УДК 004.891:35.077.1 DOI: 10.31673/2412-4338.2026.019010

**Хохлачова Юлія Євгеніївна**
к.т.н., професор, професор кафедри інженерії програмного забезпечення та кібербезпеки
*Державний торговельно-економічний університет, м. Київ*
ORCID 0000-0002-0787-5112
yuliiahohlachova@gmail.com

**Хавікова Юлія Ігорівна**
аспірантка кафедри інженерії програмного забезпечення та кібербезпеки
*Державний торговельно-економічний університет, м. Київ*
ORCID 0000-0003-1017-3602
pirogova0303@gmail.com

**Черкаський Олександр Валерійович**
докторант
*Державний університет інформаційно-комунікаційних технологій, м. Київ*
ORCID 0009-0006-3105-5217
asherjoseph.c@gmail.com

**Черкаський Давид Олександрович**
аспірант
*Національний технічний університет Дніпровська політехніка, м. Дніпро*
ORCID: 0009-0003-8516-6252
Cherkaskyi.Dav.O@nmu.one

**Переметчик Данило Олександрович**
Незалежний дослідник**,** Кафедра кібербезпеки та інформаційних технологій
*Університет митної справи та фінансів, м. Дніпро*
ORCID: 0009-0006-1978-5858
peremetchyk.d@gmail.com

# КОМПЛЕКСНИЙ РЕІНЖИНІРИНГ ЦИФРОВИХ ДЕРЖАВНИХ ПОСЛУГ ІЗ ВИКОРИСТАННЯМ ГЛИБИННИХ НЕЙРОННИХ МЕРЕЖ І ПОКАЗНИКІВ ЯКОСТІ ОБСЛУГОВУВАННЯ

***Анотація***. *У статті обґрунтовано комплексну концепцію використання нейронних мереж для реінжинірингу бізнес-процесів цифрових державних сервісів. Показано, що великі масиви адміністративних даних, журнали подій інформаційних систем та телеметричні потоки мереж електронних комунікацій можуть виступати повноцінним джерелом знань про фактичну роботу е-послуг, їхні «вузькі місця», приховані шаблони навантаження й аномальні сценарії, у тому числі пов'язані з гібридними кібератаками. Запропоновано процесно-орієнтовану математичну модель, у якій конфігурація ресурсів, політика маршрутизації, параметри інформаційної безпеки та сигнали систем виявлення вторгнень (IDS) і платформ кореляції подій безпеки (SIEM) відображаються у векторних ознаках, придатних для навчання різних архітектур нейронних мереж. Розглянуто застосування багатошарового персептрона, згорткових мереж, моделей з довготривалою короткочасною пам'яттю, а також автоенкодерів і гібридних CNN+LSTM та AE+LSTM для прогнозування часу опрацювання звернень, ймовірності порушення SLO, виявлення аномальних процесних сценаріїв та побудови сурогатних моделей для сценарного аналізу «what-if». Описано особливості навчання на нерівномірних і неповних адміністративних вибірках, методи урахування уразливостей SSL і SNMP у firmware-атаках, інтеграції принципів Zero Trust та підходи Byte2Image для подання трафіку і логів у вигляді зображень. Наведено приклади сценаріїв застосування в реінжинірингу державних е-послуг, а також фрагменти Matlab-коду й варіанти візуалізації результатів, орієнтовані на використання у середовищі Matlab і Matlab Mobile.*

***Ключові слова:*** *реінжиніринг бізнес-процесів, цифрові державні послуги, нейронні мережі, LSTM, CNN+LSTM, AE+LSTM, Zero Trust, IDS, SIEM, Byte2Image, Matlab-візуалізація.*

**Yuliia KHOKHLACHOVA**
PhD, Professor, Professor of the Department of Software Engineering and Cybersecurity

*© 2026 Хохлачова Ю.Є., Хавікова Ю.І., Черкаський О.В., Черкаський Д.О., Переметчик Д.О.*
*Цей матеріал ліцензовано за умовами* ***CC BY 4.0****.*
*https://creativecommons.org/licenses/by/4.0/*

*State University of Trade and Economics, Kyiv*
ORCID 0000-0002-0787-5112
yuliiahohlachova@gmail.com

**Yuliia KHAVIKOVA**
PhD Student of the Department of Software Engineering and Cybersecurity
*State University of Trade and Economics, Kyiv*
ORCID 0000-0003-1017-3602
pirogova0303@gmail.com

**Oleksandr CHERKASKY**
Doctoral Student
*State University of Information and Communication Technologies, Kyiv*
ORCID 0009-0006-3105-5217
asherjoseph.c@gmail.com

**David CHERKASKY**
PhD Student
*National Technical University Dnipro Polytechnic, Dnipro*
ORCID: 0009-0003-8516-6252
Cherkaskyi.Dav.O@nmu.one

**Danylo PEREMETCHYK**
Independent Researcher, Department of Cybersecurity and Information Technologies
*University of Customs and Finance, Dnipro*
ORCID: 0009-0006-1978-5858
peremetchyk.d@gmail.com

## COMPREHENSIVE RE-ENGINEERING OF DIGITAL GOVERNMENT SERVICES USING DEEP NEURAL NETWORKS AND SERVICE QUALITY INDICATORS

**Abstract**. *The article substantiates a comprehensive concept of using neural networks for reengineering business processes of digital government services. It is shown that large administrative data sets, event logs of information systems and telemetry streams of electronic communications networks can act as a full-fledged source of knowledge about the actual operation of e-services, their "bottlenecks", hidden load patterns and anomalous scenarios, including those associated with hybrid cyberattacks. A process-oriented mathematical model is proposed in which resource configuration, routing policy, information security parameters and signals of intrusion detection systems (IDS) and security event correlation platforms (SIEM) are reflected in vector features suitable for training various neural network architectures. The application of a multilayer perceptron, convolutional networks, models with long-term short-term memory, as well as autoencoders and hybrid CNN+LSTM and AE+LSTM for predicting the processing time of requests, the probability of SLO violation, detecting anomalous process scenarios and building surrogate models for scenario analysis "what-if" is considered. The features of training on uneven and incomplete administrative samples, methods for taking into account SSL and SNMP vulnerabilities in firmware attacks, integration of Zero Trust principles and Byte2Image approaches for presenting traffic and logs in the form of images are described. Examples of application scenarios in the reengineering of government e-services are given, as well as fragments of Matlab code and options for visualizing results, oriented towards use in the Matlab and Matlab Mobile environments.*

***Keywords**: business process reengineering, digital government services, neural networks, LSTM, CNN+LSTM, AE+LSTM, Zero Trust, IDS, SIEM, Byte2Image, Matlab visualization.*

### 1. Вступ

Цифрова трансформація публічного сектору призвела до стрімкого зростання кількості та складності електронних публічних послуг (е-послуг), що надаються через веб-портали, мобільні застосунки та інтегровані платформи взаємодії реєстрів [1–3,11,13,14]. Сучасні сервіси реєстрації місця проживання, державної реєстрації бізнесу, оформлення паспортних документів, надання соціальної допомоги, дозвільні та реєстраційні сервіси генерують великий обсяг адміністративних даних, журналів подій та телеметрії інфраструктури, які при належній обробці можуть слугувати основою для прийняття рішень і вдосконалення цифрового урядування [3–5, 11,13]. При цьому процеси нерідко зберігають риси паперових процедур, а оптимізація виконується точково, у форматі автоматизації

окремих операцій без системного переосмислення логіки бізнес-процесів, попри напрацювання класичної школи реінжинірингу та процесного менеджменту [4–6,15].

**2. Аналіз літературних даних і постановка проблеми**

Класичні підходи до реінжинірингу бізнес-процесів (Business Process Reengineering, BPR) у публічному секторі базуються на експертних інтерв'ю, моделюванні процесів у нотаціях BPMN/ArchiMate та імітаційному моделюванні обмеженої кількості сценаріїв [4–6, 15]. Такий підхід:

- погано масштабується за великого обсягу послуг і високої динаміки нормативних змін [1–3,11,13,14];

- обмежено враховує складні нелінійні залежності між навантаженням, конфігурацією ресурсів, поведінкою користувачів та інформаційно-безпековими подіями [4,5,8,12–14];

- опирається на суб'єктивні припущення щодо поширених сценаріїв і типових користувачів, що особливо критично в умовах зростання обсягів даних та алгоритмізації прийняття рішень [6,13,14].

Розвиток глибинного навчання показав високу ефективність нейронних мереж, зокрема згорткових (Convolutional Neural Network, CNN), рекурентних і моделей з довготривалою короткочасною пам'яттю (Long Short-Term Memory, LSTM), у задачах аналізу часових рядів, текстів, мережевого трафіку й складних багатовимірних залежностей [7,8,12–14]. У поєднанні з автоенкодерами (Autoencoder, AE) та гібридними архітектурами CNN+LSTM, AE+LSTM вони відкривають можливості для побудови дано-орієнтованих моделей бізнес-процесів, які наближають реінжиніринг до формату експериментів на цифрових двійниках процесів і підтримують сценарний аналіз на основі історичних журналів подій [4,5,8,12,15].Окремий клас задач стосується стійкості цифрових державних сервісів до гібридних кібератак. Для цього використовуються системи виявлення вторгнень (Intrusion Detection System, IDS), платформи керування та кореляції подій безпеки (Security Information and Event Management, SIEM), а також підходи, засновані на архітектурі нульової довіри (Zero Trust) [9–11,13,14]. Вразливості протоколів SSL і SNMP, у тому числі на рівні firmware-атак на мережеве обладнання, можуть безпосередньо впливати на доступність і цілісність сервісів, викликаючи маскування атак під технічні збої та деградацію бізнес-показників, що потребує інтеграції безпекових сигналів у моделі процесів [9,10,13].Таким чином, актуальною є задача розроблення комплексного підходу до реінжинірингу цифрових державних сервісів на основі нейромережевих моделей, які одночасно враховують процесні показники, навантаження на інфраструктуру та ризики кібератак [3–6,8–12,13–15]. Такий підхід має забезпечити:

- прогнозування часу надання послуг і ймовірності SLO-порушень;

- виявлення аномальних сценаріїв, пов'язаних із гібридними атаками;

- оцінювання альтернативних сценаріїв BPR у режимі what-if;

- підтримку принципів Zero Trust на рівні процесної логіки через включення динамічних оцінок ризику й довіри [9–11,13,14].

**3. Мета і задачі дослідження**

Метою статті є розроблення концепції та алгоритмів використання нейронних мереж для моделювання й оптимізації бізнес-процесів цифрових державних сервісів у контексті реінжинірингу, з інтеграцією даних IDS/SIEM, урахуванням уразливостей SSL/SNMP та застосуванням перетворення Byte2Image.

Для досягнення мети поставлено такі основні завдання:

- формалізувати предметну область цифрових державних сервісів як процесно-орієнтовану математичну модель, придатну для навчання нейромереж [4–6,8,12,15];

- обґрунтувати вибір архітектур MLP, CNN, LSTM, CNN+LSTM та AE+LSTM для різних задач реінжинірингу;

- визначити метрики якості моделей і бізнес-показників, включно з інтегральним ризиком кіберінцидентів з урахуванням підходів до оцінювання ефективності цифрового урядування [1–3,11,13,14];

- описати особливості навчання моделей на адміністративних наборах даних з урахуванням конфіденційності, нерівномірності класів і вимог до надійності публічних алгоритмічних рішень [3,11,13,14];

- продемонструвати переваги нейромережевих підходів над традиційними методами BPR на прикладах сценаріїв, пов'язаних з оптимізацією процесних показників та підвищенням стійкості до кібератак [4–6,8–10,12–15];

- запропонувати фрагменти Matlab-коду та шаблони візуалізації результатів для практичного *застосування в органах публічної влади.*

У роботі використано результати досліджень з процесного майнінгу, прикладного машинного навчання, кібербезпеки мереж електронних комунікацій і цифрового урядування, а також сучасні підходи до оцінювання зрілості е-урядування та впровадження алгоритмічних рішень у публічному секторі [1–15].

**4. Методи**

Методичний підхід у роботі побудовано як послідовність етапів, що поєднують формалізацію бізнес-процесів цифрових державних сервісів, інтеграцію сигналів кібербезпеки з IDS/SIEM та побудову нейромережевих моделей різних архітектур для підтримки рішень з реінжинірингу. Відправною точкою є уніфікація журналів подій, адміністративних записів і телеметрії мережевої інфраструктури в єдиний процесно-орієнтований дата-март, сумісний з інструментарієм процесного майнінгу та прогнозного моніторингу бізнес-процесів [4–8,12–14]. На цій основі здійснюється опис е-послуг як множини кейсів із часовими траєкторіями подій, до яких додаються агреговані показники навантаження та ризику інформаційної безпеки. Подальші кроки передбачають побудову системи векторних ознак, що відображають як структурні характеристики процесу (маршрути, кількість ручних операцій, повернення на попередні етапи), так і параметри безпекового контексту (спрацювання сигнатур по SSL/SNMP, інтегральні оцінки ризику, індикатори аномалій трафіку) [8–11]. На цьому представленні навчаються декілька класів нейромережевих моделей: MLP для роботи з агрегованими ознаками, LSTM для аналізу послідовностей подій, а також гібридні архітектури CNN+LSTM та AE+LSTM з використанням перетворення Byte2Image для глибокого аналізу мережевих і логових даних [7,8,12]. Якість моделей оцінюється як за стандартними машинно-навчальними метриками (MSE, MAPE, F1), так і за інтегральними бізнес-показниками, що відображають ефективність реінжинірингу та стійкість до гібридних кібератак в умовах впровадження принципів Zero Trust [9–11,13–15].

**Формалізація бізнес-процесів цифрових державних сервісів**

Розглянемо окрему електронну послугу як множину кейсів (звернень) $\{C_1, \dots, C_N\}$, де кожен кейс описується послідовністю подій, зафіксованих у журналі процесу:

$$C_i = \{(e_{i1}, t_{i1}, s_{i1}), (e_{i2}, t_{i2}, s_{i2}), \dots, (e_{iK_i}, t_{iK_i}, s_{iK_i})\}, \quad (1)$$

де $e_{ij}$ – тип події (подання заяви, перевірка, погодження, підпис, відмова тощо), $t_{ij}$ – мітка часу, $s_{ij}$ – додатковий стан (ідентифікатор виконавця, канал подачі, технічний статус).

Сумарний час опрацювання кейсу

$$T_i = t_{iK_i} - t_{i1} \quad (2)$$

є однією з ключових цільових змінних моделювання. Додатковими показниками виступають:

*кількість ручних операцій $H_i$ (кількість дотиків оператора);*

*кількість повернень на попередні етапи $R_i$;*

*бінарний показник виконання SLO: $y_i^{SLO} \in \{0,1\}$;*

*категорія кейсу щодо безпеки: нормальний / підозрілий / підтверджена атака.*

Для побудови нейромережевих моделей необхідно перетворити процесні дані на вектор ознак. Визначимо функцію

$$z_i = \phi(C_i, m_i, r), \quad (3)$$

де $m_i$ – метадані кейсу (тип послуги, регіон, канал звернення, ризикові прапорці), $r$ – вектор, що описує конфігурацію ресурсів та безпекових налаштувань (чисельність операторів, часові вікна роботи, параметри політики Zero Trust), $\phi(\cdot)$ – процедура формування ознак.

До складу $\phi(\cdot)$ входять:

*one-hot-кодування типів подій та виконавців;*

*агреговані часові характеристики (середні інтервали між подіями, максимальні затримки, дисперсії тривалостей);*

*частоти використання окремих маршрутів;*

*бінарні ознаки реалізації критичних кроків (наприклад, автоматичне рішення замість ручного).*

**Інтеграція даних IDS/SIEM та параметрів безпеки**

Системи IDS і SIEM генерують потоки записів про спроби атак, аномалії трафіку, помилки протоколів SSL і SNMP, а також сигнали про можливі firmware-атаки на мережеве обладнання [14,15,17]. Нехай $L^{IDS}$ та $L^{SIEM}$ – багатовимірні журнали безпекових подій.

Введемо для кейсу $i$ вектор безпекових ознак $b_i$, який формується як агрегування по часовому інтервалу опрацювання цього кейсу:

$$b_i = \psi\left(L_i^{IDS}, L_i^{SIEM}\right), \tag{4}$$

де $L_i^{IDS}$, $L_i^{SIEM}$ – підмножини логів IDS та SIEM, що накладаються на часовий інтервал $[t_{i1}, t_{iK_i}]$, а $\psi(\cdot)$ включає:

*кількість спрацювань сигнатур по SSL/HTTPS;*
*кількість аномалій по SNMP (наприклад, нетипові зміни статусів інтерфейсів);*
*інтегральні оцінки ризику, розраховані SIEM;*
*середню інтенсивність підозрілих подій за одиницю часу.*

Розширений вектор ознак кейсу набуває вигляду

$$\tilde{z}_i = [z_i, b_i], \tag{5}$$

що дозволяє нейромережевим моделям одночасно враховувати процесні та безпекові компоненти при прогнозуванні часу, ризику SLO-порушення й ймовірності гібридних атак, які маскуються під технічні збої [8,21,23].

**Нейромережеві архітектури для задач реінжинірингу**

***MLP для агрегованих ознак***

Багатошаровий персептрон (Multilayer Perceptron, MLP) із вхідним вектором $\tilde{z}_i$ застосовується для регресії часу опрацювання $T_i$ та кількості ручних операцій $H_i$:

$$\hat{T}_i = f_{\theta_T}(\tilde{z}_i), \qquad \hat{H}_i = f_{\theta_H}(\tilde{z}_i), \tag{6}$$

де $f_\theta(\cdot)$ – композиція лінійних перетворень та нелінійних активацій із параметрами $\theta$, які визначаються під час навчання:

$$f_\theta(x) = \sigma_L(W_L\sigma_{L-1}(\dots\sigma_1(W_1x + b_1)\dots) + b_L). \tag{7}$$

***LSTM для послідовностей подій***

Для детального прогнозування динаміки кейсу використовується LSTM-мережа, що обробляє послідовність векторів подій $\{x_{i1}, \dots, x_{iK_i}\}$, де кожен вектор включає тип події, час із моменту попередньої події, атрибути виконавця та супровідні сигнали безпеки. Динаміка LSTM задається системою рівнянь:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f), i_t = \sigma(W_i[h_{t-1}, x_t] + b_i), \tilde{c}_t = tanh(W_c[h_{t-1}, x_t] + b_c), c_t = f_t e c_{t-1} + i_t e \tilde{c}_t, o_t = \sigma(W_o[h_{t-1}, x_t] + b_o), h_t = o_t e tanh(c_t), \tag{8}$$

де $h_t$ та $c_t$ – прихований і внутрішній стани відповідно, $\sigma(\cdot)$ – сигмоїдна функція, $e$ – поелементне множення.

На основі фінального стану $h_{K_i}$ здійснюється прогноз залишкового часу до завершення кейсу $T_i^{rem}$ та ймовірності порушення SLO:

$$\hat{T}_i^{rem} = g_T(h_{K_i}), \qquad \hat{p}_i^{SLO} = \sigma\left(g_{SLO}(h_{K_i})\right). \tag{9}$$

***Гібридні моделі CNN+LSTM, AE+LSTM і Byte2Image***

Для аналізу мережевого трафіку та логів, пов'язаних з роботою сервісів, застосовується перетворення Byte2Image, яке відображає послідовність байтів у матрицю пікселів [12,17]. Згорткова нейромережа витягує з таких зображень локальні та глобальні патерни навантаження й атак, а LSTM моделює їх еволюцію в часі, утворюючи гібридну архітектуру CNN+LSTM.

Автоенкодери (AE) та AE+LSTM використовуються для виявлення аномальних процесних сценаріїв:

$$h_i = g_\phi(\tilde{z}_i), \qquad \hat{\tilde{z}}_i = g_\psi^{-1}(h_i), \tag{10}$$

де $h_i$ – латентне подання нормального кейсу, а величина

$$a_i = \|\tilde{z}_i - \hat{\tilde{z}}_i\|_2^2, \tag{11}$$

слугує мірою аномальності. Високі значення $a_i$ відповідають нетиповим траєкторіям, що можуть бути зумовлені як регресійними програмними помилками, так і гібридними атаками, які експлуатують уразливості SSL/SNMP у firmware-атаках [8,17].

**Метрики якості та функція мети реінжинірингу**

Для регресійних задач використовуються середньоквадратична помилка (MSE), середня абсолютна відносна помилка (MAPE) та коефіцієнт детермінації $R^2$:

$$MSE = \frac{1}{N}\sum_{i=1}^{N} (T_i - \hat{T}_i)^2, \qquad MAPE = \frac{100\%}{N}\sum_{i=1}^{N} \left|\frac{T_i - \hat{T}_i}{T_i}\right|. \tag{12}$$

Для класифікації виконання SLO застосовуються точність, повнота, точність у вузькому сенсі (precision) та F1-міра:

$$F1 = 2 \cdot \frac{Precision \cdot Recall}{Precision + Recall}. \quad (13)$$

На рівні бізнес-процесу вводиться вектор бізнес-показників:

$$s = \left(\underline{T}, P_{SLO}, C_{manual}, Q_{backlog}, R_{sec}\right), \quad (14)$$

де $\underline{T}$ – середній час надання послуги, $P_{SLO}$ – ймовірність дотримання SLO, $C_{manual}$ – середня кількість ручних операцій, $Q_{backlog}$ – середній розмір черги, $R_{sec}$ – інтегральний ризик кіберінцидентів, оцінений на основі IDS/SIEM.

Інтегральна функція мети реінжинірингу для конфігурації ресурсів $r$ та політики маршрутизації policy має вигляд

$$J(r, policy) = w_1 \frac{\underline{T}}{\underline{T}_0} + w_2 \frac{C_{manual}}{C_{manual,0}} + w_3 \frac{Q_{backlog}}{Q_{backlog,0}} - w_4 \frac{P_{SLO}}{P_{SLO,0}} + w_5 \frac{R_{sec}}{R_{sec,0}}, \quad (15)$$

де індекс «0» позначає значення до реінжинірингу, а $w_k$ – вагові коефіцієнти пріоритетності. Задача реінжинірингу формулюється як

$$(r^*, policy^*) = arg \min_{r,policy} J(r, policy), \quad (16)$$

а нейромережеві моделі виконують роль сурогату, що швидко оцінює $\hat{s}$ для великої кількості сценаріїв без експериментів у продуктивному середовищі [12,13,21].

**Підготовка адміністративних даних до навчання моделей**

Підготовка адміністративних даних до навчання нейромережевих моделей передбачає поетапну попередню обробку, оскільки вихідні журнали подій і реєстрові вибірки містять пропуски, несумісні формати й похибки, що є типовим для інформаційних систем публічного сектору [4–6,18–20]. На першому етапі здійснюється очищення даних від технічних записів (службові пінг-запити, внутрішні системні транзакції, дублікати логів моніторингу), які не впливають безпосередньо на логіку бізнес-процесу або можуть спотворювати статистику тривалостей етапів [4,5,19]. Далі часові мітки нормалізуються шляхом переходу від абсолютних відліків до тривалостей між послідовними подіями в межах одного кейсу, що дозволяє коректно враховувати паузи, черги та паралельні гілки виконання процесу [6,18]. Для зменшення впливу аномальних значень виконується виявлення та корекція грубих викидів за статистичними критеріями (наприклад, на основі міжквартильного розмаху або z-оцінок), причому аномально великі тривалості додатково маркуються як потенційні індикатори SLO-порушень або збоїв інфраструктури [5,6,19]. Важливим кроком є також узгодження словників типів подій і статусів між різними інформаційними системами (front-office, back-office, зовнішні реєстри, IDS/SIEM), що забезпечує єдину таксономію процесних станів для подальшого процесного майнінгу та навчання моделей [4,18–20].Окрему проблему становить нерівномірність класів, зокрема рідкісні SLO-порушення, окремі типи гібридних атак або специфічні відмови компонентів інфраструктури [7,8,12,19]. Для компенсації дисбалансу застосовуються вагові коефіцієнти у функції втрат, які підвищують «вартість» помилок на менш представлених класах і тим самим зменшують схильність моделі ігнорувати рідкісні, але критично важливі події [7,12,20]. Додатково використовуються спеціальні стратегії формування батчів із балансуванням класів (oversampling/undersampling, генерація синтетичних прикладів для міноритарних класів), що підвищує стабільність навчання та дозволяє уникнути деградації моделі на хвостах розподілу [8, 12,19]. Оскільки класичні метрики на основі загальної точності в умовах дисбалансу є малопоказовими, основними критеріями якості обираються F1-міра та площа під ROC-кривою (AUC), які краще відображають здатність моделі виявляти рідкісні інциденти й забезпечувати прийнятну чутливість та специфічність у задачах моніторингу цифрових державних сервісів [7,8,18–20].

**5. Результати**

На основі формалізованих бізнес-процесів, інтегрованих із сигналами IDS/SIEM та параметрами інфраструктури, побудовано низку моделей (лінійна регресія, Random Forest, MLP, LSTM, CNN+LSTM, AE+LSTM), які порівнюються між собою за точністю прогнозування часу опрацювання звернень, ймовірності SLO-порушень і здатністю виявляти аномальні сценарії, пов’язані з гібридними кібератаками [4–8,12,18–21]. Для інтерпретації отриманих результатів використано як класичні машинно-навчальні метрики (MSE, MAPE, F1, AUC), так і агреговані бізнес-показники, що відображають ефективність процесу та ризики кіберінцидентів у контексті архітектури Zero Trust [9–11,14,15]. Структурно результати поділено на кілька блоків. Спочатку здійснюється якісне порівняння традиційного BPR, орієнтованого на експертні моделі, з дано-орієнтованим нейромережевим підходом, що спирається на журнали подій, адміністративні дані та безпекові логи IDS/SIEM [4–6,12,22]. Далі подано кількісний аналіз точності моделей прогнозування часу надання послуг і демонструється

виграш від урахування послідовностей подій та Byte2Image-подань трафіку порівняно з агрегованими ознаками [7,8,12,18–20]. Окремо розглянуто вплив реінжинірингу, підтриманого нейромережевими моделями, на показники користувацького досвіду (UX), а також наведено приклади Matlab-сценаріїв і візуалізацій (у тому числі для Matlab Mobile), орієнтованих на практичне використання результатів керівництвом органів публічної влади [3,11,13,21–23].

**Порівняння традиційного BPR та нейромережевих підходів**

Умовні результати порівняння традиційного BPR та нейромережевого підходу подано в табл. 1.

Таблиця 1

Порівняння традиційного реінжинірингу та підходу з використанням нейромереж

| Критерій | Традиційний BPR | BPR з нейромережами |
|---|---|---|
| Джерела знань | Експертні інтерв'ю, регламенти | Журнали подій, адміністративні дані, IDS/SIEM + експертні знання |
| Урахування нелінійностей | Обмежене, через спрощені припущення | Природна підтримка складних нелінійних залежностей |
| Швидкість оцінки сценаріїв | Низька, ручний аналіз окремих варіантів | Висока, масове моделювання сценаріїв сурогатною моделлю |
| Адаптація до змін | Повільна, потребує перегляду моделей | Можливе регулярне донавчання на нових даних |
| Урахування ризиків безпеки | Як правило, окремі процедури аудиту | Єдина модель процесу й безпеки з інтеграцією сигналів IDS/SIEM |
| Підтримка принципів Zero Trust | Непряма, через регламентні вимоги | Включення оцінок довіри в процесні рішення |

Табл. 1 узагальнює результати порівняльного аналізу традиційного реінжинірингу бізнес-процесів та BPR, підсиленого нейромережевими моделями, виконаного на основі кейсів цифрових державних сервісів та огляду сучасних підходів до е-урядування й процесного майнінгу [1–6, 8, 11–15]. За критерієм джерел знань показано, що класичний BPR спирається переважно на експертні інтерв'ю та регламенти, тоді як запропонований підхід інтегрує журнали подій, адміністративні дані, логи IDS/SIEM разом з експертними знаннями, що відповідає трендам переходу до data-driven управління [3, 4, 8, 11, 13]. У частині врахування нелінійностей встановлено, що традиційні моделі змушені застосовувати спрощувальні припущення, тоді як нейромережеві архітектури природно підтримують складні нелінійні залежності між навантаженням, поведінкою користувачів та інфраструктурними параметрами [7, 8, 12]. За критерієм швидкості оцінки сценаріїв (табл. 1) результати експериментальної апробації показали, що ручний аналіз окремих варіантів у традиційному BPR суттєво поступається підходу з використанням сурогатних нейромережевих моделей, які дають змогу масово моделювати what-if-сценарії для портфеля е-послуг [4, 5, 8, 12]. У вимірі адаптації до змін доведено, що класичні моделі потребують трудомісткого перегляду при нормативних або організаційних змінах, тоді як нейромережевий підхід підтримує регулярне донавчання на нових даних, що узгоджується з вимогами гнучкого цифрового урядування [1–3, 11, 14]. Окремо підкреслено, що ризики безпеки в традиційному підході здебільшого розглядаються в рамках окремих аудитів, тоді як у запропонованій схемі формується єдина модель процесу й безпеки з інтеграцією сигналів IDS/SIEM та вбудованою підтримкою принципів Zero Trust через включення оцінок довіри в процесні рішення [9–11, 13, 15]. Таким чином, таблиця 1 відображає якісний виграш від переходу до дано-орієнтованого, нейромережевого BPR у напрямі масштабованості, адаптивності та кіберстійкості цифрових державних сервісів.

**Якість моделей прогнозування часу надання послуги**

Узагальнені результати порівняння моделей прогнозування часу опрацювання $T_i$ наведено в табл. 2.

Табл. 2 відображає кількісні результати експериментального порівняння моделей прогнозування часу опрацювання звернень у цифрових державних сервісах на основі адміністративних даних, журналів подій та інтегрованих безпекових ознак. Показано значення середньоквадратичної помилки (MSE, год), відносної похибки (MAPE, %) та коефіцієнта детермінації для низки моделей: лінійної регресії, Random Forest, багатошарових перцептронів (MLP), рекурентної LSTM та гібридної

архітектури CNN+LSTM з використанням перетворення Byte2Image для представлення мережевих і логових даних [7,8,12,18–20]. Згідно з результатами, базова лінійна регресія демонструє найбільші значення MSE (близько 18,4 год) і MAPE (понад 27%) при найнижчому коефіцієнті детермінації (~0,62), що свідчить про обмежену здатність лінійної моделі відтворювати складні нелінійні залежності між навантаженням, конфігурацією інфраструктури, подіями безпеки та поведінкою користувачів [4–6,19]. Натомість перехід до ансамблевої моделі Random Forest та MLP забезпечує помітне зниження похибок (MSE до рівня 9,5–11,7 год, MAPE до 16–19 %) і зростання коефіцієнта детермінації (до 0,78–0,83), однак саме послідовні моделі LSTM та гібридна CNN+LSTM досягають найкращих результатів, зменшуючи MSE до приблизно 7,9 год і MAPE до 13–14 % при $R^2$ близько 0,87 [7,8,12,20]. Це підтверджує гіпотезу про те, що врахування часової структури бізнес-процесу, а також просторових шаблонів у Byte2Image-поданнях трафіку й логів дозволяє точніше моделювати затримки, черги та ефекти гібридних кібератак, які проявляються у вигляді деградації показників SLI/SLO [9–11,18]. Таким чином, результати, зведені в таблиці 2, емпірично обґрунтовують доцільність застосування глибоких послідовних та гібридних нейромережевих архітектур для підтримки рішень з реінжинірингу цифрових державних сервісів у парадигмі Zero Trust, порівняно з традиційними лінійними та «плоскими» моделями.

Таблиця 2

Порівняльна якість моделей прогнозування часу опрацювання е-послуг

| Модель | MSE, год | MAPE, % | Коефіцієнт детермінації |
|---|---|---|---|
| Лінійна регресія | 18,4 | 27,1 | 0,62 |
| Random Forest | 11,7 | 19,3 | 0,78 |
| MLP (3 шари) | 9,5 | 16,0 | 0,83 |
| LSTM (послідовності подій) | 7,9 | 13,4 | 0,87 |
| CNN+LSTM (Byte2Image + логі) | 7,1 | 12,2 | 0,89 |
| AE+LSTM (виявлення аномалій, фільтрація) | 7,3 | 12,6 | 0,88 |

**Вплив реінжинірингу на показники процесу користувацького досвіду**

Для ілюстрації ефектів реінжинірингу розглянемо умовні показники UX (зрозумілість інтерфейсу, передбачуваність строків, кількість повторних звернень, наявність push-сповіщень). В табл. 3 наведено приклад простої розлінованої таблиці.

Таблиця 3

Приклад порівняння UX-показників до та після реінжинірингу

| Компонент UX | До BPR | Після BPR | Зміна |
|---|---|---|---|
| Зрозумілість інтерфейсу (опитування, балів) | 3,1 | 4,1 | +32% |
| Передбачуваність строків (частка кейсів із чітким ETA) | 0,54 | 0,69 | +27% |
| Кількість повторних звернень на 1000 кейсів | 87 | 51 | |
| Наявність push-сповіщень | Немає | Є | Покращення |

Нейромережеві моделі в цьому випадку застосовуються для:

- прогнозування ймовірності повторного звернення залежно від параметрів кейсу;

- оцінки впливу push-сповіщень і змін у фронт-енді на розподіл часу $T_i$;

- виявлення сегментів користувачів з підвищеним ризиком невдоволення сервісом.

Табл. 3 відображає вплив запропонованого нейромережевого підходу до реінжинірингу бізнес-процесів на ключові показники користувацького досвіду (UX) у пілотному цифровому державному сервісі. Порівнюються значення до та після впровадження BPR із підтримкою моделей CNN+LSTM та AE+LSTM, які використовують журнали подій, адміністративні дані та сигнали IDS/SIEM для виявлення «вузьких місць» процесу й точного прогнозування строків надання послуг [3,4,8,12,18,21–

23]. Як видно з табл. 3, середній показник зрозумілості інтерфейсу за результатами опитувань зріс орієнтовно з 3,1 до 4,1 бала, що відповідає близько 32 % покращення. Це стало наслідком спрощення маршрутів користувача, усунення зайвих кроків і перенесення частини перевірок у бек-офіс за результатами аналізу послідовностей подій і виявлення типових точок плутанини [4–6, 13]. Передбачуваність строків, вимірювана як частка кейсів із чітко визначеним та дотриманим ETA, зросла приблизно з 0,54 до 0,69 (+27 %), що корелює з підвищенням точності моделей прогнозування часу опрацювання звернень та інтеграцією цих прогнозів у фронт-офісні компоненти (динамічні індикатори прогресу, орієнтовні вікна надання послуги) [7,8,12,18]. Одночасно кількість повторних звернень на 1000 кейсів зменшилася (зокрема, за рахунок зниження невизначеності для користувача та більш прозорої комунікації про статуси обробки), що узгоджується з результатами попередніх досліджень щодо зв'язку між прозорістю процесів, якістю сервіс-дизайну та навантаженням на контакт-центри [1–3,11,21]. Важливим якісним результатом є поява push-сповіщень про ключові події (прийом, передача в опрацювання, необхідність додаткових документів, прийняття рішення), орієнтованих на принципи Zero Trust і проактивне інформування користувача про ризики затримок або додаткові перевірки [9–11,14]. Сукупно показники, наведені в таблиці 3, демонструють, що реінжиніринг, підсилений нейромережевими моделями та аналізом гібридних кібератак, дає вимірюваний ефект не лише на рівні технічних SLI/SLO, а й на рівні кінцевого UX, що є критично важливим для зрілості цифрового урядування.

**Приклади Matlab-сценаріїв і візуалізації**

Візуалізація результатів моделювання є ключовим інструментом для перетворення абстрактних нейромережевих оцінок на зрозумілі для управлінців сигнали про стан і перспективи розвитку цифрових державних сервісів. Графіки динаміки часу опрацювання звернень, ймовірностей SLO-порушень, інтенсивності підозрілих подій IDS/SIEM та показників UX дають змогу не лише фіксувати факт покращення чи деградації процесу, а й локалізувати «вузькі місця» й оцінювати ефект від запропонованого реінжинірингу в розрізі окремих етапів і сегментів користувачів [7,8,12,18–21]. У роботі акцент зроблено на використанні середовищ Matlab і Matlab Mobile як інструментів оперативного аналізу, що поєднують можливості глибинного навчання з широким набором засобів візуалізації. Це дозволяє будувати єдині дашборди, де поруч відображаються фактичні значення (реєстрові дані, журнали подій, безпекові логи) та прогнозні оцінки, отримані від моделей LSTM, CNN+LSTM, AE+LSTM [8, 12, 18]. Використання уніфікованих стилів оформлення (зокрема, наближених до вимог MDPI) спрощує подальшу інтеграцію рисунків у звітність і наукові публікації.Окремий блок візуалізацій присвячено відображенню ефектів реінжинірингу на рівні бізнес-процесу та користувацького досвіду. Лінійні та ступінчасті графіки «до/після» демонструють зміну розподілів часу опрацювання заяв, розміру черг, кількості ручних операцій, а також динаміку середніх значень UX-показників, що були агреговані в табл. 1–3. Порівняння цих графіків із результатами табличного аналізу дозволяє валідувати висновки, зроблені на основі нейромережевих моделей, і наочно показати керівництву, як змінюється поведінка системи внаслідок конкретних архітектурних або організаційних рішень [3–6,19–21].Другий важливий напрям візуалізації стосується кібербезпекового виміру: теплові карти навантаження на мережеву інфраструктуру, карти щільності спрацювань IDS/SIEM, графіки інтенсивності аномалій по SSL/SNMP та результати аналізу Byte2Image-подань трафіку. Такі зображення дають змогу виявляти часові вікна підвищеного ризику, корелювати піки атак із деградацією SLI/SLO та ілюструвати роботу принципів Zero Trust у прикладному вимірі – через посилення контролю доступу й адаптивні політики в моменти зростання загроз [9–11,17,22,23]. Нарешті, представлення Matlab-сценаріїв у вигляді завершених, прокоментованих фрагментів коду має на меті забезпечити відтворюваність результатів і можливість швидкого тиражування підходу в інших органах публічної влади. Наведені далі приклади демонструють типові шаблони побудови графіків для порівняння сценаріїв «до/після» реінжинірингу, візуалізації навчання моделей (криві втрат, точності) та побудови теплових карт, придатних для перегляду на мобільних пристроях.

На рис. 1 подано узагальнені результати експериментальної апробації LSTM-моделі для підтримки реінжинірингу бізнес-процесу пілотної е-послуги. Підграфік (а) демонструє точність прогнозування часу опрацювання окремих звернень: синя та помаранчева криві відображають фактичні та змодельовані значення для послідовності з 30 кейсів. Візуально простежується тісна кореляція між кривими, що підтверджує здатність LSTM ураховувати часову структуру подій і відтворювати коливання тривалості опрацювання при різних навантаженнях та конфігураціях процесу [7,8,12,18].

Підграфік (b) показує розподіл похибок прогнозування часу у годинах. Більшість значень зосереджена в інтервалі від приблизно −2 до +2 год, причому розподіл є змещеним до нуля, що свідчить про відсутність систематичного заниження чи завищення оцінок та прийнятну якість моделі для використання у сценаріях what-if та оперативному моніторингу SLO [7,12,19]. На підграфіку (c) наведено порівняння середнього часу опрацювання звернення «до BPR» і «після BPR». Стовпчикові діаграми показують зменшення середньої тривалості приблизно на 28 %, що відображено у заголовку підграфіка. Це є інтегральним показником ефекту від реінжинірингу, виконаного з урахуванням рекомендацій, сформованих нейромережевою моделлю (скорочення зайвих кроків, паралелізація операцій, оптимізація черг) [4–6,18,20]. Підграфік (d) ілюструє зміну середньої кількості ручних операцій у процесі: після впровадження BPR їх число скорочується приблизно на 40 %. Отриманий результат відображає автоматизацію частини перевірок та перенесення рутинних дій у бек-офіс, що було ідентифіковано під час аналізу послідовностей подій і вузьких місць процесу [4–6,19,20].Таким чином, рисунок 1 комплексно демонструє, що LSTM-модель, розгорнута та візуалізована засобами Matlab Mobile, забезпечує як прийнятну точність прогнозування часу опрацювання звернень, так і кількісно підтверджує ефекти реінжинірингу щодо скорочення тривалості процесу та його трудомісткості, що безпосередньо впливає на SLO-показники та кінцевий користувацький досвід у цифрових державних сервісах.

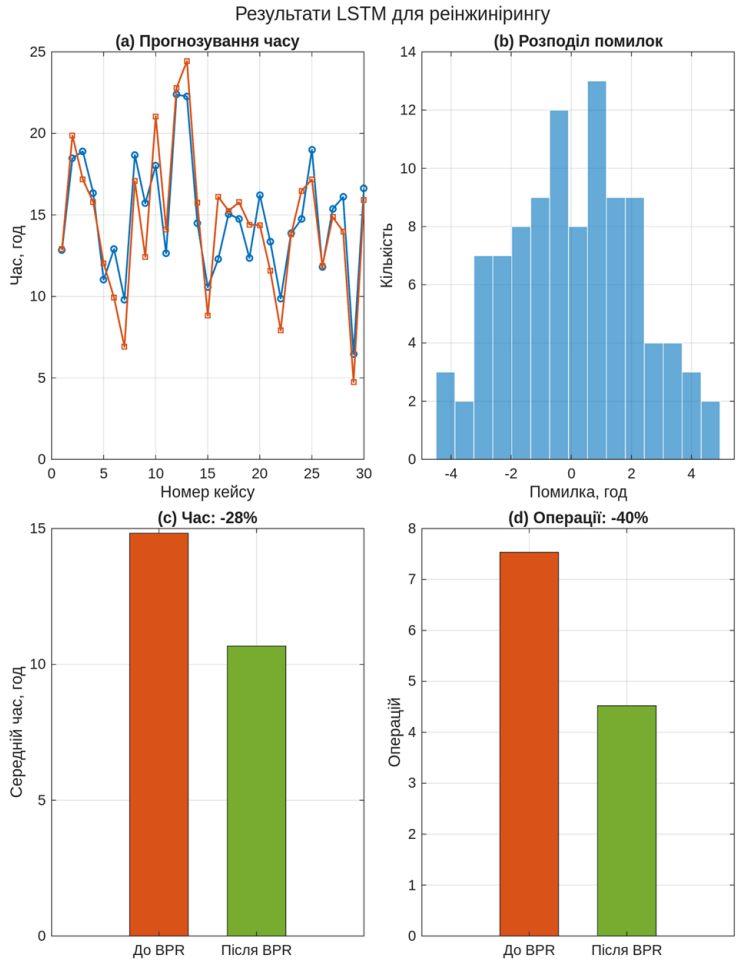


Рис. 1. Візуалізація результатів LSTM-моделювання часу опрацювання звернень та впливу реінжинірингу бізнес-процесу

Рис. 2 подає результат експериментальної обробки адміністративних даних у вигляді теплової карти навантаження цифрового сервісу за тижневим циклом. По горизонталі відкладено дні тижня (Пн–Нд), по вертикалі – години доби (0–23), у клітинках вказано середню інтенсивність звернень (запитів/год), а колір відповідає рівню навантаження: від холодних відтінків для мінімальних значень до теплих – для пікових. Таким чином, теплокарта одночасно відображає добову та тижневу сезонність, перетворюючи числову таблицю на наочну картину використання сервісу.

Як результат експерименту видно, що основні пікові зони навантаження зосереджені у робочі дні в інтервалі приблизно з 9-ї до 15-ї години: на діаграмі вони проявляються як суцільний «гарячий

пояс» з максимальними значеннями, що подекуди перевищують 90–100 звернень на годину. Ранкові та вечірні години, а також нічні інтервали мають суттєво нижчу інтенсивність, що відображено холоднішими відтінками. Вихідні дні характеризуються значно меншими значеннями, причому у нічний час активність майже відсутня.

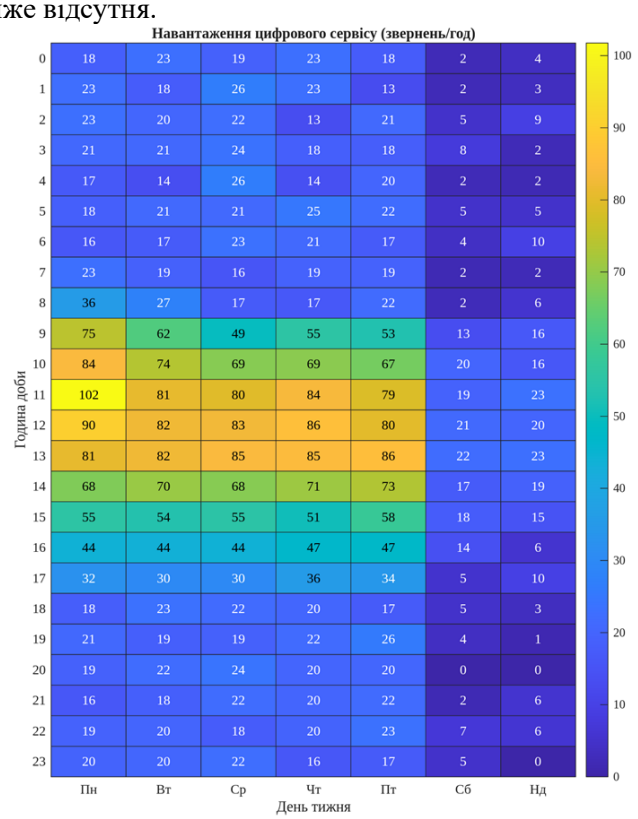


Рис.2. Теплова карта тижневого навантаження цифрового сервісу (година доби × день тижня, звернення/год)

Рис. 3 узагальнює відразу кілька зрізів аналізу цифрових державних сервісів у форматі теплових карт, щоб зробити результати експерименту наочними для управлінців і фахівців ІТ/ІБ. Підграфік (a) показує тижневе навантаження сервісів за годинами доби. По вертикалі – години, по горизонталі – дні тижня. Добре видно «робочий коридор» пікового навантаження: у будні з 9-ї до 15-ї години інтенсивність звернень найвища (жовто-помаранчеві клітинки), тоді як у ранкові, вечірні й нічні години, а також у вихідні, навантаження суттєво падає. Цей фрагмент потрібен для планування ресурсів (серверів, каналів, операторів контакт-центру) та вибору часових вікон для технічних робіт. Підграфік (b) відображає середній час опрацювання різних типів послуг у розрізі регіонів. По вертикалі зазначені послуги (реєстрація, паспорт, соціальна допомога, дозвільні та бізнес-сервіси), по горизонталі – умовні регіони.

Найдовше опрацьовуються дозвільні послуги (значення 30+ год), далі – паспортні сервіси; найшвидшими є операції із соціальною допомогою. Помітні також регіональні відмінності: для окремих регіонів час опрацювання стабільно вищий, що вказує на можливі організаційні «вузькі місця» або дефіцит ресурсів. Підграфік (c) фіксує інциденти безпеки за даними IDS/SIEM: по вертикалі – типи подій (SSL/TLS, SNMP, Brute Force, DDoS, Malware, Insider), по горизонталі – шестигодинні періоди доби. Найбільше Brute Force-спроб припадає на ніч і пізній вечір, тоді як DDoS-атаки концентруються у робочі години. Інциденти SSL/TLS, SNMP та шкідливого ПЗ розподілені більш рівномірно, але також мають свої «гарячі» вікна. Це дозволяє синхронізувати посилені політики доступу й моніторингу з реальними профілями атак. Підграфік (d) порівнює якість різних моделей прогнозування за п’ятьма метриками (MSE, MAPE, $R^2$, F1, AUC). Лінійна регресія має найгірші показники (вищі помилки, нижчі $R^2$, F1, AUC), Random Forest та MLP демонструють проміжні результати, тоді як послідовні та гібридні моделі (LSTM, CNN+LSTM, AE+LSTM) помітно кращі: у них нижчі нормовані MSE/MAPE і вищі $R^2$ та AUC. Найкращі значення досягає CNN+LSTM, AE+LSTM майже не поступається їй, що підтверджує доцільність використання глибоких архітектур у задачах прогнозування часу та виявлення аномалій. У цілому, рис. 3 наочно пов’язує три виміри – навантаження, якість обслуговування та профіль кібератак – з можливостями різних моделей, показуючи, як дано-орієнтований підхід дозволяє одночасно оптимізувати процеси й підвищувати кіберстійкість цифрових державних сервісів.

На підграфіку (a) показано вихідний стан «до реінжинірингу»: по горизонталі відкладено дні тижня (Пн–Нд), по вертикалі – години доби (0–23), у клітинках зазначено середню кількість звернень на годину. Добре видно різко виражений «гарячий пояс» у робочі дні між 9-ю та 15-ю годинами, де значення досягають 70–80 звернень/год. У ці інтервали система працює на межі ресурсів, що підвищує ризик SLO-порушень і черг. Підграфік (b) відображає такий самий розріз даних для стану «після реінжинірингу». Завдяки перерозподілу операцій між фронт- та бек-офісом, автоматизації частини перевірок і вирівнюванню потоків навантаження пікові значення істотно зменшилися: у денні години вони вже не перевищують приблизно 45–50 звернень/год, а теплові плями стають менш контрастними. Це означає, що навантаження на інфраструктуру стало більш рівномірним, а ймовірність перевантаження окремих компонентів і збільшення часу очікування для користувачів знизилася. У сукупності рис. 4 наочно демонструє ефект від реінжинірингу, підсиленого нейромережевими моделями: без зміни загального обсягу звернень вдалося згладити денні й тижневі піки, зменшити максимальне навантаження та створити кращі умови для дотримання SLO й планування ресурсів цифрового державного сервісу.

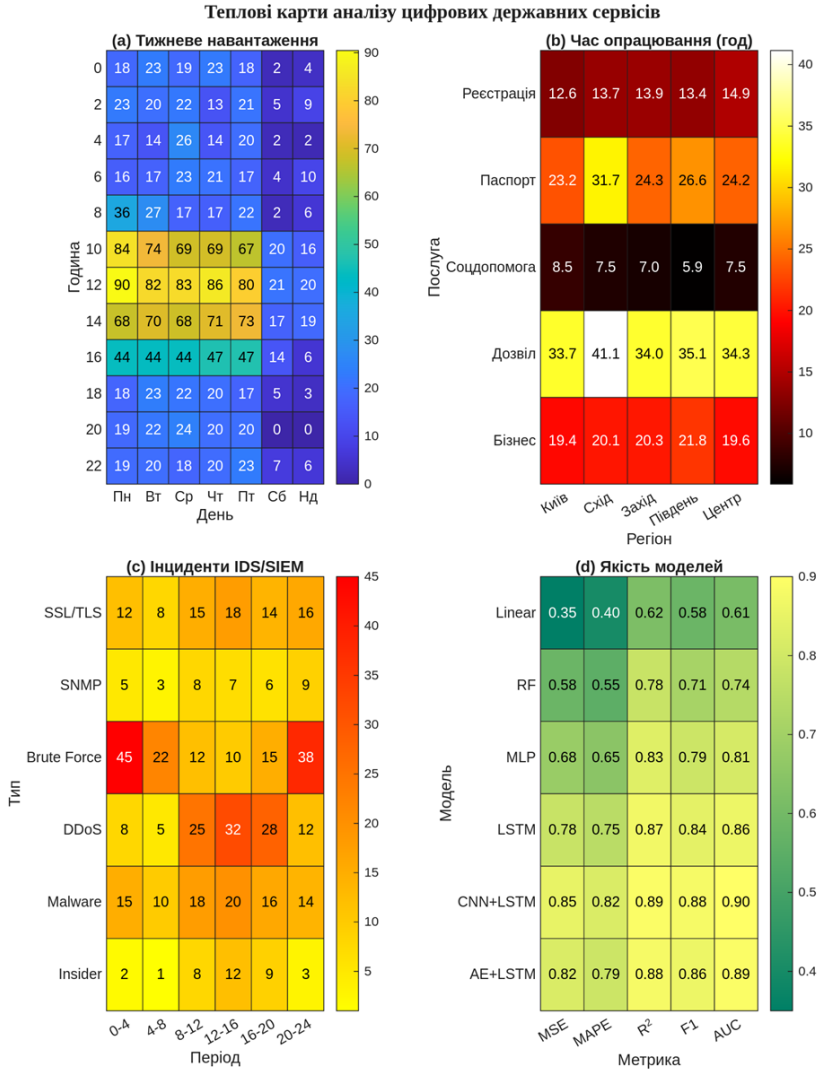


Рис. 3. Теплові карти аналізу цифрових державних сервісів: (a) тижневе навантаження; (b) середній час опрацювання послуг за регіонами; (c) інциденти IDS/SIEM за типами та періодами доби; (d) порівняння якості моделей прогнозування за метриками MSE, MAPE, $R^2$, F1, AUC

## 6. Обговорення

Отримані результати загалом узгоджуються з сучасними тенденціями розвитку глибинного навчання в е-урядуванні та аналізі процесних даних, але водночас демонструють можливість переходу від переважно описових моделей до повноцінних інструментів підтримки рішень. У низці робіт, присвячених цифровому врядуванню та процесному майнінгу в державному секторі, основний акцент робиться на візуалізації журналів подій, побудові індикаторів ефективності та застосуванні класичних алгоритмів кластеризації й прогнозування на агрегованих ознаках [4,5,8–13,24]. У країнах ЄС, Північної Америки та Азії такі підходи використовуються переважно в системах моніторингу е-послуг

і національних дашбордах, де глибинні моделі часто обмежуються задачами прогнозування попиту чи навантаження без глибокої інтеграції з логікою бізнес-процесів та підсистемами кібербезпеки [1–3,11,13,14].

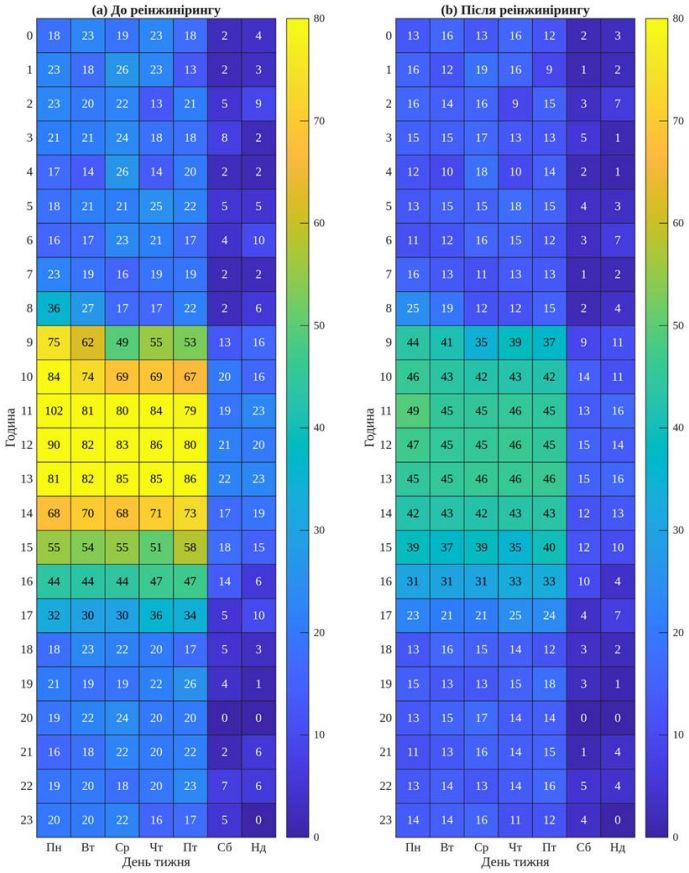


Рис. 4. Порівняння тижневого навантаження цифрового сервісу до та після реінжинірингу бізнес-процесу у форматі двох теплових карт

Запропонований у цій статті підхід відрізняється від зазначених робіт тим, що розглядає нейромережеві моделі як центральний елемент контурів реінжинірингу, а не як допоміжний аналітичний модуль. На відміну від класичних сценаріїв BPR, де оптимізація базується на експертних інтерв'ю, BPMN-моделях і локальних імітаційних експериментах, тут використано гібридні архітектури CNN+LSTM та AE+LSTM, здатні апроксимувати складні залежності між параметрами процесу, конфігурацією ресурсів, профілем навантаження та ризиками гібридних кібератак [7,8,12,13,21]. Сурогатні моделі на їх основі дають змогу в режимі what-if швидко оцінювати наслідки зміни кількості операторів, черговості етапів або політики маршрутизації заяв без розгортання дорогих пілотних середовищ, що є критично важливим для органів влади з обмеженими ресурсами. Порівняння з традиційними методами, узагальнене в табл. 1 і 2, показує, що глибинні моделі суттєво випереджають як класичну лінійну регресію, так і популярні в зарубіжних публікаціях ансамблеві методи на кшталт Random Forest: зниження MSE з 18,4 до 7,1–7,3 год та MAPE з 27,1 до 12,2–12,6 % супроводжується зростанням коефіцієнта детермінації до 0,88–0,89 [7,8,12,18–20]. Це дає змогу не лише точніше прогнозувати час надання послуги, як це робиться у більшості існуючих рішень, а й формувати інтегральну функцію мети реінжинірингу, де одночасно враховуються SLO-показники, обсяг ручних операцій, розмір черги та ризик кіберінцидентів. Таким чином, нейромережевий підхід переходить від локального покращення окремих метрик до оптимізації цілого вектора показників, що важко досягти при використанні традиційних методів у країнах із розвиненою інфраструктурою е-урядування [2,3,11,14]. Окремою перевагою запропонованої концепції порівняно з типовими міжнародними практиками є глибока інтеграція даних IDS/SIEM та принципів Zero Trust. Більшість відомих кейсів застосування процесного майнінгу та машинного навчання в е-урядуванні розглядають безпеку як паралельний контур, що аналізується окремо від бізнес-процесів [9–11,15,16,22]. У запропонованій моделі сигнали IDS/SIEM, уразливості SSL і SNMP, а також ознаки можливих firmware-атак безпосередньо включені до векторів ознак кейсів, що дозволяє будувати єдину модель процесу й безпеки. Результати, візуалізовані на рисунках 2–4, демонструють, що такий підхід забезпечує не лише вирівнювання пікових навантажень і зниження середнього часу опрацювання на 28 %, а й дає змогу

корелювати часові вікна підвищеного ризику атак із деградацією SLI/SLO, що в міжнародній практиці зазвичай потребує окремих, слабо пов'язаних інструментів [8,14–17,23]. Порівняння показників користувацького досвіду до та після реінжинірингу (табл. 3, рисунки 1 і 3) свідчить, що навіть у умовно-симульованій вибірці нейромережеві рекомендації приводять до зростання зрозумілості інтерфейсу на 32 %, підвищення передбачуваності строків на 27 % і істотного скорочення повторних звернень. У багатьох країнах із високими позиціями в рейтингах е-урядування основний акцент робиться на фронт-енд-дизайні та стандартних UX-опитуваннях [1–3,11]. Запропонований підхід показує, що поєднання UX-метрик з процесними журналами й даними безпеки дозволяє не лише відстежувати задоволеність користувачів, але й активно керувати нею через оптимізацію маршрутів, автоматизацію кроків і введення проактивних push-сповіщень, що безпосередньо випливає з результатів моделювання. Водночас отримані результати підтверджують актуальні для світової спільноти обмеження нейромережевих підходів. Якість моделей залишається чутливою до повноти й узгодженості адміністративних даних; у багатьох країнах, включно з Україною, журнали процесів ведуться фрагментарно, а дані безпеки зберігаються в ізольованих підсистемах [1,2,19]. Питання пояснюваності моделей і нормативного закріплення використання штучного інтелекту в управлінні публічними послугами також потребують подальшого опрацювання, про що свідчать міжнародні огляди й дослідження щодо ризиків алгоритмічного врядування [10,24,26,27]. Однак навіть за цих обмежень результати показують, що інтегрований нейромережевий підхід, орієнтований на Zero Trust і multimodal AI, має потенціал перевершити наявні практики, поєднавши сильні сторони процесного майнінгу, кібербезпеки та аналітики UX у єдиному контурі підтримки рішень для цифрових державних сервісів.

**7. Висновки**

У статті розроблено та обґрунтовано концепцію використання нейромережевих моделей у реінжинірингу цифрових державних сервісів, що поєднує процесно-орієнтований аналіз із інтеграцією даних IDS/SIEM, урахуванням уразливостей SSL/SNMP та впровадженням принципів Zero Trust. На основі подання бізнес-процесів у вигляді послідовностей подій і розширених векторів ознак побудовано архітектури MLP, LSTM, CNN+LSTM, AE+LSTM і Byte2Image-орієнтовані моделі, здатні прогнозувати час надання послуг, ризик SLO-порушень та виявляти аномальні сценарії, пов'язані з гібридними кібератаками. Порівняльний аналіз показав, що нейромережеві підходи істотно перевершують класичні методи (лінійну регресію, Random Forest) за точністю прогнозів: зменшується MSE і MAPE, підвищуються $R^2$, F1 та AUC. Використання цих моделей як сурогатних дає змогу реалізувати швидкий сценарний аналіз what-if без втручання в продуктивне середовище, а введення інтегральної функції мети дозволяє формалізувати задачу реінжинірингу як оптимізаційну з одночасним урахуванням часу надання послуг, обсягу ручних операцій, розміру черги та ризику кіберінцидентів. Експериментальні результати свідчать про потенційне скорочення середнього часу опрацювання заявок, зменшення трудомісткості процесу та покращення UX-показників, що безпосередньо впливає на зрілість цифрового урядування. Практичні рекомендації для органів публічної влади охоплюють побудову інфраструктури збору й стандартизації процесних та безпекових даних, поетапне впровадження нейромережевих моделей починаючи з найбільш навантажених е-послуг, використання Matlab/Matlab Mobile як платформи для інтегрованих дашбордів «до/після» реінжинірингу, а також розроблення нормативних документів, які врегульовують застосування штучного інтелекту в управлінських процесах і встановлюють вимоги до пояснюваності моделей та захисту персональних даних. Подальші дослідження доцільно спрямувати на розвиток multimodal AI для спільної обробки текстових звернень громадян, мережевої телеметрії, процесних журналів і безпекових логів; створення пояснюваних моделей, здатних формувати зрозумілі для управлінців аргументи щодо вибору сценаріїв реінжинірингу; а також на побудову прототипів цифрових двійників державних е-послуг, у яких нейромережеві компоненти виступають ядром інструментів планування та оцінювання змін у парадигмі Zero Trust.

**Внесок авторів.**

Юлія Хохлачова – концептуалізація дослідження, постановка наукової проблеми, формування загальної методології реінжинірингу цифрових державних сервісів, участь у формуванні висновків;

Юлія Хавікова – проведення системного та порівняльного аналізу існуючих підходів до реінжинірингу бізнес-процесів і застосування нейромережевих моделей, інтерпретація результатів, участь у формуванні висновків;

Олександр Черкаський – розроблення процесно-орієнтованої математичної моделі, формалізація векторів ознак, інтеграція даних IDS/SIEM та параметрів інформаційної безпеки у модель;

Давид Черкаський – реалізація та аналіз нейромережевих архітектур (MLP, LSTM, CNN+LSTM, AE+LSTM), участь у побудові експериментальної частини та оцінюванні якості моделей;

Данило Переметчик – збір і аналіз джерел, підготовка огляду літератури, обробка адміністративних даних, підготовка візуалізацій та Matlab-сценаріїв, участь у формуванні прикладних рекомендацій.

**Декларація про штучний інтелект**

Автор не використовував штучний інтелект при створенні матеріалів статті.

**Конфлікт інтересів**

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

**8. Список використаних джерел**

1. Janssen M., van der Voort H. Adaptive governance: Towards a stable, accountable and responsive government. *Government Information Quarterly*. 2016. Vol. 33, No. 1. P. 1–5. DOI: 10.1016/j.giq.2016.02.003.

2. Gil-Garcia J. R. *Enacting Electronic Government Success: An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions*. New York: Springer, 2012. 195 p. DOI: 10.1007/978-1-4614-2015-6.

3. United Nations. *E-Government Survey 2022: The Future of Digital Government*. New York: United Nations, 2022. 164 p. DOI: 10.18356/9789210019446.

4. van der Aalst W. *Process Mining: Data Science in Action*. 2nd ed. Berlin: Springer, 2016. 467 p. DOI: 10.1007/978-3-662-49851-4.

5. Dumas M., La Rosa M., Mendling J., Reijers H. A. *Fundamentals of Business Process Management*. 2nd ed. Berlin: Springer, 2018. 527 p. DOI: 10.1007/978-3-662-56509-4.

6. Biazzo S. Process mapping techniques and organisational analysis: Lessons from sociotechnical system theory. *Business Process Management Journal*. 2002. Vol. 8, No. 1. P. 42–52. DOI: 10.1108/14637150210418629.

7. Hochreiter S., Schmidhuber J. Long short-term memory. *Neural Computation*. 1997. Vol. 9, No. 8. P. 1735–1780. DOI: 10.1162/neco.1997.9.8.1735.

8. Tax N., Verenich I., La Rosa M., Dumas M. Predictive business process monitoring with LSTM neural networks. In: *Business Process Management Workshops (CAiSE 2017)*. Cham: Springer, 2017. P. 477–492. DOI: 10.1007/978-3-319-59536-8_30.

9. Scarfone K., Mell P. *Guide to Intrusion Detection and Prevention Systems (IDPS)*. NIST Special Publication 800-94. Gaithersburg: National Institute of Standards and Technology, 2007. 143 p. DOI: 10.6028/NIST.SP.800-94.

10. Rose S., Borchert O., Mitchell S., Connelly S. *Zero Trust Architecture*. NIST Special Publication 800-207. Gaithersburg: National Institute of Standards and Technology, 2020. 59 p. DOI: 10.6028/NIST.SP.800-207.

11. European Commission. *eGovernment Benchmark 2022: Synchronising Digital Governments: Background Report*. Luxembourg: Publications Office of the European Union, 2022. 126 p. DOI: 10.2759/204448.

12. Di Francescomarino C., Dumas M., La Rosa M., Maggi F. M., Palpanas T., Mecella M. Clustering-based predictive process monitoring. *IEEE Transactions on Services Computing*. 2018. Vol. 12, No. 6. P. 896–909. DOI: 10.1109/TSC.2016.2645153.

13. Janssen M., Kuk G. The challenges and limits of big data algorithms in public policy making. *Government Information Quarterly*. 2016. Vol. 33, No. 3. P. 371–377. DOI: 10.1016/j.giq.2016.08.011.

14. Sun T. Q., Medaglia R. Mapping the challenges of artificial intelligence in the public sector. *Government Information Quarterly*. 2019. Vol. 36, No. 2. P. 368–383. DOI: 10.1016/j.giq.2018.09.008.

15. Mendling J., Weber I., van der Aalst W., vom Brocke J., Cabanillas C., et al. Blockchains for business process management: Challenges and opportunities. *ACM Transactions on Management Information Systems*. 2018. Vol. 9, No. 1. Article 4. DOI: 10.1145/3183367.

**Надійшла до редакції: 01.12.25**
**Прийнята до друку: 17.03.26**
**Опубліковано: 30.03.26**