НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ
ІМ. Г.Є. ПУХОВА

ДОРОГИЙ ЯРОСЛАВ ЮРІЙОВИЧ

УДК 04.93’1

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОЦЕСІВ ПРОЕКТУВАННЯ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Спеціальність 05.13.05 – комп’ютерні системи та компоненти

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана в Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України.

Науковий консультант: чл.-кор. НАН України,
доктор технічних наук, професор
Мохор Володимир Володимирович
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, директор

Офіційні опоненти: доктор технічних наук, професор
Мухін Вадим Євгенійович
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри математичних методів системного аналізу

доктор технічних наук, професор
Саченко Анатолій Олексійович
Західноукраїнський національний університет, завідувач кафедри інформаційно-обчислювальних систем та управління

доктор технічних наук, професор
Ланде Дмитро Володимирович
Інститут проблем реєстрації інформації НАН України, завідувач відділу спеціалізованих засобів моделювання

Захист відбудеться "23" квітня 2021 року о 14 годині на засіданні спеціалізованої вченої ради Д 26.185.01 Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитися в бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

Автореферат розісланий "19" березня 2021 р.

Вчений секретар
спеціалізованої вченої ради В.В. Душеба

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Автоматизація процесів критичної інформаційної інфраструктури (КІІ) поряд з незаперечними перевагами неминуче веде і до негативних явищ. Найбільш характерним негативним фактором виступає прогресуюча інформатизація криміналу і терористичних угруповань, що істотно загострює проблему протиборства в сфері інформаційних ресурсів.

Першочерговими об'єктами протиправних дій терористичних і кримінальних спільнот є інформаційні ресурси критичної інфраструктури (КІ), збиток від порушення інформаційної безпеки яких може призвести до техногенних катастроф з людськими жертвами.

До критичних інфраструктур, поряд з системами управління інфраструктурою зв'язку, фінансів, енергетики, транспорту, водопостачання та надзвичайних служб, відносяться органи державного управління, в тому числі і системи управління силових структур. Під КІІ розуміють автоматизовані системи управління та інформаційно-телекомунікаційні мережі (ІТМ), в яких циркулюють інформаційні потоки, що вимагають особливого захисту.

Стійка тенденція наростання потоку інформації, що циркулює в системах управління різного призначення, призводить до необхідності впровадження мережевих автоматизованих методів передачі та обробки критичної інформації. Одним із шляхів вирішення цієї проблеми є розгортання сучасної ІТ-інфраструктури на базі сучасних мережевих технологій.

Технологія розробки ІТ-інфраструктур досить глибоко опрацьована, однак проектування і впровадження КІІ стримується через властиву їм специфіку, яку можна звести до трьох чинників:

1) відсутність прийнятного математичного інструментарію для оцінки альтернативних проектних рішень, вибору ефективних елементів з існуючого набору пропонованих типових засобів інформаційної сфери КІІ з врахуванням особливих вимог, які до неї ставляться;

2) умови експлуатації, що здійснюється при постійних потужних інформаційних впливах, обумовлених підвищеним інтересом до інформаційних ресурсів КІІ;

3) забезпечення вибору оптимальної архітектури КІІ в залежності від задач проектування, а в подальшому, від реального навантаження на її елементи.

Успішне проектування КІІ стає можливим при вирішенні задач представлення та обґрунтування вибору архітектури критичної інформаційної інфраструктури, оцінки і вибору ефективних елементів та компонент з існуючого набору пропонованих типових засобів. Тому актуальним є завдання створення прийнятного математичного інструментарію для оцінки ефективності вибору проектних рішень та окремих елементів архітектури критичної інформаційної інфраструктури з існуючого набору пропонованих типових засобів інформаційної сфери КІІ, та їх вибору з точки зору забезпечення заданих критеріїв проектування критичної інформаційної інфраструктури.

Для вирішення проблеми забезпечення високої експлуатаційної надійності функціонування КІІ в умовах інформаційної протидії потрібне теоретичне і технічне

обґрунтування адаптивних алгоритмів функціонування КІІ в умовах перешкод природної та організованої структури, які б дозволили відслідковувати наявність ресурсів та навантаження на елементи критичної інформаційної інфраструктури, та у разі необхідності, виконувати балансування навантаження або робити перерозподіл наявних ресурсів з метою забезпечення функціонування критичних сервісів, що визначає актуальність досліджень в напрямку вирішення проблем, обумовлених другим з чинників.

Третій чинник обумовлений забезпеченням вибору оптимальної архітектури КІІ, яка в залежності від задач проектування, а в подальшому, від реального навантаження на її елементи, повинна комплектуватися певним набором функціональних блоків, при якій буде забезпечуватися гарантована ефективність її функціонування в особливі періоди кризових ситуацій, коли інтенсивність навантаження зростає. На даний час технологія такого вибору відсутня. Вирішення даної проблеми потребує теоретичного дослідження та є ще одним з актуальних завдань дисертаційного дослідження.

Для вирішення вказаних проблем необхідна розробка і дослідження нових інформаційних технологій, які враховують взаємозв'язок показників критичності систем та елементів і рівня гарантованості підтримуваних ІТ-сервісів і процесів. Вагомий вплив на дослідження проблем критичних інфраструктур надали роботи вітчизняних і зарубіжних вчених: О.Г. Корченка, С.О.Гнатюка, В.С. Харченка, А.Л. Станівського, М.А. Ястребенецького, С. Руссо, М. Fusani, О.І.Роліка, С.Ф.Теленика.

З огляду на це, актуальними, в науковому та практичному аспектах, є:

– проблема пошуку нових підходів до проектування критичних інформаційних інфраструктур, які б системно враховували всю множину зазначених вище факторів, і можливості засобів, які входять до їх складу;

– проблема розробки і розвитку методів моделювання та підтримки прийняття рішень в КІІ та розробка на їх основі єдиної системи проектування, що дозволяє проектувати, аналізувати, розвивати КІІ та підтримувати гарантований рівень якості критичних ІТ-сервісів і процесів, синхронно зі змінами в ній.

Зв’язок роботи з науковими програмами, планами, темами. Тема дисертаційної роботи відповідає планам науково-дослідної та навчальної роботи кафедри автоматики та управління в технічних системах Національного технічного університету України «Київський політехнічний інститут» та науково-дослідної роботи Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова. Дисертаційна робота розпочата на кафедрі автоматики і управління в технічних системах Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», завершена у відділі «Математичного та комп’ютерного моделювання» Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України і виконувалась в рамках наступних НДР: «Розроблення і дослідження моделей, методів та технологій проектування, програмування і управління хмарними ІТ-інфраструктурами» (номер державної реєстрації № 01113U002285), «Платформа розроблення, експлуатації і розвитку критичних ІТ-інфраструктур для роботи з великими даними» (номер державної реєстрації № 0116U003801) та «Хмарна платформа розроблення і управління функціонуванням критичних ІТ-

інфраструктур, що опрацьовують великі обсяги даних» (номер державної реєстрації № 0117U000537).

Метою дисертаційної роботи є підвищення ефективності процесів проектування критичної інформаційної інфраструктури шляхом розробки методів представлення процесу прийняття рішень щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, оцінки альтернативних проектних рішень, вибору оптимальної конфігурації компонент та вдосконалення критичної інформаційної інфраструктури.

Для досягнення зазначеної мети в роботі сформульовані і вирішені такі наукові проблеми та завдання:

– виконано аналіз сучасного стану і особливостей проблеми проектування, обґрунтування рішень і вдосконалення критичних інформаційних інфраструктур та досліджено потенційні можливості сучасних фрейворків опису архітектури підприємства та підходів до обґрунтування рішень щодо архітектури при проектуванні критичних інформаційних інфраструктур;

– проведено аналіз та визначено основні критерії та показники оптимальності проектування та функціонування критичних інформаційних інфраструктур;

– розроблено і досліджено комплекс математичних та комп’ютерних моделей та методів проектування, вдосконалення і розв’язання повсякденних завдань КІІ;

– оцінено ефективність застосування розроблених методів і моделей проектування КІІ;

– розроблено єдину систему проектування КІІ.

Об'єктом дослідження є процеси проектування критичної інформаційної інфраструктури.

Предметом дослідження є методи і засоби математичного та комп’ютерного моделювання процесів представлення процесу прийняття рішень щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, оцінки альтернативних проектних рішень, вибору оптимальної конфігурації компонент та вдосконалення критичної інформаційної інфраструктури.

Методи дослідження. Теоретичною і методологічною основою дослідження є теорія складних багаторівневих ієрархічних систем, теорія інформації та управління, теорія надійності, теорія експертних систем, теорія прийняття рішень, теорія матриць, теорія кінцевих графів і мереж, теорія множин, математична логіка і теорія алгоритмів, елементи теорії масового обслуговування і основи обчислювальної математики, основи теорії математичного моделювання, елементи теорії штучного інтелекту.

Обґрунтованість і достовірність отриманих результатів забезпечується коректним застосуванням апробованого і загальноприйнятого математичного апарату, ідентифікацією, верифікацією даних на основі комп’ютерного і імітаційного моделювання, зіставленням розрахунків на основі розроблених моделей з відомими еталонними чисельними рішеннями, перевіреними натурними експериментами, розбіжність з якими не перевищує заданого рівня достовірності,

широкою апробацією отриманих результатів на Міжнародних та Всеукраїнських конференціях, публікацією в реферованих журналах ДАК України, а також експертизою технічних рішень, підтверджених актами про впровадження та використання результатів дисертаційного дослідження.

Наукова новизна одержаних результатів роботи полягає в вирішенні актуальної науково-прикладної проблеми, яка полягає в удосконаленні процесів вибору і обґрунтування проектних рішень щодо критичної інформаційної інфраструктури на підставі: використання розширених UML-моделей; розроблених методів представлення процесу прийняття рішень щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, оцінки альтернативних проектних рішень, вибору оптимальної конфігурації компонент критичної інформаційної інфраструктури; методів розвитку критичної інформаційної інфраструктури; подальшого розвитку концепції проектування критичної інформаційної інфраструктури; створення та застосування єдиної системи проектування критичної інформаційної інфраструктури. Наукова новизна одержаних результатів полягає в наступному:

1. Вперше запропоновано модель перетворення розширених UML-діаграм, які відображають процес прийняття рішення щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, в розмічені транзиційні системи, що дозволяє використати в подальшому весь спектр методів та алгоритмів, розроблених для розмічених транзиційних систем, для дослідження проблем, пов’язаних з проектуванням критичної інформаційної інфраструктури.

2. Вперше запропоновано постановку задачі верифікації параметризованих моделей архітектурних рішень критичної інформаційної інфраструктури в термінах теорій розмічених транзиційних систем та темпоральної логіки, що дозволяє використати в подальшому весь спектр методів та алгоритмів, розроблених для цих теорій, для верифікації/генерації проектних рішень критичної інформаційної інфраструктури.

3. Вперше запропоновано метод обґрунтування проектних рішень щодо архітектури критичної інформаційної інфраструктури, в якому для порівняння альтернативних проектних рішень запропоновано застосування множини з трьох показників ризику, що враховують досяжність цілей проектного рішення, можливість його імплементації та дотримання вимог щодо критичності, та ентропійного підходу для оцінювання їх взаємного впливу для задачі проектування критичної інформаційної інфраструктури, що дозволяє обрати найкращий варіант проектного рішення та оцінити вплив окремих проектних рішень або елементів на інші проектні рішення щодо архітектури критичної інформаційної інфраструктури або на весь дизайн архітектури в цілому.

4. Вперше запропоновано метод структурної оптимізації нейронних мереж прямого поширення, який використовує розширений набір атомарних операцій над нейронною мережею та дозволяє отримувати оптимальну для вхідних даних структуру нейронної мережі, що значно підвищує можливості адаптаційного вибору моделей нейронних мереж для розв’язання задач функціонування критичних інформаційних інфраструктур.

5. Вперше запропоновано керовану моделлю систему розподілу ресурсів критичної інформаційної інфраструктури, яка використовує методи оптимізації структури нейронних мереж прямого поширення та навантаження на елементи критичної інформаційної інфраструктури, що дозволяє в автоматичному режимі розподіляти ресурси критичної інформаційної інфраструктури з метою їх оптимального використання та задоволення потреб сервісів та компонент, що їх використовують.

6. Удосконалено метод представлення та обґрунтування архітектури критичної інформаційної інфраструктури на основі розширених UML-діаграм, який, на відміну від відомих, дозволяє фіксувати пропозиції архітектора в процесі прийняття рішення щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, що спрощує та пришвидшує пошук архітектури критичної інформаційної інфраструктури під конкретну задачу, а також дає можливість накопичувати історію проведених міркувань та обґрунтувань при її виборі.

7. Удосконалено метод оцінки та вибору оптимальної конфігурації компонент критичної інформаційної інфраструктури, що на відміну від вже відомих використовує Марківський процес прийняття рішень за декількома критеріями пошуку одночасно, який дозволяє оцінити та вибрати оптимальну конфігурацію компонент критичної інформаційної інфраструктури відповідно до заданих критеріїв, що полегшує та пришвидшує вибір конкретної конфігурації критичної інформаційної інфраструктури під визначені цілі та завдання її проектування.

8. Удосконалено метод розподілу ресурсів критичної інформаційної інфраструктури на базі генетичного алгоритму з чіткими параметрами, який відрізняється від вже відомих використанням модифікованої фітнес-функції, що надає можливість знайти оптимальне співвідношення між марнуванням ресурсів та забезпеченням сервісів і визначити оптимальну схему розподілу ресурсів в центрах обробки даних з врахуванням критичності окремих процесів та сервісів.

9. Набула подальшого розвитку концепція проектування критичної інформаційної інфраструктури на базі компенсаційно-декомпенсаційного підходу пошуку архітектурних рішень, яка на відміну від вже відомих, визначає фреймворк опису архітектури підприємства, відповідні критерії вибору та стратегії їх застосування, метод обґрунтування рішень щодо вибору альтернативних архітектурних рішень при проектуванні критичної інформаційної інфраструктури, що значно підвищує швидкість її проектування.

Теоретична та практична цінність роботи. Теоретична значимість роботи полягає в розробці науково-методичного апарату, який може представляти загальнонауковий інтерес для проблеми проектування критичних інформаційних інфраструктур. Теоретична частина роботи може розглядатися в якості прикладного елемента методології системного аналізу при вирішенні проблем зазначеного класу.

Практична значимість роботи полягає в розробці ефективних комп’ютерних методів проектування архітектури критичної інформаційної інфраструктури, що дозволяють вирішувати проблему автоматизованого проектування КІІ відповідно до

поставлених цілей та з забезпеченням необхідного рівня функціональної надійності її експлуатації.

Теоретичні дослідження і наукові результати роботи доведені до інженерних рішень у вигляді реалізованих в інформаційній технології методик, моделей, алгоритмів, придатних для практичного використання при проектуванні КІІ. Запропоновані методи, моделі та алгоритми дозволяють підвищити ефективність функціонування існуючих КІІ або побудувати нові ефективні КІІ.

Реалізація наукових результатів. Розроблений науково-методичний апарат і технічні рішення використовувалися при проектуванні та побудові єдиної інформаційної системи МВС України як критичної інформаційної інфраструктури органів системи МВС.

Використання результатів дисертаційних досліджень підтверджено відповідними актами впровадження (МВС України, ДП «ІНФОТЕХ», ТОВ «Оллі Транс», ТОВ «І-Хаб»).

Особистий внесок здобувача. Всі положення, які виносяться на захист, належать особисто автору. Частина з них наведена в одноосібних наукових працях [2–12].

В роботах, які опубліковано в співавторстві, особисто здобувачу належать: [1] – порівняльний аналіз методів обґрунтування архітектурних рішень; [13] – порівняльний аналіз ФОАП; [14] – принципи побудови критичної інформаційної інфраструктури міністерства; [15] – метод структурної оптимізації нейронної мережі; [16] – метод структурної оптимізації нейронної мережі; [17] – метод структурної оптимізації нейронної мережі; [18] – метод структурної оптимізації нейронної мережі; [19] – підхід до оцінювання ризику в критичних інформаційних інфраструктурах; [20] – модель системи управління ризиком критичної інформаційної інфраструктури; [21] – підхід до оцінювання ризику в критичних інформаційних інфраструктурах; [22] – модель розподілу ресурсів критичної інформаційної інфраструктури з чіткими параметрами; [23] – метод оптимізації навантаження критичної інформаційної інфраструктури; [24] – метод інтеграції для розподілених систем при реалізації проекту критичної інформаційної інфраструктури; [25] – підхід до проектування систем управління безпекою інформації; [26] – аналіз методів верифікації параметричних моделей, [27] – аналіз ФОАП в рамках створення системи управління безпекою інформації, [28] – метод структурної оптимізації нейронної мережі; [29] – метод оптимізації навантаження критичної інформаційної інфраструктури; [30] – порівняльний аналіз фреймворків для реалізації нейронних мереж.

Апробація результатів наукових досліджень. Результати досліджень доповідалися на наукових семінарах, конференціях і симпозіумах:

– 2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) (Одеса, 2014 р.) [31];

– International Scientific-Practical Conference “Problems and Prospects of Intergration of Science and Technology” (Лондон, 2015 р.) [32];

– ІІ міжнародна науково-практична конференція «Інформаційні технології та взаємодії» (Київ, 2015 р.) [33];

– II міжнародна науково-практична конференція «Актуальні проблеми розвитку науки і техніки» (Київ, 2015 р.) [34];

– Міжнародна наукова конференція ІТБ-2015 (Київ, 2015 р.) [35];

– V міжнародна науково-технічна конференція «Проблеми інформатизації» (Київ, 2015 р.) [36];

– The Congress on Information Technology, Computational and Experimental Physics 2015 (CITCEP 2015) (Краков, 2015 р.) [37];

– Second International Scientific-Practical Conference "Problems of Infocommunications. Science and Technology" (IEEE PIC S&T' 2015) (Харьків, 2015 р.) [38];

– Summer Infocom 2016: 2-а Міжнародна науково-практична конференція (Київ, 2016 р.) [39];

– V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем» (Львів, 2016 р.) [40];

– Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, 2016 р.) [41];

– V Міжнародна науково-практична конференція «Кібербезпека інформаційних технологій /// Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах» (Чернівці, 2016 р.) [42];

– II Міжнародна науково-практична конференція «Актуальні проблеми моделювання ризиків і загроз виникнення надзвичайних ситуацій на об'єктах критичної інфраструктури» (Київ, 2016 р.) [43];

– 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS' 2017) (Бухарест, 2017 р.) [44];

– V заочная научная конференция «Фундаментальные и прикладные исследования в современной науке» (Харьков, 2017 р.) [45];

– VI Міжнародна науково-практична конференція (I Міжнародний симпозіум «Практичне застосування нелінійних динамічних систем в інфокомунікаціях», PREDT-2017) (Чернівці, 2017 р.) [46];

– III міжнародна науково-практична конференція «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації» (Київ, 2017 р.) [47];

– 14th IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET2018) (Lviv-Slavske, 2018 р.) [48];

– VII Міжнародна науково-практична конференція «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах (PREDT-2018)» (Чернівці, 2018 р.) [49];

– XI Міжнародна науково-практична конференція «ІНТЕРНЕТ-ОСВІТА-НАУКА-2018» (Вінниця, 2018 р.) [50];

– Summer InfoCom 2018: VI Міжнародна науково-практична конференція з інформаційних систем та технологій (Київ, 2018 р.) [51].

Публікації. Основні результати наукових досліджень опубліковані в 51 науковій праці, з них: 2 монографії, 28 наукових статей в фахових виданнях, що входять до наукометричних баз даних (SCOPUS – 2), 21 публікація у працях і матеріалах наукових конференцій (SCOPUS – 4). 11 публікацій підготовлено одноосібно, англійською мовою – 12.

Структура та обсяг роботи. Дисертаційна робота складається з анотації, вступу, 6 розділів, висновків, списку використаних джерел, що містить 286 найменувань та 4 додатки. Загальний обсяг дисертації складає 370 сторінок. Основний зміст роботи викладено на 315 сторінках (з них п’ять повністю зайнято ілюстраціями). Дисертація містить 108 рисунків, 31 таблицю.

ОСНОВНИЙ ЗМІСТ РОБОТИ

Вступ містить загальну характеристику роботи, актуальність проблеми, мету та завдання дослідження, відомості про зв'язок роботи з науковими програмами, планами, темами, відзначені наукова новизна й практична цінність отриманих результатів, особистий внесок здобувача в роботах у співавторстві, відомості про апробацію результатів роботи.

У першому розділі розглянуто критичну інформаційну інфраструктуру як об’єкт дослідження, проведено аналіз проблем проектування критичною інформаційною інфраструктурою та вимог до її функціонування. Далі наведено аналіз фреймворків опису архітектури підприємства за 4 різними групами основних елементів для аналізу архітектури. Показано, що всі архітектурні фреймворки підтримують мету розвитку архітектури. Зокрема, RM-ODP має особливу спрямованість на розробку архітектури програмного забезпечення. TOGAF, DoDAF і FEAF більш спрямовані на питання щодо архітектури підприємства, такі як архітектурне планування, еволюція та системна сумісність. Вони використовують різні точки зору для моделювання архітектури підприємства і мають різні ступені специфічності для цих точок зору.

Основною метою ФОАП є спрощення визначення, загального розуміння та стандартизація практик опису та створення архітектури. Їх довгостроковими цілями є підтримка стратегічного планування щодо архітектури, використання бази знань щодо архітектурних рішень для підтримки її еволюції. Моделі бізнесу та архітектури, створені за допомогою цих фреймворків, описують напрямки розвитку архітектури, архітектури “to-be” та стратегії переходу від поточної архітектури до майбутньої архітектури для підприємства.

Всі проаналізовані ФОАП або опускають або мають дуже стислий опис обґрунтування дизайну архітектури, незважаючи на те, що вони мають вирішальне значення для проектування КІТІ.

Далі в розділі проведено аналіз методів обґрунтування проектних рішень.

Всі проаналізовані методи обґрунтування проектних рішень не можуть бути використані у вихідному стані для проектування та обґрунтування проектних рішень критичної інформаційної інфраструктури. Тому пропонується використати новий підхід RECAD, створений та адаптований для обґрунтування проектних рішень при побудові критичної інформаційної інфраструктури.

У другому розділі наведено основні означення розмічених транзиційних систем, використаного для опису пропонованих моделей та методу представлення архітектурних рішень критичної інформаційної інфраструктури, який отримав назву *методу представлення та обґрунтування дизайну критичної архітектури (RECAD).* RECAD має на меті допомогти архітекторам створювати та документувати архітектурний дизайн з акцентом на архітектурні рішення та обґрунтування проекту. RECAD охоплює три типи знань архітектури: проектні питання, проектні рішення та результати проектування. Ці об'єкти знань представлені стандартними об'єктами уніфікованого моделювання (UML). Проблема проектування – це матеріали, які впливають на прийняття дизайнерських/проектних рішень. Ця сутність інкапсулює такі поняття, як функціональні вимоги (наприклад, сценарії та діаграма співпраці), нефункціональні вимоги (наприклад, всі атрибути якості) та контексти проекту. Вона також фіксує інформацію про проектні рішення та обґрунтування проекту. Результати проектування включають в себе отримані рішення. Прикладами є класи, компоненти, інтерфейс та спосіб використання. Будь-який індивідуальний тип об'єкту архітектурного знання фіксується шляхом застосування заздалегідь визначеного тегового шаблону стереотипу. Концептуальна модель підходу представлена рис. 2.1.

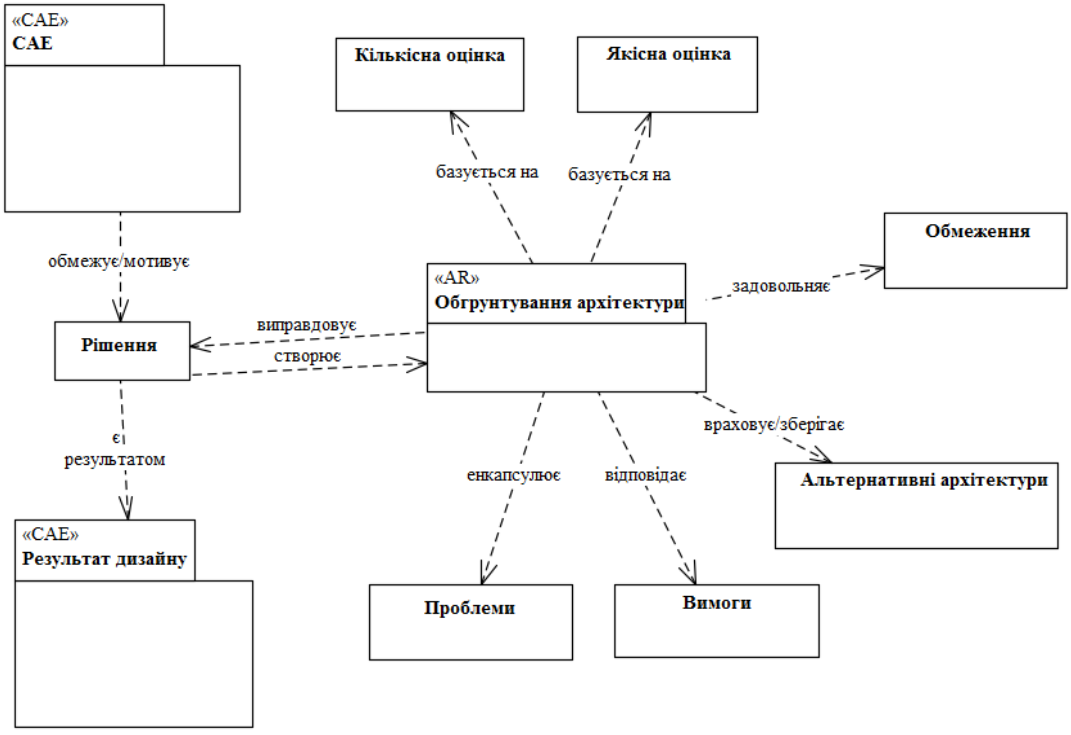

Рисунок 2.1 – Концептуальна модель RECAD

Фактично RECAD представляється ациклічним графом, який пов'язує елементи архітектури *CAE* з елементами обґрунтування архітектури *AR* за допомогою направленого відношення *ARtr*. *CAE* є критичним або не критичним архітектурним елементом, який приймає участь в *Рішенні* як вхідне значення (*Мотиваційна причина*) або як вихідне значення (*Результат дизайну*). AR енкапсулює результат *Обґрунтування архітектури* для *Рішення*. Так як *AR* має

відношення типу 1:1 з *Рішенням,* для даного підходу він представляє точку прийняття рішення щодо обґрунтування архітектури. Відношення між *CAE* та *AR* представляється за допомогою направленої асоціації ARtr, яка є причинно-наслідковим зв'язком.

Означення 2.1. Модель RECAD – це РТС $RECAD = (CAE, CAE^0, AR, A, R, \sum, L)$, де *CAE* – множина вузлів, що представляють критичні та некритичні елементи архітектури, CAE^0 - підмножина *CAE* початкових станів елементів архітектури, *AR* – множина вузлів, які представляють обґрунтування архітектури, A – скінченна множина міток дій, $\sum$ - множина змінних системи, L - функція розмітки елементів $L: CAE \to 2^{\Sigma}$, R – множина $R \subseteq (CAE \times AR) \cup (AR \times CAE)$ направлених зв'язків між вузлами, для якої виконуються наступні умови:

1. всі вузли AR повинні бути асоційовані з хоча б одною причиною та одним наслідком, тобто для $\forall r \in AR$ існує така причина $e \in CAE$, що $(e,r) \in R$ і існує такий наслідок $e' \in CAE$, що $(r,e') \in R$;

2. не існує підмножини з множини *R*, яка утворює направлений цикл.

Основною формою модельної конструкції є шлях виду $\{CAE_1, CAE_2, ...\} \to AR_1 \to \{CAE_a, CAE_b, ...\}$, де CAE_1, CAE_2 - входи, або причини рішення AR_1, а CAE_a, CAE_b - виходи, або наслідки цього рішення. На рис. 2.9 представлена UML діаграма, яка демонструє означену модельну конструкцію. Кратність відношень діаграми показує, що мотиваційні та результуючі *CAE* є непустими множинами, з'єднаними через єдиний елемент *AR*. Обмеження унікальності на діаграмі визначає, що кожний екземпляр *CAE* не може бути відображеним більше, ніж один раз.

Рисунок 2.2 – Причинно-наслідковий зв'язок між *CAE* та *AR*

Направлені зв'язки ARtr представляють причинно-наслідкові відношення. *CAE* призводить до *AR* через мотивацію або обмеження *Рішення, AR* в свою чергу генерує *CAE* типу *Результат дизайну* маючи *Обґрунтування архітектури*. *CAE* може бути одночасно вхідним і вихідним, якщо використовується для двох *Рішень*. У якості вхідного він може представляти собою артефакт наступних типів: вимога, прецедент, клас, імплементація. Як вихідний – новий або переглянутий елемент дизайну.

В RECAD архітектурні елементи CAE є артефактами, які формують частини дизайну архітектури. Вони включають бізнес-потреби, які потрібно задовольнити, технічні та організаційні обмеження, що накладаються на проект архітектури, припущення, які потрібно перевірити, та об'єкти дизайну, які є результатом архітектурного проектування.

Елементи архітектури можуть також бути класифіковані за точками зору на архітектуру. Причина такої класифікації – мати можливість фокусуватись на різних аспектах проектного рішення. В даному дослідженні, згідно з результатами аналізу ФОАП, використовуються точки зору на архітектуру підходу TOGAF. Для класифікації використано наступні точки зору на архітектуру: бізнес-логіка, рівень даних, застосування, технології. А також додану нову точку зору на архітектуру, орієнтовану на критичні елементи.

Підхід RECAD надає можливість використовувати три типи обґрунтувань архітектури: кількісний, якісний та за допомогою альтернативної архітектури. Якісне обґрунтування представляє процес обґрунтування та аргументи у текстовій формі, фактично, за та проти для кожного проектного рішення. Кількісне обґрунтування використовує різні критерії при оцінюванні проектних рішень. Третій тип передбачає документування та зберігання відкинутих альтернативних проектних рішень та їх подальший перегляд з метою оцінки достатності наявних параметрів оцінювання наявних архітектурних проектів, а також для майбутнього використання в інших проектах.

Слід зазначити, що архітектурне рішення може еволюціонувати з часом. Причиною цьому можуть бути як зміни в бізнес-процесам підприємства, так і зміни самого бізнес-середовища. Еволюціонуючи, можна втратити вихідний архітектурний проект та опис процесу обґрунтування рішень щодо цього проекту. Тому потрібно якимось чином зберігати всю історію еволюції проекту. Для цього пропонується використовувати розширену модель RECADe.

Означення 2.2. Розширена модель RECADe – це РТС $RECADe = (CAE, CAE^0, AR, A, R, \sum, L)$, на якій задана бієктивна функція відображення $SSf : (CAE \to CAE_h) \cup (AR \to AR_h)$ між архітектурними елементами або обґрунтуваннями архітектури, де:

$RECAD_{cur} = (CAE_{cur}, CAE^0_{cur}, AR_{cur}, A_{cur}, R_{cur}, \sum_{cur}, L_{cur})$ - актуальна модель архітектури і виконуються наступні умови:

- $CAE_{cur} \subseteq CAE$, $AR_{cur} \subseteq AR$, $A_{cur} \subseteq A$, $\sum_{cur} \subseteq \sum$, $CAE^0_{cur} \subseteq CAE^0$,
- $L_{cur} : CAE_{cur} \to 2^{\sum_{cur}}$, $R_{cur} \subseteq R \cap ((CAE_{cur} \times AR_{cur}) \cup (AR_{cur} \times CAE_{cur}))$,
- не існує підмножини з множини R_{cur}, яка утворює направлений цикл;

$RECAD_h = (CAE_h, CAE^0_h, AR_h, A_h, R_h, \sum_h, L_h)$ - історична модель архітектури і виконуються наступні умови:

- $CAE_h \subseteq CAE$, $AR_h \subseteq AR$, $A_h \subseteq A$, $\sum_h \subseteq \sum$, $CAE^0_h \subseteq CAE^0$,
- $L_h : CAE_h \to 2^{\sum_h}$, $R_h \subseteq R \cap ((CAE_h \times AR_h) \cup (AR_h \times CAE_h))$;
- не існує підмножини з множини R_h, яка утворює направлений цикл;

і для яких виконуються наступні умови:

1. $CAE_h = CAE \setminus CAE_{cur}$, 2. $AR_h = AR \setminus AR_{cur}$, 3. $A_h = AR \setminus A_{cur}$,
4. $\sum_h = \sum \setminus \sum_{cur}$, 5. $CAE_h^0 = CAE^0 \setminus CAE_{cur}^0$, 6. $L_h = L \setminus L_{cur}$.

На рис. 2.3 представлена відповідна модель UML-діаграма.

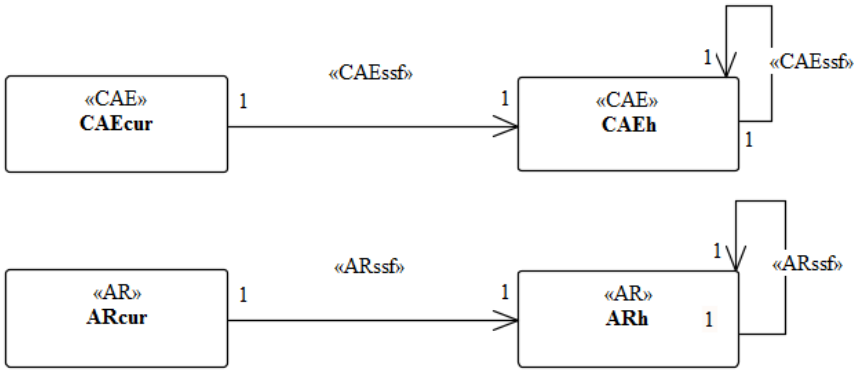

Рисунок 2.3 – UML-діаграма розширеної моделі CARELe

Імплементація підходу RECAD за допомогою UML. Для імплементації архітектурного елементу *CAE* визначено новий стереотип <<CAE>>. Даний стереотип розширює можливості UML-конструктів типу «об'єкт» та «клас» щодо підтримки властивостей відстежуваності та критичності. Це означає, що до існуючих конструктів додаються додаткові характеристики та атрибути з метою покращення процесу обґрунтування рішень. Додаткові атрибути стереотипу <<CAE>> імплементовані як теговані значення (tagged values).

З метою моделювання бізнес-орієнтованих точок зору, які містять вимоги, фактори середовищ та припущення використовується створений стереотип <<CAE>> для розширення елементів UML таких як клас, об'єкт, артефакт та прецедент (рис. 2.4).

Використання таких елементів дозволяє створювати моделі з різними точками зору на архітектуру.

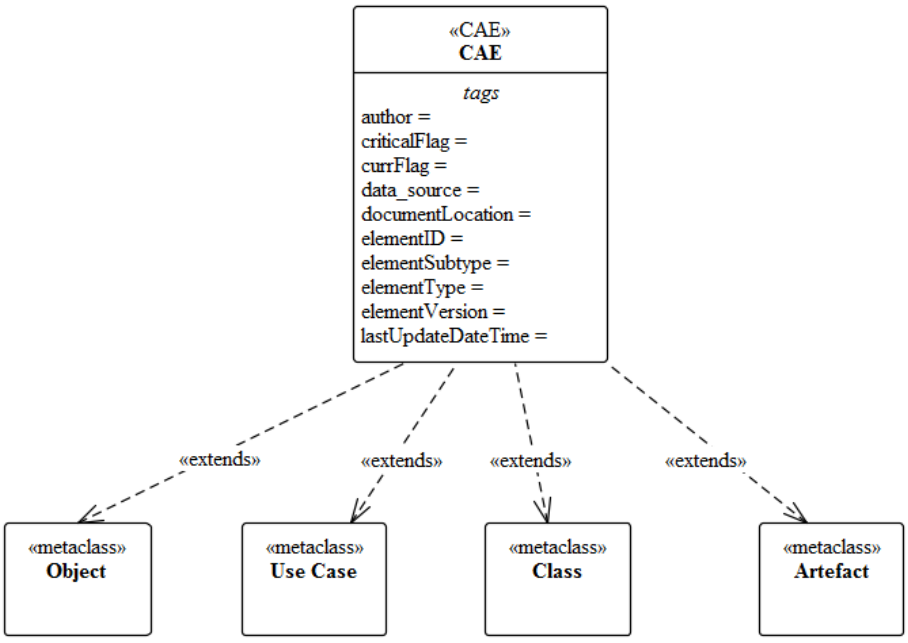

Рисунок 2.4 – Розширення елементів UML стереотипом <<CAE>>

Для імплементації елементу «*обгрунтування рішення*» використано стереотип <<AR>>, який розширяє можливості UML-конструкту «Пакет». Додаткові атрибути стереотипу <<AR>> імплементовані як теговані значення.

Стереотип <<AAR>> надає шаблон для документування альтернативних проектних рішень, які були відкинуті.

Відношення між *CAE* та *AR* представляється за допомогою направленої асоціації з новоствореним стереотипом <<ARtr>>.

Введені моделі RECAD та RECADe дозволяють представити та описати окремі конкретні проектні рішення щодо систем, компонент та процесів, які входять до архітектури критичної інформаційної інфраструктури.

Визначимо для моделі RECAD її асинхронну паралельну композицію (Означення 2.3).

Означення 2.3. Нехай задані РТС $RECAD_1 = (CAE_1, CAE_1^0, AR_1, A_1, R_1, \Sigma_1, L_1)$ та $RECAD_2 = (CAE_2, CAE_2^0, AR_2, A_2, R_2, \Sigma_2, L_2)$ такі, що $CAE_1 \cap CAE_2 = \varnothing, AR_1 \cap AR_2 = \varnothing,$ $A_1 \cap A_2 = \varnothing, \Sigma_1 \cap \Sigma_2 = \varnothing.$ Нехай також задана синхронізаційна пара $\Lambda = (\Delta, \bar{}), \Delta \subseteq A_1, \bar{}: \Delta \to A_2.$ Тоді модель $RECAD = (CAE, CAE^0, AR, A, R, \Sigma, L) =$ $= RECAD_1 \|_\Lambda RECAD_2$ називається паралельною композицією РТС $RECAD_1$ і $RECAD_2$, якщо:

- вірні співвідношення
  $CAE = CAE_1 \times CAE_2, AR = AR_1 \times AR_2, S^0 = S_1^0 \times S_2^0,\ A = A_1 \cup A_2 \setminus (\Delta \cup \bar{\Delta}), \Sigma = \Sigma_1 \cup \Sigma_2,$
- вірно $L: CAE \to 2^\Sigma,\ L((cae_1, cae_2)) = L(cae_1) \cup L(cae_2),$
- відношення $R \subseteq ((CAE_1 \times CAE_2) \times A \times (AR_1 \times AR_2)) \cup ((AR_1 \times AR_2) \times A \times (CAE_1 \times CAE_2))$ задається наступним чином: $((s,u),a,(t,v)) \in R$ тоді і тільки тоді, коли виконується одна з трьох умов:
  - виконується перехід першої моделі: $(s,a,t) \in R_1, u = v$;
  - виконується перехід другої моделі: $(u,a,v) \in R_2, s = t$;
  - виконується синхронний обмін повідомленнями: $(s,b,t) \in R_1, (u,b,v) \in R_2, a = \tau$.

Таким чином, модель архітектурного рішення критичної інформаційної інфраструктури можна представити наступним чином (Означення 2.4).

Означення 2.4. Модель архітектурного рішення критичної інформаційної інфраструктури визначається у вигляді паралельної композиції всіх окремих проектних рішень щодо систем, компонент та процесів, які входять до архітектури критичної інформаційної інфраструктури, заданих у вигляді РТС RECAD, тобто: $M = RECAD_1 \|_{\Lambda_1} .. \|_{\Lambda_{n-1}} RECAD_n$, де $RECAD_1, ..., RECAD_n$ - відповідні РТС, $\Lambda_1, ..., \Lambda_{n-1}$ - задані на моделі пари синхронізації.

Задача верифікації моделей архітектурних рішень критичних інформаційних інфраструктур. Задача верифікації моделей архітектурних рішень критичних інформаційних інфраструктур формулюється наступним чином:

Задача 2.1. Дана модель архітектурного рішення $M = P_1 \| ... \| P_n$, де $P_1, ..., P_n$ - РТС RECAD критичної інформаційної інфраструктури. Задана формула

(специфікація) φ темпоральної логіки відносно змінних моделі М. Необхідно перевірити виконуваність формули φ моделі М (позначається як $M \models \varphi$).

Задача верифікації параметризованих моделей архітектурних рішень критичних інформаційних інфраструктур.

Для КІІ, в яких число процесів залежить від початкової конфігурації, можуть бути побудовані моделі з кінцевим числом станів для кожної початкової конфігурації системи. Так як множина початкових конфігурацій нескінченна, то і множина моделей архітектурних рішень з різним числом процесів нескінченна. Верифікація декількох, випадково обраних моделей, з цієї множини не гарантує виконуваність специфікації на всіх моделях множини. Для таких систем розглядається задача, яка в загальному випадку формулюється наступним чином:

Задача 2.2. Дано нескінченне сімейство скінченних моделей архітектурних рішень КІІ $\mathcal{F}=\{M_n\}$, параметризоване за параметром $n \in N$. Задана формула (специфікація) φ темпоральної логіки. Необхідно перевірити виконуваність формули φ на всіх моделях $\mathcal{F}$, тобто $M_n \models \varphi$ для всіх n. Ця задача в літературі отримала назву верифікації параметризованих моделей (ВПМ).

Постановка задачі 2.2 потребує уточнення, так як в загальній постановці явно не вказується спосіб визначення сімейства F та специфікації φ. Тому, фактично будемо розглядати наступний варіант задачі 2.2.

Задача 2.3. Дано нескінченне сімейство скінченних моделей архітектурних рішень КІІ $\mathcal{F}=\{M_n\}$, параметризоване за параметром $n \in N$. Кожна модель $M_n = Q \| P_1 \| ... \| P_n$ складається з РТС фіксованої моделі RECAD Q та n екземплярів РТС альтернативних моделей P_i. Зафіксована кінцева множина $I \subseteq \mathbb{N}$ індексів альтернативних моделей, що наблюдаються, екземплярів прототипів P. Специфікація φ темпоральної логіки задається відносно змінних визначених моделей $P_i, i \in I$ та змінних моделі Q. Необхідно перевірити виконуваність формули φ на всіх моделях сімейства $\mathcal{F}$, тобто $M_n \models \varphi$ для всіх n.

Фактично, в постановці задачі 2.3 використовується лише одна фіксована модель Q та n екземплярів прототипів P. Можна розглядати варіант задачі, в якому присутні декілька фіксованих моделей $Q_1,...Q_m$ та декілька альтернативних моделей $P^a, P^b, ..., P^z$, а модель $M_n = Q_1 \| ... \| Q_m \| P_1^a \| ... \| P_{n_a}^a ... \| P_1^z \| ... \| P_{n_z}^z$, де $n_a + ... + n_z = n$. В деяких випадках, ця задача зводиться до постановки задачі 2.3 за допомогою побудови РТС моделі Q у вигляді паралельної композиції моделей $Q_1,...Q_m$, а РТС прототипу P у вигляді паралельної композиції РТС прототипів $P^a, P^b, ..., P^z$.

Запропонована постановка задач у вигляді (2.1-2.3) дозволяє застосувати для верифікації побудованих моделей широке коло формалізованих методів верифікації параметризованих моделей, заданих у вигляді РТС.

У розділі 3 представлений детальний опис методу обґрунтування архітектури критичної інформаційної інфраструктури на базі ентропійного підходу, наведено основні базові елементи математичного апарату підходу, використаних для опису моделей даного методу обґрунтування архітектури у формалізованому вигляді. Запропонований метод дозволяє автоматизувати процес обґрунтування архітектури критичної IT-архітектури в досить зручний спосіб та дає можливість досліднику відстежувати вплив змін окремого елемента архітектури на всю архітектуру в цілому.

Як вже було зазначено вище, RECAD підтримує декілька варіантів оцінювання процесу обґрунтування архітектури. В цій роботі особливу увагу приділено кількісним методам оцінювання процесу.

В даному підході прийняття рішення базується на оцінюванні вартості, переваг та ризиків варіантів дизайну архітектури.

У випадку, коли є декілька варіантів побудови системи, які досягають тієї ж самої мети, архітектор спробує якимось чином обрати найкращий варіант. Для цього, в першу чергу, будуть відкинуті всі варіанти, які не працюють або не задовольняють вимогам. Наступним кроком архітектор спробує найти варіант дизайну, який при максимальних перевагах дизайну потребує мінімальних витрат на реалізацію. Поставлена задача може виявитися надто складною через велику кількість варіантів дизайну архітектури.

Пропонований метод зберігає відповідні розрахунки за допомогою елементу UML «Кількісна оцінка архітектури» (QNEA). Індекс вартості архітектури (architecture cost index, ACI) являє собою відносний зважений показник вартості архітектури за шкалою від 1 до 10. Даний індекс враховує безліч різних витрат на архітектуру, серед яких:

– витрати на розробку – сюди відносяться витрати на розробку критичної інформаційної інфраструктури та вимоги щодо навчання персоналу;

– витрати на платформу – вартість обладнання та програмного забезпечення для побудови критичної інформаційної інфраструктури;

– витрати на підтримку – витрати на підтримку працездатності критичної інформаційної інфраструктури, модифікацію та адаптацію програмного забезпечення, обладнання тощо;

– потенційні витрати – витрати, які можуть потенційно виникнути в ході дизайну або експлуатації критичної IT- інфраструктури.

Індекс переваг архітектури (architecture benefits index, ABI) – відносний зважений показник переваг архітектури за шкалою від 1 до 10, що визначає рівень задоволення вимог, висунутих перед архітектурою.

Розглянемо наступний приклад. Потрібно визначити, яку СУБД використати при реалізації підсистеми єдиної інформаційної системи МВС «Єдине розподілене сховище даних» (рис. 3.1).

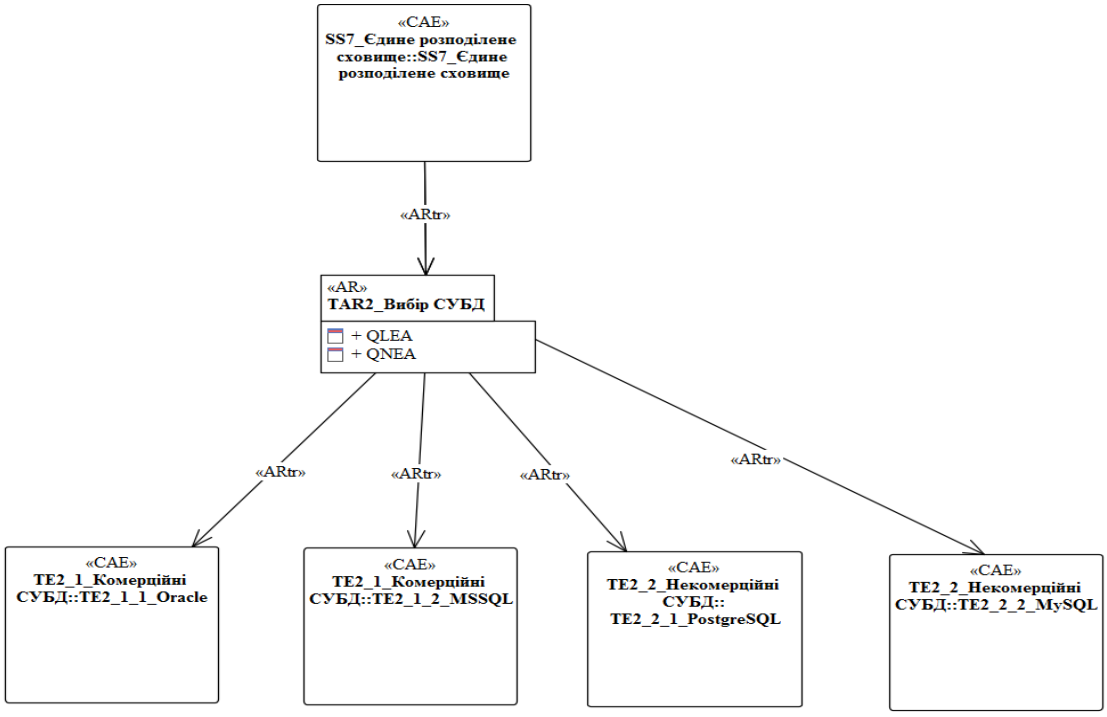

Рисунок 3.1 – Приклад обґрунтування рішення

Для визначення відповідного варіанту архітектури до уваги беруться наступні фактори:

– витрати:
  - вартість ліцензій;
  - витрати на підтримку;
  - витрати на навчання персоналу;
  - витрати на впровадження;
  - витрати на інтеграцію;
– переваги:
  - продуктивність;
  - гнучкість рішення;
  - надійність рішення;
  - масштабованість рішення;
  - безпечність рішення.

Кожний фактор оцінюємо за шкалою від 0 до 2.

При проектуванні архітектури часто виникають деякі невизначеності дизайну. Явне представлення цих невизначеностей дозволяє архітектору в певний момент часу до них повернутись та визначити їх. В даному методі використовуються наступні показники:

– ризик визначеності результату дизайну (outcome certainty risk, OCR) – визначає ризик або рівень невизначеності досягнення архітектурним проектом результату дизайну, представленого індексом переваг архітектури;

– ризик визначеності імплементації дизайну (implementation certainty risk, ICR) – визначає ризик або рівень невизначеності виникнення непередбачених ситуацій при імплементації архітектурного рішення;

– ризик визначеності вимог щодо критичності дизайну (criticality certainty risk, CCR) – визначає ризик або рівень невизначеності порушення вимог до заданого рівня критичності при імплементації архітектурного рішення.

Оцінювання ризиків є важливим процесом при проектуванні критичної інформаційної інфраструктури, так як надає архітектору інструментарій для всебічної оцінки можливих перешкод, які можуть виникати в процесі проектування та обґрунтування рішень щодо вибору оптимальної архітектури критичної інформаційної інфраструктури.

Для оцінювання та порівняння альтернативних варіантів архітектурних рішень використання наведених вище показників є досить незручним. Для оптимізації процесу порівняння введемо декілька нових параметрів:

– рівень очікуваної переваги (expected benefit, EB), який визначається як:

$$EB = (1 - OCR)(1 - CCR) * ABI, \quad (3.1)$$

– рівень очікуваної вартості (expected cost, EC), який визначається як:

$$EC = (1 + ICR) * (1 + CCR) * ACI, \quad (3.2)$$

– коефіцієнт відношення «Витрати-переваги» (cost-benefit ratio, CBR), який визначається як:

$$CBR = \frac{EB}{EC} = \frac{(1 - OCR)(1 - CCR) * ABI}{(1 + ICR) * (1 + CCR) * ACI}. \quad (3.3)$$

Саме останній коефіцієнт і є тим зручним елементом, який дозволяє порівнювати між собою альтернативні проектні рішення.

В табл. 3.1 наведений розрахунок нових параметрів щодо прикладу, зазначеного вище.

Таблиця 3.1 – Результати оцінювання вибору СУБД

СУБД	**Oracle**	**PostgreSQL**	**MySQL**	**MSSQL**
Індекс вартості архітектури (ACI)	9	3	3.5	5.5
Індекс переваг архітектури (ABI)	10	7.5	5	5
Ризик визначеності результату дизайну (OCR)	0.2	0.2	0.6	0.4
Ризик визначеності імплементації дизайну (ICR)	0.2	0.3	0.5	0.5
Ризик визначеності вимог щодо критичності дизайну (CCR)	0.2	0.5	0.8	0.8
Рівень очікуваної переваги (EB)	6.4	3	0.4	0.6
Рівень очікуваної вартості (EC)	12.96	5.85	9.45	14.85
Коефіцієнт відношення «Витрати-переваги» (CBR)	0.49	0.51	0.04	0.04

Як видно з табл. 3.1, найкращим рішенням для імплементації підсистеми ЄІС МВС «Єдине розподілене сховище даних» є використання СУБД PostgreSQL. Відповідно до представлених розрахунків СУБД має найбільше значення коефіцієнту CBR.

Для визначення значень ризиків OCR, ICR та CCR використовується метод експертних оцінок. Для дослідження впливу одних проектних рішень на інші пропонується використати ентропійний підхід.

Нехай для деякого проектного рішення A апріорі відома множина з n загроз безпеці проектування цього рішення, які впливають на результат і імплементацію дизайну та порушення вимог критичності і впорядкована множина з m станів збитку внаслідок реалізації цих загроз:

$$x_1, x_2, .., x_i, .., x_m, \quad (3.4)$$
$$i = \overline{1, m}.$$

Очевидно, що $n \le m$. Це вказує на існування не тотожних загроз безпеці, які призводять до однакового збитку. Прикладом цьому можуть бути загрози внаслідок реалізації яких збитки рівні нулю.

Крім цього, під впорядкованістю розуміється, що

$$0 \le x_1 \le x_2 \le .. \le x_i \le .. \le x_m \le x_{\max}, \quad (3.5)$$

де $x_{\max}$ – максимальний збиток, рівний повному ліквідуванню усіх елементів проектного рішення A за нескінченно малий проміжок часу без будь-яких залишків. Крім цього вважатимемо, що відомий розподіл імовірностей p_i на множині x_i, а саме: збиток x_1 виникає з імовірністю p_1, збиток x_2 – з імовірністю p_2, збиток x_i – з імовірністю p_i.

З огляду на це, повною множиною подій $x_1, x_2, .., x_i, .., x_m$ назвемо таку множину станів збитку, що внаслідок реалізації загрози безпеці проектування рішення обов'язково наступить один з них. Оскільки стани збитку $x_1, x_2, .., x_i, .., x_m$ повної множини подій задані з їх імовірностями

$$p_1, p_2, .., p_i, .., p_m, \quad (3.6)$$
$$p_i \ge 0, \sum_{i=1}^{m} p_i = 1,$$

то вважатимо заданою кінцеву схему

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_i & \dots & x_m \\ p_1 & p_2 & \dots & p_i & \dots & p_m \end{pmatrix}. \quad (3.7)$$

За допомогою кінцевої схеми описуватимемо стан невизначеності при забезпеченні результату та імплементації дизайну, виконання вимог щодо критичності дизайну. При цьому ступінь цієї невизначеності різна для різних схем. Тому для оцінювання ступеня невизначеності заданої кінцевої схеми використовується ентропійна міра

$$H_A(p_1, p_2, .., p_i, .., p_m) = -\sum_{i=1}^{m} p_i \lg p_i, \quad (3.8)$$

де $H_A(p_1, p_2, .., p_i, .., p_m)$ – ентропія кінцевої схеми. Якщо одне зі значень імовірності дорівнює одиниці, то функція $H_A(p_1, p_2, .., p_i, .., p_m) = 0$. Цьому відповідає випадок, коли завчасно можна передбачити реалізацію загрози проектному рішенню з повною достовірністю і, як наслідок, відсутністю невизначеності. Тоді як при

фіксованому m найбільша невизначеність описуватиметься кінцевою схемою з рівноймовірними реалізаціями загроз.

Враховуючи вищенаведене, для кожного проектного рішення AR визначається наступна кінцева схема:

$$X = \begin{pmatrix} x_1 & x_2 & x_3 \\ OCR & ICR & CCR \end{pmatrix}. \qquad (3.9)$$

За допомогою властивостей ентропії архітектор має можливість оцінювати вплив одних проектних рішень на інші. Наприклад, оцінити вплив збою критичного елементу на весь дизайн в цілому.

Далі наведений опис моделі оцінки та вибору оптимальної конфігурації компонент критичної інформаційної інфраструктури за допомогою Марківського процесу прийняття рішень, яка дозволяє обирати оптимальну конфігурацію компонент на базі визначених критеріїв.

Пропонована модель має наступні параметри:

F – скінченна множина філій підприємства ($F = \{1,..,f\}$);

P – скінченна множина платформ IT ($P = \{1,..,p\}$);

T – скінченна множина відліків часу ($T = \{1,..,t\}$);

I – скінченна множина критеріїв проектування;

Z – множина категорій запитів на зміну архітектури ($Z = \{1,..,z\}$);

$f \in F$ – значення індексу філії підприємства;

$p \in P$ – значення індексу платформи IT;

$z \in Z$ – значення індексу запиту на зміну архітектури;

$i \in I$ – значення індексу критерію проектування;

$b_t \in I$ – бюджет нового проекту в момент часу t;

c_{fp} – вартість проектування/переходу на нову платформу p для філії f з врахуванням всіх витрат на ПЗ, апаратні засоби, інтеграцію та впровадження;

a_{fpz} – вартість виконання запиту на зміну архітектури z на платформу p для філії f;

b_{fpzi} – виграш від виконання запиту на зміну архітектури z на платформу p для філії f за критерієм i.

Простір станів моделі описується наступними змінними:

x_{zf} – кількість запитів на зміну архітектури z, що ще не виконані для філії f;

cur_{fp} – поточна платформа філії f;

X – матриця значень x_{zf};

CUR – матриця значень cur_{zf};

S – стан процесу ($S=[X,CUR,t]$).

Випадкові величини, що використовуються в моделі:

pr_{zft} – кількість запитів на зміну архітектури z для філії f в момент часу t;

PR – матриця значень pr_{zft}.

Простір рішень моделі описується наступними змінними:

y_{zft} – кількість запитів на зміну архітектури z для філії f в момент часу t, що потрібно виконати;

l_{fpt} – флаг переходу на платформу p для філії f в момент часу t, що потрібно виконати;

Y – масив змінних простору рішень;

$\Re(S)$ – множина можливих рішень для стану S;

$C^i(Y)$ – виграш за критерієм i, пов'язаний з рішенням Y;

$C(Y)$ – виграш за всіма критеріями, пов'язаний з рішенням Y;

$RWD_n^i(S)$ – максимальне очікуване значення виграшу на n-му етапі в стані S за критерієм i;

$RWD(S)$ – максимальне очікуване значення виграшу на n-му етапі в стані S за критерієм i.

Модель має певний ряд обмежень. Для стану $S=[X,CUR,t]$ змінні простору станів в Y повинні задовольняти наступні обмеження:

– обмеження бюджету проекту:

$$\sum_f \sum_p c_{fp} l_{fpt} + \sum_z \sum_f a_{zpf} y_{zft} \le b_t; \tag{3.10}$$

– обмеження об'єму проекту:

$$y_{zft} \le x_{zf}; \tag{3.11}$$

– вимоги щодо платформ:

$$\sum_p l_{fpt} = 1, \forall f, \tag{3.12}$$

$$y_{zft} \ge 0. \tag{3.13}$$

Всі рішення Y, що задовольняють вимогам (3.12)–(3.13), для стану S формують множину можливих рішень $\Re(S)$. Модель є гнучкою. Можна додати додаткові обмеження. Наприклад, можна врахувати виконання проектних рішень, що забезпечують цілісність системи та її безпеку.

Кожне можливе прийняте рішення має певну кількість безпосередньо очікуваних витрат та виграшів. По-перше, очікуваний виграш b_{fzi} за критерієм i при виконанні запиту на зміну архітектури z для філії f. Також підприємство бере на

себе витрати a_{fz} на виконання запиту на зміну архітектури z для філії f. Додатково, можуть також бути витрати c_{fp}, пов'язані з міграцією філії f на платформу p.

Враховуючи наведене вище, виграш на черговому етапі проектування за критерієм i, пов'язаний з рішенням Y, можна розрахувати за формулою:

$$C^i(Y)=\sum_z\sum_f\sum_i b_{zfi}y_{zft}-\sum_f\sum_p c_{fp}l_{fpt}-\sum_z\sum_f a_{fz}y_{fzt}. \tag{3.14}$$

Значення $C^i(Y)$ може бути як позитивним, так і негативним. Якщо $\sum_z\sum_f\sum_i b_{zfi}y_{zft}>\sum_f\sum_p c_{fp}l_{fpt}+\sum_z\sum_f a_{fz}y_{fzt}$, то виграш, пов'язаний з вибраними проектними рішеннями, представлений першим термом функції виграшу на черговому етапі проектування, переважує витрати, які потрібно зробити.

Невизначеність поставленої задачі полягає у частоті запитів на зміну від кожної філії. В даній роботі вважається, що значення PR є статично незалежними. Нехай $S=[X],\ [CUR]$ – поточний стан, $Y\in\Re(S)$ – вибраний масив рішень і $S'=[X'],\ [CUR']$ – стан після виконання запиту на зміну. Тоді значення стану S' змінюється відповідно до (3.15)–(3.17):

$$x'_{zf}=x_{zf}-y_{zft}+pr_{zft}, \tag{3.15}$$

$$cur'_{fp}=l_{fpt}, \tag{3.16}$$

$$t'=t+1. \tag{3.17}$$

Ймовірність переходу з стану S в стан S' для рішення Y визначається як (3.18):

$$P_{SS'(Y)}=\prod_{f\in F}\prod_{z\in Z}\wp\left\{pr_{zft}\mid cur_{fp}=x'_{zf}-x_{zf}+y_{zft}\right\}. \tag{3.18}$$

Функції пошуку моделі наступні:

$$RWD^i_1(S)=\max_{Y\in\Re(S)}C^i(Y), \tag{3.19}$$

$$RWD^i_n(S)=\max_{Y\in\Re(S)}\left\{C^i(Y)+\sum_{S'}P_{SS'}(Y)RWD^i_{n-1}(S')\right\},\ n>1, \tag{3.20}$$

$$RWD(S)=\max_{Y\in\Re(S)}\sum_i\sum_j^n RWD^i_j(S). \tag{3.21}$$

При роботі з критичними інформаційними інфраструктурами, оцінка вибору конкретного варіанту реалізації архітектури є однією з проблем, з якою стикаються всі методи, які використовуються для проектування. Запропонована модель є водночас модульною та масштабованою в тому сенсі, що має достатню гнучкість у виборі та використанні як простих, так і складних критеріїв вибору архітектури для критичної інформаційної інфраструктури. Модульність досягається за рахунок використання різних конфігурацій елементів, тоді як масштабованість представлена у двох формах:

– масштабованість при побудові моделі (топологія і функціональність) критичної інформаційної інфраструктури;

– масштабованість з точки зору використання різного роду критеріїв, необхідних для порівняння варіантів реалізації. З точки зору моделювання, пропонований підхід дозволяє створювати моделі оцінки варіантів реалізації на базі різних критеріїв, які можна далі використовувати як вхідні моделі для подальшого порівняння за допомогою інших критеріїв, що в свою чергу, дає можливість знайти оптимальну архітектуру критичної інформаційної інфраструктури. Таким чином, модель дозволяє накопичувати моделі оцінки варіантів реалізації для багаторазового використання.

І на останок, в розділі наведена модель оцінки впливу забезпечуючих систем на архітектуру критичної інформаційної інфраструктури, побудовану на базі розширених гібридних відкритих автоматів, яка дозволяє оцінити вплив забезпечуючих систем на архітектуру критичної інформаційної інфраструктури з можливим врахуванням ймовірнісного характеру поведінки окремих її елементів та деяких якісних показників, що можуть впливати на критичну інформаційну інфраструктуру.

Хоча кожна критична інформаційна інфраструктура зазвичай розглядається як окрема система, всі її системи сильно взаємопов'язані з різним рівнем взаємозалежності між ними. Як приклад, для роботи інформаційно-телекомунікаційної системи (ІТС) на рівні заявленої якості обслуговування потрібна безперебійна робота системи постачання електроенергії, в той час як якість роботи самої системи електропостачання залежить від стабільної роботи каналів передачі інформації ІТС.

Нехай критична інформаційна інфраструктура С представлена у вигляді сукупності систем і компонент Ω. Тоді, представимо нашу Ω у вигляді РВГА:

$$\Omega = (D, S, S_0, I, O, Z, L, G, T, \tau, F, SP, P, R, V),$$

де D – скінченна множина дискретних станів системи (компоненти) критичної інформаційної інфраструктури Ω. Множина поділяється на наступні множини: D_{sf} – множину безпечних станів, D_{cr} – множину критичних станів та D_t – множину термінальних станів;

S – скінченна множина неперервних станів системи (компоненти) критичної інформаційної інфраструктури Ω. Множина поділяється на наступні множини: S_{sf} – множину безпечних станів, S_{cr} – множину критичних станів та S_t – множину термінальних станів;

$S_0 \subseteq SxD$ – скінченна множина початкових станів, $s_0 \in S_{sf}, d_0 \in D_{sf}$;

$I = \Xi \cup \Psi$ – скінченна множина входів, яка поділяється на: Ξ – множина внутрішніх входів (в рамках одного компонента), Ψ – множина зовнішніх входів (між компонентні входи);

O – скінченна множина вихідних станів.

Запис $(s, d) \in SxD$ описує зміну стану компоненти Ω, яка має:

– початковий стан $S_0 \subseteq SxD$;

– динаміку зміни станів, що описується вектором $\phi : SxDxI \to R^n$;

– функцію виходу $\varphi : SxDxI \to O$;

– множину дозволених станів та входів $Z \to 2^{SxI}$;

– $L \subseteq DxD$ – скінченну множину відміток переходів, що включає спеціальний символ †;

– множину умов $G : L \to 2^{SxI}$, що ініціюють перехід між дискретними станами;

– відношення скидання $T : LxSxS$, що скидає значення входу $s \in S$ перед кожним переходом;

τ – диспетчер часу;

F – розподіл втручань в роботу компонентів;

SP – набір специфікацій;

P – набір політик;

R – набір вимог безпеки;

V – набір вразливостей.

Перехід є детермінованим та відбувається за умовою G у випадку, коли $l \in L \setminus \{\dagger\}$, або ймовірнісним, у випадку, коли $l = \dagger$. В останньому випадку, значення стану формується випадково згідно розподілу F.

Взаємодіючими учасниками в такій моделі є:

- компоненти (телекомунікаційні, промислові і т. ін.);
- системи;
- інфраструктури;
- оператори систем критичної інформаційної інфраструктури;
- супротивники;
- середовище.

Їх логіка функціонування описується наборами специфікацій SP, політиками P та вимогами безпеки R.

Середовище контролює часові та просторові аспекти всіх подій в моделі та диспетчеризує всі зміни станів відповідно до τ, використовуючи для цього розподіли F. Розподіл дає можливість створювати стратегії виходу з ладу доступних компонентів та використовується для вирішення проблем одночасного виникнення подій в критичній інформаційній інфраструктурі та їх обробки.

Таку модель дуже зручно представити у вигляду направленого графу (рис. 3.2).

Кожна вершина такого графу представляє собою дискретний стан $d \in D$. Ребра направленого графу представляють собою дискретні переходи між станами. Наприклад, ребро $(d_1, d_2) \in L$ починається в вершині $d_1 \in D$ і закінчується в вершині $d_2 \in D$. Кожний перехід відбувається при виконанні умови $G(d_1, d_2)$ або випадково, якщо $L(d_1, d_2) = \dagger$. В кінці переходу, при зміні значення неперервного стану, відбувається скидання відношення T.

Простий шлях (спрацювання РВГА) складається з послідовності інтервалів τ безперервної еволюції, що змінюються дискретними переходами. Виконання починається з деякого початкового стану $(d_0, s_0) \in S_0$. Модель залишається в

дискретному стані d_i доки неперервний стан $s_i \in S$ та/або значення входу $i \in I$ мають допустимі значення Z. В той же час, значення виходу $o \in O$ визначається як $\varphi(s_i, d_i, i)$. Якщо $s_i \in S$ та/або значення входу $i \in I$ досягає умови переходу $G(d_i, d_j)$, то зміна стану відбувається миттєво, а значення безперервного стану визначається шляхом відношення T.

Кожну критичну інформаційну інфраструктуру можна представити як композицію різних РВГА. На рис. 3.3 представлена композиція двох РВГА.

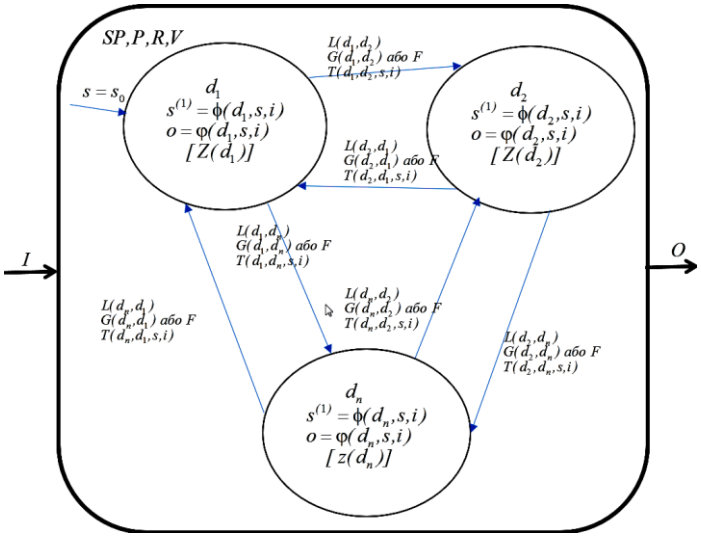

Рисунок 3.2 – Модель у вигляді направленого графу

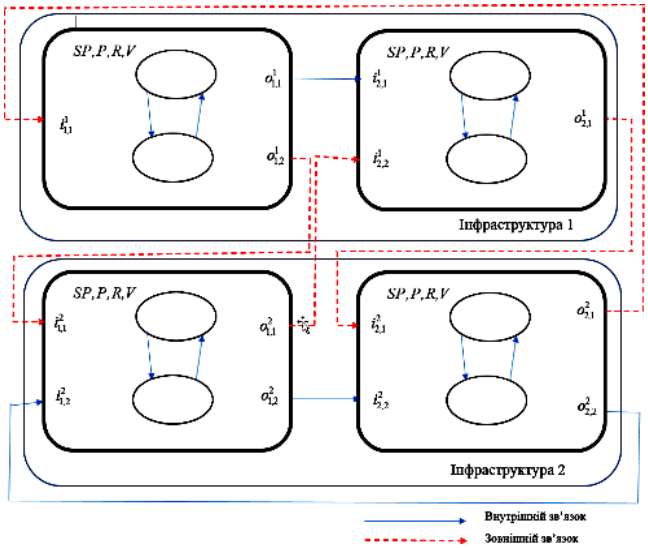

Рисунок 3.3 – Композиція автоматів

При роботі з критичними інформаційними інфраструктурами, масштабованість є однією з проблем, з якою стикаються всі методи, які використовуються для моделювання взаємозалежності. Запропонований підхід є водночас модульним та масштабованим в тому сенсі, що має достатню гнучкість у виборі та використанні як високоточних, так і простих моделей для критичної інформаційної інфраструктури.

У четвертому розділі представлений детальний опис методу аналізу стану і оцінювання елементів проектних рішень критичної інформаційної інфраструктури, побудованого за допомогою методу структурної оптимізації нейронних мереж, наведено основні базові елементи та операції методу. Запропонований метод дозволяє побудувати класифікатори на базі нейронних мереж з оптимальною структурою та використати їх для оцінювання елементів проектних рішень критичної ІТ-архітектури та їх впливу на інші елементи та архітектуру в цілому. Далі наведений опис моделей управління ресурсами критичної інформаційної інфраструктури, побудованих з використанням нечіткої логіки, генетичних алгоритмів та методу рою часток. І насамкінець, наведений детальний опис методу верифікації даних в інформаційних ресурсах критичної інформаційної інфраструктури, який дозволяє підвищити якість даних шляхом усунення дублювання, неправильних значень тощо.

Метод структурної оптимізації нейронних мереж використовує наступні елементарні структурні операції над мережею:

– додавання синапсу між двома випадково вибраними незв'язаними вузлами або нейронами мережі – операція Syn_{ADD};

– видалення синапсу між двома випадково вибраними незв'язаними вузлами або нейронами мережі – операція Syn_{DEL};

– переміщення синапсу між двома випадково вибраними незв'язаними вузлами або нейронами мережі – операція Syn_{MOD};

– зміна функції активації нейрона для випадково вибраного нейрона – операція A_{MOD};

– серіалізація вузла або нейрона – операції - Ser_{NODE} і Ser_{NR};

– паралелізація вузла або нейрона – операції Par_{NODE} і Par_{NR};

– додавання вузла або нейрона – операції Add_{NODE} і Add_{NR};

– створення нового шару – операція L_{ADD};

– видалення шару НМ – операція L_{DEL}.

Використання чи невикористання наведених структурних операцій залежить від складності поставленої задачі.

На початку роботи алгоритму створюється мережа із одним прихованим шаром, заданою кількістю нейронів та функцією активації. Оскільки початкові значення синаптичних ваг вибираються довільним чином, початкова мережа проходить задану кількість навчальних епох.

У кожній ітерації алгоритму виконується пошук усіх можливих мутацій поточної мережі: видалення кожного синапсу, видалення кожного нейрону усіх прихованих шарів і т. д. Далі, мережі, отримані внаслідок виконання кожної мутації, навчаються протягом заданої кількості епох незалежно одна від іншої.

Після навчання мереж усіх можливих мутацій виконується вибір та схрещення кращих з них для отримання комбінованих мутацій. Як критерій для порівняння мереж використовується значення ціни на тренувальній вибірці. Для створення комбінованих мутацій використовуються лише ті мережі, значення цін яких є меншими за ціну пустої мутації.

Після отримання комбінованих мутацій вони порівнюються та вибирається найкраща. Ця мережа і є результатом роботи ітерації.

Алгоритм припиняє роботу якщо отримана мережа є гіршою (має більше значення ціни) за мережу в попередній ітерації.

Якщо мережа є кращою, відбувається перехід до наступної ітерації.

На рис. 4.11 схематично відображені елементи критичної інформаційної інфраструктури (елементи CAE та AR), їх окремі характеристики та напрямки впливу одних елементів на інші. Тут CAE_j^i, $i \in [1;m]; j \in [1;N_i]$ AR_j^i, $i \in [1;l]; j \in [1;N_i]$, – (елементи CAE та AR), а стрілками відображений вплив одних елементів на якість параметрів проектування інших. На даному графі можна побачити, як елемент CAE_2^1 впливає на два елементи – AR_1^1 та AR_2^1.

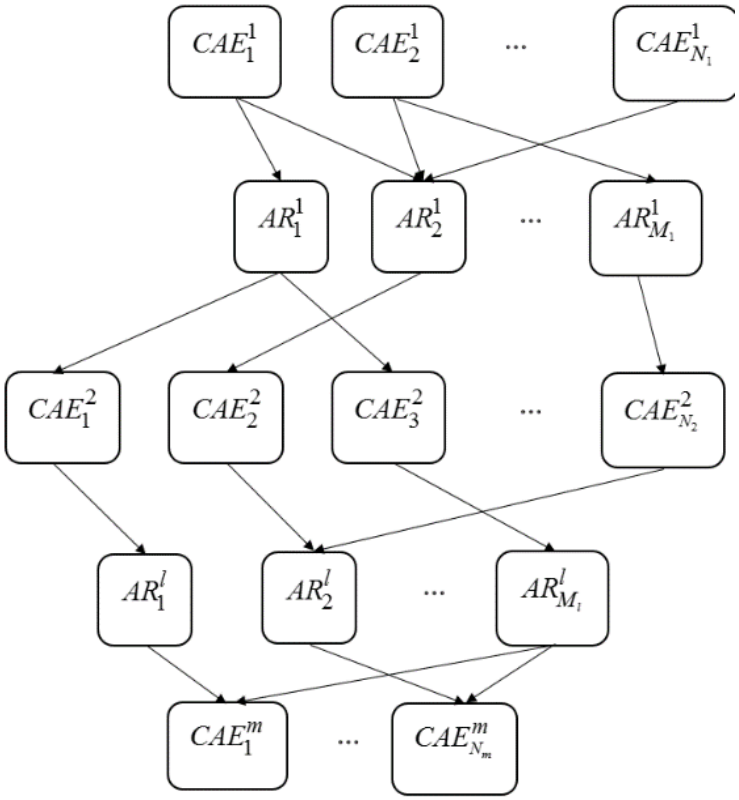

Рисунок 4.1 – Елементи критичної інформаційної інфраструктури

Такий граф будується архітектором автоматично на базі UML-діаграм проектного рішення, він же і визначає, які характеристики елементів критичної інформаційної інфраструктури необхідно враховувати при розрахунках якісної оцінки вибору включення даних елементів до проектного рішення і їх параметрів.

Позначимо параметри, що впливають на якість елемента, як

$$P_j^i = \{p_{j,1}^i, p_{j,2}^i, \dots\} \tag{4.1}$$

Кожному параметру $p_{j,m}^i \in P_j^i$, а також самим елементам CAE_j^i та AR_j^i буде відповідати лінгвістична змінна з лінгвістичними значеннями «відмінно», «задовільно», «незадовільно». Вони будуть характеризувати роботу даного елемента критичної інформаційної інфраструктури. Нейронна мережа, яка розраховує якісну оцінку вибору включення даних елементів, на вхід буде приймати числові значення параметрів проектування, а на виході видавати якісну оцінку, відповідну одному з лінгвістичних значень. Таким чином, така нейронна мережа буде виконувати роль класифікатора - розбивати простір параметрів проектування на зони, відповідні якісним оцінкам вибору розглянутих елементів. Дані якісні оцінки архітектор може потім використати для прийняття рішень щодо включення окремих елементів проекту до основного проектного рішення, а також для віднесення елементів з менш якісною оцінкою до альтернативних проектних рішень. Розраховані оцінки зберігаються в об’єкті QNEA відповідних елементів AR.

Модель розподілу ресурсів на базі алгоритму структурної оптимізації дає можливість оптимально розмістити ресурси.

Для формального опису моделі, введемо наступні поняття:

R - множина ресурсів;

P - множина фізичних машин;

V - множина віртуальних машин;

v_i - віртуальна машина i;

v_i^r - необхідність віртуальної машини i у ресурсі r;

P_{all} - множина задіяних (аллокованих) фізичних машин;

p_j - фізична машина j;

p_j^r - наявність ресурсу r у фізичної машини j;

V_i - множина віртуальних машин що призначені p_j.

Нашою метою є мінімізація кількості задіяних фізичних машин, тим саме мінімізуючи використання спожитої енергії:

$$P_{all} = \left\{ p_j \in P \,|\, \left|V_j\right| > 0 \right\} \tag{4.2}$$

Опишемо додаткові критерії оптимізації:

Усі віртуальні машини повинні бути розміщені:

$$V = \bigcup_{p_j \in P} V_j \tag{4.3}$$

Кожна віртуальна машина може бути розміщена лише на одній фізичній машині:

$$V_i \bigcap V_j = \varnothing,\ i \neq j \tag{4.4}$$

Для кожної фізичної машини, сумарне споживання кожного ресурсу її аллокованих віртуальних машин не повинне перевищувати об’єм доступного ресурсу фізичної машини:

$$p_j^r \geq \sum_{v_i \in V_j} v_i^r,\ r \in R \tag{4.5}$$

Кожне рішення у популяції характеризується хромосомою, що має структуру N-мірного вектору:

$$C = (p_1, p_2, ..., p_N) \tag{4.6}$$

N - кількість віртуальних машин,

p_i - фізична машина, що призначена i-тій віртуальній машині.

У запропонованій структурі кожна хромосома містить N генів, кожен з яких визначає позицію кожної віртуальної машини. Така структура хромосоми дає можливість простим чином дотримуватись виконання обмежень (4.3) та (4.4).

Для досягнення оптимального розподілу усіх ресурсів, визначимо функцію пристосованості кожного індивіда популяції (4.5), (4.6) та (4.7):

$$f(i) = -(k+1) \sum_{r \in R} \sum_{p_j \in P_{all}} \frac{w_j^r p_j^r}{p_j^r} \tag{4.5}$$

$$u_j^r = \frac{\sum_{v_i \in V_j} v_i^r}{p_j^r} \tag{4.6}$$

$$w_j^r = 1 - u_j^r \tag{4.7}$$

де u_j^r - використання ресурсу r фізичною машиною j,

w_j^r - марнування ресурсу r фізичною машиною j,

k – кількість фізичних машин, для яких споживання ресурсів є надмірним.

До об'єктів критичної інформаційної інфраструктури пред'являють особливі вимоги щодо забезпечення високої доступності. Введемо наступні поняття:

– відмовостійкість – здатність системи до подальшої роботи після відмови одного із її елементів;

– неперервна доступність – здатність системи до безперервного обслуговування, незалежно від часу відмови вузлів системи;

– високодоступність – здатність системи до подальшої роботи після відмови одного із вузлів, з можливими перервами у роботі.

Як правило, при реалізації неперервної доступності виникає багато труднощів, подолання яких вимагає значних фінансових витрат. Водночас, існують ситуації, коли необхідно забезпечити відмовостійкість системи без жорстких вимог до неперервності доступу.

Розміщення елементів будь-якого високодоступного кластеру завжди повинне виконувати наступну вимогу: основні та резервні елементи критичної інформаційної інфраструктури повинні знаходитись на різних фізичних серверах. Алгоритми, що наведені у попередніх розділах, можуть бути просто модифіковані для уведення додаткових вимог щодо розміщення віртуальних машин шляхом впровадження додаткових "ресурсів".

У (4.5) ресурс є кумулятивним об'єктом: сумарне споживання ресурсу дорівнює сумі споживань цього ресурсу кожною віртуальною машиною. Для кожного елементу високодоступного кластеру, що повинен знаходитись на окремій фізичній машині, визначимо його "спільний" ресурс за (4.8):

$$u_j^c = \begin{cases} +\infty, \left|V_j \cap V^c\right| > 1 \\ 1, \left|V_j \cap V^c\right| \le 1 \end{cases} \tag{4.8}$$

де V^c – множина віртуальних машин, що належать кластеру c.

Таким чином, при виявленні на одній фізичній машині більш ніж одного елементу кластеру, у фітнес-функцію вводиться додаткова штрафна величина. Для більш загального випадку, коли необхідно виконати розміщення кластеру, що використовує певну мінімальну кількість фізичних серверів, визначимо ресурс за (4.9) та (4.10):

$$u_j^c = \begin{cases} +\infty, \left|V_j \cap V^c\right| > 1 \\ 1, \left|V_j \cap V^c\right| \le I \end{cases} \tag{4.9}$$

$$I = C - k + 1 \tag{4.10}$$

де C – кількість елементів високодоступного кластеру;

k – мінімальна кількість різних фізичних машин, що повинні бути задіяні.

Проте під час експлуатації можуть виникати ситуації, що потребують

корегувати поточне розміщення:

– збільшення споживання ресурсів компонентом інфраструктури;

– відмова одного або декількох серверів;

– необхідність планового оновлення обладнання або програмного забезпечення.

У системах з підвищеними вимогами до надійності повинні існувати засоби динамічного балансування навантаження. Для здійснення цієї вимоги необхідно модифікувати фітнес-функцію таким чином, щоб вона враховувала властивості як початкового розміщення, так і нового. Розроблена фітнес-функція представлена у (4.11) та складається із трьох компонентів. На відміну від (4.5), в якій компоненти марнування та перевикористання ресурсів поєднувались через множення безрозмірних величин, у (4.11) усі компоненти приведені до однієї величини – фінансових витрат, що понесе компанія-власник критичної інформаційної інфраструктури. Така реалізація функції оцінки є простішою, більш наявною та краще піддається аналізу:

$$F(A_0, A) = F_w(A) + F_0(A) + F_m(A_0, A) \qquad (4.11)$$

де A_0 - стан початкового розміщення;

A - стан нового розміщення;

$F_w(A)$ - витрати марнування ресурсів інфраструктури за нового розміщення;

$F_0(A)$ – витрати, пов’язані із недостатнім забезпеченням сервісів інфраструктури;

$F_m(A_0, A)$ - витрати на приведення інфраструктури із стану A_0 до стану A

Таким чином, мінімальне значення фітнес-функції буде являти собою оптимальне співвідношення між марнуванням ресурсів та забезпеченням сервісів.

Модель розподілу ресурсів на базі методу роя часток описується наступним чином.

Кожна частка описується наступною групою векторів:

$$(\vec{x}_i, \vec{v}_i, \vec{p}_i) \qquad (4.12)$$

$$\vec{x}_i = (x_{i1}, x_{i2}, ..., x_{iD}) \qquad (4.13)$$

$$\vec{v}_i = (v_{i1}, v_{i2}, ..., v_{iD}) \qquad (4.14)$$

$$\vec{p}_i = (p_{i1}, p_{i2}, ..., p_{iD}) \qquad (4.15)$$

Кожна частка має позицію (4.13), швидкість руху (4.14) та найкраще рішення, що було досягнуто часткою в просторі рішень (4.15). На початку роботи алгоритму позиції часток генеруються випадково. Розмірність векторів визначається розмірністю задачі оптимізації. Серед усіх часток найкраще рішення популяції має вигляд:

$$\vec{g}_i = (g_{i1}, g_{i2}, ..., g_{iD}).$$

На кожній ітерації вектори позиції та швидкості кожної частки змінюються за наступними формулами:

$$v_{id}[t+1] = w v_{id}[t] + c_1 r_1 (p_{id} - x_{id}[t]) + c_2 r_2 (p_{gd} - x_{id}[t])$$

$$x_{id}[t+1] = x_{id}[t] + v_{id}[t+1]$$

де $i = 1,2,...,m$ – кількість часток; p_i – позиція i-ї частки; p_g – найкраще рішення популяції; $d = 1,2,...,D$ – розмірність часток; r_1, r_2 – випадкові числа; c_1 – індивідуальна швидкість навчання; c_2 – соціальна швидкість навчання; w – коефіцієнт інерції.

Параметр c_1 визначає власну здатність індивіда до пошуку рішення, тоді як параметр c_2 визначає соціальну комунікацію, тобто вплив соціального середовища на рух частки. Визначення оптимальних значень обох параметрів є предметом багатьох досліджень. За допомогою МРЧ виконується пошук оптимального рішення, оновлюючи популяцію часток у кожній ітерації. Критерієм зупинки може бути досягнення максимальної кількості ітерацій або бажаного мінімального значення помилки.

Найважливішим кроком проектування успішного МРЧ є вибір правильного подання рішення, яке точно описує відношення між частками МРЧ та задачею, що вирішується. При розміщенні N віртуальних машин кожна частка буде представлена у вигляді N-мірного вектору. Вектори позиції та швидкості визначаємо так:

$$x_i^k = (x_{i1}^k, x_{i2}^k, .., x_{in}^k),\ v_i^k = (v_{i1}^k, v_{i2}^k, .., v_{in}^k)$$

де x_i^k – позиція j-ї віртуальної машини i-ї частки у k-й ітерації;, v_i^k – швидкість j-ї віртуальної машини i-ї частки у k-й ітерації.

Оригінальний МРЧ використовується для задач оптимізації, в яких елементами простору рішень є неперервні дійсні числа. Саме неперервна природа алгоритму є складною перешкодою для використання алгоритму у комбінаторних задачах. Існує багато методів виправлення цього недоліку, одним із яких є метод найменшого значення позиції (НЗП). За допомогою цього методу, неперервні значення позиції перетворюються у таку послідовність розміщень:

$$s_i^k = (s_{i1}^k, s_{i2}^k, ..., s_{in}^k) \quad (4.16)$$

$$r_i^k = (r_{i1}^k, r_{i2}^k, ..., r_{in}^k) \quad (4.17)$$

$$r_{ij}^k = s_{ij}^k \bmod M \quad (4.18)$$

Остаточний вектор ідентифікаторів фізичних машин (ФМ) (4.17) вираховується за формулою (4.18).

Розглянуті методи розподілу ресурсів використані для побудови керованої моделлю системи розподілу ресурсів, яка описана в шостому розділі.

Метод верифікації даних в інформаційних ресурсах критичної інформаційної інфраструктури будується на використанні шаблонів даних.

Кожне поле даних програмно нормалізується з метою їх приведення до уніфікованого формату (тільки великі літери і цифри, без пробілів, знаків пунктуації). Всі поля нормалізованої база даних хешуються за допомогою алгоритму SHA-512. Саме цей тип хешування обрано через його поширеність та наявність підтримки у сучасних СКБД. Саме за такою процедурою пропонується обробити всі поля даних з метою їх подальшої використання для первинного його

наповнення у разі застосування хешованих ПД. Наступним кроком передбачається поступове внесення всіх записів шляхом додаткової обробки кожного запису. Така обробка передбачає створення додаткової таблиці БД, що буде містити записи для кожного запису даних у вигляді додаткових полів з хеш-кодами від шаблонів комбінацій полів даних, вже попередньо оброблених та представлених у вигляді хеш-кодів (див. табл. 4.3).

Кожен шаблон комбінації перетворюється в 64-байтовий хеш-код за допомогою одностороннього алгоритму хешування SHA-512. До кожного результуючого коду додається додатковий байт, який вказує кількість відсутніх полів даних для хеш-коду. Кожна комбінація є достатньою для того, щоб впевнено розрізняти об’єкт. Далі, генерується випадковий унікальний код UID і зв’язується з хеш-кодами комбінацій. UID і його зв’язані хеш-коди зберігаються на сервері і використовуються для визначення об’єкту.

Таблиця 4.3 – Шаблони комбінацій даних

Хеш-код	**Шаблони комбінацій**
1	$X_1 + \ldots + X_M + \text{choice}_U^L (Z)$
…	$X_1 + \ldots + X_M + \text{choice}_U^L (Z)$
Q	$X_1 + \ldots + X_M + \text{choice}_U^L (Z)$

Правило співставлення хеш-кодів та об’єктів. Кожний хеш-код складається з 64-байтового хеш-значення, яке обчислюється з шаблону комбінації ПД за допомогою одностороннього алгоритму хешування та додаванням 1 додаткового байту, яке вміщує кількість пропущених полів даних у хеш-коді. Таким чином, будь-яка помилка в полі даних, що використовуються в комбінації, призведе до помилки співставлення хеш-коду.

Пропонується використовувати 3 типи хеш-кодів: ідеальний, хороший і поганий. Для кожного хеш-коду використовуються 2 параметри для визначення його типу: нижній поріг (L) і верхній поріг (U) (див. табл. 4.4). Для ідеального хеш-коду вимагається, щоб кількість пропущених полів даних дорівнювала або була меншою L. Кількість відсутніх полів даних для генерації хорошого хеш-коду обмежується інтервалом (L, U). Якщо кількість пропущених полів даних більше U, то хеш-код буде визначений як поганий. Співпадіння k ідеальних хеш-кодів для двох записів БД свідчить про те, що вони ймовірно належать одному і тому ж об’єкту, а співпадіння між двома хорошими хеш-кодами для двох записів визначають ці хеш-коди ймовірними кандидатами, що належать одному і тому ж об’єкту.

При введенні нових записів до інформаційного масиву автоматично підраховується кількість ідеальних та хороших співпадінь. Це надасть можливість з’ясувати, чи є вже даний об’єкт у БД.

Таблиця 4.4 – Пороги відсутніх полів для визначення типу хеш-коду

Параметри	**Шаблон 1**	**…**	**Шаблон Q**
Нижній поріг	l_1	…	l_Q
Верхній поріг	u_1	…	u_Q

Для цього використовуються 3 параметри для визначення відповідності об’єкту: поріг для ідеального співпадіння (P), поріг для хорошого співпадіння (G) і поріг для змішаного співпадіння (X). Два записи збігаються один з одним, якщо кількість ідеальних співпадінь більша або рівна P, або кількість хороших співпадінь більша або рівна G, або сума ідеальних і хороших співпадінь більша або рівна X.

Наведений метод може бути адаптований під дані будь-якого типу та призначення.

У п’ятому розділі представлений детальний опис використаного в роботі прикладу критичної інформаційної інфраструктури – ЄІС МВС, наведена її структура та функціональні можливості. Далі наведене дослідження моделі оцінки впливу забезпечуючих систем на архітектуру критичної інформаційної інфраструктури. Дана модель використана при проектуванні ЦОД ЄІС МВС, що дозволило врахувати взаємозалежність систем охолодження та електроживлення на всю роботу ЦОД, і таким чином, якісно продумати резервування відповідних систем. На прикладі вибору структури ЦОД ЄІС МВС досліджена модель оцінки та вибору оптимальної конфігурації компонент критичної інформаційної інфраструктури за допомогою Марківського процесу прийняття рішень. Наведені дослідження методу структурної оптимізації нейронних мереж для різних класів задач, доведена його працездатність та надійність. Далі, досліджено дві моделі розподілу ресурсів критичної інформаційної інфраструктури. Перша модель побудована з використанням методу структурної оптимізації нейронних мереж, друга модель – з використанням методу роя часток. Обидві моделі дають можливість оптимально розподіляти ресурси критичної інформаційної інфраструктури в ЦОД. І насамкінець, продемонстровано використання методу верифікації даних на прикладі верифікації персональних даних при створенні сервісу ідентифікації фізичних осіб ЄІС МВС.

У шостому розділі дисертації представлений детальний опис концепції проектування критичної інформаційної інфраструктури, визначені її основні принципи та положення. Далі наведено опис узагальненої архітектури критичної інформаційної інфраструктури, визначені її основні рівні функціонування та наведено її життєвий цикл. Запропонована загальна схема пошуку проектних рішень на базі компенсаційно-декомпенсаційного підходу до проектування та обґрунтування проектних рішень щодо критичної інформаційної інфраструктури та відповідна візуалізація для відображення стратегій обґрунтування рішень, стратегій прийняття рішень стосовно архітектури критичної інформаційної інфраструктури.

Запропонована концепція інтегрує в єдину систему проектування критичної інформаційної інфраструктури сам процес дизайну архітектурних проектів критичної інформаційної інфраструктури, моделювання, верифікацію та обґрунтований вибір кращого архітектурного рішення за визначеними критеріями та його представлення у вигляді виробничої структури з певним визначеним життєвим циклом та функціональними задачами.

Пропонована концепція проектування КІІ орієнтована на створення єдиного універсального середовища проектування інформаційної інфраструктури підприємств з критичною інфраструктурою і представляє собою систему шляхів, методів вирішення проблеми підвищення ефективності процесу проектування КІІ, що об’єднує наступні принципи та положення:

1. Чотирирівнева узагальнена структура КІІ.
2. Життєвий цикл КІІ.
3. Загальна схема пошуку проектних рішень щодо архітектури на базі компенсаційно-декомпенсаційного підходу.
4. Виокремлення чотирьох точок зору на архітектуру.
5. Критерій оптимальності проектування КІІ.
6. Виокремлення чотирьох універсальних процесів при проектування КІІ.
7. Використання розширених UML-діаграм для представлення процесу міркувань щодо архітектури.
8. Використання розмічених транзиційних систем та темпоральних логік для формалізації моделей архітектурних проектів та їх верифікації.
9. Використання методів штучного інтелекту для побудови моделей оцінювання та обґрунтування архітектурних проектів.
10. Використання методів штучного інтелекту для побудови моделей вдосконалення критичної інформаційної інфраструктури.
11. Представлення єдиної системи проектування КІІ (ЄСПК) у вигляді замкнутої системи.
12. Інтегроване проектування КІІ.
13. Врахування вимог бізнес-процесів.

Більшість вищезазначених принципів не є новими, але в запропонованій концепції проектування КІІ вони вперше застосовані в сукупності. Крім того, тут не тільки систематизовані відомі методи і технології з подальшою інтеграцією їх в ЄСПК, але і пропонуються оригінальні методи і підходи. Реалізація пропонованої концепції відбувається за допомогою ЄСПК, яка забезпечує централізоване проектування КІІ.

Крім систематизації відомих та пропонованих технологій, однією з основних задач концепції є трансформація процесу мислення архітекторів ЄСПК - відмова від фрагментарного підходу, орієнтованого на проектування окремих елементів та систем КІІ та прийняття системного бачення, що розглядає ЄСПК як цілісну систему, підпорядковану цілям підприємства з критичною інфраструктурою.

Одним з основних елементів концепції проектування КІІ є загальна схема пошуку проектних рішень на базі компенсаційно-декомпенсаційного підходу, яка

представлена на рис. 6.1. Її основне завдання – надати архітектору керівництво до дій по проектуванню архітектури КІІ.

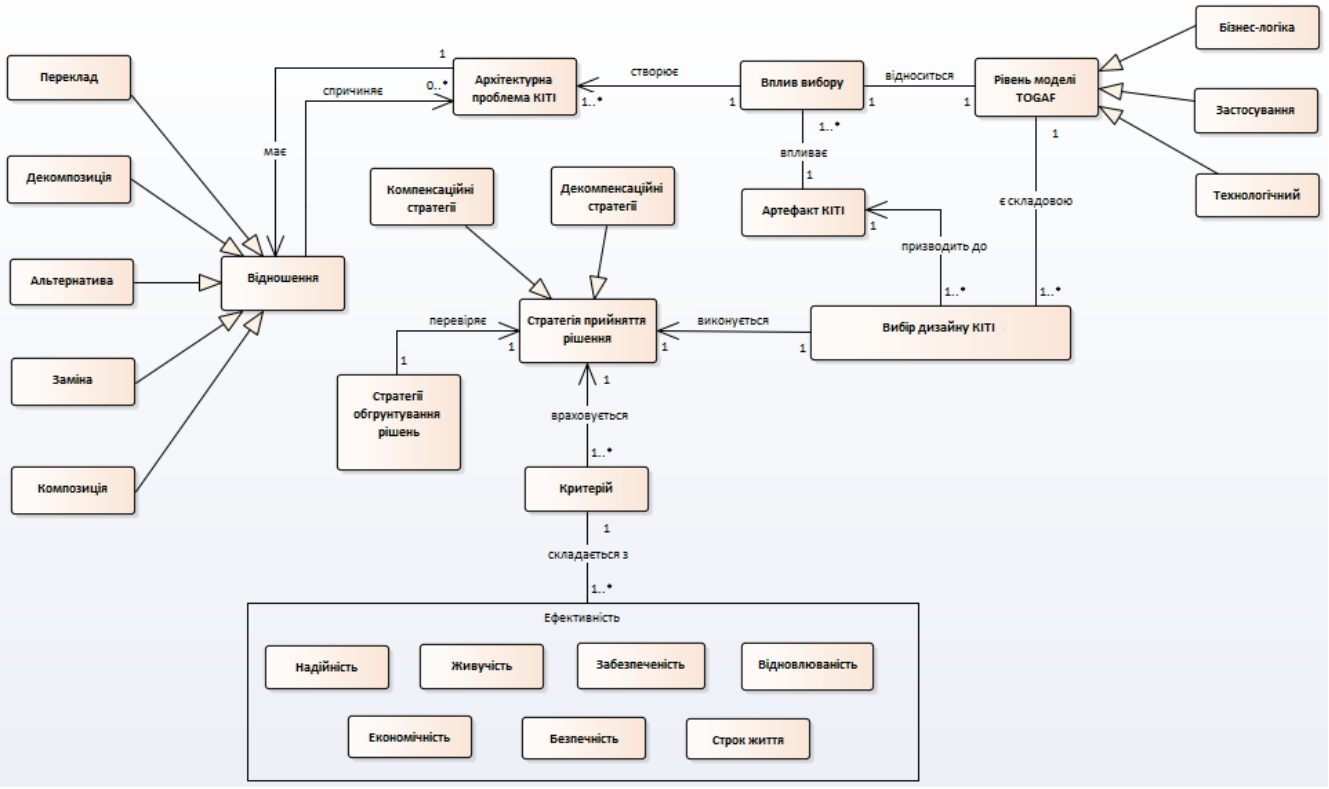

Рисунок 6.1 – Загальна схема пошуку проектних рішень

Самим головним елементом концепції є єдина система проектування критичної інформаційної інфраструктури (ЄСПК), яка включає наступні елементи (рис. 6.2):

– середовище для моделювання Enterprise Architect;
– систему верифікації та перетворення моделей;
– керовану моделлю систему розподілу ресурсів критичної інформаційної інфраструктури;
– систему автоматичного розгортання та управління критичною інформаційною інфраструктурою;
– систему обґрунтування проектних рішень.

Перший елемент ЄСПК використовується для створення розширених UML-моделей проектних рішень та фіксації за їх допомогою всіх міркувань в процесі пошуку оптимальної архітектури конкретних проектних рішень. Даний елемент дозволяє сформувати архітектору конкретні специфікації окремих проектних рішень (компоненти, програмні засоби тощо), отриманих у результаті їх пошуку у відповідності до принципів, критеріїв та підходу, які описані в концепції, а також отримати файл проекту у вигляді XMI, який потім буде використано при автоматичній верифікації моделей проектних рішень.

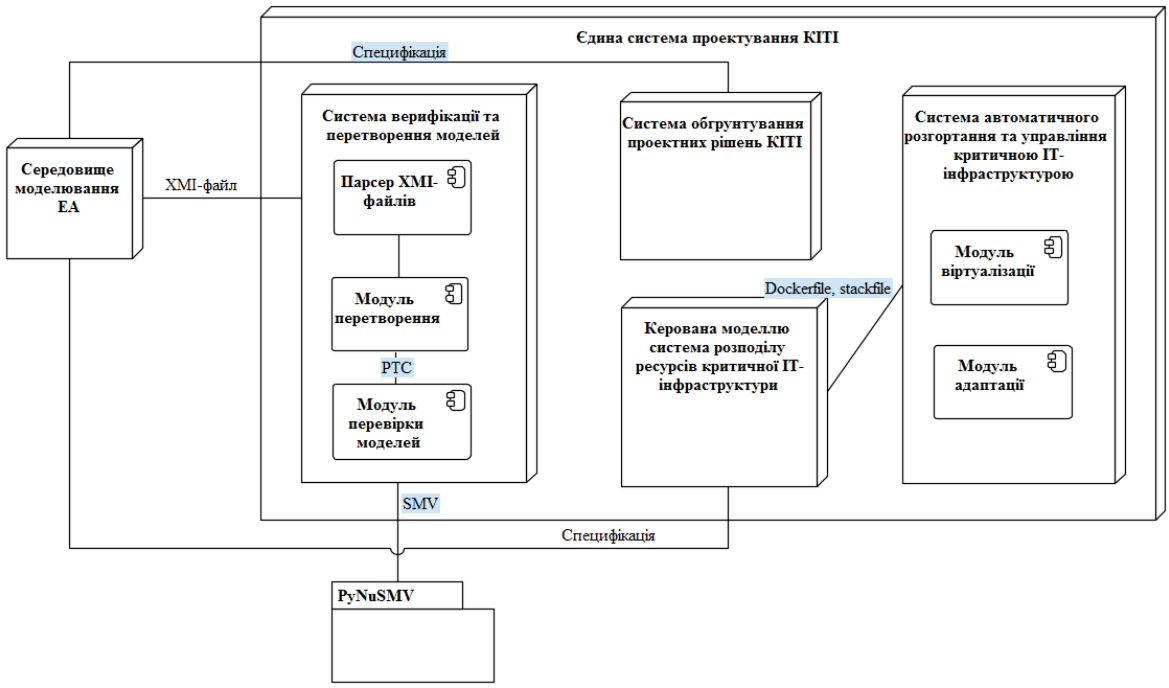

Рисунок 6.2 – Діаграма розгортання ЄСПК

Система верифікації та перетворення моделей включає наступні елементи:

– парсер XMI-файлів;

– модуль перетворення діаграм з XMI-файлів в розмічені транзиційні системи;

– модуль перевірки моделей.

Система дозволяє витягнути з ЕА діаграми у вигляді XMI-файлів та трансформувати їх в нотацію SMV. Після трансформації їх можна перевірити на правильність за допомогою модуля верифікації моделей, створеного на базі пакету PyNuSMV.

Система обгрунтування проектних рішень дозволяє провести дослідження отриманих проектних рішень за варіантами специфікацій з ЕА за допомогою побудованих моделей та визначити оптимальні рішення.

Керована моделлю система розподілу ресурсів критичної інформаційної інфраструктури дозволяє під задану конфігурацію ресурсів та компонент керувати процесом автоматичного розгортання критичної інформаційної інфраструктури. Система розраховує оптимальний варіант розміщення ресурсів та генерує відповідні файли конфігурацій Dockerfile та Stackfile.

Система автоматичного розгортання та управління критичною інформаційною інфраструктурою розгортає відповідно до отриманих Dockerfile та Stackfile фізичну інфраструктуру, запускає відповідні сервіси та управляє нею у відповідності з заданими критеріями.

Керована моделлю система розподілу ресурсів критичної інформаційної інфраструктури має архітектуру типу “клієнт-сервер”. Діаграма розгортання системи наведена на рис. 6.3. Загалом, система складається з двох частин:

1) серверного застосунку, що виконує навчання нейронної мережі та реалізує алгоритм структурної оптимізації;
2) клієнтського застосунку, що реалізує графічний інтерфейс користувача.

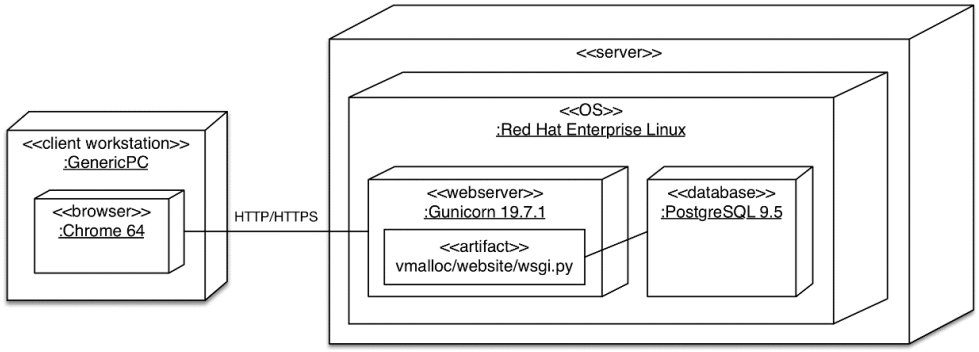

Рисунок 6.3 – Діаграма розгортання системи

Логічно система розділена на 4 компоненти, кожен з яких може бути замінений незалежно один від одного (рис. 6.4). До складу входять:

– головний модуль управління – здійснює аналіз, планування та управління станом критичної IT-інфрастурктури;

– система розрахунку розміщення – здійснює пошук субоптимального розміщення елементів критичної інформаційної інфраструктури за прийнятний час;

– модуль рішення задачі пакування – здійснює пошук субоптимального рішення задачі багатомірного пакування за прийнятних час. Модуль є необхідним для розрахунку розміщення;

– система управління інфраструктурою – здійснює фактичне управління станом об’єктів критичної IT інфраструктури.

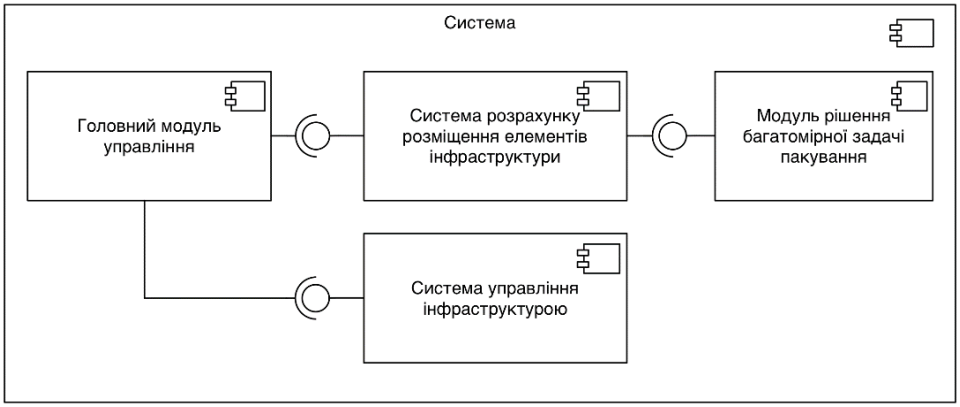

Рисунок 6.4 – Діаграма компонентів системи

ВИСНОВКИ

В дисертаційній роботі вирішена актуальна науково-прикладна проблема, яка полягає в удосконаленні процесів вибору і обґрунтування проектних рішень щодо критичної інформаційної інфраструктури на підставі: використання розширених UML-моделей; розроблених методів представлення процесу прийняття рішень щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, оцінки альтернативних проектних рішень, вибору оптимальної конфігурації компонент критичної інформаційної інфраструктури; методів розвитку критичної інформаційної інфраструктури; подальшого розвитку концепції проектування

критичної інформаційної інфраструктури; створення та застосування єдиної системи проектування критичної інформаційної інфраструктури.

Проведені дослідження дозволили отримати наступні наукові та практичні результати:

1. Досліджено потенційні можливості сучасних фрейворків опису архітектури підприємства та підходів до обґрунтування рішень щодо архітектури при проектуванні КІІ, що дозволило визначити критерій та показники оптимальності проектування та функціонування критичних інформаційних інфраструктур.

2. Розроблено модель перетворення розширених UML-діаграм, які відображають процес прийняття рішення щодо вибору та обґрунтування архітектури критичної інформаційної інфраструктури, в розмічені транзиційні системи. Використання даної моделі дозволяє архітектору застосовувати математичні методи на базі розмічених транзиційних систем для дослідження властивостей проектних рішень, представлених у вигляді розширених UML-діаграм.

3. Сформульовано постановку задачі верифікації параметризованих моделей архітектурних рішень критичної інформаційної інфраструктури в термінах теорій розмічених транзиційних систем та темпоральної логіки, що дозволяє використати в подальшому весь спектр методів та алгоритмів, розроблених для цих теорій, для верифікації/генерації проектних рішень критичної інформаційної інфраструктури.

4. Розроблено метод обґрунтування проектних рішень щодо архітектури критичної інформаційної інфраструктури, в якому для порівняння альтернативних проектних рішень застосовуються множина з трьох показників ризику, що враховують досяжність цілей проектного рішення, можливість його імплементації та дотримання вимог щодо критичності, та ентропійний підхід для оцінювання їх взаємного впливу для задачі проектування критичної інформаційної інфраструктур. Метод дозволяє архітектору обирати найкращий варіант проектного рішення та оцінювати вплив окремих проектних рішень або елементів на інші проектні рішення щодо архітектури критичної інформаційної інфраструктури або на весь дизайн архітектури в цілому. Використання даного методу дозволило врахувати вплив окремих проектних рішень або елементів на інші проектні рішення щодо архітектури при проектуванні єдиної інформаційної системи Міністерства внутрішніх справ України.

5. Розроблено метод проектування критичних інформаційних інфраструктур на базі розширених відкритих гібридних автоматів, який поширює застосування відкритих гібридних автоматів для задачі проектування критичної інформаційної інфраструктури. Застосування методу дозволило при проектуванні ЦОД ЄІС МВС врахувати проблему взаємозалежності телекомунікаційної системи від систем охолодження та електроживлення, і таким чином, якісно продумати резервування відповідних систем.

6. Розроблено метод структурної оптимізації нейронних мереж прямого поширення, який дозволяє отримувати оптимальну для вхідних даних структуру нейронної мережі, що значно підвищує можливості адаптаційного вибору моделей нейронних мереж для розв’язання задач функціонування критичних інформаційних

інфраструктур. Метод перевірено на різних типах вхідних даних та показано його ефективність для розв’язанні окремих класів задач класифікації та розпізнавання.

7. Розроблено та програмно реалізовано метод верифікації даних в інформаційних ресурсах критичної інформаційної інфраструктури, який використовує процеси хешування і може застосовуватися для даних в знеособленому вигляді, що дозволило значно пришвидшити процес верифікації та скоротити кількість невизначених даних в національних електронних інформаційних ресурсах України при проведенні державного експерименту з верифікації даних.

8. Розроблено та програмно реалізовано керовану моделлю систему розподілу ресурсів критичної інформаційної інфраструктури, яка використовує методи оптимізації структури нейронних мереж та оптимізації навантаження критичної інформаційної інфраструктури, що дозволило в автоматичному режимі розподіляти ресурси критичної інформаційної інфраструктури з метою їх оптимального використання та задоволення потреб сервісів та компонент, що їх використовують.

9. Розроблено метод представлення та обґрунтування архітектури критичної інформаційної інфраструктури на основі розширених UML-діаграм, який дозволив спростити та пришвидшити пошук оптимальної архітектури ЄІС МВС, а також надав можливість зберегти всю історію проведених міркувань та обгрунтувань при її виборі.

10. Розроблено та програмно реалізовано метод оцінки та вибору оптимальної конфігурації компонент критичної інформаційної інфраструктури на базі Марківського процесу прийняття рішень, який дозволив оцінити та вибрати оптимальну конфігурацію компонент при проектуванні ЦОД ЄІС МВС України, що дало можливість значно скоротити час на розробку відповідного технічного завдання.

11. Розроблено та програмно реалізовано метод розподілу ресурсів критичної інформаційної інфраструктури на базі генетичного алгоритму з чіткими параметрами, що надає можливість швидко визначити оптимальну схему розподілу ресурсів в центрах обробки даних з врахуванням критичності окремих процесів та сервісів. Даний метод використано для оптимізації розподілення ресурсів в ЦОД ЄІС МВС.

12. Розроблено та програмно реалізовано метод оптимізації навантаження критичної інформаційної інфраструктури, який використовує метод рою часток, що надав можливість швидко визначити оптимальну схему розміщення віртуальних машин та критичних сервісів на них з врахуванням вимог щодо критичності окремих сервісів та процесів, і відповідно, оптимізувати розподіл ресурсів в ЦОД ЄІС МВС.

13. Отримали подальший розвиток концепція проектування критичної інформаційної інфраструктури, типова виробнича архітектура ІТ-інфраструктури, життєвий цикл критичної інформаційної інфраструктури та метод верифікації параметризованих моделей архітектурних рішень критичної інформаційної інфраструктури, що дало можливість створити єдину систему проектування

критичної інформаційної інфраструктури та набір інструментарію, який дозволяє значно прискорити та підвищити ефективність процесів проектування критичної інформаційної інфраструктури.

14. Розроблена єдина система проектування критичної інформаційної інфраструктури впроваджена на підприємстві ДП «ІНФОТЕХ», що дозволило скоротити час проектування ЦОД ЄІС МВС України на 20%.

15. Результати дисертаційного дослідження використані Міністерством внутрішніх справ України при формуванні технічних завдань на ЦОД ЄІС МВС України та функціональних підсистем ЄІС МВС, що дозволило скоротити час на визначення відповідних специфікацій обладнання та програмних компонент на 18%.

16. Впровадження методу пошуку сумнівних записів при виконанні завдання верифікації даних в національних електронних інформаційних реєстрах дозволило Міністерству внутрішніх справ України скоротити час на виконання верифікації на 90% та скоротити кількість невизначених записів в ресурсах до 2%.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії, в яких опубліковані основні наукові результати дисертації:

[1] Я. Дорогий, та В. Цуркан, “Методи представлення та обгрунтування архітектури критичної IT-інфраструктури,” in Engineering sciences: development prospects in countries of Europe at the beginning of the third millennium: Collective monograph, vol. 1, Riga: Izdevnieciba “Baltija Publishing,” 2018, pp. 197–237.

[2] Я. Дорогий, “Моделі і методи представлення архітектурних рішень критичної IT-інфраструктури,” in *Modern engineering research: topical problems, challenges and modernity: Collective monograph*, Riga: Izdevnieciba “Baltija Publishing,” 2020, pp. 127–156, doi: 10.30525/978-9934-588-47-1.7.

Наукові праці, в яких опубліковані основні наукові результати дисертації:

[3] Y. Y. Dorogyy, “Management of Critical It-Infrastructures,” *Inf. Telecommun. Sci.*, №1, с. 10–15, Aug. 2014, doi: 10.20535/2411-2976.12014.10-15.

[4] Я. Дорогий, “Життєвий цикл критичної IT-інфраструктури,” *Електроніка та зв’язок*, Т. 20, №4, с. 100–105, 2015.

[5] Я. Дорогий, “Порівняльний аналіз методів представлення та обгрунтування архітектури критичної IT-інфраструктури,” *Вісник НТУ «ХПІ». Серія Механіко-технологічні системи та комплекси*, Т. 33, №1255, с. 42–54, 2017.

[6] Я. Дорогий, “Мета-модель компенсаційно-декомпенсаційного підходу до проектування архітектури критичної IT-інфраструктури,” *Вісник університету України Інформатика, обчислювальна техніка та кібернетика*, Т.1, №19, с. 170–177, 2017.

[7] Я. Дорогий, “Розробка підходу до проектування, моделювання та дослідження критичної IT-інфраструктури,” *Технологічний аудит та резерви виробництва*, Т. 5, №2(37), с. 34–41, 2017.

[8] Y. Dorogyy, “Development of a model for optimal configuration components selection for architecture of critical IT infrastructure at its designing,” *Технологічний аудит та резерви виробництва*, no. 6/2(38), pp. 19–27, 2017.

[9] Я. Дорогий, “Алгоритм структурної оптимізації нейронної мережі,” *Вісник НТУУ «КПІ», «Інформатика, управління та обчислювальна техніка»*, №61, с. 169–173, 2014.

[10] Я. Дорогий, “ТС-сумісна архітектура критичної ІТ-інфраструктури,” *Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка збірник наукових праць*, №65, с. 123–126, 2017.

[11] Я. Дорогий, “Розподіл ресурсів критичної ІТ-інфраструктури з використанням хмарних технологій,” *Електроніка та зв’язок*, Т. 1, №90, с. 42–49, 2016.

[12] Я. Дорогий, “Технологія пошуку сумнівних записів при створенні єдиного реєстру ідентифікації фізичних осіб України,” *Inf. Technol. Secur.*, Т. 7, №2, с. 114–125, 2019.

[13] Y. Dorogyy, O. Doroga-Ivaniuk, V. Tsurkan, and S. Telenyk, “Comparative analysis of the architecture designing platform for critical it infrastructure,” *Inf. Technol. Secur.*, vol. 5, no. 2, pp. 90–118, 2017.

[14] Я. Дорогий, І. Бондаренко, Т. Шемседінов, та С. Стиренко, “Аналіз проблем побудови критичної ІТ-інфраструктури міністерства,” *Inf. Technol. Secur.*, Т.1, №10, с. 96–107, 2018.

[15] Y. Dorogyy, S. Telenyk, V. Tsurkan, and D. Halushko, “Structural optimization of neural network in qualitative evaluation method of IT-infrastructure functioning,” *Inf. Telecommun. Sci.*, vol. 6, no. 2, pp. 36–43, 2015.

[16] Я. Дорогий, О. Дорога-Іванюк, В. Цуркан, та Д. Ференс, “Застосування алгоритму структурної оптимізації нейронної мережі в задачах класифікації даних,” *Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка збірник наукових праць*, №62, с. 100–104, 2015.

[17] О. Дорога-Іванюк, Я. Дорогий, та Д. Ференс, “Реалізація алгоритму структурної оптимізації нейронної мережі,” *Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка збірник наукових праць*, №63, с. 101–106, 2015.

[18] G. Nowakowski, Y. Dorogyy, and O. Doroga-Ivaniuk, “Neural network structure optimization algorithm,” *J. Autom. Mob. Robot. Intell. Syst.*, vol. 12, no. 1, pp. 5–13, 2018, doi: 10.14313/JAMRIS_1-2018/1. ISSN 1897-8649 (Print) / ISSN 2080-2145 (Online) **(SCOPUS)**

[19] Я. Дорогий, Є. Максименко, О. Крук, та В. Цуркан, “Оцінювання ризику безпеки інформації на основі спектрального підходу,” *Inf. Technol. Secur.*, Т.3, №2(5), с. 138–146, 2015.

[20] Я. Дорогий, В. Мохор, В. Цуркан, та О. Крук, “Функціональне моделювання системи керування ризиком безпеки інформації,” *Захист інформації*, Т.18, №1, с. 74–80, 2016.

[21] Я. Дорогий, О. Бакалинський, О. Богданов, С. Михайлов, В. Цуркан, та В. Мохор, “Використання ентропійного підходу для оцінювання ризиків безпеки інформації,” *Inf. Technol. Secur.*, Т.4, №2(7), с. 255–261, 2016.

[22] Я. Дорогий, Д. Ференс, та О. Дорога-Іванюк, “Модель розподілу ресурсів критичної IT-інфраструктури з чіткими параметрами на основі генетичного алгоритму,” *Inf. Technol. Secur.*, Т.2, №11, с. 124–144, 2018.

[23] Я. Дорогий, Д. Ференс, та О. Дорога-Іванюк, “Модель розподілу ресурсів критичної IT-інфраструктури з чіткими параметрами на основі методу рою часток,” *Електронне моделювання*, Т. 41, №2, с. 1–15, 2019.

[24] А. Йовенко, та Я. Дорогий, “Вибір методу інтеграції розподілених гетерогенних модулів для розробки корпоративних систем,” *Вісник університету України Інформатика, обчислювальна техніка та кібернетика*, Т. 1, №18, с. 14–22, 2016.

[25] Я. Дорогий, В. Мохор, та В. Цуркан, “Концептуальна модель описання архітектури системи управління інформаційною безпекою,” *Безпека інформації*, Т. 25, №3, с. 162–166, 2019.

[26] Я. Дорогий, та В. Цуркан, “Огляд методів верифікації параметризованих моделей,” *Збірник наукових праць Національного університету кораблебудування імені адмірала Макарова*, №1(479), с. 82–91, 2020, doi: https://dpo.org/10.15589/znp2020.1(479).10.

[27] Я. Ю. Дорогий, В. В. Мохор, В. В. Цуркан, та Ю. М. Штифурак, “Структури архітектури систем управління безпекою інформації,” *Інформатика та математичні методи в моделюванні*, т. 9, № 4, с. 209–221, 2019, doi: 10.15276/imms.v9.no4.209.

[28] G. Nowakowski, Y. Dorogyy, and O. Doroga-Ivaniuk, “The realisation of neural network structural optimization algorithm,” in *Annals of Computer Science and Information Systems (ACSIS)*, vol. 11, 2017, pp. 1365–1371. ISSN 2300-5963 **(SCOPUS)**

[29] Д. Ференс, та Я. Дорогий, “Оптимізація розміщення віртуальних машин у хмарних інфраструктурах за допомогою гнучкого алгоритму на базі генетичного програмування,” *Інфокомунікаційні системи та технології*, Т. 1, №1, 2017. ISSN 2520-6257.

[30] К. Левченко, та Я. Дорогий, “Порівняння часу виконання базових операцій фреймворків машинного навчання,” *Інфокомунікаційні системи та технології*, Т. 2, №2, с. 27–31, 2018. ISSN 2520-6257.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

[31] S. Telenyk, O. Rolick, M. Bukasov, Y. Dorogiy, D. Halushko, and A. Pysarenko, “Qualitative evaluation method of IT-infrastructure elements functioning”, in *Proc. 2014 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2014*, 2014, pp. 165–169, doi: 10.1109/BlackSeaCom.2014.6849031. **(IEEE, SCOPUS)**

[32] Y. Dorogyy and K. Valchuk, “Comparison between serialization formats”, in *Collection of Conference Papers of International Scientific-Practical Conference “Problems and Prospects of Intergration of Science and Technology”*, 2015.

[33] Я. Дорогий, І. Козлюк, В. Цуркан, та В. Мохор, “Критична інфраструктура: вразливості, загрози, ризики,” на *II міжн. наук.-практ. конф. «Інформаційні технології та взаємодії»*, 2015.

[34] Я. Дорогий, та О. Дорога-Іванюк, “Критерій оптимальності побудови критичної ІТ-інфраструктури,” на *II-й міжн. наук.-практ. конф. «Актуальні проблеми розвитку науки і техніки»*, 20 грудня, 2015.

[35] Я. Дорогий, Є. Максименко, В. Цуркан, та В. Мохор, “Аналітика кібербезпеки: поняття, структура, задачі,” на *Межд. науч. конф. «ИТБ-2015», 21 октября*, 2015.

[36] О. Дорога-Іванюк, та Я. Дорогий, “Умови створення критичних процесів або сервісів критичної ІТ-інфраструктури”, на *V міжн. наук.-техн. конф. «Проблеми інформатизації», 10-11 грудня*, 2015.

[37] Y. Dorogyy, O. Doroga-Ivaniuk, B. Mart, and V. Tsurkan, “Life cycle of IT-infrastructure”, in *Proc. of The Congress on Information Technology, Computational and Experimental Physics 2015 (CITCEP 2015)*, 2015.

[38] Y. Dorogyy, O. Doroga-Ivaniuk, S. Telenik, and D. Halushko, “Qualitative evaluation method of IT-infrastructure functioning based on structural optimization of neural network”, in *Proc. 2015 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2015 - Conference Proceedings*, 2015, pp. 1–4, doi: 10.1109/INFOCOMMST.2015.7357252. **(IEEE, SCOPUS)**

[39] Д. Ференс, та Я. Дорогий, “Структурна оптимізація штучних нейронних мереж”, на *2-й Міжн. наук.-практ. конф. «Summer Infocom 2016»*, 2016.

[40] Я. Дорогий, О. Крук, В. Цуркан, та В. Мохор, “Процесна модель системи керування ризиком безпеки інформації”, на *V Міжнар. наук.-техн. конф. “Захист інформації і безпека інформаційних систем,”* 2016.

[41] Я. Дорогий, О. Крук, В. Цуркан, та В. Мохор, “Дерево вузлів функціональної моделі системи керування ризиком безпеки інформації”, на *Міжн. наук.-практ. конф. “Безпека інформації в інформаційно-телекомунікаційних системах”, 25-26 травня*, 2016.

[42] Я. Дорогий, О. Крук, В. Мохор, та В. Цуркан, “Модель потоків даних системи керування ризиком безпеки інформації”, на *V-й міжн. наук.-практ. конф. "Кібербезпека інформаційних технологій /// Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах*, 2016.

[43] Я. Дорогий, О. Крук, В. Цуркан, та В. Мохор, “Функціональна модель системи керування ризиком безпеки інформації”, на *II-й міжн. наук.-практ. конф. “Актуальні проблеми моделювання ризиків і загроз виникнення надзвичайних ситуацій на обєктах критичної інфраструктури”*, 2016.

[44] Y. Y. Dorogyy, O. O. Doroha-Ivaniuk, U. Dzelendzyak, and K. Tomczyk, “Usage of structural optimization algorithm of neural nets in problems of data classification,” in *Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2017*, 2017, vol. 2, pp. 983–987, doi: 10.1109/IDAACS.2017.8095234. **(IEEE, SCOPUS)**

[45] Я. Дорогий, “Проектування критичних IT-інфраструктур з використанням розмічених транзиційних систем,” на *V заочн. науч. конф. «Фундаментальные и прикладные исследования в современной науке», 31 октября*, 2017.

[46] Я. Дорогий, “Моделювання критичних IT-інфраструктур з використанням розмічених транзиційних систем”, на *VI Міжн. наук.-практ. конф. (I Міжнародний симпозіум «Практичне застосування нелінійних динамічних систем в інфокомунікаціях»), PREDT-2017, 9-11 листопада*, 2017.

[47] Я. Дорогий, О. Дорога-Іванюк, та В. М. В. Цуркан, “Cyber resilience: the concept of information security in cyberspace,” на *III-й міжн. наук.-практ. конф. «Актуальні питання забезпечення кібернетичної безпеки та захисту інформації»*, 2017.

[48] Y. Dorogyy, “Meta model of compensatory-decompensational approach for architecture of critical it infrastructure designing,” in *Proc. 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 - Proceedings*, 2018, vol. 2018-April, pp. 223–228, doi: 10.1109/TCSET.2018.8336191. **(IEEE, SCOPUS)**

[49] Я. Дорогий, В. Мохор, та В. Ц. Ю. Штифурак, “Моделі оцінювання ризику кібербезпеки”, на *VII-й Міжн. наук.-практ. конф. «Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах (PREDT-2018)», 8-10 листопада*, 2018.

[50] А. Горносталь, та Я. Дорогий, “Мурашиний алгоритм кластеризації,” на *XI-й Міжн. наук.-практ. конф. "ІНТЕРНЕТ-ОСВІТА-2018*, 2018.

[51] Я. Дорогий, та К. Левченко, “Порівняння фреймворків машинного навчання”, на *VI-й Міжн. наук.-практ. конф. з інформ. сист. та техн. «Summer InfoCom 2018»*, 2018.

АНОТАЦІЯ

Дорогий Я.Ю. Методі підвищення ефективності процесів проектування критичної інформаційної інфраструктури. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.05 – комп’ютерні системи та компоненти. − Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2021.

Розробка математичних та комп’ютерних моделей процесів проектування та функціонування критичної інформаційної інфраструктури відноситься до числа складних проблем як в теоретичному, так і практичному плані, через те, що опис

об'єкта здійснюється в динамічному режимі з урахуванням оцінки показників всіх її елементів.

З огляду на це, актуальними, в науковому та практичному аспектах, є:

– проблема пошуку нових підходів до проектування критичних інформаційних інфраструктур, які б системно враховували всю множину зазначених вище факторів, і можливості засобів, які входять до їх складу;

– проблема розробки і розвитку методів моделювання та підтримки прийняття рішень в критичній інформаційній інфраструктурі та розробка на їх основі єдиної системи проектування, що дозволяє проектувати, аналізувати, розвивати критичну інформаційну інфраструктуру та підтримувати гарантований рівень якості критичних ІТ-сервісів і процесів, синхронно зі змінами в ній.

На основі аналізу основних існуючих підходів до вирішення поставленої проблеми показано, що створення нових методів та моделей є актуальним завданням для подолання виявлених проблем і вимагає використання відповідних інформаційних технологій для їх вирішення. Таким чином, для досягнення поставленої мети в роботі отримано цілий ряд наукових результатів.

Ключові слова: єдина система проектування, критична інформаційна інфраструктура, керована моделлю система розподілу ресурсів, оптимізація структури, архітектура, нейронна мережа, оптимізація навантаження, розподіл ресурсів.

АННОТАЦИЯ

Дорогий Я.Ю. Методы повышения эффективности процессов проектирования критической информационной инфраструктуры. – На правах рукописи.

Диссертация на соискание ученой степени доктора технических наук по специальности 05.13.05 – компьютерные системы и компоненты. – Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, Киев, 2021.

Разработка математических и компьютерных моделей процессов проектирования и функционирования критической информационной инфраструктуры относится к числу сложных проблем как в теоретическом, так и практическом плане, потому что описание объекта осуществляется в динамическом режиме с учетом оценки показателей всех ее элементов.

Учитывая это, актуальными, в научном и практическом аспектах, являются:

– проблема поиска новых подходов к проектированию критических информационных инфраструктур, которые системно учитывали все множество указанных выше факторов и возможности средств, входящих в их состав;

– проблема разработки и развития методов моделирования и поддержки принятия решений в критической информационной инфраструктуре и разработка на их основе единой системы проектирования, позволяет проектировать, анализировать, развивать критическую информационную инфраструктуру и поддерживать гарантированный уровень качества критических ИТ-сервисов и процессов, синхронно с изменениями в ней.

На основе анализа основных существующих подходов к решению поставленной проблемы показано, что создание новых методов и моделей является актуальной задачей для преодоления выявленных проблем и требует использования соответствующих информационных технологий для их решения. Таким образом, для достижения поставленной цели в работе получено целый ряд научных результатов.

Ключевые слова: единая система проектирования, критическая информационная инфраструктура, управляемая моделью система распределения ресурсов, оптимизация структуры, архитектура, нейронная сеть, оптимизация нагрузки, распределение ресурсов.

ABSTRACT

Dorogyy Y.Y. Methods for improving critical information infrastructure design processes. – As the manuscript.

Dissertation for obtaining a scientific degree of Doctor of Technical Sciences in specialty 05.13.05 – computer systems and components. – Pukhov Institute for Modelling in Energy Engineering of the NAS of Ukraine, Kyiv, 2021.

The development of mathematical and computer models for the processes of designing and operating a critical information infrastructure is one of a number of complex problems, both theoretically and practically, due to the fact that the description of the object is dynamically taking into account the evaluation of all its elements. In this regard, relevant in scientific and practical aspects are:

– the problem of finding new approaches to the design of critical information infrastructures that would systematically take into account the whole set of factors mentioned above and the capabilities of the tools that make up them;

– the problem of designing and developing methods for modeling and supporting decision-making in critical information infrastructure and developing on their basis a single system of design that allows to design, analyze, develop critical information infrastructure and maintain the guaranteed quality level of critical IT services and processes, synchronously with changes in it.

Based on the analysis of the main existing approaches to solving the problem, it is shown that the creation of new methods and models is an urgent task for overcoming the identified problems and requires the use of appropriate information technologies to solve them. Thus, a number of scientific results were obtained in order to achieve this goal.

A method for substantiating design decisions on critical information infrastructure architecture based on entropy approach is proposed and developed which extends the use of an entropy risk assessment approach to the critical information infrastructure design task, which allowed for the impact of individual design decisions or elements on other architectural design decisions when designing a unified MIA information system.

A method of designing critical information infrastructures based on advanced open hybrid automata is proposed and investigated, which extends the use of open hybrid automata for the task of designing a critical information infrastructure, which allowed in the design of data center of a unified information system of the Ministry of Internal Affairs

to consider the problem of interconnection and interdependence of power systems way, think carefully about the backup of the respective systems.

The proposed and investigated method of structural optimization of neural networks, which generalizes the known methods, greatly expands the set of atomic operations over the neural network and allowed to obtain the optimal structure of the neural network for input data in the construction of models of resource allocation of critical information infrastructure.

The proposed and implemented method of verification of data in critical information infrastructure resources, which uses hashing processes and can be applied to data in the impersonal form, which allowed to significantly speed up the verification process and reduce the amount of uncertain data in the national electronic information resources of Ukraine when conducting a state experiment data.

A model-driven system for critical information infrastructure resource allocation that utilizes methods of optimizing neural network structure and optimizing critical information infrastructure load has been proposed and implemented, allowing automatic allocation of critical information infrastructure resources to optimally utilize and satisfy server needs that they use.

A method of presenting and substantiating the architecture of critical information infrastructure was proposed and developed, which allowed to present the decision-making process for the selection and justification of the architecture of critical information infrastructure by means of extended UML diagrams, which greatly simplified and accelerated the search for the optimal architecture of a unified information system of Ukraine it also provided an opportunity to accumulate a history of reasoning and justification for its choice.

A method of estimating and selecting the optimal configuration of critical information infrastructure components based on the Markov decision-making process was proposed and implemented, which allowed to evaluate and select the optimal configuration of components in the design of the data center of the unified information system of the Ministry of Internal Affairs of Ukraine, which made it possible to significantly reduce the time to develop the relevant technical task.

A clear and well-defined critical information infrastructure resource allocation method is proposed, which utilizes a neural network structure optimization method that has made it possible to quickly determine the optimal resource allocation scheme in data centers, taking into account the criticality of individual processes and services, and accordingly optimize resource allocation Data Center of the unified MIA information system.

A method for optimizing the load of critical information infrastructure is proposed and implemented, which uses the particle swarm method, which allowed to quickly determine the optimal layout of virtual machines and critical services on them, taking into account the requirements for criticality of individual services and processes, and, accordingly, to optimize the distribution of resources in the data center unified MIA information system.

The concept of critical information infrastructure design, typical industrial IT architecture, the life cycle of critical information infrastructure and the method of

verification of parameterized models of architectural solutions of critical information infrastructure were further developed, which allowed to create a unified system of critical infrastructure design, which can significantly accelerate and increase the efficiency of the critical information infrastructure design process.

Keywords: unified design system, critical information infrastructure, model-driven resource allocation system, structure optimization, architecture, neural network, load optimization, resource allocation.