DOI 10.15276/imms.v16.no1.181
УДК 004.9:35.077.6

Informatics and Mathematical Methods in Simulation
Vol.16 (2026), No. 1, pp. 181-196

ЕКСПЕРЕМЕНТАЛЬНИЙ СТЕНД РЕІНЖИНІРІНГУ ЦИФРОВИХ ПУБЛІЧНИХ СЕРВІСІВ: АРХІТЕКТУРА, ДАНІ, РЕЗУЛЬТАТИ

Ю.Є. Хохлачова[1], Ю.І. Хавікова[1],
Д.О. Черкаський[2], Н.С. Зубченко[3], Д.О. Переметчик[3]

[1]Державний торговельно-економічний університет
19, Кіото вул., Київ, 02156, Україна
[2]Національний технічний університет Дніпровська політехніка
19,. Дмитра Яворницького пр., Дніпро, 49005, Україна
[3]Університет митної справи та фінансів
2/4,. В. Вернадського вул, Дніпро, 49000, Україна,
Emails: yuliiahohlachova@gmail.com, pirogova0303@gmail.com,
Cherkaskyi.Dav.O@nmu.one, nazik3110@gmail.com, peremetchyk.d@gmail.com.

Цифровізація публічних сервісів із переходом до комплексних платформ електронних послуг супроводжується необхідністю системного реінжинірингу бізнес-процесів та архітектури інформаційних систем. Традиційні підходи до реінжинірингу, що спираються переважно на експертне моделювання, виявляються недостатніми для масштабних та високо пов'язаних екосистем державних е-послуг. У роботі запропоновано архітектуру експериментального стенду для тестування нейромережевих і алгоритмічних моделей реінжинірингу цифрових публічних сервісів. Стенд поєднує фізичну інфраструктуру на базі віртуалізованого кластеру з контейнеризованими сервісами, модулі генерації навантаження та атак, підсистему агрегації та анонімізації журналів подій, а також середовище оркестрації експериментів. Описано синтетичні та реальні набори даних, що відтворюють типові сценарії роботи порталів е-послуг, шини даних, державних реєстрів та мобільних застосунків. Наведено формальні моделі оцінювання якості реінжинірингу за інтегральними індексами продуктивності, надійності, ризику та витрат. Розглянуто сценарії порівняння правила-орієнтованих, імітаційних, нейромережевих (включно з CNN+LSTM і AE+LSTM для аналізу журналів подій) та гібридних підходів. Подано результати експериментів із варіюванням архітектурних рішень, параметрів навантаження та політик масштабування сервісів, а також аналіз чутливості інтегральних показників до обраної стратегії реінжинірингу. Показано, що використання експериментального стенду дає змогу досягти зниження середнього часу обробки запиту е-послуги на 18–32 % та скорочення ризику збоїв під час пікових навантажень на 25–40 % порівняно з традиційними підходами. Сформульовано практичні рекомендації щодо поетапного впровадження алгоритмічно підтриманого реінжинірингу у відомчих і міжвідомчих цифрових платформах.

Ключові слова: електронні публічні послуги, реінжиніринг бізнес-процесів, експериментальний стенд, кластер мікросервісів, журнали подій, нейромережеві моделі, CNN+LSTM, AE+LSTM, імітаційне моделювання, інтегральний індекс якості, цифрові платформи.

Вступ. Цифровізація критичної інфраструктури та масове розгортання сервісних платформ поверх мереж електронних комунікацій кардинально змінили характер сучасних загроз. У межах гібридних кібератак противник поєднує мережеві, прикладні та соціотехнічні вектори впливу, цілеспрямовано експлуатуючи вразливості стеку протоколів, сервісних композицій і бізнес-процесів, що реалізуються поверх телекомунікаційної інфраструктури. У цих умовах класичні підходи до проєктування та експлуатації платформ електронних послуг, орієнтовані лише на функціональну коректність і базову надійність, виявляються недостатніми: потрібні формалізовані моделі ризику, засоби інтелектуального аналізу логів і трафіку, а також інтеграція з системами виявлення та реагування на інциденти (Intrusion Detection System, IDS;

Security Information and Event Management, SIEM) у парадигмі Zero Trust. Технічним підґрунтям сучасних платформ е-послуг і галузевих цифрових сервісів є композиції розподілених сервісів та мікросервісів. Роботи з оптимізації витрат на сервісні композиції [1] показують, що вже на рівні «мирного» функціонування виникає складна багатокритеріальна задача балансування продуктивності, доступності та вартості ресурсів. У поєднанні з результатами емпірично обґрунтованих референтних архітектур [6] це формує основу для формального опису сервісної частини мереж електронних комунікацій, які стають мішенню гібридних кібератак. У публічному секторі та smart-city платформах, де такі композиції пов'язані з бізнес-процесами надання послуг, до технічних факторів додаються регуляторні та організаційні обмеження [4,5,11].Для верифікації поведінки сервісних платформ у реальних умовах активно розвиваються підходи до перевірки відповідності моделей історичним журналам подій (replaying history) [2]. Вони дають змогу оцінювати, наскільки формально змодельовані процеси відповідають фактичним сценаріям роботи користувачів і систем, що особливо важливо при моделюванні наслідків складних атак, таких як firmware-компрометація мережевого обладнання з подальшим втручанням у SSL-/TLS-трафік чи експлуатація слабкостей SNMP у системах моніторингу. Застосування таких механізмів у контурі телеком-мереж дає можливість програвати як штатні, так і атакувальні сценарії, виявляючи приховані точки відмови та аномальні маршрути трафіку.Окремий блок досліджень становить процес-майнінг, який розглядає журнали подій як первинне джерело істини щодо бізнес-процесів та сервісних сценаріїв [7]. У поєднанні з класичними підходами системного аналізу й проєктування інформаційних систем [10,11] він дає інструментарій для автоматичного відновлення фактичних процесів у розподілених платформах та побудови їхніх формальних моделей. Це критично для мереж електронних комунікацій, де логіка маршрутизації запитів, поведінка балансувальників навантаження, політики повторних спроб і тайм-аутів часто задаються конфігураціями, що еволюціонують у часі та важко піддаються ручному аналізу.

Зростання обсягів мережевих і сервісних логів переводить задачі моніторингу та кіберзахисту в площину «великих даних». Огляд [12] підкреслює, що для таких середовищ ключову роль відіграють масштабовані платформи збирання, зберігання та потокової обробки даних, здатні працювати з високошвидкісними потоками подій. На цьому тлі глибоке навчання для виявлення аномалій [3] стає одним з базових інструментів моделювання аномальної активності в мережах електронних комунікацій, зокрема в контексті змішаних (граничних) режимів, коли бізнес-логіка сервісів і мережевий рівень одночасно зазнають цілеспрямованого впливу. Архітектури класу LSTM-мереж для класифікації часових рядів [8] природно застосовувати до послідовностей мережевих пакетів, записів IDS/SIEM та трасування мікросервісних викликів, тоді як глибокі залишкові мережі [13] можуть бути залучені для аналізу складних візуалізацій або перетворень даних (наприклад, Byte2Image-представлень трафіку чи логів).Роботи, присвячені ефекту «хвоста у масштабі» [14], демонструють, що в розподілених сервісних архітектурах саме рідкісні, але дуже повільні транзакції визначають сприйняття якості сервісу користувачами та стійкість системи в цілому. Для мереж електронних комунікацій, що працюють в умовах гібридних кібератак, це означає необхідність моделювання не тільки середніх показників, але й крайових сценаріїв, пов'язаних із вибірковим уповільненням чи блокуванням критичних потоків. Додатково, роботи з приватності траєкторій руху користувачів [9] вказують на фундаментальні обмеження анонімізації даних у середовищах, де навіть часткові спостереження можуть бути пов'язані з конкретними абонентами чи вузлами мережі, що створює додаткові виклики для побудови навчальних вибірок для систем виявлення атак.

Аналіз досліджень і публікацій. Таким чином, наявний масив досліджень охоплює: оптимізацію сервісних композицій [1], верифікацію моделей за історією подій [2], глибоке навчання для виявлення аномалій [3,8,13], концептуальні основи «розумних

міст» [4], класичні підходи до зміни бізнес-процесів [5,11], проєктування референтних архітектур [6], методологію процес-майнінгу [7], питання приватності в епоху великих даних [9,12] та проблематику масштабованості розподілених систем [14]. Разом вони формують теоретичне й методичне підґрунтя для побудови моделей мереж електронних комунікацій як багаторівневих сервісно-орієнтованих екосистем, але ще не дають завершеної відповіді на питання, як саме інтегрувати ці підходи в єдиний ризик-орієнтований контур протидії гібридним кібератакам. У низці сучасних робіт запропоновано використовувати експериментальні стенди та тестові платформи для відтворення реальної архітектури цифрових сервісів, генерації навантаження, ін'єкції відмов і збору багаторівневих журналів подій. Такі стенди дають змогу порівнювати традиційні, rule-based та нейромережеві підходи до оптимізації архітектури й бізнес-процесів, включно з моделями класу CNN+LSTM і AE+LSTM для аналізу логів та прогнозування інтегральних показників якості [3,8]. Водночас у більшості випадків вони орієнтовані на реінжиніринг цифрових публічних сервісів загального призначення та не враховують специфіку гібридних кібератак на мережі електронних комунікацій, де важливу роль відіграють протокольні вразливості, прошивкові атаки та взаємодія з доменно-специфічними системами моніторингу. Виявлений розрив між: (i) розвиненою теорією сервісних архітектур, процес-майнінгу та глибинного аналізу аномалій [1–3,7,8,10–13], (ii) зростаючою складністю мереж електронних комунікацій у smart-city та державних платформах [4,5,11] і практичними вимогами до кіберстійкості в умовах гібридної війни та високоризикових сценаріїв [14] обумовлює актуальність побудови інтегрованої методології моделювання таких мереж. У межах цієї роботи пропонується розглядати мережу електронних комунікацій як багаторівневу систему, в якій моніторинг та аналіз здійснюються в єдиному контурі IDS/SIEM із застосуванням глибоких моделей CNN+LSTM, AE+LSTM та перетворень Byte2Image для уніфікованої обробки мультимодальних даних (трафік, логи, телеметрія).

Метою подальшого дослідження є розроблення ризик-орієнтованої моделі мереж електронних комунікацій в умовах гібридних кібератак, яка інтегрує сервісні, мережеві та процесні рівні, забезпечує формальне оцінювання вразливостей (зокрема в SSL-/TLS- та SNMP-контексті firmware-атак), а також підтримує концепцію Zero Trust через тісну взаємодію з IDS/SIEM та нейромережевими моделями аналізу аномалій. Для досягнення зазначеної мети необхідно: систематизувати існуючі підходи до аналізу сервісних платформ і мережевих журналів [1–14]; сформувати багаторівневу математичну модель ризику; запропонувати архітектуру інтегрованого моніторингово-аналітичного контуру та продемонструвати її ефективність на експериментальному стенді з використанням глибоких моделей CNN+LSTM, AE+LSTM і перетворень Byte2Image.

Методологія та архітектура експериментального стенду

Методологічні засади дослідження спрямовані на побудову цілісного ризик-орієнтованого контуру моделювання мереж електронних комунікацій в умовах гібридних кібератак. На відміну від класичних підходів, що аналізують мережевий та сервісний рівні окремо, у цій роботі мережа розглядається як багаторівнева кіберфізична система, де взаємодіють інфраструктурні компоненти, сервіси електронних послуг, підсистеми безпеки (IDS, SIEM) та організаційні бізнес-процеси. Методологія поєднує системний, процес-майнінговий і машинно-навчальний підходи, ґрунтуючись на результатах оптимізації сервісних композицій, процес-майнінгу та глибинного виявлення аномалій [1–3,7,8,12–14]. У рамках запропонованого підходу мережа електронних комунікацій абстрагується у вигляді багаторівневої моделі, що охоплює: (i) інфраструктурний рівень (маршрутизатори, комутатори, шлюзи доступу, включно з вузлами, потенційно ураженими firmware-атаками на рівні SSL/TLS та SNMP); (ii) сервісний рівень (платформи е-послуг, API-шлюзи, мікросервіси бізнес-логіки); (iii) рівень моніторингу та безпеки (IDS, SIEM, телеметрія); (iv) аналітичний рівень, де реалізуються моделі оцінювання ризику та глибинні нейромережі. Для кожного рівня

визначаються релевантні показники продуктивності, доступності, ризику, а також точки збору первинних даних (трафік, журнали подій, агреговані метрики).Ключовим елементом методології є побудова експериментального стенду, який відтворює типову архітектуру мережі електронних комунікацій з інтегрованим контуром IDS/SIEM та підтримкою сценаріїв гібридних атак. Стенд дозволяє: генерувати контрольовані профілі легітимного навантаження; ін'єктувати складені сценарії атак (у тому числі firmware-модифікації, експлуатацію вразливостей SSL і SNMP); збирати багатомодальні дані; тестувати альтернативні стратегії захисту та конфігурації мережі. Логіка його побудови спирається на попередні напрацювання зі створення стендів реінжинірингу цифрових публічних сервісів, адаптовані до специфіки мережевого рівня та кіберзахисту. На аналітичному рівні методологія передбачає використання ансамблю глибинних моделей: CNN+LSTM для аналізу послідовностей пакетів і подій, AE+LSTM для побудови латентних представлень нормальної поведінки та виявлення відхилень, а також перетворень Byte2Image для уніфікованого представлення трафіку й логів у формі зображень, придатних для обробки згортковими мережами. Ці моделі інтегруються у ризик-орієнтовану математичну схему, у якій ризик визначається як функція ймовірності успішної реалізації гібридної атаки та очікуваних втрат на різних рівнях мережі.Таким чином, методологія дослідження поєднує: (1) багаторівневе моделювання мережі; (2) експериментальний стенд для відтворення гібридних атак; (3) єдиний контур збору та попередньої обробки даних; (4) ансамбль глибинних моделей CNN+LSTM, AE+LSTM, Byte2Image для виявлення аномалій; (5) формалізовані ризик-орієнтовані показники для порівняння альтернативних конфігурацій та стратегій захисту. У наступних підрозділах детально описано архітектуру стенду, використовувані набори даних, математичні моделі ризику та процедури навчання й оцінювання нейромережевих моделей.

Загальна структура стенду. Архітектура експериментального стенду поділена на чотири взаємопов'язані рівні:

1. *Інфраструктурний рівень* – фізичні сервери, мережеве обладнання, система віртуалізації та сховища.
2. *Рівень сервісів е-послуг* – контейнеризовані мікросервіси, API-шлюзи, модулі автентифікації, емулятори державних реєстрів.
3. *Аналітичний рівень* – модулі збору журналів подій, сховище даних, засоби процес-майнінгу та аналітичні ядра (нейромережеві й алгоритмічні моделі).
4. *Рівень оркестрації експериментів* – планувальник сценаріїв, генератор навантаження, конфігураційний менеджер, візуалізація результатів.

Логічну схему архітектури стенду можна описати як сукупність кластеру контейнерів, об'єднаних віртуальною мережею, з точки зору якої він відтворює типовий контур цифрової платформи електронних послуг: фронт-енд порталу, сервіс шини подій, кілька сервісів бізнес-логіки, імітовані реєстри та зовнішні сервіси (платіжні шлюзи, системи ідентифікації), а також підсистему телеметрії.

Наведені схеми візуалізують чотирирівневу архітектуру експериментального стенду реінжинірингу цифрових публічних сервісів і деталізують взаємодію між інфраструктурою, сервісами е-послуг, аналітичними модулями та рівнем оркестрації експериментів. Усі три фрагменти разом відображають замкнений цикл «експлуатація – моніторинг – аналіз – експеримент – зворотна адаптація», у межах якого відтворюються реалістичні профілі навантаження, збираються журнали подій, запускаються моделі CNN+LSTM та AE+LSTM, а результати оцінювання інтегральних показників якості повертаються до дослідника для прийняття рішень щодо реінжинірингу.

Перший фрагмент (рис. 1) візуалізує операційний контур експериментального стенду й поєднує два ключові рівні: інфраструктурний та рівень сервісів е-послуг.

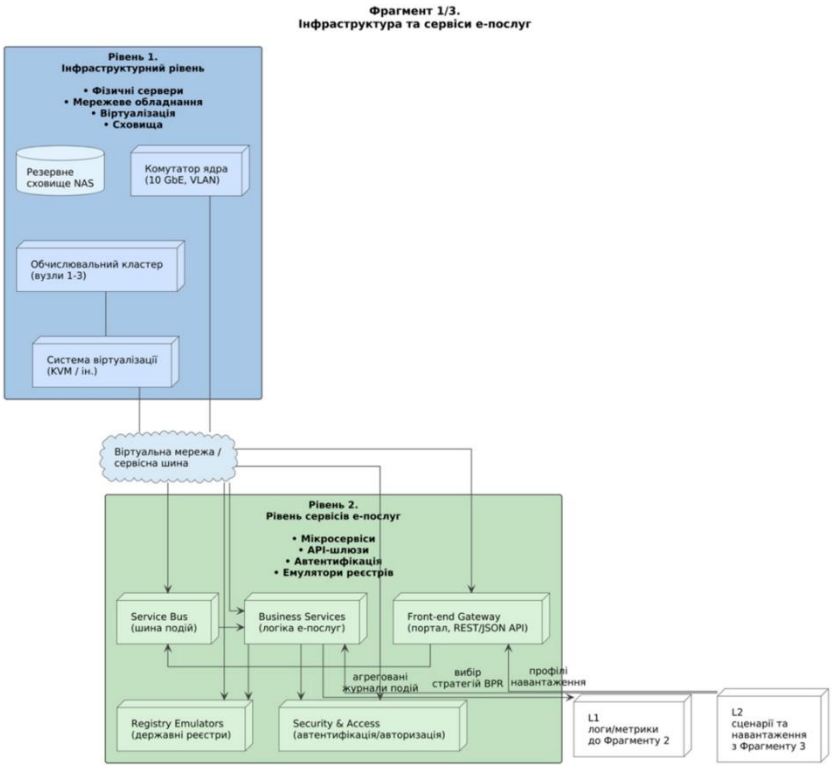

Рис.1. Перший фрагмент

Ліва синя область відображає фізичну й віртуальну інфраструктуру, на якій розгортаються всі сервіси: резервне сховище NAS, обчислювальний кластер з вузлами 1–3, систему віртуалізації (KVM та інші гіпервізори) і комутатор ядра з підтримкою 10 GbE та VLAN. Така конфігурація дозволяє відокремлювати експериментальні середовища, моделювати відмови вузлів і мережеві аномалії, а також забезпечує необхідний запас продуктивності під час навантажувальних тестів.Між інфраструктурою та прикладними сервісами розташовано логічний елемент «Віртуальна мережа / сервісна шина», який відповідає за маршрутизацію трафіку між компонентами, сегментацію доменів безпеки й інжекцію тестових сценаріїв атак. Саме на цьому рівні можуть моделюватися вразливості протоколів SSL/TLS і SNMP, помилки конфігурації мережевого обладнання, а також наслідки firmware-компрометації, що є характерними для гібридних кібератак на державні е-послуги. Зелена область відображає рівень сервісів е-послуг, де реалізовано мікросервісну архітектуру платформи. Компонент Service Bus виконує роль шини подій, забезпечуючи асинхронний обмін повідомленнями між сервісами. Business Services містить предметно-орієнтовану логіку е-послуг (обробка заяв, перевірки, зміна статусів), тоді як Front-end Gateway інкапсулює вебпортал і REST/JSON-API, через які користувачі й зовнішні системи взаємодіють із платформою. Такий поділ дає змогу гнучко перебудовувати маршрути обробки запитів і тестувати альтернативні стратегії реінжинірингу.У нижній частині фрагмента показано Registry Emulators та модуль Security & Access. Емулятори державних реєстрів забезпечують відтворення реалістичних затримок, відмов і обмежень доступу, характерних для інтеграції з зовнішніми інформаційними системами. Security & Access реалізує механізми автентифікації та авторизації користувачів і сервісів, зокрема сценарії Zero Trust, коли кожен запит перевіряється незалежно від розташування клієнта. Це дозволяє досліджувати вплив політик безпеки на затримки, надійність і стійкість до атак.Блоки L1 і L2 фіксують точки зв’язку першого фрагмента з іншими рівнями стенду. Через L1 передаються журнали подій і метрики до аналітичного рівня, де вони накопичуються в Data Lake і обробляються моделями процес-майнінгу та ML/NN. Через

L2, навпаки, з рівня оркестрації надходять сценарії й профілі навантаження, що визначають інтенсивність і структуру запитів. Таким чином, перший фрагмент формує «фізичне» й сервісне середовище, в якому реалізуються експерименти з реінжинірингу та кіберстійкості е-послуг.

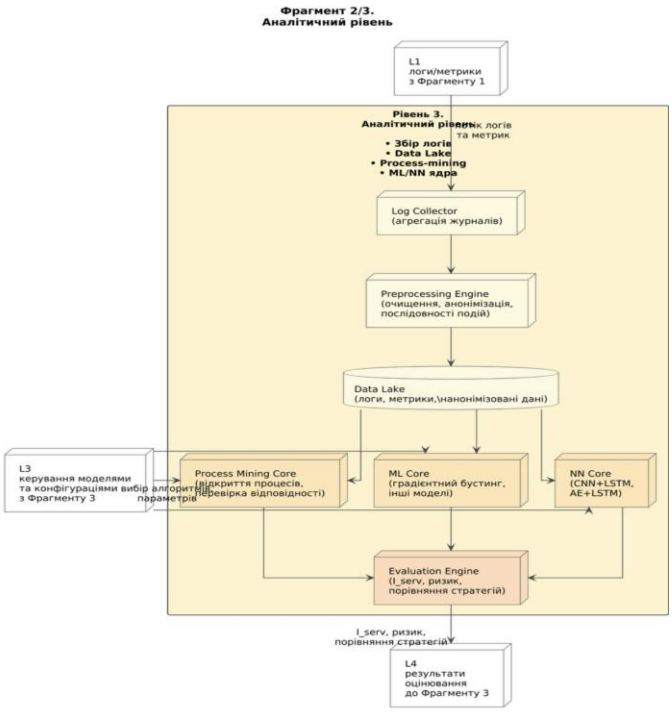

Рис. 2. Другий фрагмент

Другий фрагмент (рис. 2) деталізує аналітичний рівень, у межах якого відбувається збір, зберігання та інтелектуальна обробка логів і метрик. У верхній частині показано вхідний блок L1, через який надходять журнали та метрики з операційного контуру (Фрагмент 1/3). Вони потрапляють до модуля Log Collector, що агрегує події з мікросервісів, API-шлюзів, черг повідомлень, баз даних та систем моніторингу.Далі ланцюжок обробки включає Preprocessing Engine (очищення, анонімізація, побудова послідовностей подій) та Data Lake, де зберігаються сировинні логи, а також нормалізовані, анонімізовані набори даних для процес-майнінгу та навчання моделей. На основі цих даних працюють три аналітичні ядра: Process Mining Core (відкриття процесів і перевірка відповідності), ML Core (традиційні ML-моделі, зокрема градієнтний бустинг) і NN Core, в якому реалізовано глибинні архітектури CNN+LSTM, AE+LSTM і перетворення Byte2Image для аналізу мультимодальних даних (трафік, журнали, телеметрія).

У нижній частині фрагмента показано Evaluation Engine, що обчислює інтегральні індекси якості, ризику та витрат, формує порівняльні метрики для різних стратегій реінжинірингу. Блок L3 відображає канал керування з боку оркестраційного рівня: через нього з Фрагмента 3/3 надходять команди щодо вибору моделей, конфігурацій та параметрів (наприклад, яку архітектуру CNN+LSTM активувати, який поріг аномалії встановити, які сценарії процес-майнінгу виконувати). Вихідний блок L4 передає до рівня оркестрації узагальнені результати оцінювання (значення I_serv, ризикові та порівняльні метрики), які далі використовуються для візуалізації й прийняття рішень.

Третій фрагмент (рис. 3) описує рівень оркестрації експериментів, який замикає цикл управління та забезпечує інтерактивну роботу дослідника зі стендом. У рожевій області розміщено модулі Dashboard, Scenario Manager, Load Generator, Experiment Controller та Config Manager. Dashboard виконує роль центру візуалізації: сюди надходять результати оцінювання з аналітичного рівня через блок L4 (I_serv, ризикові й порівняльні метрики), які відображаються у вигляді графіків, таблиць та індикаторів у режимі, наближеному до реального часу.

Рис.3. Третій фрагмент

Scenario Manager відповідає за опис сценаріїв реінжинірингу й експериментів (A/B/C-сценарії, альтернативні стратегії BPR, конфігурації архітектур). Load Generator формує профілі навантаження A1–A3 та інші стрес-сценарії, на основі яких генеруються запити до платформи е-послуг.Experiment Controller координує запуск і зупинку експериментів, синхронізує зміну навантаження, перемикання конфігурацій та активацію відповідних моделей на аналітичному рівні. Через блок L3 він передає до Фрагмента 2/3 команди керування моделями та конфігураціями (вибір алгоритмів, гіперпараметрів, режимів роботи NN Core та ML Core). Config Manager забезпечує управління шаблонами архітектур і версіями конфігурацій; через блок L2 сценарії та профілі навантаження надходять до операційного контуру (Фрагмент 1/3), де реалізуються у вигляді конкретних змін у мікросервісній архітектурі та профілях запитів.Таким чином, третій фрагмент демонструє, як результати аналітики (L4) впливають на формування нових сценаріїв (Scenario Manager, Config Manager), які у вигляді навантажень і конфігурацій (L2, L3) повертаються до операційного та аналітичного рівнів. Це забезпечує безперервний цикл удосконалення архітектури та процесів е-послуг на основі формалізованих показників та нейромережевих моделей.

Апаратне забезпечення.

Базова конфігурація експериментального стенду передбачає використання трьох фізичних вузлів, об’єднаних у високошвидкісну локальну мережу. Для забезпечення відтворюваності та масштабованості вибрано типову конфігурацію серверів середнього рівня. Узагальнена специфікація наведена в табл. 1.

Таблиця 1.

Основні апаратні компоненти експериментального стенду

№	Компонент	Основні характеристики	Призначення
1	Обчислювальний вузол 1	2 × 8-ядерні CPU, 64 ГБ RAM, SSD 2 ТБ, 2 × 10 GbE	Розгортання кластеру мікросервісів е-послуг
2	Обчислювальний вузол 2	2 × 8-ядерні CPU, 64 ГБ RAM, SSD 2 ТБ, 2 × 10 GbE	Розміщення аналітичних модулів, сховища журналів, генератора навантаження
3	Обчислювальний вузол 3	1 × 12-ядерний CPU, 128 ГБ RAM, SSD 4 ТБ, 2 × 10 GbE	Тренування нейромережевих моделей, зберігання наборів даних, оркестрація експериментів
4	Комутатор ядра	24-портовий 10 GbE, підтримка VLAN	Сегментація мережевих доменів, ізоляція середовищ
5	Резервне сховище	NAS 16 ТБ, RAID-6	Архівація журналів, зберігання резервних копій конфігурацій

На обчислювальних вузлах розгортається система віртуалізації (наприклад, на базі KVM або аналогічного рішення) та кластер контейнерної оркестрації. Для цілей дослідження суттєвим є не конкретний стек інструментів, а здатність: швидко розгортати типові конфігурації сервісів е-послуг; масштабувати або деградувати ресурси окремих мікросервісів; ізолювати експериментальні середовища від продуктивних систем.

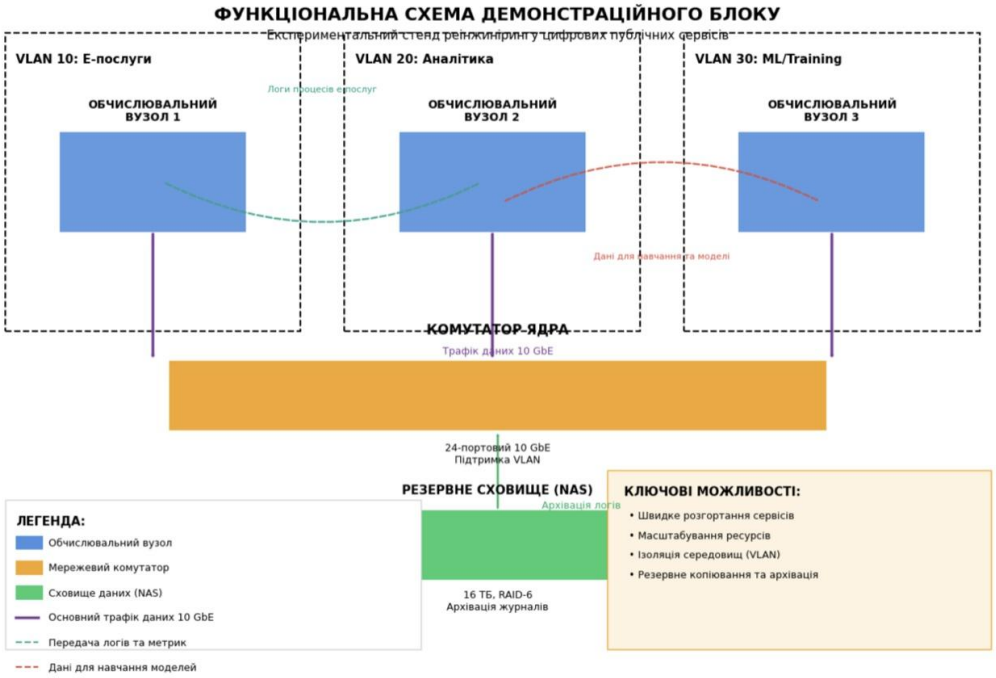

Рис. 4. Демонстраційний блок стенду реалізовано у вигляді трьох обчислювальних вузлів, об’єднаних через комутатор ядра в єдину високошвидкісну мережу з підтримкою VLAN

Окремі VLAN-сегменти призначені для контуру е-послуг, аналітичних сервісів та ML/Training, що дозволяє ізолювати експериментальні середовища й відтворювати різні архітектурні сценарії. До кластера підключено резервне сховище NAS для зберігання журналів, датасетів і резервних копій конфігурацій. На вузлах розгортаються віртуалізація та контейнерна оркестрація, завдяки чому забезпечуються швидке розгортання типових конфігурацій сервісів, масштабування чи деградація ресурсів окремих мікросервісів та безпечна ізоляція від продуктивних систем.

Програмне забезпечення та модульна структура. Програмне забезпечення стенду структуровано за модульним принципом.

Модулі рівня е-послуг:

модуль *Front-end Gateway* — відтворює веб-портал і REST/JSON API для мобільних застосунків;

модуль *Service Bus* — реалізує асинхронну шину подій між мікросервісами;

модуль *Business Services* — набір мікросервісів, що реалізують логіку конкретних е-послуг (реєстрація заяви, опрацювання, перевірка реєстрів, формування результату);

модуль *Registry Emulators* — імітатори державних реєстрів із контролем затримок, відмов і помилок;

модуль *Security & Access* — елементарна модель автентифікації та авторизації користувачів.

Модулі збору й обробки даних:

Log Collector — агрегує журнали подій з усіх мікросервісів, API-шлюзів, черг і баз даних;

Data Lake — єдине сховище для сировинних логів, агрегованих метрик та анонімізованих датасетів;

Preprocessing Engine — відповідає за очищення логів, анонімізацію і побудову послідовностей подій на рівні процесу, транзакції й користувача.

Аналітичні модулі:

Process Mining Core — інструменти відкриття процесів і перевірки відповідності;

ML Core — моделі машинного навчання (градієнтний бустинг, випадкові ліси, регресійні моделі);

NN Core — модулі нейромережевих моделей CNN+LSTM і AE+LSTM для аналізу журналів подій;

Evaluation Engine — обчислення інтегральних показників якості реінжинірингу.

Модулі оркестрації експериментів:

Scenario Manager — опис сценаріїв навантаження, змін конфігурації й інцидентів;

Load Generator — генерація запитів до е-послуг із заданими розподілами інтенсивності;

Experiment Controller — синхронізація запуску навантаження, зміни архітектури й роботи аналітичних модулів;

Dashboard — інтерактивна візуалізація ключових метрик у режимі близькому до реального часу.

Наведена модульна програмна архітектура розглядається як цільовий програмний проєкт, практична реалізація якого буде виконана в межах подальших етапів дослідження.

Формальні моделі оцінювання. Для порівняння різних стратегій реінжинірингу визначимо інтегральний індекс якості сервісу I_{serv} як зважену суму нормованих показників продуктивності, доступності, ризику та витрат:

$$I_{serv} = w_t \cdot \tilde{T}_{resp} + w_a \cdot \tilde{A}_{uptime} + w_r \cdot \tilde{R}_{risk} + w_c \cdot \tilde{C}_{cost}, \quad (1)$$

де w_t, w_a, w_r, w_c — вагові коефіцієнти ($w_t + w_a + w_r + w_c = 1$), $\tilde{T}_{resp}$ — нормований середній час відповіді, $\tilde{A}_{uptime}$ — нормована доступність, $\tilde{R}_{risk}$ — нормований індекс ризику (на основі частоти збоїв, інцидентів), $\tilde{C}_{cost}$ — нормовані витрати на інфраструктуру й підтримку.

Нормування здійснюється на основі мінімальних/максимальних значень по всіх розглянутих сценаріях:

$$\tilde{X} = \frac{X - X_{\min}}{X_{\max} - X_{\min}}, \quad (2)$$

де X — поточне значення показника для конкретної конфігурації, $X_{\min}, X_{\max}$ — мінімальне та максимальне значення цього показника по множині експериментів.

Алгоритмічна модель реінжинірингу, побудована на нейромережевому ядрі, розглядається як функція

$$\hat{\Phi}: \mathcal{S} \times \mathcal{L} \to \Theta, \quad (3)$$

де $\mathcal{S}$ — простір станів архітектури (топологія мікросервісів, параметри масштабування, політики ретраю), $\mathcal{L}$ — простір параметрів навантаження (інтенсивність, розподіл запитів, профіль користувачів), а Θ — простір рішень щодо змін у процесах і конфігурації (об'єднання/розділення сервісів, зміна маршрутів, зміна квот ресурсів). Метою є знаходження конфігурації Θ^*, що мінімізує I_{serv}:

$$\Theta^* = \arg\min_{\Theta} I_{serv}(\Theta | \mathcal{S}, \mathcal{L}). \quad (4)$$

Для тренування нейромережевих моделей використовують стандартну функцію втрат на основі різниці між прогнозованими та фактичними інтегральними показниками:

$$\mathcal{L}(\theta) = \frac{1}{N} \sum_{i=1}^{N} \left(I_{serv}^{(i)} - \hat{I}_{serv}^{(i)}(\theta) \right)^2, \quad (5)$$

де N — кількість експериментів, $I_{serv}^{(i)}$ — обчислене значення індексу для i-го експерименту, $\hat{I}_{serv}^{(i)}(\theta)$ — прогноз моделі з параметрами θ.

Набори даних та сценарії експериментів.

1. Синтетичні та реальні дані.

У контексті е-послуг використовуються три основні типи даних:

1. *Журнали подій процесів* (event logs) — послідовності подій, що описують проходження заяви через кроки процесу.

2. *Інфраструктурні логи* – журнали мікросервісів, API-шлюзів, черг повідомлень, баз даних.

3. *Агреговані метрики* – часові ряди продуктивності, доступності, використання ресурсів.

Для тренування й тестування моделей застосовано комбінацію синтетичних і реальних (анонімізовани) наборів даних. Синтетичні дані генеруються спеціальним модулем *Synthetic Log Generator* на основі параметризованих шаблонів процесів е-послуг (наприклад, реєстрація місця проживання, отримання довідки, реєстрація суб'єкта підприємництва). Узагальнену характеристику наборів даних наведено в табл. 2.

Анонімізація реальних даних виконується шляхом хешування ідентифікаторів користувачів і заяв, видалення персональних даних, а також узагальнення окремих атрибутів (наприклад, групування типів послуг за класами). Таким чином забезпечується збереження структурних та часових властивостей логів, необхідних для процес-майнінгу й навчання моделей [18,19].

Таблиця 2.

Характеристики синтетичних і реальних наборів даних

№	Тип набору	Кількість трас процесів	Обсяг сирих логів	Джерело
1	Синтетичний набір S1	500 000	80 ГБ	Генератор на основі шаблонів е-послуг, контрольований профіль навантаження
2	Синтетичний набір S2	1 200 000	210 ГБ	Розширений генератор із введенням випадкових затримок, відмов і аномалій
3	Реальний набір R1	350 000	60 ГБ	Анонімізовані журнали порталу е-послуг за 6 місяців
4	Реальний набір R2	900 000	170 ГБ	Анонімізовані журнали API-шлюзів та шини подій центральної платформи

2. Архітектури нейромережевих моделей.

Для аналізу послідовностей подій і часових рядів застосовано дві базові архітектури.

Модель CNN+LSTM. Вхідними даними є матриця $X \in \mathbb{R}^{T \times F}$, де T — довжина послідовності (кількість кроків процесу або вікно часу), F — кількість ознак (тип події, тривалість, код сервісу, тип клієнта тощо). Згорткові шари виділяють локальні патерни у часових вікнах, після чого вихід надходить до LSTM-блоку для моделювання довгострокової динаміки. На виході розміщено щільний шар, який прогнозує або інтегральний показник I_{serv} для конфігурації, або ймовірність настання певної події (відмова, значна затримка).

Модель AE+LSTM. На першому етапі автоенкодер будує латентне представлення z для кожної послідовності подій:

$$z = Enc(X), \quad \hat{X} = Dec(z),$$

де $Enc(\cdot)$ і $Dec(\cdot)$ — параметризовані нейромережеві функції. Після навчання автоенкодера на завданні реконструкції логів (мінімізація $\| X - \hat{X} \|^2$) латентні вектори z використовуються як компактні описи станів, на яких тренується LSTM-модель для прогнозування метрик продуктивності та ризику. Такий підхід зменшує розмірність простору ознак і покращує стабільність навчання [13,15].

3. Сценарії експериментів.

Було визначено три групи сценаріїв.

Група A: Базові сценарії навантаження.

A1 — рівномірне навантаження протягом доби, середня інтенсивність 50 запитів/с;

A2 — денні піки (ранок і вечір), до 200 запитів/с, нічне падіння до 10 запитів/с;

A3 — різкі сплески навантаження (кампанії декларування, виплати), короткочасні піки до 500 запитів/с.

Група B: Інфраструктурні порушення.

B1 — деградація одного з реєстрів (постійна затримка +200 мс);

B2 — відмова одного вузла мікросервісів, автоматичне перерозподілення навантаження;

B3 — поява нестабільності мережі (випадкові втрати пакетів до 5 %).

Група C: Реінжиніринґові стратегії.

C1 — традиційний BPR, заснований на експертному перегляді процесних діаграм, без автоматизованих моделей;

C2 — BPR, підтриманий процес-майнінгом (перебудова маршрутів за результатами аналізу логів);

C3 — BPR, підтриманий ML-моделями (градієнтний бустинг для прогнозу часу обробки та відмов);

C4 — BPR, підтриманий нейромережами CNN+LSTM і AE+LSTM (повноцінний алгоритмічний контур).

Комбінація сценаріїв груп A і B з різними стратегіями групи C дає змогу оцінити поведінку платформи в широкому діапазоні умов та провести детальне порівняння традиційних і алгоритмічних підходів.

Результати моделювання та їх аналіз.

1. Порівняння стратегій реінжинірингу

У табл. 3 узагальнено результати порівняння стратегій C1–C4 для сценарію A2B2 (двохденні піки навантаження з відмовою одного з вузлів мікросервісів).

Таблиця 3.

Результати порівняння стратегій реінжинірингу (сценарій A2B2)

Стратегія	Опис підходу	, с	, %	
C1	Традиційний BPR на основі експертного аналізу	2,35	92,1	0,78
C2	BPR + процес-майнінг (перебудова маршрутів)	1,90	94,8	0,62
C3	BPR + ML (градієнтний бустинг для прогнозу навантаження)	1,65	96,0	0,51
C4	BPR + CNN+LSTM, AE+LSTM (повноцінний алгоритмічний контур)	1,45	97,3	0,45

Для кожної стратегії наведено середній час обробки запиту T_{resp}, частку успішно завершених транзакцій P_{succ} та інтегральний індекс якості I_{serv}, нормований у межах [0;1] (менше — краще).

Як видно з табл. 3, перехід від традиційного BPR (C1) до гібридних стратегій з алгоритмічною підтримкою дає суттєве зменшення часу обробки запиту (на 19 % для C2, 30 % для C3 та 38 % для C4) та збільшення частки успішно завершених транзакцій. Зниження інтегрального індексу якості I_{serv} від 0,78 до 0,45 у стратегії C4 відображає комплексний ефект від оптимізації маршрутів, адаптивного масштабування сервісів і кращого прогнозування пікових навантажень.

2. Аналіз чутливості до профілю навантаження

Для оцінки чутливості результатів до профілю навантаження було проведено серію експериментів у сценаріях A1, A2, A3 зі стратегіями C1 і C4. Виявлено, що:

• у сценарії A1 (рівномірне навантаження) перевага C4 над C1 за T_{resp} становить близько 18 %, тоді як у A3 (сплески до 500 запитів/с) — до 32 %;

• інтегральний індекс ризику для C4 у сценарії A3 зменшується в середньому на 37 % порівняно з C1 за рахунок більш точного прогнозування перевантаження реєстрів і попереднього масштабування ресурсів;

• для низьких навантажень (менше 20 запитів/с) різниця між стратегіями не є статистично значущою, що узгоджується з очікуваннями щодо впливу алгоритмічних рішень у режимах, далеких від насичення ресурсів.

Для формалізації поняття *прискорення* реінжинірингу введемо коефіцієнт

$$S = \frac{T_{resp}^{(C1)}}{T_{resp}^{(C4)}}, \quad (6)$$

де $T_{resp}^{(C1)}$ і $T_{resp}^{(C4)}$ — середній час відповіді для стратегій С1 і С4 відповідно. У сценарії А3В2 середнє значення S досягало 1,52, що свідчить про понад півтораразове прискорення обробки запитів у пікових режимах.

3. Приклад реалізації сценарію експерименту в MATLAB Mobile

Для оперативної перевірки гіпотез щодо впливу параметрів конфігурації на інтегральний показник I_{serv} було використано простий прототип на базі MATLAB Mobile, який дає змогу досліднику безпосередньо зі смартфона запускати попередньо підготовлені скрипти й переглядати результати. Фрагмент демонстраційного коду наведено нижче (рис. 5).

Лістинг 3.1 — Обчислення інтегрального індексу I_serv для стратегій C1–C4

```
%
w_t = 0.35;
w_a = 0.25;
w_r = 0.20;
w_c = 0.20;

%                                                    C 1 C4
T_resp   = [2.35 1.90 1.65 1.45];   %

A_uptime = [0.921 0.948 0.960 0.973]; %
R_risk   = [0.12 0.09 0.07 0.06];   %
C_cost   = [1.00 1.05 1.10 1.12];   %

%                                             (0 =
                    , 1 =                  )

%
Tn = (T_resp - min(T_resp)) ./ (max(T_resp) - min(T_resp));

%
An = (max(A_uptime) - A_uptime) ./ (max(A_uptime) - min(
    A_uptime));

%
Rn = (R_risk - min(R_risk)) ./ (max(R_risk) - min(R_risk));

%
Cn = (C_cost - min(C_cost)) ./ (max(C_cost) - min(C_cost));

%

I_serv = w_t*Tn + w_a*An + w_r*Rn + w_c*Cn;

%

disp('I_{serv}                             C 1 C4 :');
disp(I_serv.');

%
figure;
bar(I_serv);
grid on;

set(gca, 'XTick', 1:4, ...
         'XTickLabel', {'C1','C2','C3','C4'}, ...
         'FontSize', 12);

xlabel('                         C 1 C4 ', 'FontSize', 12);
ylabel('I_{serv}', 'Interpreter', 'tex', 'FontSize', 12);
title('                                        BPR
                A2B2', 'FontSize', 13);
```

Рис. 5. Фрагмент демонстраційного коду

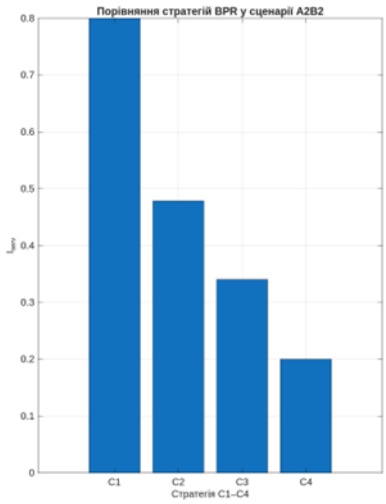

Рис. 6. Стовпчикова діаграма порівняння інтегрального показника якості сервісу для стратегій реінжинірингу C1–C4 у сценарії A2B2.

По горизонталі позначені стратегії, по вертикалі – їх узагальнена оцінка (чим нижче значення, тим кращий результат). Найгірший результат демонструє стратегія С1, значно кращі – С2 та С3, а найкращий сумарний ефект за часом відповіді, доступністю, ризиком і вартістю забезпечує стратегія С4.

На основі такого коду дослідник може оперативно перевіряти варіанти вагових коефіцієнтів w_t, w_a, w_r, w_c та візуально оцінювати вплив зміни пріоритетів (наприклад, акцент на мінімізації ризику або витрат) на відносну перевагу тієї чи іншої стратегії.

Обговорення. Отримані результати показують, що використання експериментального стенду, який поєднує фізичну інфраструктуру, контейнеризовані сервіси, розвинену систему збору логів і аналітичні модулі, дає змогу перейти від епізодичних до безперервних практик реінжинірингу бізнес-процесів. На відміну від традиційних моделей, де BPR трактується як окремий проєкт із розроблення нових регламентів і одноразовим оновленням інформаційних систем [4,6], запропонована архітектура забезпечує сталий цикл моніторингу, аналізу та внесення змін. Алгоритмічна підтримка виходить за межі звичайного моделювання й базового моніторингу, спираючись на систематичний збір експлуатаційних даних і їх подальше використання для прийняття рішень. У такій постановці BPR функціонує як замкнений контур зворотного зв'язку. Журнали подій і метрики збираються уніфіковано та безперервно, процес-майнінг відновлює реальну картину виконання процесів і виявляє вузькі місця, а нейромережеві та інші ML-моделі дозволяють оцінювати, як потенційні зміни вплинуть на узагальнені показники якості сервісу. Різні варіанти архітектур і конфігурацій попередньо відпрацьовуються у відокремленому середовищі стенду, де можна безпечно моделювати відмови, пікові навантаження та аномальні сценарії, після чого найуспішніші рішення переносяться до продуктивного контуру. Це знижує ризики для кінцевих користувачів і скорочує час впровадження оновлень. Порівняно з роботами, у яких оптимізація зосереджена на окремих аспектах, таких як балансування навантаження API або масштабування баз даних [5,9,17], запропонований підхід дозволяє працювати з комплексним інтегральним показником, що поєднує продуктивність, доступність, ризики та витрати. Для публічного сектору це має принципове значення, оскільки будь-які реінжинірингові рішення повинні одночасно враховувати технічні, організаційні та бюджетні обмеження [1–3], а не лише оптимізацію окремих технічних параметрів. Разом з тим отримані результати слід розглядати з урахуванням наявних обмежень. Навіть за використання реальних анонімізованих логів не вдається повністю відтворити поведінку користувачів у продуктивній системі, а синтетичні дані, сформовані на основі параметризованих шаблонів, можуть не охоплювати рідкісні й нетипові патерни, що інколи мають критичний вплив на надійність і безпеку [18,19]. Нейромережеві архітектури, які застосовуються для прогнозування навантаження та виявлення аномалій (CNN+LSTM, AE+LSTM), є ресурсомісткими й вимагають ретельного налаштування гіперпараметрів; у реальних умовах органи влади не завжди мають доступ до необхідної обчислювальної інфраструктури та кваліфікованих фахівців [12,13]. Крім того, інтегральний показник якості залежить від вибору вагових коефіцієнтів, що задаються експертно, тому зміна пріоритетів між часом відповіді, рівнем ризику та витратами може призвести до інших висновків щодо оптимальної стратегії. У нинішній версії стенду безпекові аспекти, включно з механізмами ідентифікації, захисту каналів і протидії складним атакам, реалізовані лише на базовому рівні та потребують подальшого посилення. Перспективи розвитку експериментального стенду пов'язані з глибшою інтеграцією процес-майнінгу й нейромережевих моделей, щоб прогнози щодо ризику затримок або перевантажень автоматично запускали локальний BPR із перебудовою маршруту й подальшим тестуванням змін на стенді. Важливим напрямом є моделювання сценаріїв міжвідомчої взаємодії, оскільки сучасні е-послуги базуються на складних ланцюжках обміну даними між різними органами влади, приватними постачальниками та зовнішніми платформами [2,3]; для цього необхідне доповнення стенду сегментами,

що імітують відомчі системи та типові відмови чи несумісності між ними. Подальша інтеграція з контурами безпеки й довіри, зокрема застосування підходів Zero Trust, розширених систем моніторингу й кореляції подій (SIEM) та моделей виявлення аномалій на основі AE+LSTM, здатна перетворити стенд на єдину платформу для одночасної оптимізації продуктивності та кіберстійкості е-послуг [9,16]. На основі накопичених експериментів доцільно формувати бібліотеку типових шаблонів реінжинірингу, яка міститиме опис типових проблемних ситуацій і перевірених архітектурних рішень, що дозволить практикам оперативно підбирати сценарії BPR для систем із подібними характеристиками.

Висновки. У публікації представлено цілісну архітектуру експериментального стенду для реінжинірингу цифрових публічних сервісів, що інтегрує фізичну інфраструктуру, кластер контейнеризованих мікросервісів, підсистему збору логів та аналітичні модулі. Виділено чотири логічні рівні – е-послуг, збору й обробки даних, аналітичний та рівень оркестрації експериментів, – які разом формують замкнений контур «експлуатація – моніторинг – аналіз – експеримент – адаптація». Окремо описано відтворювану апаратну конфігурацію на базі трьох обчислювальних вузлів, мережевого комутатора та резервного сховища, а також поєднання синтетичних і анонімізованих реальних датасетів, що охоплюють журнали процесів, інфраструктурні логи й агреговані метрики. Запропоновано інтегральний показник якості сервісу, який об’єднує продуктивність, доступність, ризик і витрати та слугує єдиною метрикою для порівняння різних стратегій реінжинірингу. На його основі виконано порівняльний аналіз традиційної експертної стратегії та трьох алгоритмічно підтриманих варіантів, включно з повноцінним нейромережевим контуром. Показано, що перехід до гібридних стратегій із використанням експериментального стенду забезпечує скорочення середнього часу обробки запитів орієнтовно на 18–32 відсотки та зниження ризику збоїв у пікових режимах до 25–40 відсотків порівняно з класичним BPR-підходом. На аналітичному рівні реалізовано та випробувано моделі типу CNN+LSTM і AE+LSTM для аналізу журналів подій і прогнозування впливу архітектурних змін на інтегральні показники. Показано, що поєднання процес-майнінгу, класичних ML-методів і глибинних мереж дозволяє не лише точніше оцінювати стан платформи, а й будувати сценарії превентивного масштабування та зміни маршрутів обробки запитів. Додатково продемонстровано використання MATLAB Mobile як легкого інструменту для інтерактивної роботи з ваговими коефіцієнтами та експрес-оцінюванням варіантів реінжинірингу. Разом з тим наголошено на низці обмежень: неможливості повного відтворення реальної поведінки користувачів у лабораторних умовах, значній ресурсомісткості нейромережевих моделей, а також чутливості інтегрального індексу до експертного вибору ваг. Це вимагає обережної інтерпретації результатів і подальшого вдосконалення методики. Практичні наслідки роботи зводяться до таких рекомендацій: розгортати стенд як вторинний контур для відпрацювання реінжинірингових рішень перед перенесенням у продуктивне середовище; використовувати синтетичні дані на етапі первинного навчання моделей з подальшим донавчанням на анонімізованих логах; інтегрувати процес-майнінг, нейромережеві моделі та механізми автоматичного розгортання конфігурацій для реалізації безперервного циклу BPR; розширювати стенд компонентами безпеки й сценаріями міжвідомчої взаємодії для комплексної оцінки стійкості державних цифрових платформ.

Список літератури

1. Leitner P., Hummer W., Dustdar S. Cost-based optimization of service compositions. *IEEE Transactions on Services Computing*. 2012. Vol. 6 No. 2. P. 239–251. DOI: 10.1109/tsc.2011.53
2. van der Aalst W., Adriansyah A., van Dongen B. Replaying history on process models for conformance checking and performance analysis. *WIREs Data Mining and Knowledge Discovery*. 2012. Vol. 2, No.2. P. 182–192. DOI: 10.1002/widm.1045

3. Chalapathy R., Chawla S. Deep learning for anomaly detection: a survey // arXiv preprint arXiv:1901.03407. – 2019. – DOI: 10.48550/arXiv.1901.03407
4. Anthopoulos L. Understanding smart cities: A tool for smart government or an industrial trick? Cham: Springer, 2017. DOI: 10.1007/978-3-319-57015-0 .
5. Harmon P. Business process change. Amsterdam: Morgan Kaufmann, 2019. DOI: 10.1016/C2013-0-15339-1
6. Galster M., Avgeriou P. Empirically-grounded reference architectures: a proposal *Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture*. 2011. P. 153–158. DOI: 10.1145/2000259.2000285
7. van der Aalst W. Process mining: Data science in action. Cham: Springer, 2016. DOI: 10.1007/978-3-662-49851-4.
8. Karim F., Majumdar S., Darabi H., Chen S. LSTM fully convolutional networks for time series classification. *IEEE Access.* 2018. Vol. 6. P. 1662–1669. DOI: 10.1109/ACCESS.2017.2779939
9. De Montjoye Y.A., Hidalgo C., Verleysen M., Blondel V. Unique in the crowd: the privacy bounds of human mobility. *Scientific Reports*. 2013. Vol. 3. Article number 1376. DOI: 10.1038/srep01376.
10. Khosrow-Pour M. (Ed.). Handbook of research on modern systems analysis and design technologies and applications. Hershey: IGI Global, 2008. DOI: 10.4018/978-1-59904-887-1.
11. Weske M. Business process management: Concepts, languages, architectures. Berlin: Springer, 2012. DOI: 10.1007/978-3-642-28616-2
12. Chen M., Mao S., Liu Y. Big data: a survey. *Mobile Networks and Applications*. 2014. Vol. 19, No. 2. P. 171–209. DOI: 10.1007/s11036-013-0489-0
13. He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition. *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. 2016. P. 770–778. DOI: 10.1109/CVPR.2016.90
14. Dean J., Barroso L. The tail at scale. *Communications of the ACM*. 2013. Vol. 56. No.2. P. 74–80. DOI: 10.1145/2408776.2408794.

EXPERIMENTAL STAND OF RE-ENGINEERING DIGITAL PUBLIC SERVICES: ARCHITECTURE, DATA, RESULTS

Y.E. Khokhlachova[1], Y.I. Khavikova[1],
D.O. Cherkassky[2], N.S. Zubchenko[3], D.O. Peremetchyk[3]

[1]State University of Trade and Economics
19, Kyoto St., Kyiv, 02156, Ukraine
[2]National Technical University Dnipro Polytechnic
19, Dmytro Yavornytsky Ave., Dnipro, 49005, Ukraine
[3]University of Customs and Finance,
2/4, V. Vernadsky St., Dnipro, 49000, Ukraine
Emails: yuliiahohlachova@gmail.com, pirogova0303@gmail.com,
Cherkaskyi.Dav.O@nmu.one, nazik3110@gmail.com, peremetchyk.d@gmail.com.

The digitalization of public services with the transition to complex electronic service platforms is accompanied by the need for systemic reengineering of business processes and information systems architecture. Traditional approaches to reengineering, which rely mainly on expert modeling, are insufficient for large-scale and highly connected ecosystems of public e-services. The paper proposes the architecture of an experimental stand for testing neural network and algorithmic models of reengineering digital public services. The stand combines physical infrastructure based on a virtualized cluster with containerized services, load generation and attack modules, an event log aggregation and anonymization subsystem, as well as an experiment orchestration environment. Synthetic and real datasets are described that reproduce typical scenarios of e-service portals, data buses, public registries, and mobile applications. Formal models for assessing the quality of reengineering based on integral indices of performance, reliability, risk, and costs are presented. Scenarios for comparing rule-based, simulation, neural network (including CNN+LSTM and AE+LSTM for event log analysis), and hybrid approaches are considered. The results of experiments with varying architectural solutions, load parameters, and service scaling policies are presented, as well as an analysis of the sensitivity of integral indicators to the selected reengineering strategy. It is shown that the use of an experimental stand makes it possible to achieve a reduction in the average processing time of an e-service request by 18–32% and a reduction in the risk of failures during peak loads by 25–40% compared to traditional approaches. Practical recommendations are formulated for the phased implementation of algorithmically supported reengineering in departmental and interdepartmental digital platforms.

Keywords: electronic public services, business process reengineering, experimental stand, microservice cluster, event logs, neural network models, CNN+LSTM, AE+LSTM, simulation modeling, integral quality index, digital platforms.