інтеграція цифрових двійників із системами моніторингу в реальному часі, засобами штучного інтелекту та прогнозної аналітики відкриває нові

горизонти для превентивного технічного обслуговування, розумного управління ресурсами та підвищення кіберстійкості. У перспективі, цифрові двійники можуть стати незамінною частиною стратегічного планування та управління критичними об’єктами, особливо в умовах швидкої урбанізації та цифровізації інфраструктур.

Нижче наведемо кілька прикладів експериментальних досліджень, які демонструють використання цифрових двійників для оптимізації критичної IT-інфраструктури.

Оптимізація обслуговування багатокомпонентних систем за допомогою цифрових двійників. У дослідженні, опублікованому в Journal of Intelligent Manufacturing, було представлено інноваційний підхід до оптимізації технічного обслуговування складних інженерних систем за допомогою цифрових двійників. Створена модель дозволяє не лише відстежувати поточний стан компонентів у реальному часі, а й прогнозувати їхнє зношення або потенційні відмови на основі аналітики даних. Це дає змогу своєчасно планувати ремонтні роботи, мінімізувати незаплановані простої, зменшити витрати на обслуговування та підвищити загальну надійність системи. Крім того, інтеграція цифрового двійника з алгоритмами штучного інтелекту підсилює здатність моделі до самооптимізації та адаптації до змін середовища експлуатації.

Використання цифрових двійників для виявлення вторгнень у промислові керуючі системи. У статті, опублікованій на платформі arXiv, розглядається розробка цифрового двійника для промислової системи з акцентом на моделювання кіберзагроз і тестування ефективності механізмів захисту. Цифровий двійник імітує поведінку фізичної інфраструктури, дозволяючи в безпечному віртуальному середовищі запускати різноманітні сценарії кібератак. Завдяки інтеграції з аналітичними інструментами та алгоритмами машинного навчання, система здатна виявляти, класифікувати та оперативно реагувати на потенційні загрози в режимі реального часу. Такий підхід не лише підвищує стійкість критичних систем до вторгнень, а й сприяє проактивному вдосконаленню політик кібербезпеки.

Оптимізація ресурсів аеропортових терміналів на основі цифрових двійників. У дослідженні, опублікованому в журналі Applied Mathematics and Nonlinear

Sciences, аналізується застосування цифрових двійників для удосконалення логістичних процесів і оптимізації розподілу ресурсів у зонах обслуговування аеропортів. Створена модель цифрового двійника враховує динаміку транспортування, розташування об’єктів, потоки пасажирів і вантажів, а також змінні погодні та оперативні умови. Завдяки цьому вдається зменшити загальну відстань переміщення техніки та персоналу, скоротити час очікування і покращити координацію між службами. Результатом є підвищення загальної ефективності аеропортової інфраструктури, зниження експлуатаційних витрат і покращення якості сервісу для клієнтів.

Енергетичні цифрові двійники в розумних виробничих системах. У статті, опублікованій в Journal of Manufacturing Systems, представлено розробку енергетично орієнтованого цифрового двійника, спрямованого на оптимізацію споживання енергії в рамках виробничих процесів. Цей цифровий двійник формує інтегровану систему, яка забезпечує постійний двосторонній зв’язок між фізичними об’єктами на виробництві та їхньою віртуальною моделлю. Завдяки безперервному збору та аналізу даних у реальному часі, система здатна адаптивно змінювати параметри процесу - з урахуванням навантаження, енергоспоживання та виробничих цілей. Такий підхід сприяє не лише досягненню високої енергоефективності, а й зменшенню викидів вуглецю, зниженню операційних витрат та підвищенню загальної стійкості виробництва.

Ці дослідження переконливо демонструють значний потенціал цифрових двійників у трансформації підходів до управління та обслуговування критичної IT-інфраструктури. Завдяки здатності відображати фізичні системи у віртуальному середовищі з високим ступенем точності, цифрові двійники забезпечують безперервний моніторинг у реальному часі, своєчасне виявлення відхилень, моделювання можливих сценаріїв збоїв і оперативне прийняття рішень. Крім того, вони сприяють гнучкому плануванню технічного обслуговування, оптимізації використання ресурсів, підвищенню енергоефективності та стійкості до кіберзагроз. Таким чином, цифрові двійники не лише підвищують надійність і ефективність IT-систем, а й відкривають нові можливості для інноваційного розвитку

інфраструктури в умовах зростаючої складності та динамічних викликів.

Нижче розлянемо практичне застосування методу оптимізації критичної IT-інфраструктури НЕК «Укренерго» за допомогою цифрових двійників.

Побудова цифрового двійника IT-інфраструктури НЕК «Укренерго». Ціль: створити віртуальну модель критичної IT-інфраструктури компанії, яка включає в себе мережеве обладнання, сервери, системи керування мережею, SCADA-системи та інформаційні шлюзи. Інструменти: використання платформ для цифрових двійників (наприклад, Siemens Digital Twin, Ansys Twin Builder або спеціалізовані SCADA-інтегровані рішення), у поєднанні з власними модулями моніторингу й збору телеметрії. Архітектура: поєднання віртуального середовища з даними з фізичних сенсорів і логів подій у реальному часі.

Інтеграція з системами моніторингу та телеметрії. Джерела даних: лог-файли, телеметрія з мережевого обладнання, трафік між серверами, журнали доступу. Призначення: забезпечення постійного потоку даних для валідації цифрового двійника й тренування алгоритмів оптимізації та прогнозування. Інструменти збору даних: Prometheus, Grafana, Zabbix, ELK Stack або індивідуальні агентські рішення.

Оптимізація розподілу навантаження. Завдання: балансування навантаження між серверами та вузлами з урахуванням поточних і прогнозованих навантажень. Алгоритм: використання градієнтних методів або генетичних алгоритмів для вибору найкращої конфігурації віртуальних машин, розподілу запитів і резервування каналів. Результат: зменшення перевантажень, пришвидшення обробки запитів, зниження пікових навантажень на ключові вузли.

Прогнозування інцидентів і технічних збоїв. Метод: застосування алгоритмів машинного навчання (наприклад, LSTM або Random Forest) для виявлення аномалій на основі історичних даних. Роль цифрового двійника: тестування гіпотетичних сценаріїв відмов без ризику для реальної системи. Практична користь: своєчасне попередження про можливі інциденти, що дозволяє планувати превентивні дії.

Тестування нових рішень та змін в ізольованому середовищі. Приклад: перед впровадженням нових політик кібербезпеки, оновлень програмного забезпечення або зміни архітектури - всі зміни перевіряються на цифровому двійнику. Переваги:

мінімізація ризиків простоїв та конфліктів, забезпечення безпеки змін без втручання в роботу продуктивної системи.

Енергетична ефективність та управління споживанням ресурсів Модель: цифровий двійник фіксує споживання енергії кожного вузла IT-інфраструктури. Оптимізація: впровадження адаптивного керування енергоспоживанням - наприклад, вимкнення резервних серверів у непікові години або перенесення задач у менш навантажені дата-центри. Результат: зменшення енергоспоживання до 15–25% на окремих сегментах.

Підвищення кіберзахисту. Роль цифрового двійника: використовується як полігон для тестування сценаріїв кібератак та оцінки ефективності протидії (наприклад, DDoS, вторгнення, спроби підміни даних). Інструменти: симуляція атак, збирання статистики, навчання алгоритмів виявлення. Практичний ефект: покращення готовності до інцидентів, формування планів реагування, зниження ризику компрометації критичних вузлів.

Інтелектуальне управління всією системою. Концепція: автоматизоване прийняття рішень на основі даних з цифрового двійника. Приклад: система самостійно вирішує, які процеси варто перемістити, які сервери перезапустити або які політики посилити. Платформи: AIOps (Artificial Intelligence for IT Operations), поєднані з цифровим двійником.

Для глибшого дослідження застосування цифрових двійників критичної інфраструктури на практиці нами був розроблений проєкт: «Цифровий двійник IT-інфраструктури НЕК «Укренерго»»

Мета - створити цифрову копію IT-інфраструктури НЕК «Укренерго», яка:

- інтегрує реальні дані від SCADA, мережевих пристроїв і серверів;
- забезпечує безперервний моніторинг, симуляцію сценаріїв інцидентів та оптимізацію роботи;
- підтримує виявлення збоїв і кіберзагроз;
- дозволяє експериментувати з оновленнями та змінами без шкоди для живої інфраструктури.

Компоненти цифрового двійника IT-інфраструктури НЕК «Укренерго».

Центральне ядро цифрового двійника: Об'єктно-орієнтоване представлення IT-активів (сервери, мережі, шлюзи, SCADA). Симуляційне ядро (на основі фізичних та інформаційних моделей). Обробник подій і тригерів (аномалії, перевантаження, вторгнення).

Інтеграція з фізичними джерелами: SNMP, NetFlow для мережевих пристроїв (комутатори, маршрутизатори). SCADA-протоколи: Modbus, DNP3, IEC 61850. Серверні моніторингові агенти: Zabbix, Prometheus, psutil.

Інформаційні шлюзи (DMZ / API): Проксі для збору даних із зовнішніх систем. Безпечні MQTT/REST API для інтеграції з цифровим ядром.

Аналітичні й прогнозні модулі: Алгоритми виявлення аномалій (ML/AI). Прогнозування навантаження та обслуговування. Симулятори кіберзагроз.

Візуалізація та Dashboard: Grafana, Siemens Twin Viewer або власний UI. 3D/2D моделі об'єктів, теплові карти, топологія мережі. Архітектура цифрового двійника (рис. 4.2)

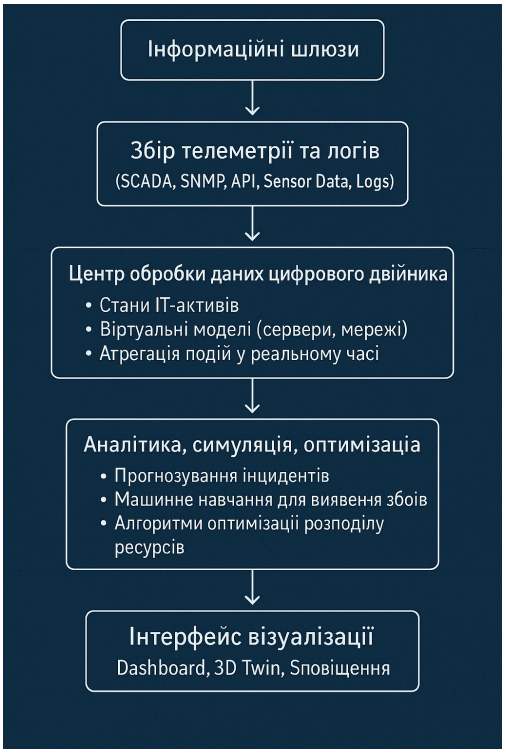

Рисунок 4.2 - Архітектура цифрового двійника

Інструменти та платформи:

- Siemens NX & Mindsphere, Ansys Twin Builder, Altair SmartWorks - для складного цифрового моделювання;
- Zabbix / Prometheus / Grafana - для збору метрик, логів і моніторингу;
- Python + FastAPI + Pandas + scikit-learn - для аналітики, обробки подій, створення API;
- Node-RED / MQTT / OPC-UA - для потоків даних між SCADA і цифровим двійником;
- Docker / Kubernetes - для віртуалізації та гнучкого розгортання.

Приклад сценаріїв застосування:

- прогнозування перевантаження SCADA-серверів на основі історичних трендів CPU/IO;
- симуляція атаки на шлюз IEC 104 - перевірка дій цифрового двійника, план відновлення;
- автоматична оптимізація маршрутизації трафіку між регіональними дата-центрами в реальному часі;
- моделювання планового оновлення ПЗ - оцінка впливу без шкоди для основної мережі;
- раннє виявлення кіберзагроз через цифрового агента, що аналізує мережеву поведінку.

Розробка цифрового двійника ІТ-інфраструктури НЕК «Укренерго» демонструє потужний потенціал сучасних цифрових технологій для підвищення ефективності, надійності та кіберстійкості критичних енергетичних систем. Інтеграція даних у реальному часі з віртуальним середовищем дає змогу здійснювати постійний моніторинг стану обладнання, своєчасно виявляти аномалії, прогнозувати збої, оптимізувати розподіл ресурсів і тестувати сценарії в безпечному цифровому середовищі.

Такий підхід дозволяє зменшити експлуатаційні витрати, мінімізувати ризики відмов та покращити оперативне управління інфраструктурою, що є надзвичайно важливим для стабільної роботи національної енергетичної системи в умовах

сучасних кіберзагроз і підвищених вимог до надійності. Цифрові двійники відкривають нові горизонти для трансформації енергетики та цифровізації стратегічних підприємств України.

4.3 Висновки до четвертого розділу

Розроблений метод оптимізації критичної IT інфраструктури цифровими двійниками є сучасним підходом, що поєднує віртуальне моделювання, аналітику в реальному часі та алгоритми штучного інтелекту для досягнення максимальної ефективності, надійності та адаптивності системи. Особливістю методу є можливість динамічного аналізу та прогнозування роботи системи в режимі реального часу з метою виявлення вузьких місць і підвищення ефективності її функціонування.

Проведено аналіз експериментів та досліджень методу оптимізації критичної IT інфраструктури цифровими двійниками. Результати експериментальних досліджень підтверджують їх ефективність у забезпеченні безперервної роботи, надійності та безпеки систем.

Для глибшого дослідження застосування цифрових двійників критичної інфраструктури на практиці нами був розроблений проєкт: Цифровий двійник IT-інфраструктури НЕК «Укренерго». Результати дослідження демонструють зниження ризиків відмов, підвищення ефективності управління ресурсами та покращення стійкості системи до зовнішніх загроз.

ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено метод для забезпечення безперебійного працювання критичної інфраструктури, особливістю яких є використання цифрових двійників на практиці та отримано такі результати:

1. Проналізовано відомі методи і технології моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників.
2. Виділено ключові особливості оптимізації та моделювання критичної IT інфраструктури цифровими двійниками.
3. Розглянуто цільову функцію та алгоритми оптимізації критичної IT інфраструктури цифровими двійниками.
4. Розроблено метод оптимізації критичної IT інфраструктури цифровими двійниками та досліджено практичне застосування цифрових двійників у критичній інфраструктурі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Gao J., & Wu J. (2022). Digital Twins in Critical Infrastructure. *Information*, Vol. 15(8), P. 454. https://doi.org/10.3390/info15080454

2. Esnoul C., Colomo-Palacios, R., Jee E., Chockalingam S., Eidar Simensen J., Bae D.-H. Report on the 3rd international workshop on engineering and cybersecurity of critical systems (EnCyCriS-2022). *ACM SIGSOFT Softw. Eng. Notes.* 2023. Vol. 48, P. 81–84. https://doi.org/10.1145/3573074.3573095

3. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. *Reliab. Eng. Syst. Saf.* 2014. Vol. 121. P. 43–60. https://doi.org/10.1016/j.ress.2013.06.040

4. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* 2015. Vol. 8. P. 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

5. Rathnayaka B., Siriwardana C., Robert D., Amaratunga D., Setunge S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. *Int. J. Disaster Risk Reduct.* 2022. Vol. 78, P. 103123. https://doi.org/10.1016/j.ijdrr.2022.103123

6. Khan Babar A. H., Ali Y. Framework construction for augmentation of resilience in critical infrastructure: Developing countries a case in point. *Technol. Soc.* 2022. Vol. 68, P. 101809. https://doi.org/10.1016/j.techsoc.2021.101809

7. Wells E.M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: *A systematic literature review. Prog. Disaster Sci.* 2022. Vol. 15, P. 100244. https://doi.org/10.1016/j.pdisas.2022.100244

8. Chowdhury N., Gkioulos V. Cyber security training for critical infrastructure protection: *A literature review. Comput. Sci. Rev.* 2021. Vol. 40, P. 100361. https://doi.org/10.1016/j.cosrev.2021.100361

9. Ani U.P.D., He H., Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: *Manufacturing in perspective. J. Cyber Secur. Technol.* 2017. Vol. 1, P. 32–74. https://doi.org/10.1080/23742917.2016.1252211

10. Ghorbani A. A. Bagheri E. The state of the art in critical infrastructure protection: A framework for convergence. *Int. J. Crit. Infrastruct.* 2008. Vol. 4, P. 215–244. https://doi.org/10.1504/IJCIS.2008.017438

11. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst.* 2001. Vol. 21, P. 11–25. https://doi.org/10.1109/37.969131

12. Brown, G., Carlyle M., Salmerón J., Wood K. Defending critical infrastructure. *Interfaces* 2006. Vol. 36, P. 530–544. https://doi.org/10.1287/inte.1060.0252

13. Aradau C. Security that matters: Critical infrastructure and objects of protection. *Secur. Dialogue* 2010. Vol. 41, P. 491–514. https://doi.org/10.1177/0967010610382687

14. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex approach to assessing resilience of critical infrastructure elements. *Int. J. Crit. Infrastruct. Prot.* 2019. Vol. 25, P. 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003

15. Lee II, E.E., Mitchell J.E., Wallace W.A. Restoration of services in interdependent infrastructure systems: *A network flows approach. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* 2007. Vol. 37, P. 1303–1317. https://doi.org/10.1109/TSMCC.2007.905859

16. Laplante P., Amaba B. Artificial intelligence in critical infrastructure systems. *Computer* 2021, Vol. 54, P. 14–24. https://doi.org/10.1109/MC.2021.3055892

17. Groenewold M.R., Burrer S.L., Ahmed F., Uzicanin A., Free H., Luckhaupt S.E. Increases in Health-Related Workplace Absenteeism Among Workers in Essential Critical Infrastructure Occupations During the COVID-19 Pandemic-United States, March-April 2020. *MMWR Morb. Mortal. Wkly. Rep.* 2020. Vol. 69, P. 853–858. https://doi.org/10.15585/mmwr.mm6927a1

18. Jiang Y., Yin S., Li K., Luo H., Kaynak O. Industrial applications of digital twins. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* 2021. Vol. 379, P. 20200360. https://doi.org/10.1098/rsta.2020.0360

19. Tao F., Qi Q. Make more digital twins. *Nature* 2019. Vol. 573, P. 490–491. https://doi.org/10.1038/d41586-019-02849-1

20. Batty M. Digital twins. Environ. Plan. *B Urban Anal. City Sci.* 2018. Vol. 45, P. 817–820. https://doi.org/10.1177/2399808318796416

21. Stark R., Fresemann C., Lindow K. Development and operation of digital twins for technical systems and services. *CIRP Ann.* 2019. Vol. 68, P. 129–132. https://doi.org/10.1016/j.cirp.2019.04.024

22. Sharma A., Kosasih E., Zhang J., Brintrup A., Calinescu A. Digital twins: State of the art theory and practice, challenges, and open research questions. *J. Ind. Inf. Integr.* 2022, Vol. 30, 100383. https://doi.org/10.1016/j.jii.2022.100383

23. El Saddik, A. Digital twins: The convergence of multimedia technologies. *IEEE MultiMedia* 2018. Vol. 25, P. 87–92. https://doi.org/10.1109/MMUL.2018.023121167

24. Lampropoulos G. Artificial intelligence, big data, and machine learning in industry 4.0. In Encyclopedia of Data Science and Machine Learning; IGI Global: Hershey, PA, USA, 2023. P. 2101–2109. https://doi.org/10.4018/978-1-7998-9220-5.ch125

25. Piras G., Agostinelli S., Muzi F. Digital Twin Framework for Built Environment: *A Review of Key Enablers. Energies* 2024. Vol. 17, P. 436. https://doi.org/10.3390/en17020436

26. Liu C., Zhang P., Xu X. Literature Review of Digital Twin Technologies for Civil Infrastructure. *J. Infrastruct. Intell. Resil.* 2023. Vol. 2, P. 100050. https://doi.org/10.1016/j.iintel.2023.100050

27. Thacker S., Kelly S., Pant R., Hall J.W. Evaluating the benefits of adaptation of critical infrastructures to hydrometeorological risks. *Risk Anal.* 2018. Vol. 38, P. 134–150. https://doi.org/10.1111/risa.12839

28. Thacker S., Barr S., Pant R., Hall J.W., Alderson D. Geographic hotspots of critical national infrastructure. *Risk Anal.* 2017. Vol. 37, P. 2490–2505. https://doi.org/10.1111/risa.12840

29. Bloomfield R.E., Popov P., Salako K., Stankovic V., Wright, D. Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliab. Eng. Syst. Saf.* 2017. Vol. 167, P. 198–217. https://doi.org/10.1016/j.ress.2017.05.030

30. Delvosalle C., Robert B., Nourry J., Yan G., Brohez S., Delcourt J. Considering critical infrastructures in the land use planning policy around seveso plants. *Saf. Sci.* 2017. Vol. 97, P. 27–33. https://doi.org/10.1016/j.ssci.2016.08.001

31. Lam J.S.L., Liu C., Gou X. Cyclone risk mapping for critical coastal infrastructure: Cases of East Asian seaports. *Ocean Coast. Manag.* 2017. Vol. 141, P. 43–54. https://doi.org/10.1016/j.ocecoaman.2017.02.015

32. Gonzalez-Granadillo G., Garcia-Alfaro J., Debar H. A polytope-based approach to measure the impact of events against critical infrastructures. *J. Comput. Syst. Sci.* 2017. Vol. 83, P. 3–21. https://doi.org/10.1016/j.jcss.2016.02.004

33. Espada R., Apan A., McDougall K. Vulnerability assessment of urban community and critical infrastructures for integrated flood risk management and climate adaptation strategies. *Int. J. Disaster Resil. Built Environ.* 2017. Vol. 8, P. 375–411. https://doi.org/10.1108/IJDRBE-03-2015-0010

34. Ongkowijoyo C., Doloi H. Determining critical infrastructure risks using social network analysis. *Int. J. Disaster Resilience Built Environ.* 2017. Vol. 8, P. 5–26. https://doi.org/10.1108/IJDRBE-05-2016-0016

35. Aradau C. Security that matters: Critical infrastructure and objects of protection. *Secur. Dialogue.* 2010. Vol. 41, P. 491–514. https://doi.org/10.1177/0967010610382687

36. Van Staalduinen M.A., Khan F., Gadag V., Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. *Reliab. Eng. Syst. Saf.* 2017. Vol. 157, P. 23–34. https://doi.org/10.1016/j.ress.2016.08.014

37. Imteaj A., Khan I., Khazaei J., Amini M.H. Fedresilience: A federated learning application to improve resilience of resource-constrained critical infrastructures. *Electronics*. 2021. Vol. 10, 1917. https://doi.org/10.3390/electronics10161917

38. Depina I., Divić V., Munjiza A., Peroš B. Perfomance-based wind engineering assessment of critical telecommunication infrastructure subjected to bora wind. *Eng. Struct.* 2021. Vol. 236, 112083. https://doi.org/10.1016/j.engstruct.2021.112083

39. Hendricks M.D., Van Zandt S. Unequal protection revisited: Planning for environmental justice, hazard vulnerability, and critical infrastructure in communities of color. *Environ. Justice.* 2021. Vol. 14, P. 87–97. https://doi.org/10.1089/env.2020.0054

40. Chowdhury N., Gkioulos V. Cyber security training for critical infrastructure protection: *A literature review. Comput. Sci. Rev.* 2021, Vol. 40, 100361. https://doi.org/10.1016/j.cosrev.2021.100361

41. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. *Int. J. Crit. Infrastruct. Prot.* 2015. Vol. 8, P. 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002

42. Zheng Y., Yang S., Cheng H. An application framework of digital twin and its case study. *J. Ambient. Intell. Humaniz. Comput.* 2019. Vol. 10, P. 1141–1153. https://doi.org/10.1007/s12652-018-0911-3

43. Chen Y. Integrated and intelligent manufacturing: Perspectives and enablers. *Engineering.* 2017. Vol. 3, P. 588–595. https://doi.org/10.1016/J.ENG.2017.04.009

44. Haag S., Anderl R. Digital twin–proof of concept. *Manuf. Lett.* 2018. Vol. 15, P. 64–66. https://doi.org/10.1016/j.mfglet.2018.02.006

45. Schluse M., Priggemeyer M., Atorf L., Rossmann J. Experimentable digital twins—Streamlining simulation-based systems engineering for industry 4.0. *IEEE Trans. Ind. Inform.* 2018. Vol. 14, P. 1722–1731. https://doi.org/10.1109/TII.2018.2804917

46. VrabiČ R., Erkoyuncu J.A., Butala P., Roy R. Digital twins: Understanding the added value of integrated models for through-life engineering services. *Procedia Manuf.* 2018. Vol. 16, P. 139–146. https://doi.org/10.1016/j.promfg.2018.10.167

47. Talkhestani B.A., Jung T., Lindemann B., Sahlab N., Jazdi N., Schloegl W., Weyrich M. An architecture of an intelligent digital twin in a cyber-physical production system. *at-Automatisierungstechnik* 2019. Vol. 67, P. 762–782. https://doi.org/10.1515/auto-2019-0039

48. Kritzinger W., Karner M., Traar G., Henjes J., Sihn W. Digital twin in manufacturing: A categorical literature review and classification. *IFAC-PapersOnLine* 2018. Vol. 51, P. 1016–1022. https://doi.org/10.1016/j.ifacol.2018.08.474

49. Malakuti S., Grüner S. Architectural aspects of digital twins in IIoT systems. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings, New York, NY, USA, Vol. 24–28 September 2018. P. 1–2. https://doi.org/10.1145/3241403.3241417

50. Vachálek J., Bartalskỳ L., Rovnỳ O., Šišmišová D., Morháč M., Lokšík M. The digital twin of an industrial production line within the industry 4.0 concept. In Proceedings of the 2017 21st International Conference on Process Control (PC), Strbske Pleso, Slovakia, 6–9 June 2017; IEEE: New York, NY, USA, 2017. P. 258–262. https://doi.org/10.1109/PC.2017.7976223

51. Tao F., Cheng J., Qi Q., Zhang M., Zhang H., Sui F. Digital twin-driven product design, manufacturing and service with big data. *Int. J. Adv. Manuf. Technol.* 2018. Vol. 94, 3563–3576. https://doi.org/10.1007/s00170-017-0233-1

52. Bao J., Guo D., Li J., Zhang J. The modelling and operations for the digital twin in the context of manufacturing. *Enterp. Inf. Syst.* 2019. Vol. 13, P. 534–556. https://doi.org/10.1080/17517575.2018.1526324

53. Rasheed A., San O., Kvamsdal T. Digital Twin: Values, Challenges and Enablers From a Modeling Perspective. *IEEE Access.* 2020. Vol. 8, 21980–22012. https://doi.org/10.1109/ACCESS.2020.2970143

54. Shahzad M., Shafiq M.T., Douglas D., Kassem M. Digital Twins in Built Environments: An Investigation of the Characteristics, Applications, and Challenges. *Buildings.* 2022. Vol. 12, P. 120.

55. Eckhart M., Ekelhart A. Towards security-aware virtual environments for digital twins. In Proceedings of the 4th ACM Workshop on Cyber-Physical System Security, New York, NY, USA. 22 May 2018. P. 61–72. https://doi.org/10.1145/3198458.3198464

56. Ellegaard O., Wallin J.A. The bibliometric analysis of scholarly production: How great is the impact? *Scientometrics*. 2015. Vol. 105, P. 1809–1831. https://doi.org/10.1007/s11192-015-1645-z

57. Gusenbauer M., Haddaway N.R. Which academic search systems are suitable for systematic reviews or meta-analyses? Evaluating retrieval qualities of google scholar, PubMed, and 26 other resources. *Res. Synth. Methods*. 2020. Vol. 11, P. 181–217. https://doi.org/10.1002/jrsm.1378

58. Donthu N., Kumar S., Mukherjee D., Pandey N., Lim W.M. How to conduct a bibliometric analysis: An overview and guidelines. *J. Bus. Res.* 2021. Vol. 133, P. 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

59. Aria M., Cuccurullo C. Bibliometrix: An r-tool for comprehensive science mapping analysis. *J. Informetr.* 2017. Vol. 11, P. 959–975. https://doi.org/10.1016/j.joi.2017.08.007

60. Mongeon P., Paul-Hus A. The journal coverage of web of science and scopus: A comparative analysis. *Scientometrics*. 2015. Vol. 106, P. 213–228. https://doi.org/10.1007/s11192-015-1765-5

61. Zhu J., Liu W. A tale of two databases: The use of web of science and scopus in academic papers. *Scientometrics*. 2020. Vol. 123, P. 321–335. https://doi.org/10.1007/s11192-020-03387-8

62. Page M.J., McKenzie J.E., Bossuyt P.M., Boutron I., Hoffmann T.C., Mulrow C.D., Shamseer L., Tetzlaff J.M., Akl E.A., Brennan S.E., et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *Int. J. Surg.* 2021. Vol. 88, P. 105906. https://doi.org/10.1016/j.ijsu.2021.105906

63. Tao F., Zhang H., Liu A., Nee A.Y.C. Digital Twin in Industry: State-of-the-Art. *IEEE Trans. Ind. Inf.* 2019. Vol. 15, P. 2405–2415. https://doi.org/10.1109/TII.2018.2873186

64. Rosen R., Von Wichert G., Lo G., Bettenhausen K.D. About the importance of autonomy and digital twins for the future of manufacturing. *IFAC-PapersOnLine*. 2015. Vol. 48, P. 567–572. https://doi.org/10.1016/j.ifacol.2015.06.141

65. Qi Q., Tao F., Zuo Y., Zhao D. Digital Twin Service towards Smart Manufacturing. *Procedia CIRP*. 2018. Vol. 72, P. 237–242. https://doi.org/10.1016/j.procir.2018.03.103

66. Tao F., Zhang M. Digital twin Shop-Floor: A new Shop-Floor paradigm towards smart manufacturing. *IEEE Access*. 2017. Vol. 5, 20418–20427. https://doi.org/10.1109/ACCESS.2017.2756069

67. Lu Y., Liu C., Wang K.I.-K., Huang H., Xu X. Digital twin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robot. Comput. -Integr. Manuf.* 2020. Vol. 61, 101837. https://doi.org/10.1016/j.rcim.2019.101837

68. Uhlemann T.H.-J., Lehmann C., Steinhilper R. The digital twin: Realizing the cyber-physical production system for industry 4.0. *Procedia Cirp*. 2017. Vol. 61, P. 335–340. https://doi.org/10.1016/j.procir.2016.11.152

69. Tao F., Qi Q., Wang L., Nee A.Y.C. Digital Twins and Cyber–Physical Systems toward Smart Manufacturing and Industry 4.0: Correlation and Comparison. *Engineering*. 2019. Vol. 5, P. 653–661. https://doi.org/10.1016/j.eng.2019.01.014

70. Zhang J., Yu Q., Zheng F., Long C., Lu Z., Duan Z. Comparing keywords plus of WOS and author keywords: A case study of patient adherence research. *J. Assoc. Inf. Sci. Technol*. 2016. Vol. 67, P. 967–972. https://doi.org/10.1002/asi.23437

71. Barricelli B.R., Fogli D. Digital twins in human-computer interaction: A systematic review. *Int. J. Hum. – Comput. Interact.* 2024. Vol. 40, P. 79–97. https://doi.org/10.1080/10447318.2022.2118189

72. Kaššaj M., Peráček T. Synergies and Potential of Industry 4.0 and Automated Vehicles in Smart City Infrastructure. *Appl. Sci.* 2024. Vol. 14, 3575. https://doi.org/10.3390/app14093575

73. Attaran S., Attaran M., Celik B.G. Digital Twins and Industrial Internet of Things: Uncovering operational intelligence in industry 4.0. *Decis. Anal. J.* 2024. Vol. 10, 100398. https://doi.org/10.1016/j.dajour.2024.100398

74. Guo J., Bilal M., Qiu Y., Qian C., Xu X., Choo K.K.R. Survey on digital twins for Internet of Vehicles: Fundamentals, challenges, and opportunities. *Digit. Commun. Netw.* 2024. Vol. 10, P. 237–247. https://doi.org/10.1016/j.dcan.2022.05.023

75. Tao F., Zhang H., Zhang C. Advancements and challenges of digital twins in industry. *Nat. Comput. Sci.* 2024. Vol. 4, P. 169–177. https://doi.org/10.1038/s43588-024-00603-w

76. Negri E., Fumagalli L., Macchi M. A review of the roles of digital twin in CPS-based production systems. *Procedia Manuf.* 2017. Vol. 11, P. 939–948. https://doi.org/10.1016/j.promfg.2017.07.198

77. Laplante P., Amaba B. Artificial intelligence in critical infrastructure systems. *Computer* 2021. Vol. 54, P. 14–24. https://doi.org/10.1109/MC.2021.3055892

78. Radanliev P., De Roure D., Nicolescu R., Huth M., Santos O. Digital twins: Artificial intelligence and the IoT cyber-physical systems in industry 4.0. *Int. J. Intell. Robot. Appl.* 2022. Vol. 6, P. 171–185. https://doi.org/10.1007/s41315-021-00180-5

79. Rathore M.M., Shah S.A., Shukla D., Bentafat E., Bakiras S. The role of AI, machine learning, and big data in digital twinning: A systematic literature review, challenges, and opportunities. *IEEE Access* 2021. Vol. 9, 32030–32052. https://doi.org/10.1109/ACCESS.2021.3060863

80. Lv Z., Xie S. Artificial intelligence in the digital twins: State of the art, challenges, and future research topics. *Digit. Twin* 2022. Vol. 1, P. 12. https://doi.org/10.12688/digitaltwin.17524.2

81. Bordukova, M.; Makarov, N.; Rodriguez-Esteban, R.; Schmich, F.; Menden, M.P. Generative artificial intelligence empowers digital twins in drug discovery and clinical trials. *Expert Opin. Drug Discov.* 2023. Vol. 19, P. 33–42. https://doi.org/10.1080/17460441.2023.2273839

ДОДАТОК А

(обов’язковий)

ПРЕЗЕНТАЦІЯ РОБОТИ

Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп’ютерної інженерії та інформаційних систем

«Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників»

Виконав: студент 2 курсу, група КІ2м-23-1 Дмитро АНДРЄЄВ
Керівник: канд. екон. наук, доцент Світлана САЧЕНКО

Зв'язок роботи з науковими програмами, планами, темами.

У сучасних умовах безперебійна робота об'єктів критичної інфраструктури - таких як енергетичні системи, об'єкти зв'язку, транспортні вузли, системи водопостачання та водовідведення, установи охорони здоров'я, банківські установи й IT-інфраструктури - є ключовим чинником національної безпеки, соціальної стабільності та економічної стійкості. Порушення функціонування таких систем через технічні збої, зовнішні атаки, людські помилки або стихійні лиха можуть мати серйозні наслідки: від масштабних відключень і паралічу логістичних ланцюгів до обмеження доступу до життєво важливих послуг, значних економічних втрат і загроз життю та здоров’ю населення.

Інноваційним і перспективним напрямом для забезпечення стабільності критичних систем є впровадження технології цифрових двійників (Digital Twins). Цифровий двійник - це динамічна віртуальна копія фізичного об'єкта, системи або процесу, що створюється на основі реальних технічних характеристик та актуальних даних. Така модель підтримує двосторонній зв’язок із фізичним прототипом, що дає змогу не лише візуалізувати його поточний стан, а й аналізувати історичні дані, виявляти тренди розвитку чи деградації, моделювати аварійні сценарії, а також автоматизовано приймати рішення для оптимізації роботи й усунення потенційних вразливостей.

Перелік публікацій

За темою кваліфікаційної роботи опубліковано одну наукову статтю і науковому журналі категорії Б

Dmytro Andrieiev, Oleksii Lyhun, Andriy Drozd. MONITORING SYSTEM FOR CRITICAL INFRASTRUCTURE OBJECTS BASED ON DIGITAL TWINS. *Computer Systems and Information Technologies*, 2025. №1.

Метою даної дипломної роботи є дослідження системи моніторингу об’єктів критичної інфраструктури, а також покращення ефективності оптимізації критичної IT інфраструктури цифровими двійниками, яка здатна в режимі реального часу збирати дані, аналізувати їх, прогнозувати відмови та візуалізувати поточний стан IT-активів.

Поставлена мета досягається розв’язанням таких основних завдань:

-аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників;

-виділити ключові особливості оптимізації та моделювання критичної IT інфраструктури цифровими двійниками;

-розглянути цільову функцію та алгоритми оптимізації критичної IT інфраструктури цифровими двійниками;

-розробити метод оптимізації критичної IT інфраструктури цифровими двійниками та дослідити практичне застосування цифрових двійників у критичній інфраструктурі.

Об’єктом дослідження є процес моніторингу об'єктів критичної інфраструктури на основі цифрових двійників.

Предметом дослідження є процес оптимізації та моделювання об'єктів критичної інфраструктури на основі цифрових двійників.

Наукова новизна отриманих результатів:

- розроблено метод для забезпечення безперебійного роботи критичної інфраструктури, особливістю яких є використання цифрових двійників на практиці.

На основі проведених досліджень розроблено метод оптимізації критичної інфраструктури цифровими двійниками.

Практична значимість отриманих результатів полягає у розробленні проєкту «Цифровий двійник ІТ-інфраструктури НЕК «Укренерго».

Для розв’язання поставлених задач використовувалися метод оптимізації та моделювання критичної інфраструктури цифровими двійниками.

Моніторинг об'єктів критичної інфраструктури: виклики та рішення

У сучасних умовах стабільне функціонування об'єктів критичної інфраструктури, таких як енергетичні системи, транспортні вузли, водопостачання, об'єкти зв'язку, охорони здоров'я та фінансові системи, є основоположним чинником забезпечення національної безпеки, соціальної стабільності та економічної стійкості. Порушення роботи критичних систем, спричинені технічними несправностями, кіберзагрозами, людським фактором або природними катастрофами, можуть мати катастрофічні наслідки: масштабні перебої в обслуговуванні населення, порушення логістичних мереж, економічні втрати та загрози для життя і здоров’я громадян. У цьому контексті особливої важливості набуває впровадження систем постійного моніторингу, які забезпечують раннє виявлення загроз, профілактичне обслуговування, підвищення ситуаційної обізнаності, відповідність вимогам безпеки та ефективне реагування на надзвичайні події.

Цифрові двійники: інноваційна технологія для забезпечення надійності критичних систем

Використання цифрових двійників (Digital Twins) є одним із найбільш перспективних напрямів підвищення ефективності моніторингу та управління об'єктами критичної інфраструктури. Цифровий двійник являє собою динамічну віртуальну модель фізичного об'єкта, системи або процесу, яка створюється на основі актуальних даних і реальних технічних характеристик. Завдяки двосторонньому зв’язку між фізичним об'єктом і його цифровим відображенням стає можливим не лише візуалізувати поточний стан системи, але й аналізувати історичні дані, прогнозувати розвиток подій, моделювати аварійні сценарії та автоматизовано приймати рішення для оптимізації роботи і підвищення безпеки. Використання цифрових двійників у поєднанні з технологіями штучного інтелекту, машинного навчання, хмарних обчислень і 5G створює нові можливості для побудови стійкої, ефективної та адаптивної критичної інфраструктури.

Оптимізація критичної IT-інфраструктури за допомогою цифрових двійників

У сучасних умовах розвитку технологій підтримка стабільної роботи IT-інфраструктури є критично важливою для забезпечення безпеки, ефективності та стійкості організацій. Використання цифрових двійників відкриває нові можливості для моніторингу, аналізу та оптимізації критичних систем. Цифровий двійник, що являє собою динамічну віртуальну копію фізичної інфраструктури, забезпечує оперативне відстеження робочих параметрів у реальному часі, дозволяє прогнозувати можливі збої та планувати технічне обслуговування. Завдяки аналізу даних цифровий двійник оптимізує споживання енергії, мінімізує простої, покращує розподіл ресурсів та забезпечує вищий рівень кіберстійкості. Такий підхід сприяє підвищенню надійності роботи систем, зниженню експлуатаційних витрат та досягненню стратегічних цілей підприємства в умовах цифрової трансформації.

Етапи методу оптимізації за допомогою цифрових двійників

1. Збір телеметричних даних з усіх вузлів системи

На цьому етапі відбувається безперервне отримання інформації з усіх елементів критичної IT-інфраструктури (сервери, мережеве обладнання, системи зберігання даних тощо). Дані включають навантаження на процесори, мережевий трафік, рівень енергоспоживання, температурні показники, логи збоїв тощо.

2. Аналіз поточного стану та виявлення «вузьких місць»

Зібрані дані обробляються аналітичними модулями, включаючи інструменти штучного інтелекту та машинного навчання. Визначаються аномалії, перевантаження окремих компонентів, затримки в передачі даних, недостатня відмовостійкість.

3. Моделювання сценаріїв поведінки при зміні навантаження або відмові компонентів

Цифровий двійник дозволяє безпечно симулювати різні ситуації: збільшення навантаження, збої окремих вузлів, атаки або аварії.

4. Оптимізація параметрів роботи системи

На основі результатів моделювання система або експерт формує оптимальні налаштування: балансування навантаження, зміна пріоритетів у трафіку, перерозподіл ресурсів, оновлення політик безпеки.

5. Реалізація змін у реальному середовищі або на рівні рекомендацій

Залежно від типу системи, зміни можуть бути впроваджені автоматично або у вигляді рекомендацій для IT-фахівців. Важливо забезпечити безпечний перехід без негативного впливу на поточні процеси.

6. Зворотній зв'язок – оцінка ефективності змін та самонавчання

Після впровадження змін цифровий двійник продовжує моніторинг системи. Оцінюється, наскільки успішними були зміни. Алгоритми самонавчання адаптують модель для майбутніх рішень.

Поетапний підхід дозволяє не лише підвищити ефективність роботи IT-інфраструктури, а й забезпечити її стійкість до зовнішніх і внутрішніх загроз.

Побудова цифрового двійника критичної інфраструктури НЕК "Укренерго"

Мета: створити віртуальну модель критичної IT-інфраструктури компанії, яка включає в себе мережеве обладнання, сервери, системи керування мережею, SCADA-системи та інформаційні шлюзи.

Інструменти: використання платформ для цифрових двійників (наприклад, Siemens Digital Twin, Ansys Twin Builder або спеціалізовані SCADA-інтегровані рішення), у поєднанні з власними модулями моніторингу й збору телеметрії.

Архітектура: поєднання віртуального середовища з даними з фізичних сенсорів і логів подій у реальному часі.

Компоненти цифрового двійника

Центральне ядро цифрового двійника: Об'єктно-орієнтоване представлення IT-активів (сервери, мережі, шлюзи, SCADA). Симуляційне ядро (на основі фізичних та інформаційних моделей). Обробник подій і тригерів (аномалії, перевантаження, вторгнення).

Інтеграція з фізичними джерелами: SNMP, NetFlow для мережевих пристроїв (комутатори, маршрутизатори). SCADA-протоколи: Modbus, DNP3, IEC 61850. Серверні моніторингові агенти: Zabbix, Prometheus, psutil.

Інформаційні шлюзи (DMZ / API): Проксі для збору даних із зовнішніх систем. Безпечні MQTT/REST API для інтеграції з цифровим ядром.

Аналітичні й прогнозні модулі: Алгоритми виявлення аномалій (ML/AI). Прогнозування навантаження та обслуговування. Симулятори кіберзагроз.

Візуалізація та Dashboard: Grafana, Siemens Twin Viewer або власний UI. 3D/2D моделі об'єктів, теплові карти, топологія мережі.

Інструменти та платформи:

-Siemens NX & Mindsphere, Ansys Twin Builder, Altair SmartWorks - для складного цифрового моделювання;

-Zabbix / Prometheus / Grafana - для збору метрик, логів і моніторингу;

-Python + FastAPI + Pandas + scikit-learn - для аналітики, обробки подій, створення API;

-Node-RED / MQTT / OPC-UA - для потоків даних між SCADA і цифровим двійником;

-Docker / Kubernetes - для віртуалізації та гнучкого розгортання.

Приклад сценаріїв застосування:

-прогнозування перевантаження SCADA-серверів на основі історичних трендів CPU/IO;

-симуляція атаки на шлюз IEC 104 - перевірка дій цифрового двійника, план відновлення;

-автоматична оптимізація маршрутизації трафіку між регіональними дата-центрами в реальному часі;

-моделювання планового оновлення ПЗ - оцінка впливу без шкоди для основної мережі;

-раннє виявлення кіберзагроз через цифрового агента, що аналізує мережеву поведінку.

Створення цифрового двійника ІТ-інфраструктури НЕК «Укренерго» наочно демонструє широкі можливості сучасних цифрових рішень у зміцненні ефективності, надійності та кіберстійкості ключових енергетичних систем. Завдяки поєднанню даних у реальному часі з віртуальним моделюванням забезпечується безперервний контроль за станом обладнання, оперативне виявлення відхилень і збоїв, прогнозування несправностей, раціональний розподіл ресурсів та випробування різних сценаріїв у безпечному цифровому середовищі.

Цей інноваційний підхід дозволяє суттєво знизити витрати на обслуговування, зменшити ймовірність відмов і підвищити ефективність управлінських рішень — що критично важливо для надійного функціонування національної енергосистеми в умовах зростаючих кіберзагроз. Цифрові двійники відкривають перспективи для глибокої трансформації енергетичного сектору та цифрової модернізації стратегічно важливих підприємств України.

ДОДАТОК Б

(обов'язковий)

НАУКОВА ПРАЦЯ ЗДОБУВАЧА

Dmytro Andrieiev, Oleksii Lyhun, Andriy Drozd. MONITORING SYSTEM FOR CRITICAL INFRASTRUCTURE OBJECTS BASED ON DIGITAL TWINS. *Computer Systems and Information Technologies*, 2025. №1. URL: https://csitjournal.khmnu.edu.ua/index.php/csit/issue/archive

UDC 004.7

DMYTRO ANDRIEIEV, OLEKSII LYHUN, ANDRIY DROZD

Khmelnytskyi National University

MONITORING SYSTEM FOR CRITICAL INFRASTRUCTURE OBJECTS BASED ON DIGITAL TWINS

Critical infrastructures are fundamental to the seamless operation of modern societies, encompassing sectors such as energy, healthcare, transportation, and communications. Ensuring their reliability, performance, continuous operation, safety, maintenance, and protection is a national priority for countries worldwide.

The digital twins play a crucial role in critical infrastructure, as they enhance security, resilience, reliability, maintenance, continuity, and operational efficiency across all sectors. Among the benefits offered by digital twins are intelligent and autonomous decision-making, process optimization, improved traceability, interactive visualization, and real-time monitoring, analysis, and prediction. Furthermore, the study revealed that digital twins have the capability to bridge the gap between physical and virtual environments, can be used in combination with other technologies, and can be integrated into various contexts and industries.

The use of digital twins was explored as the foundation for developing a modern monitoring system for critical infrastructure facilities enables multi-level assessment of asset conditions in real time, ensuring precise threat detection, anomaly identification, and timely decision-making. Integration with artificial intelligence and big data technologies allows not only the collection and analysis of large volumes of information but also the creation of adaptive behavioral models for systems in emergency situations.

Special attention was given to the method of optimizing critical IT infrastructure using digital twins, which combines virtual modeling, predictive algorithms, and automated management. The proposed approach enhances the reliability of digital systems, minimizes downtime, optimizes maintenance costs, and strengthens cybersecurity. This system is especially relevant in the context of growing risks and increasing demands for the stability of strategically important infrastructure assets.

The application of digital twins for monitoring and optimizing critical infrastructure demonstrates considerable potential for improving its resilience, safety, and operational efficiency. The approaches discussed in the study confirm the relevance of implementing digital models as tools for timely risk identification, failure prediction, and informed decision-making. By integrating such technologies, organizations can reduce operational costs, minimize downtime, and improve the overall stability of infrastructure operations. Therefore, digital twins represent a vital step toward the digital transformation and modernization of mission-critical systems across various sectors.

Keywords: digital twins, critical infrastructure, cybersecurity

Д. Л. Анрдєєв, О. О. Лигун, А. І. Дрозд,

Хмельницький національний університет

Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників

Критична інфраструктура є основою безперебійного функціонування сучасного суспільства, охоплюючи такі сектори, як енергетика, охорона здоров'я, транспорт і зв'язок. Забезпечення їхньої надійності, продуктивності, безперервної роботи, безпеки, обслуговування та захисту є національним пріоритетом для країн усього світу.

Цифрові двійники мають вирішальне значення для критичної інфраструктури, адже вони сприяють підвищенню безпеки, стійкості, надійності, обслуговування, безперервності та ефективності роботи інфраструктури в усіх секторах. Серед переваг, які пропонують цифрові двійники, можна виділити інтелектуальне та автономне прийняття рішень, оптимізацію процесів, покращену трасованість, інтерактивну візуалізацію, а також можливості для моніторингу, аналізу та прогнозування в режимі реального часу. Крім того, дослідження показало, що цифрові двійники здатні усувати розрив між фізичним і віртуальним середовищами, можуть використовуватися разом із іншими технологіями та інтегруватися у різноманітні контексти й галузі.

Застосування цифрових двійників, як основи для створення сучасної системи моніторингу об’єктів критичної інфраструктури, дозволяє здійснювати багаторівневу оцінку стану об’єктів у реальному часі, забезпечуючи високоточне виявлення загроз, виявлення аномалій та своєчасне прийняття рішень. Інтеграція з технологіями штучного інтелекту та великих даних дозволяє не лише збирати та аналізувати великі обсяги інформації, а й створювати адаптивні моделі поведінки систем у надзвичайних ситуаціях.

Особливу увагу приділено методу оптимізації критичної IT-інфраструктури за допомогою цифрових двійників, що поєднує віртуальне моделювання, алгоритми прогнозування та автоматизоване управління. Запропонований підхід забезпечує підвищення надійності цифрових систем, мінімізацію часу простоїв, оптимізацію витрат на обслуговування та підвищення рівня кіберзахисту. Така система є надзвичайно актуальною в умовах підвищених ризиків та вимог до стабільності роботи стратегічно важливих об’єктів інфраструктури.

Застосування цифрових двійників для моніторингу та оптимізації критичної інфраструктури демонструє значний потенціал у підвищенні її стійкості, безпеки та функціональної ефективності. Розглянуті в дослідженні підходи підтверджують актуальність впровадження цифрових моделей як інструменту для своєчасного виявлення ризиків, прогнозування відмов і прийняття обґрунтованих управлінських рішень. Завдяки інтеграції таких технологій можна досягти зниження експлуатаційних витрат, зменшення часу простоїв та підвищення загальної стабільності роботи інфраструктури. Таким чином, цифрові двійники є важливим кроком на шляху до цифровізації та модернізації критично важливих систем у різних секторах.

Ключові слова: цифрові двійники, критична інфраструктура, кібербезпека

Introduction

Critical infrastructure encompasses both virtual and physical assets, systems, and processes, integrating technological advancements to function seamlessly across various domains. As a fundamental component of modern societies, critical infrastructure is vital for ensuring reliable, secure, and efficient operations that underpin economic prosperity and social well-being. Its definition evolves in response to societal changes to maintain community functionality and welfare. Given its essential role in a sustainable future, maintaining the resilience and continuous operation of critical infrastructure, even amid complex challenges and threats, is imperative. Cybersecurity concerns, including risks and vulnerabilities, are significant, as critical infrastructure often becomes a target for cyberattacks. Consequently, enhancing the security, availability, resilience, continuity, and performance of critical infrastructure has become an urgent national priority for many countries.

Related works

Critical infrastructure forms the backbone of contemporary society, encompassing[1, 2] sectors like energy, transportation, water supply, communications, and healthcare. The seamless operation of these sectors is vital for national security, economic stability, and public safety. However, they are susceptible to various threats, including natural disasters, cyberattacks, human errors, and deliberate sabotage. Consequently, effective monitoring[3, 4] is essential for risk mitigation and ensuring resilience. Significance of Continuous Monitoring. Implementing continuous monitoring for critical infrastructure offers several key benefits:

- Proactive Threat Detection: Identifies potential issues before they escalate, enabling timely preventive measures.
- Enhanced Operational Efficiency: Maintains optimal system performance, reducing downtime and maintenance expenses.
- Regulatory Compliance and Reporting: Facilitates adherence to standards and simplifies accurate documentation.
- Improved Incident Response: Allows for swift reactions to emergencies, minimizing adverse impacts.
- Informed Resource Allocation: Supports data-driven decisions regarding resource distribution and investment strategies.

Deploying robust monitoring systems is imperative to protect critical infrastructure and uphold societal well-being. Advancements in technology are revolutionizing the monitoring of critical infrastructure (CI) through several key innovations:

1. Internet of Things (IoT): The integration of IoT devices facilitates the deployment of extensive sensor networks, delivering real-time data on various operational parameters.
2. Artificial Intelligence (AI) and Machine Learning (ML): AI and ML algorithms enable the analysis of large datasets, identification of patterns, and prediction of potential failures, enhancing proactive maintenance strategies.
3. Cloud Computing: Cloud platforms provide scalable and cost-effective solutions for data storage, processing, and analysis, supporting the efficient management of CI monitoring systems.
4. Digital Twins: These virtual representations of physical assets allow for simulation and maintenance forecasting, improving operational efficiency and asset management.

5. 5G and Edge Computing: The implementation of 5G networks and edge computing technologies ensures faster data transmission and processing, facilitating real-time monitoring and control of critical infrastructure.

These emerging technologies collectively enhance the resilience, efficiency, and security of critical infrastructure monitoring systems. A digital twin serves as a virtual counterpart[5, 6] to a physical asset or system, leveraging data to emulate its performance and behavior. In recent years, digital twins have gained prominence, particularly within critical infrastructure sectors. In critical infrastructure contexts, digital twins offer precise representations of current system states and potential future scenarios, enabling operators to enhance operational efficiency and reduce risks. This discussion delves into the applications of digital twins in critical infrastructure[7]. Digital twins offer several advantages [8, 9], including:

1. Intelligent and autonomous decision-making.
2. Process optimization.
3. Enhanced tracking.
4. Interactive visualization and monitoring.
5. Real-time analysis and forecasting.

Digital twins have the capability to bridge the gap between physical and virtual environments, collaborate with other technologies, and integrate into various sectors.

Critical infrastructure comprises virtual and physical assets, systems, and processes that leverage technological advancements for seamless integration and operation across different domains. It is an integral part of modern societies, which are increasingly dependent on it. The definition of critical infrastructure evolves in response to the need for reliable, secure, and efficient functioning of communities, economic development, and social well-being. Given that critical infrastructure is essential for a sustainable future, ensuring its resilience and continuous operation, even under challenging conditions and threats, is crucial. Cybersecurity issues, risks, and vulnerabilities pose serious challenges to critical infrastructure, as it often becomes a target for cyberattacks. Therefore, enhancing the security, availability, resilience, continuity, and efficiency of critical infrastructure is an urgent national priority for many countries.

As digital twins are data-driven and accurate virtual replicas[10] of real-world objects, they bridge the gap between physical and virtual environments and can be utilized across various contexts and domains. By receiving input from physical objects and leveraging their diverse dimensions and capabilities, digital twins facilitate the optimization of services, products, and devices. They also enhance cybersecurity through continuous real-time monitoring.

Digital twins exhibit essential attributes such as domain specificity, synchronization, autonomy, and self-evolution. They are characterized by communication capabilities[11, 12], unique identifiers, integration of actuators and sensors, artificial intelligence, security and privacy measures, trustworthiness, and virtual representation. These features facilitate their application across various sectors. Technologies enabling digital twins include augmented reality, robotics, haptic devices, data-driven modeling, machine vision, cloud computing[13, 14], tactile internet, 5G networks, artificial intelligence, and the Internet of Things. The implementation of digital twins holds the potential to enhance the safety, resilience, continuity, and functionality of critical infrastructure across all sectors.

Digital twins can be applied across various sectors, enhancing processes and delivering numerous benefits. In the context of built environments, they assist in the planning, construction, operation, and maintenance of assets. However, successful integration[15, 16] necessitates meticulous attention to tasks, security protocols, data preservation, and temporal

factors, especially when dealing with critical infrastructure. The foundation of digital twin technology lies in the integration of three fundamental components:

1. Physical Entity: A real-world infrastructure element, such as a bridge or power plant, equipped with sensors that monitor critical parameters like temperature, strain, vibration, and pressure.

2. Comprehensive Virtual Model: A detailed digital representation created using simulation software and physical modeling techniques, such as finite element analysis.

3. Secure Data Transmission Channels: Reliable pathways that facilitate seamless real-time data flow from the physical sensors to the digital model.

Advanced analytics systems and machine learning algorithms process these data streams to predict future behavior, detect anomalies, and identify potential failures before they occur.

Implementing extensive sensor networks integrated with the Internet of Things (IoT)[17, 18] is a fundamental approach to monitoring critical infrastructure through digital twins. These sensors gather real-time operational data, which is transmitted to the digital model, facilitating continuous monitoring and analysis. For example, in civil engineering, sensors such as accelerometers, strain gauges, and fiber-optic devices can be installed on bridges and buildings to monitor structural health. Similarly, in energy systems, smart meters and SCADA[19, 20] systems collect data to oversee grid performance and anticipate operational failures. This integration enables engineers and decision-makers to swiftly detect and address potential issues, thereby enhancing the safety and resilience of critical infrastructure. Digital twins employ modeling tools that utilize sensor input to create real-time representations of an object's state. Two key methodologies include:

1. Physics-Based Modeling: Utilizing finite element analysis[21, 22] (FEA) or statistical finite element methods to predict stress distribution, fatigue, and potential failure points. These modeling techniques are particularly beneficial in civil engineering applications.

2. Machine Learning and Artificial Intelligence: Advanced algorithms[23, 24, 25] process historical and real-time data to forecast future conditions, schedule maintenance, and optimize operations. Machine learning techniques, particularly anomaly detection methods, can identify subtle patterns in sensor data that may signal early signs of equipment degradation or potential cyberattacks. This proactive approach enables timely interventions, thereby enhancing the safety and reliability of critical infrastructure.

A method for optimizing critical IT infrastructure with digital twins

A digital twin is a virtual model of a physical IT system that accurately reflects its structure, behavior, and dynamics in real time. It functions as an interactive digital replica of servers, networks, storage systems, and other key components, allowing for experimentation, simulation, and optimization without impacting the real environment.

A digital twin is a virtual model of a physical IT system that accurately reflects its structure, behavior, and dynamics in real time. It functions as an interactive digital replica of servers, networks, storage systems, and other key components,

allowing for experimentation, simulation, and optimization without impacting the real environment. The main purpose of using digital twins is optimization. Stages of the digital twin optimization method in a critical information structure (Fig. 1)

1. Collecting and processing data from the physical infrastructure The goal is to get a complete, up-to-date and detailed picture of the state of all components of the IT system. What it includes: Collecting telemetry data from all sources: servers, routers, switches, storage systems (storage), power supplies, cooling systems. Monitoring of key metrics: CPU, RAM, disk I/O, bandwidth utilization, component temperature, power consumption, latency. Detecting load patterns, anomalies, incident rates, seasonal fluctuations.

Tools: Monitoring systems: Zabbix, Prometheus, Grafana. Data collection agents: Telegraf, Collectd. Log processing systems: ELK Stack, Graylog. Data access protocols: SNMP, IPMI, Redfish, REST API.

The result is the formation of a structured data stream for building an accurate digital display.

2. Building and updating the digital model

The goal is to create an up-to-date digital copy (Digital Twin) that reflects the physical infrastructure with maximum accuracy.

This includes: Virtualization of all physical and logical components: servers, VMs, storage, network topology, management systems. Taking into account the specifications of each element: failure rate, temperature limits, delay lines, dependencies between modules. Continuous synchronization of the digital model with the physical network: via APIs, agents, or direct connections to control systems.

Tools: Digital twin platforms: Siemens NX, AnyLogic, Azure Digital Twins, IBM Maximo. CAD/CAE models, emulators and emulation environments (GNS3, EVE-NG - for the network part). Integration tools: OPC UA, MQTT, REST.

3. Analysis of the current state of the system

The goal is to identify problem areas and assess the effectiveness of the current operation.

What it includes: Building key metrics: average load, peak activity, availability, average response time, latency, resource utilization. Identification of bottlenecks - system segments that limit overall performance. Visualization of the risk zone, excessive redundancy, or vice versa - critical underload.

The result is the creation of an informed basis for modeling scenarios and selecting optimization areas.

4. Scenario modeling

The goal is to predict how the infrastructure will behave under different conditions.

This includes: Running What-if scenarios: switch failure, traffic spike, cyber incident, server hardware upgrade. Stress load simulation: DDoS simulation, 500% increase in requests in a short period of time, disconnection of selected clusters. Testing the impact of changes: for example, how moving virtual machines between data centers will affect latency.

The result is tested hypotheses about the system's behavior in critical situations without harming the real environment.

5. Application of optimization algorithms

The goal is to find the best architecture and system parameters according to the selected performance criteria.

This includes: Defining the objective function. For example: $Z = \alpha * Response\_time + \beta * Resource\_consumption + \gamma * Failure\_probability$. Application of modern optimization algorithms: Genetic - evolutionary search for the best combinations; Gradient methods - local optimization of parameters; Heuristics/metaheuristics - fast search in the face of incomplete information; Machine learning methods (Supervised, Reinforcement Learning).

Tools: SciPy, TensorFlow, PyTorch, DEAP (genetic algorithms), Optuna, RayTune.

6. Validate the results on a digital model

The goal is to check on the model whether the proposed changes really improve the situation.

What it involves: Running a simulation in an optimized configuration. Comparison of KPIs before and after: response time, utilization, power consumption, availability. Assessment of new risks: creation of new conflicts, increased load on neighboring components.

The result is confirmation that the chosen solution is stable and effective.

7. Implementation of changes in the real environment

The goal is to integrate the optimized model into the real infrastructure.

This includes: Implementation of changes through automation systems: Ansible, Puppet, Chef, Terraform. Performing migration, load balancing, changing service priorities. Monitoring how changes affect the live environment in real time.

Security: changes can be initially implemented in a test or staging environment, and then deployed gradually (canary deployment).

8. Self-learning and adaptation

The goal is to transform the digital twin into a system that adapts to environmental changes on its own.

This includes: Accumulation of historical data for trend analysis. Training of forecasting models: prediction of loads, probability of failure, optimal time for maintenance. Using Reinforcement Learning to automatically make decisions based on previous experience. Constant updating of the digital model depending on external and internal changes.

As a result, the system becomes adaptive and capable of autonomous self-improvement.

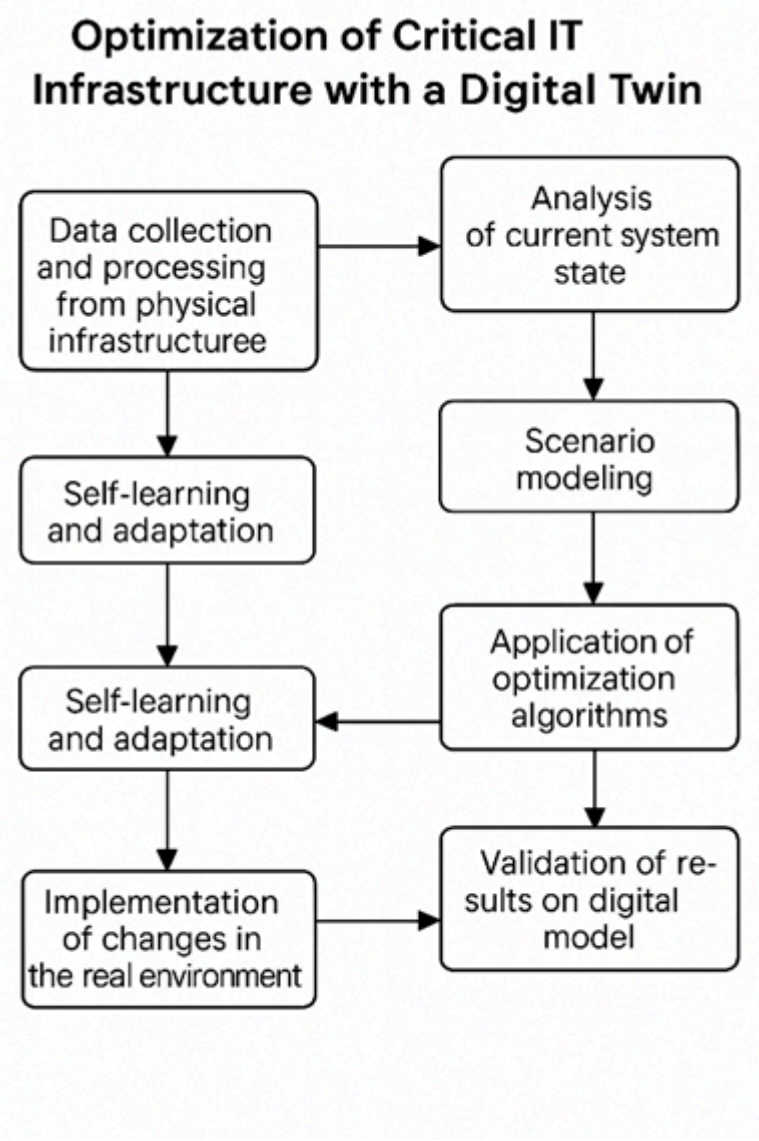

Figure 1. Optimization of critical IT infrastructure using a digital twin

The method of optimizing critical IT infrastructure using digital twins is a modern approach that combines virtual modeling, real-time analytics, and artificial intelligence algorithms to maximize system efficiency, reliability, and adaptability.

Practical application of the method of optimization of the critical IT infrastructure of NPC "Ukrenergo" using digital twins

Digital twins are playing an increasingly important role in the modernization of critical systems due to their ability to integrate virtual simulations with real-time data from physical objects. Such technologies have great potential for improving resilience to external threats, ensuring cybersecurity, efficient maintenance management, and optimizing overall system performance.

In particular, considerable attention has been paid to the use of digital twins in such industries as

- energy networks, where they help to balance the load, forecast consumption and detect failures;

- transportation infrastructure, for monitoring the condition of roads, bridges, rail systems and predicting their wear and tear;

- water supply and wastewater treatment plants, where digital models can detect leaks, improve service quality, and reduce water losses.

We have developed a study of the practical application of the method of optimizing the critical IT infrastructure of NPC “Ukrenergo” using digital twins, because it is a crucial component of the uninterrupted functioning of the power system, and its reliability directly affects energy security, resilience to cyber threats, and the efficiency of resource management.

1. Building a digital twin of the IT infrastructure of NPC “Ukrenergo”

Objective: to create a virtual model of the company's critical IT infrastructure, which includes network equipment, servers, network management systems, SCADA systems and information gateways.

Tools: the use of digital twin platforms (e.g., Siemens Digital Twin, Ansys Twin Builder, or specialized SCADA-integrated solutions), combined with proprietary monitoring and telemetry collection modules.

Architecture: a combination of a virtual environment with data from physical sensors and real-time event logs.

2. Integration with monitoring and telemetry systems

Data sources: log files, telemetry from network equipment, traffic between servers, access logs.

Purpose: to provide a constant flow of data for validating the digital twin and training optimization and forecasting algorithms.

Data collection tools: Prometheus, Grafana, Zabbix, ELK Stack, or individual agency solutions.

3. Optimization of load distribution

Objective: load balancing between servers and nodes, taking into account current and forecasted loads.

Algorithm: use of gradient methods or genetic algorithms to select the best configuration of virtual machines, distribute requests, and reserve channels.

Result: reduction of overloads, acceleration of request processing, reduction of peak loads on key nodes.

4. Predicting incidents and technical failures

Method: applying machine learning algorithms (e.g., LSTM or Random Forest) to detect anomalies based on historical data.

Role of the digital twin: testing hypothetical failure scenarios without risking the real system.

Practical benefit: timely warning of possible incidents, which allows for planning preventive actions.

5. Testing new solutions and changes in an isolated environment

Example: before implementing new cybersecurity policies, software updates, or architecture changes, all changes are tested on a digital twin.

Benefits: minimizing the risk of downtime and conflicts, ensuring the safety of changes without interfering with the operation of the productive system.

6. Energy efficiency and resource consumption management

Model: a digital twin records the energy consumption of each node of the IT infrastructure.

Optimization: Implementation of adaptive energy management, such as shutting down backup servers during off-peak hours or transferring tasks to less busy data centers.

Result: reduction of energy consumption by up to 15-25% in certain segments.

7. Improving cybersecurity

Role of a digital twin: used as a testing ground for cyberattack scenarios and to evaluate the effectiveness of countermeasures (e.g., DDoS, intrusions, data substitution attempts).

Tools: simulating attacks, collecting statistics, training detection algorithms.

Practical effect: improved incident preparedness, development of response plans, reduction of the risk of compromising critical nodes.

8. Intelligent control of the entire system

Concept: automated decision-making based on data from a digital twin.

Example: the system decides independently which processes should be moved, which servers should be restarted or which policies should be tightened.

Platforms: AIOps (Artificial Intelligence for IT Operations) combined with a digital twin.

To study the application of digital twins of critical infrastructure in practice in more depth, we developed a pilot project: Digital twin of the IT infrastructure of NPC “Ukrenergo”.

The goal is to create a digital copy of NPC “Ukrenergo's” IT infrastructure that

- integrates real data from SCADA, network devices and servers;
- ensures continuous monitoring, simulation of incident scenarios and optimization of work;
- supports detection of failures and cyber threats;
- allows you to experiment with updates and changes without harming the live infrastructure.

Components of a digital twin

The central core of the digital twin: Object-oriented representation of IT assets (servers, networks, gateways, SCADA). Simulation core (based on physical and information models). Event and trigger handler (anomalies, overloads, intrusions).

Integration with physical sources: SNMP, NetFlow for network devices (switches, routers). SCADA protocols: Modbus, DNP3, IEC 61850. Server-based monitoring agents: Zabbix, Prometheus, psutil.

Information gateways (DMZ / API): Proxies for collecting data from external systems. Secure MQTT/REST APIs for integration with the digital core.

Analytical and forecasting modules: Anomaly detection algorithms (ML/AI).

Load and service forecasting. Cyber threat simulators.

Visualization and Dashboard: Grafana, Siemens Twin Viewer, or your own UI. 3D/2D object models, heat maps, network topology.

Digital twin architecture (Fig. 2)

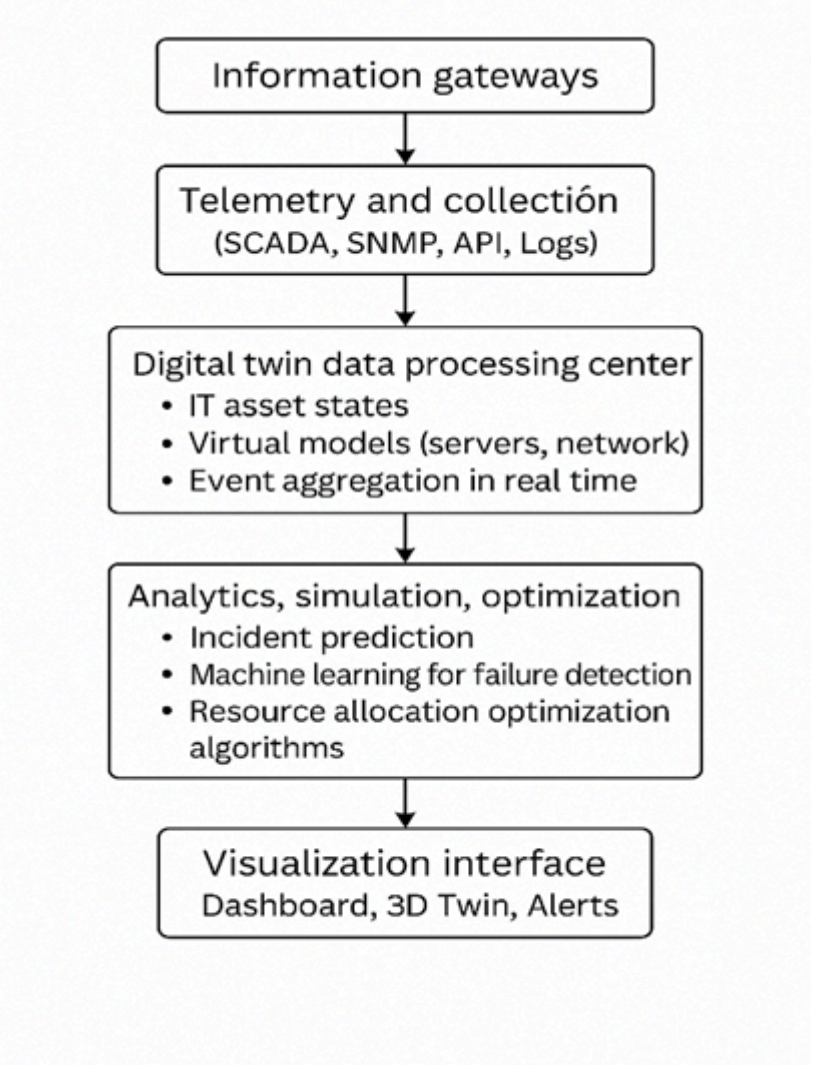

Figure 2. Digital twin architecture

Tools and platforms:

- Siemens NX & Mindsphere, Ansys Twin Builder, Altair SmartWorks - for complex digital modeling.
- Zabbix / Prometheus / Grafana - for collecting metrics, logs, and monitoring.
- Python + FastAPI + Pandas + scikit-learn - for analytics, event processing, and API development.
- Node-RED / MQTT / OPC-UA - for data flows between SCADA and digital twin.
- Docker / Kubernetes - for virtualization and flexible deployment.

Example of application scenarios:

- Predicting SCADA server overload based on historical CPU/IO trends.
- Simulation of an attack on an IEC 104 gateway - checking the actions of a digital twin, recovery plan.
- Automatic optimization of traffic routing between regional data centers in real time.

- Simulation of planned software updates - assessing the impact without affecting the main network.
- Early detection of cyber threats through a digital agent that analyzes network behavior.

Let us consider an example that demonstrates the level of overload of the IT infrastructure network of NPC “Ukrenergo” for 8 weeks:

- Without digital twins - overload accumulates, problems are detected late.
- With digital twins - problems are identified early, the level stabilizes.

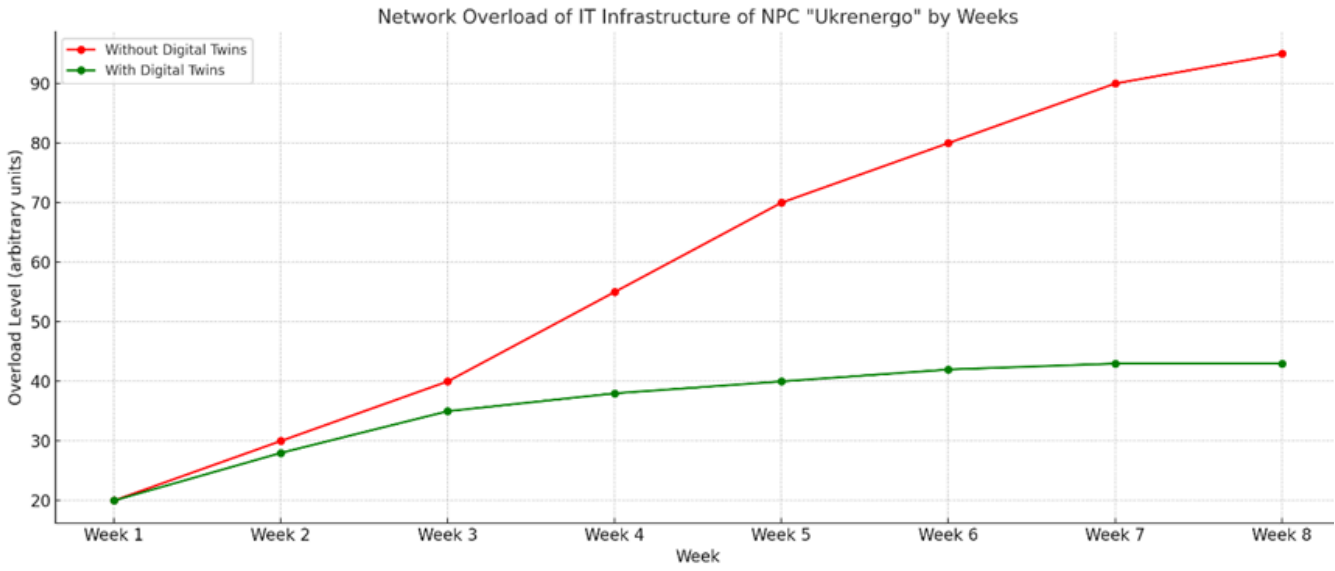

Figure 3. Network overload of IT infrastructure of NPC “Ukrenergo” by weeks

The graph below clearly demonstrates the comparative dynamics of detecting overload problems in the IT infrastructure of NPC “Ukrenergo” using two approaches: traditional - without the use of digital twins, and innovative - with their use. During the first weeks, the level of overload in the systems without digital twins gradually increases, while the detection of deviations is delayed, which leads to the accumulation of critical problems, reduced stability and increased risk of failures. During peak periods, the system cannot cope with the load, which can lead to disruption of service continuity and cybersecurity threats.

In contrast, when digital twins are used, a proactive response is observed: at the initial stages of problem development, the digital model identifies signs of overload, analyzes the causes, and allows you to make decisions to eliminate them before they become critical. As a result, the load level stabilizes, avoiding peak values ensures business continuity, and the reliability and resilience of critical IT infrastructure is significantly increased.

Digital twins are not only a monitoring tool, but also a forecasting and optimization tool that allows you to move from reactive to preventive management of critical facilities. This significantly reduces risks, saves resources, and ensures the safe operation of IT infrastructure in the face of today's challenges.

Thus, the development of a digital twin of NPC “Ukrenergo's” IT infrastructure demonstrates the powerful potential of modern digital technologies to improve the efficiency, reliability and cyber resilience of critical energy systems. Integration of real-time data with the virtual environment allows for continuous monitoring of equipment status, timely detection of anomalies, forecasting failures, optimization of resource allocation, and testing scenarios in a secure digital environment.

This approach reduces operating costs, minimizes the risk of failure, and improves operational management of the infrastructure, which is extremely important for the stable operation of the national energy system in the face of modern cyber threats and increased reliability requirements. Digital twins open up new horizons for the transformation of the energy sector and the digitalization of Ukraine's strategic enterprises.

Conclusions

Digital twins are a key technology for improving the efficiency and security of critical infrastructure. They provide an accurate real-time representation of the state of objects, enabling analysis, forecasting, and process optimization without the need for physical system intervention. Through integration with the Internet of Things (IoT), artificial intelligence (AI), cloud computing, and edge computing, digital twins contribute to advanced monitoring and infrastructure management in real time.

One of the main advantages of digital twins is their ability to autonomously make decisions, minimizing human error and enhancing rapid response to potential threats. Implementing this technology allows for failure prediction, maintenance optimization, and risk reduction of cyberattacks. Additionally, digital twins play a significant role in improving infrastructure security and resilience, ensuring quick responses to potential disruptions and maintaining the continuous operation of critical facilities.

The application of digital twins in infrastructure sectors such as transportation systems, energy complexes, water supply, and healthcare enhances their efficiency and longevity. The use of machine learning methods and big data analysis enables the identification of hidden patterns, allowing for the prediction of potential failures and the prevention of emergency situations. Furthermore, virtual models provide a safe environment for testing new development scenarios without risks to real infrastructure.

However, for the full integration of digital twins, it is necessary to address cybersecurity, data protection, and technology standardization issues. Reliable encryption mechanisms, access control, and compliance with international standards play a critical role in the secure deployment of this technology.

The method of optimizing critical IT infrastructure using digital twins is an innovative approach that combines the capabilities of virtual modeling, real-time analytics, and artificial intelligence to enhance system efficiency, reliability, and adaptability. This method enables organizations to reduce the likelihood of downtime, utilize resources more effectively, strengthen fault tolerance, and improve the overall performance of critical IT systems.

The development of a digital twin of the IT infrastructure of NPC “Ukrenergo” demonstrates the significant potential of modern digital technologies in enhancing the efficiency, reliability, and cyber resilience of critical energy systems. The integration of real-time data with virtual modeling enables continuous equipment monitoring, timely anomaly detection, failure prediction, and resource optimization in a secure digital environment.

This innovative approach helps reduce operational costs, minimize failure risks, and improve infrastructure management—factors that are crucial for the stable operation of the national energy system amid growing cyber threats. Digital twins are becoming a key tool in the digital transformation of strategic enterprises in Ukraine’s energy sector.

Overall, digital twins are a powerful tool for developing critical infrastructure, enhancing its reliability, security, and efficiency. Further research and implementation of this technology will improve infrastructure management mechanisms and ensure its seamless operation in the face of constant threats and changing environmental conditions.

References

1. Gao J., & Wu J. (2022). Digital Twins in Critical Infrastructure. Information, Vol. 15(8), P. 454. https://doi.org/10.3390/info15080454
2. Esnoul C., Colomo-Palacios, R., Jee E., Chockalingam S., Eidar Simensen J., Bae D.-H. Report on the 3rd international workshop on engineering and cybersecurity of critical systems (EnCyCriS-2022). ACM SIGSOFT Softw. Eng. Notes. 2023. Vol. 48, P. 81–84. https://doi.org/10.1145/3573074.3573095
3. Ouyang M. Review on modeling and simulation of interdependent critical infrastructure systems. Reliab. Eng. Syst. Saf. 2014. Vol. 121. P. 43–60. https://doi.org/10.1016/j.ress.2013.06.040
4. Alcaraz C., Zeadally S. Critical infrastructure protection: Requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. 2015. Vol. 8. P. 53–66. https://doi.org/10.1016/j.ijcip.2014.12.002
5. Rathnayaka B., Siriwardana C., Robert D., Amaratunga D., Setunge S. Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. Int. J. Disaster Risk Reduct. 2022. Vol. 78, P. 103123. https://doi.org/10.1016/j.ijdrr.2022.103123
6. Khan Babar A. H., Ali Y. Framework construction for augmentation of resilience in critical infrastructure: Developing countries a case in point. Technol. Soc. 2022. Vol. 68, P. 101809. https://doi.org/10.1016/j.techsoc.2021.101809
7. Wells E.M., Boden M., Tseytlin I., Linkov I. Modeling critical infrastructure resilience under compounding threats: A systematic literature review. Prog. Disaster Sci. 2022. Vol. 15, P. 100244. https://doi.org/10.1016/j.pdisas.2022.100244
8. Chowdhury N., Gkioulos V. Cyber security training for critical infrastructure protection: A literature review. Comput. Sci. Rev. 2021. Vol. 40, P. 100361. https://doi.org/10.1016/j.cosrev.2021.100361
9. Ani U.P.D., He H., Tiwari A. Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. J. Cyber Secur. Technol. 2017. Vol. 1, P. 32–74. https://doi.org/10.1080/23742917.2016.1252211
10. Ghorbani A. A. Bagheri E. The state of the art in critical infrastructure protection: A framework for convergence. Int. J. Crit. Infrastruct. 2008. Vol. 4, P. 215–244. https://doi.org/10.1504/IJCIS.2008.017438
11. Rinaldi S.M., Peerenboom J.P., Kelly T.K. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. 2001. Vol. 21, P. 11–25. https://doi.org/10.1109/37.969131
12. Brown, G., Carlyle M., Salmerón J., Wood K. Defending critical infrastructure. Interfaces 2006. Vol. 36, P. 530–544. https://doi.org/10.1287/inte.1060.0252
13. Aradau C. Security that matters: Critical infrastructure and objects of protection. Secur. Dialogue 2010. Vol. 41, P. 491–514. https://doi.org/10.1177/0967010610382687

14. Rehak D., Senovsky P., Hromada M., Lovecek T. Complex approach to assessing resilience of critical infrastructure elements. Int. J. Crit. Infrastruct. Prot. 2019. Vol. 25, P. 125–138. https://doi.org/10.1016/j.ijcip.2019.03.003

15. Lee II, E.E., Mitchell J.E., Wallace W.A. Restoration of services in interdependent infrastructure systems: A network flows approach. IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.) 2007. Vol. 37, P. 1303–1317. https://doi.org/10.1109/TSMCC.2007.905859

16. Laplante P., Amaba B. Artificial intelligence in critical infrastructure systems. Computer 2021, Vol. 54, P. 14–24. https://doi.org/10.1109/MC.2021.3055892

17. Groenewold M.R., Burrer S.L., Ahmed F., Uzicanin A., Free H., Luckhaupt S.E. Increases in Health-Related Workplace Absenteeism Among Workers in Essential Critical Infrastructure Occupations During the COVID-19 Pandemic-United States, March-April 2020. MMWR Morb. Mortal. Wkly. Rep. 2020. Vol. 69, P. 853–858. https://doi.org/10.15585/mmwr.mm6927a1

18. Jiang Y., Yin S., Li K., Luo H., Kaynak O. Industrial applications of digital twins. Philos. Trans. R. Soc. A Math. Phys. Eng. Sci. 2021. Vol. 379, P. 20200360. https://doi.org/10.1098/rsta.2020.0360

19. Tao F., Qi Q. Make more digital twins. Nature 2019. Vol. 573, P. 490–491. https://doi.org/10.1038/d41586-019-02849-1

20. Batty M. Digital twins. Environ. Plan. B Urban Anal. City Sci. 2018. Vol. 45, P. 817–820. https://doi.org/10.1177/2399808318796416

21. Stark R., Fresemann C., Lindow K. Development and operation of digital twins for technical systems and services. CIRP Ann. 2019. Vol. 68, P. 129–132. https://doi.org/10.1016/j.cirp.2019.04.024

22. Sharma A., Kosasih E., Zhang J., Brintrup A., Calinescu A. Digital twins: State of the art theory and practice, challenges, and open research questions. J. Ind. Inf. Integr. 2022, Vol. 30, 100383. https://doi.org/10.1016/j.jii.2022.100383

23. El Saddik, A. Digital twins: The convergence of multimedia technologies. IEEE MultiMedia 2018. Vol. 25, P. 87–92. https://doi.org/10.1109/MMUL.2018.023121167

24. Lampropoulos G. Artificial intelligence, big data, and machine learning in industry 4.0. In Encyclopedia of Data Science and Machine Learning; IGI Global: Hershey, PA, USA, 2023. P. 2101–2109. https://doi.org/10.4018/978-1-7998-9220-5.ch125

25. Piras G., Agostinelli S., Muzi F. Digital Twin Framework for Built Environment: A Review of Key Enablers. Energies 2024. Vol. 17, P. 436. https://doi.org/10.3390/en17020436

Dmytro Andrieiev– master's degree student, Khmelnytskyi National University, Khmelnytskyi, Ukraine,

e-mail: zonex1995@gmail.com

orcid.org/0009-0002-3524-872X

Oleksii Lyhun – PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine

e-mail: oleksii.lyhun@gmail.com

https://orcid.org/0009-0004-5727-5096

Andriy Drozd – PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine,

e-mail: andriydrozdit@gmail.com

orcid.org/0009-0008-1049-1911

ДОДАТОК В

StrikePlagiarism.com

Дата звіту 4/22/2025
Дата редагування ---

Звіт не був оцінений

Звіт подібності

метадані

Назва організації
Khmelnytskyi National University
Заголовок
Андрєєв_Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників
Автор
Дмитро АНДРЄЄВ Науковий керівник / Експерт
підрозділ
Кафедра комп'ютерної інженерії та інформаційних систем

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв	ß	4
Інтервали	A→	0
Мікропробіли	·	99
Білі знаки	ß	1
Парафрази (SmartMarks)	a	7

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

25
Довжина фрази для коефіцієнта подібності 2

19098
Кількість слів

157146
Кількість символів

Tue Apr 22 14:35:54 EEST 2025, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.260 Educational

Максимальне співпадіння з одним документом 12.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 11%**

ID: 240431 Назва: МКР Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників Додано в БД: 2025-04-22 Автора: Дмитро АНДРЄЄВ Керівники: Світлана САЧЕНКО Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	147527	1067	17386 (12%)	192 (18%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми
229435	Назва: МКР Метод оптимізації завдань у багатопроцесорних системах Додано в БД: 2025-04-15 Автора: Дмитро МАРТИНЮК Керівники: Світлана САЧЕНКО Консультанти: Опоненти:	17242 (12.0%)	191 (18.0%)

Завідувачу кафедри КІІС,
доктору філософії, доц. Ользі ПАВЛОВІЙ

Дмитро АНДРЄЄВ
ПІБ здобувача вищої освіти

ФІТ, 2 курсу, групи КІ2м-23-1

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 01.07.2022, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений(а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

25 квітня 2025 року

Протокол аналізу звіту подібності експертом

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Дмитро АНДРЄЄВ

Співавтор:

Назва: Андрєєв_Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників

Експерт:

Підрозділ: Кафедра комп'ютерної інженерії та інформаційних систем

Коефіцієнт подібності 1:15.7%

Коефіцієнт подібності 2:14.5%

Мікропробіли: 99

Заміна букв: 4

Інтервали: 0

Білі знаки: 1

Дата створення звіту: 2025-04-22 13:42:54.0

Після аналізу Звіту подібності констатую наступне:

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2025-04-22 Доцент Андрій Нічепорук

Дата експерт

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

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

Назва: Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників

Автор: Дмитро АНДРЄЄВ

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-наукова

Науковий керівник: Світлана САЧЕНКО, к.е.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

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

Підтвердження:

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

1) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з 10-40 джерелами на один фрагмент речення;
2) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає менше 18% і адресується до джерел з інтернету та бібліотеки, що, з урахуванням наведених обгрунтувань, відповідає характеру завдання і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Світлана САЧЕНКО

Гарант ОП _____ Олег САВЕНКО

Завідувач кафедри КІС _____ Ольга ПАВЛОВА

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНУ РОБОТУ

Дипломник: Дмитро АНДРЄЄВ

Тема: Система моніторингу об'єктів критичної інфраструктури на основі цифрових двійників

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень - ; кількість сторінок записки 77

1. Короткий зміст роботи та прийнятих рішень У роботі розроблено метод та засоби моніторингу об'єктів критичної інфраструктури на основі цифрових двійників

2. Висновок про відповідність роботи дипломному завданню Кваліфікаційна робота відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подано об'єкт та предмет дослідження, мету, наукову новизну та практичну цінність роботи, а також характеристику структури роботи.

У першому розділі розглянуто питання моніторингу об'єктів критичної інфраструктури, а також проведено аналіз відомих методів і технологій моніторингу об'єктів критичної інфраструктури з використанням цифрових двійників .

У другому розділі розглянуто та виділено ключові особливості оптимізації та моделювання критичної інфраструктури цифровими двійниками .

У третьому розділі було опрацьовано процес оптимізації об'єктів критичної інфраструктури на основі цифрових двійників, а саме його цільову функцію та алгоритми оптимізації критичної інфраструктури цифровими двійниками.

У четвертому розділі розглянуто ефективність методу оптимізації критичної інфраструктури цифровими двійниками, а також проведено дослідження експериментів та досліджень методу оптимізації критичної інфраструктури цифровими двійниками.

У висновках підведено підсумки досягнення результатів з розв'язання завдань дослідження.

4. Позитивні сторони роботи: ___

5. Негативні сторони роботи: ___немає.

6. Оцінка графічного оформлення та пояснювальної записки роботи: ___=_____

7. Відгук про роботу в цілому: __Робота виконана на належному рівні.

8. Інші зауваження: ___=_____

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи вважаю, що робота заслуговує оцінки «відмінно» 5,00 (А)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) __Корецька Людмила Олександрівна, к.т.н., доцент кафедри АКІТР ХНУ

" 2 " __травня__ 2025р. _____