Друковане видання ISSN 2616-6437
Онлайн видання ISSN 2708-9746

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
імені ВАДИМА ГЕТЬМАНА

Збірник наукових праць «Моделювання та інформаційні системи в економіці» входить до переліку наукових фахових видань категорії «Б». Наказ Міністерства освіти і науки України № 886 від 02.07.2020 року.

Моделювання та інформаційні системи в економіці

Збірник наукових праць

Заснований у 1965 р.

№ 102

Головний редактор *О. Є. Камінський*

КНЕУ КИЇВ 2022

УДК 311:519.2:519.86

Рекомендовано до друку Вченою радою КНЕУ
Протокол № 5 від 01.12.2022 р.

Моделювання та інформ. системи в економіці : зб. наук. праць / відп. ред. О. Є. Камінський. 2022. № 102. 204 с.

Адреса редакційної колегії:
04053, м. Київ, вул. Дегтярівська, 49-г, кімн. 82.
Київський національний економічний університет імені Вадима Гетьмана

Засновник та видавець
Державний вищий навчальний заклад
«Київський національний економічний університет імені Вадима Гетьмана»

Засновано в Міністерстві юстиції України
Свідоцтво про державну реєстрацію КВ № 11718-589Р від 11.09.2006

ЗМІСТ

CONTENTS

УДК 659.1 DOI 10.33111/mise.102.1

Агутін М.М., к.е.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет імені Вадима Гетьмана

Ahutin M.M., Candidate of Economic Science,
Associate Professor of Department of Computer Mathematics and Information Security,
KNEU named after V. Hetman

***Ключові слова**: кольорова мережа Петрі; оптимізація рекламного бюджету; рекламне просування; вебпроєкт.*

***Abstract**. The article is devoted to the topical issues of modeling advertising promotion of goods and services, as well as marketing in social media using Petri nets tools. The typical stages and marketing tools of the website advertising promotion project and options for their improvement are defined. Selected approaches to the use of labeling in colored Petri nets during the stages of the advertising promotion project.*

The purpose of the article is to improve and expand the mathematical model of advertising promotion of the Internet resource and to use the methods of modeling colored Petri nets for the analysis and improvement of advertising companies for the promotion of goods and services. The variety of technologies and means of digital marketing on the modern Internet market does not allow direct assessment of advertising promotion processes and their effectiveness. Modeling based on colored Petri nets allows you to approximate the effectiveness of using certain means of advertising promotion. A new result is the use of mathematical modeling methods and colored Petri net tools to determine the optimal means of advertising the goods and services of digital enterprises. Flexibility and ease of use, combined with the structural and functional characteristics of Petri nets, help to fully realize the potential of color Petri nets in terms of versatility in terms of project management of advertising promotion, implementing structured algorithms for better control and project management. The developed approach to the management of the advertising promotion project can be used in the marketing and advertising departments of commercial enterprises, Internet agencies and advertising firms to justify marketing activities.

***Keywords**: colored Petri net; optimization of the advertising budget; advertising promotion; Web project.*

Постановка проблеми у загальному вигляді. Успіх будь-якого проєкту рекламного просування товарів і послуг залежить від низки факторів, таких як бюджет та час здійснення проєкт, а також обраних засобів рекламного просування. Виб ір правильних засобів маркетингу та відсіювання потенційно невдалих засобів рекламного просування є найважливішим кроком для забезпечення повного успіху проєкту. Зокрема, серед факторів, що впливають на успіх проєкту рекламного просування, є декілька, включаючи недоцільно обрані засоби рекламного просування,

неадекватно визначені терміни й завдання і неправильне використання засобів маркетингу. Останній фактор відіграє ключову роль і висвітлює обрання конкретної технології та засобів рекламного просування вебпроєктів для успішної реалізації плану маркетингу. Крім того, реалізація проєкту потребує залучення багатьох маркетингових заходів, які використовуються у різних сегментах рекламного просування. Також, комплекс економічних, управлінських, фінансових та ринкових факторів робить кожен проєкт рекламного просування відмінним, оскільки непередбачені події є звичайними під час реалізації проєкту. Отже, щоб керувати складним проєктом рекламного просування, необхідно застосовувати сувору методологію, засновану на принципах і систематичних правилах.

Аналіз останніх досліджень і публікацій. Питаннями аналізу інструментів маркетингу та оцінки ефективності проєктів рекламного просування присвячено чимало досліджень таких вчених як Р. Голдміт, Ф. Котлер, С. Сеті та інших. Теоретичні підходи та методологічну основу використання мереж Перті автори К. Єнсен [1] і Дж. Петерсен [2]. Останнім часом було проаналізовано багато економіко-інформаційних та технологічних систем з використанням апарату мереж Петрі високого рівня, включаючи атрибути «колір», «час» та «ієрархія». Звідси дослідження [4] висвітлює шлях до розширених атрибутів мереж Петрі для допомоги менеджерам в управлінні параметрами проєктної рекламної та маркетингової діяльності.

Вибір найкращого варіанта поєднання засобів рекламного просування товарів та послуг лишається відкритим питанням і залежить від багатьох факторів. Вирішенню цього присвятили роботи фахівці з маркетингу. У статті пропонується один із підходів на основі кольорових мереж Петрі.

Метою статті є обґрунтування переваги кольорових мереж Петрі у сфері управління проєктами маркетингу та рекламного просування товарів та послуг. Реалізований інструмент на основі кольорових мереж Петрі дозволяє збирати більш надійну інформацію для планування та контролю проєкту рекламного просування, контролювати витрати ресурсів на використання інструментів маркетингу.

Дослідження, спрямоване на розробку нового підходу до моделювання та управління проєктами рекламного просування з використанням потужних аналітичних інструментів — кольорові мережі Петрі.

Виклад основного матеріалу дослідження. Розглянемо комплексну систему взаємодії вебсайту з клієнтами як потенційними, так і наявними. Програмна реалізація таких систем може відріз-

нятися. Розглянемо поширений приклад системи, яка використовує кілька варіантів взаємодії з клієнтом: електронна пошта, автоматичні телефонні дзвінки, повідомлення в соціальних медіа, sms- і push-повідомлення в мобільних пристроях зв'язку та ін. Маркетинговий план заходів з рекламного просування товарів і послуг вміщує низку заходів, які можуть бути як традиційними, так і новітніми.

Під час поетапного втілення плану маркетингу підприємство використовує найбільш прогресивні засоби рекламного просування:

– контекстна і пошукова реклама;
– заходи seo-просування;
– таргетинг і воронки продажів;
– CRM-системи та аналіз взаємовідносин фз клієнтами;
– маркетинг у соціальних мережах (smm);
– e-mail-розсилки;
– мобільний маркетинг (sms- і push-повідомлення);
– банерна і поведінкова реклами.

Кінцевою метою рекламного просування товарів і послуг в мереж Інтернет — отримання прибутку від продажів. Для цієї мети можуть бути використані різні напрями і засоби рекламного просування, а деякі засоби можуть використовуватись паралельно.

Ми пропонуємо модель розповсюдження рекламних повідомлень на основі кольорових мереж Петрі, який дає повний формальний опис поширення рекламної інформації. Проаналізуємо зміни стану та послідовності поведінки системи під час отримання інформації для запропонованої моделі за допомогою кольорових мереж Петрі, що дозволить обґрунтувати раціональність і коректність побудованої моделі. У межах запропонованої моделі проаналізуємо варіанти поведінки споживачів, а також розглянемо деякі нові ідеї для оптимізації впливу рекламної інформації на споживачів товарів та послуг.

Аналіз різних варіантів реалізації мереж Петрі, особливостей процесів рекламного просування в мережі Інтернет, можливість оцінити часові характеристики та параметри засобів рекламного просування показав, що найбільш адекватною реалізацією мереж Петрі для рекламного просування виступають кольорові мережі Петрі (Colored Petri Nets, CPN). Особливістю реалізації кольорових мереж Петрі є наявність вузлів переходів до наступних етапів(позицій), в яких визначається шлях проходження мережі Петрі залежно від статусу виконання попередніх етапів мережі — маркерів. Кольорові мережі Петрі, отже, дозволяють створити

імітаційну модель проєкту рекламного просування товарів і послуг, об'єктами якої є маркери рекламного просування.

Модель, заснована на кольорових мережах Петрі, здатна моделювати систему, в якій багато дій відбуваються одночасно та асинхронно. Можна розглянути моделювання паралельності та конфліктів, а також взаємоблокування системи. Крім того, використання кольорових мереж Петрі дозволяє керівнику проєкту перевіряти його стан працездатності, виявляючи ймовірні затримки діяльності. Кольорові мережі Петрі також можуть моделювати дії з відновлення та перепланування, враховуючи збої та обмеження ресурсів. Використовуючи місця та переходи, можна представити проєкт / процес динамічно графічно через підмережі, що робить можливим імітацію всієї системи. Звідси модель системи зможе представити взаємозалежність ресурсів, частковий розподіл, заміну та взаємну винятковість.

Як формальна мова моделювання кольорові мережі Петрі (далі — КМП) підходять для моделювання та імітації складних розподілених паралельних систем. Цей метод моделювання дозволяє описати динамічний робочий процес у системі завдяки її графічній функції. Кольорові мережі Петрі використовують формальний метод аналізу для визначення властивостей моделі. Він недоступний для інших методів моделювання. Якщо порівнювати з мережею Петрі модель, побудовану на КМП, то вона є простішою і чіткіше відображає процеси, що відбуваються в системі.

Характеристики кольорової мережі Петрі для рекламного просування вебресурсу задані таким списком параметрів:

$$CPN = (P, T, A, S, N, C, G, M_O), \quad (1)$$

де $P = \{p_1, p_2, ..., p_m\}$ — гранична множина послідовних етапів (станів) рекламного просування товарів і послуг окремої кампанії, $T = \{t_1, t_2, \ldots, t_k\}$ — кінцева множина вузлів переходів між етапами рекламного просування; $A = \{a_1, a_2, \ldots, a_m\}$ — кінцева множина спрямованих дуг від точок виникнення до точок призначення, які показують, де проходять інформаційні потоки; S — граничний набір ознак кольорів, який визначає типи маркерів на кожному етапі мережі Петрі; V — кінцевий набір типових змінних; C — функція визначення кольору $P \rightarrow S$, який призначається кожному етапу залежно від типу переходу; M_O — функція ініціалізації, яка визначає початковий стан маркерів мережі.

Модель системи, визначену за допомогою підходу кольорових мереж Петрі, можна описати так, як показано у багатоетапну процедуру, подану на рис. 1.

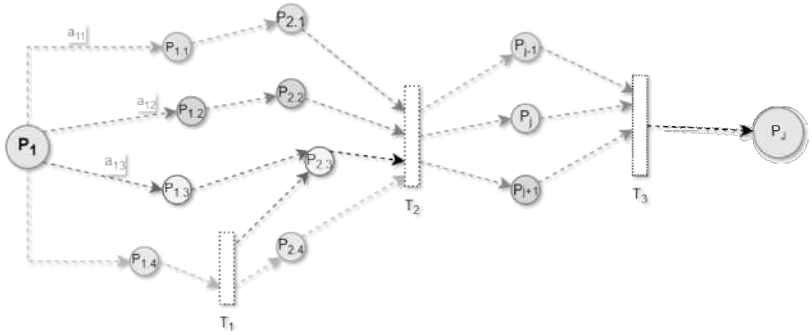


Рис. 1. Схема процесів функціонування кольорової мережі Петрі з умовними позначенням етапів проєкту, вузлів переходів і спрямованих дуг між ними

Структура розподілу етапів рекламного проєкту, яка описує та групує окремі робочі операції проєкту, організовує й визначає остаточний обсяг необхідних ресурсів. Пов'язані кроки дають можливість встановити обсяги проєкту і його ймовірні результати.

Виходячи з визначення мереж Петрі, можна так інтерпретувати компоненти мереж Петрі для проєкту рекламного просування товарів та послуг фірми:

1. Множина етапів *P* відповідає етапам або задачам рекламного просування, таким як: «надіслано рекламне push-повідомлення в мобільний додаток», «здійснено електронну розсилання рекламних e-mail листів», «клієнтом у відповідь на рекламне оголошення здійснено розміщення замовлення» тощо;

2. Множина переходів *T* мережі Петрі відповідає певним заходам, під час яких приймається рішення щодо тих чи інших подальших етапів (кроків) на основі наявної інформації, що може переключати систему з одного статусу до іншого;

3. Сукупність дуг *A* мережі призначена для зв'язку між етапами проєкту рекламного просування та множиною переходів *T*. Множина дуг визначає порядок виконання етапів та розпаралелювання задач, забезпечує процеси створення, виконання та утилізації маркерів задач рекламного просування.

4. Кожен етап виконання проєкту рекламного просування характеризується низкою змінних *V*, серед яких — витрачений час та інші ресурси.

5. У процесі вирішення завдань проєкту рекламного просування відбувається послідовний рух маркерів, які впливають на етапи (стани) як простір станів побудованої моделі.

Визначення етапів проєкту дозволяє проаналізувати кожний крок проєкту рекламного просування для ідентифікації всіх його відповідних характеристик, таких як запит ресурсів, тривалість і пріоритет. Результатом цього є визначення ресурсів і часових обмежень, а також політики пріоритетів.

Отже, усі ці елементи сприятимуть визначенню кольорів, які використовуються для маркування, побудови та симуляції моделі кольорових мереж Петрі. Аналіз результатів моделювання порівнюється зі специфікацією проєкту, щоб запланувати різні види маркетингових заходів і вибір інструментів рекламного просування для виконання конкретних завдань. Ресурси для проєкту рекламного просування можна перерозподіляти з завдань, які не перебувають на критичному шляху, до завдань, які критично важливі. У дослідженні не ставиться завдання автоматичного з'ясування цих змін.

На основі алгоритму пошуку критичного шляху для початкового мережевого графа встановлено етапність, резерви часу на кожну подію і кожен вид роботи. Крім того, в алгоритмі найкоротшого шляху, в оцінці раннього часу початку подій, запропоновано використовувати верхню межу, а під час оцінювання пізнього часу початку подій — нижню межу. Цей підхід можна інтерпретувати так: найгірший випадок раннього старту враховується час і максимальна швидкість досягнення більш пізнього часу старту.

Висновки. Моделювання рекламного просування вебресурсів і продуктів в мережі Інтернет здійснено на базі апарату кольорових мереж Петрі. Побудована модель технологічного процесу рекламного просування дозволяє оптимізувати параметри витрат часу та фінансових ресурсів на проведення рекламних та маркетингових заходів. Імітаційне моделювання проєкту рекламного просування за допомогою кольорових мереж Петрі, завдяки прийняттю концепції часу та кольорів для деталізації дій, може виробляти багато кількісної інформації про продуктивність системи, такої як споживання ресурсів, час виконання всього процесу, щоб бути корисною обробкою для кращого планування проєкту і контролювання. Гнучкість і простота використання, поєднані зі структурними і функціональними характеристиками мереж Петрі, допомагають повністю досягти потенціалу кольорових мереж Петрі щодо універсальності з позицій управління проєктом рекламного просування, реалізуючи структуровані алгоритми для кращого контролю та управління проєктом.

Було запропоновано варіант маркування маркетингових засобів і рекламних каналів просування товарів та послуг і розгляну-

то варіанти реалізації відокремлених каналів незалежно один від одного.

У подальших дослідженнях пропонується вдосконалення параметрів моделі рекламного просування з урахування особливостей різних видів засобів маркетингу, а також імітаційне модулювання окремих каналів просування в побудованій системі з урахуванням маркерів пріоритетів та часу обслуговування замовлень.

Бібліографічні посилання

1. Jensen K., Kristensen L.M. Formal Definition of Timed Coloured Petri Nets. In Coloured Petri Nets; Springer: Berlin / Heidelberg, Germany, 2009; pp. 257–271.
2. Chung TH. Modeling of Construction Scheduling with Coloured Petri Nets. in 2011 International Conference on Process Automation, Control and Computing (PACC) 2011. IEEE.
3. Peterson James P. Petri Net Theory and the Modeling of Systems. Michigan: Prentice-Hall, 1981.
4. Scott-Young C, Samson D. Project success and project team management: Evidence from capital projects in the process industries. *Journal of Operations Management*. 2008; 26: 749-766.
5. Агутін М.М., Дем'яненко В.В., Потапенко С.Д. До питання визначення розміру рекламного бюджету. *Моделювання та інформаційні системи в економіці*: зб. наук. пр. МОН України. Київ. нац.екон. ун-т ім. Вадима Гетьмана. Київ: КНЕУ, 2020. Вип. 99.

Статтю подано до редакції 24.11.2022

УДК: 004.56:530.192 DOI 10.33111/mise.102.2

Батечко Н.Г., д.пед.н., професор
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет імені Вадима Гетьмана

Чугаєва О.В., старший викладач
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет імені Вадима Гетьмана

Batechko N.H., Doctor of Pedagogical Sciences,
Professor of the Department of Computer Mathematics
and Information Security,
KNEU named after Vadym Hetman

Chugayeva O.V., Senior lecturer at the Department of Computer Mathematics
and Information Security,
KNEU named after Vadym Hetman

АНАЛІЗ СИНЕРГЕТИЧНИХ ЕФЕКТІВ В УМОВАХ ІНФОРМАЦІЙНИХ ТА КІБЕРЗАГРОЗ

ANALYSIS OF SYNERGISTIC EFFECTS IN THE CONDITIONS OF INFORMATION AND CYBER THREATS

Анотація. *У статті проаналізовано функціонування інформаційних систем із застосуванням системного та синергетичного підходів. Останнє зумовлене умовами невизначеності, хаосу глибоких суспільних трансформацій та кібервійн у сучасному інформаційному просторі. Висвітлено новітні наукові розвідки в галузі методології інформаційної безпеки та місце в ній синергетичного підходу. Розглянуто основні методологічні принципи синергетики як міждисциплінарного наукового напряму: самоорганізація, біфуркація, флуктуація, нелінійність, дисипація, атрактори. Синергічні ефекти були виділені як міждисциплінарні утворення, які пояснюють формування та самоорганізацію моделей і структур у відкритих системах. Досліджено синергетичні ефекти, властиві інформаційним системам як складному системному об'єкту. Система захисту інформації розглядається як цілісна, багатофункціональна, динамічна, відкрита структура з притаманними їй особливостями. Доведено, що традиційні погляди на дослідження функціонування таких систем наразі неефективні, оскільки вони характеризуються постійною стохастичністю та мінливістю. Як альтернативу класичним методам у дослідженні таких систем запропоновано використовувати явище інформаційної ентропії. Моніторинг зміни ентропії є необхідним та доцільним для підтримки стійкості та безпеки функціонування інформаційних систем загалом. Запропоновано моделювання процесу захисту інформації з урахуванням ентропії системи. Варто зауважити, що система забезпечення інформаційної безпеки є підсистемою національної*

безпеки України загалом, тому аналіз її функціонування в сучасних умовах війни проти російської агресії та постійних кіберзагроз ворога набуває стратегічного значення.
Ключові слова: *інформаційна безпека, процес забезпечення інформаційної безпеки, синергетичний підхід, ентропія, інформаційна ентропія, дисипативна структура.*

Abstract. *The article analyzes the functioning of information systems using systemic and synergistic approaches. The latter is caused by the conditions of uncertainty, chaos of deep social transformations and cyberwars in the modern information space. The latest scientific intelligence in the field of information security methodology and the place of a synergistic approach in it have been highlighted. The main methodological principles of synergetics as an interdisciplinary scientific area have been considered: self-organization, bifurcation, fluctuation, nonlinearity, dissipation, attractors. Synergistic effects have been highlighted as interdisciplinary formations which explain the formation and self-organization of models and structures in open systems. The synergistic effects inherent in information systems as a complex system entity have been studied. The information security system has been considered as a complete, multifunctional, dynamic, open structure with its inherent features. It has been proven that traditional views on the study of the functioning of such systems are currently ineffective, as they are characterized by constant stochasticity and variability. As an alternative to classical methods, it has been proposed to use the phenomenon of information entropy in the study of such systems. Modeling of the information security process taking into account the entropy of the system has been suggested. It is worth noting that the information security system is a subsystem of the national security of Ukraine in general, therefore, the analysis of its functioning in the modern conditions of the war against Russian aggression and constant cyber threats of the enemy acquires strategic importance.*
Keywords: *information security, the process of ensuring information security, synergistic approach, entropy, information entropy, dissipative structure.*

Постановка проблеми. У сучасних умовах інформаційних та кіберзагроз проблема забезпечення інформаційної безпеки є предметом дослідження як на рівні спеціальних установ (інститутів, центрів), так і у локальних дослідженнях окремих науковців.

За останні кілька років у вітчизняній та зарубіжній науці накопичено чималий доробок у цій галузі, який стосується властивостей інформатизації як об'єктивної характеристики розвитку суспільства, сумісних і змістовних основ інформаційної безпеки, технічних та гуманітарних проблем цього процесу.

Серед численних наукових статей полемічного характеру можна також виділити праці, що стосуються методологічного підходу до досліджуваного феномену. Таке бачення дозволяє комплексно підійти до інформаційної безпеки, відшукати внутрішні механізми її регулювання, виявляти недоліки в системі наявних знань, в основі яких варто першочергово виокремити описовість її структури та елементів.

Сучасні інформаційні та кіберзагрози, які ми спостерігаємо майже щодня, спростовують усталені уявлення про функціону-

вання інформаційної безпеки як системи в цілому і спонукають до радикально нових підходів, які б уможливили функціонування інформаційної безпеки в умовах невизначеності, хаосу, глибоких глобальних трансформацій та кібервійн.

Виходячи з цього, на нашу думку, інформаційна безпека як система може бути досліджена в межах синергетичного підходу, поєднуючи його з системним, структурно-функціональним та іншими методологічними підходами.

Аналіз останніх досліджень і публікацій. Серед останніх публікацій про застосування синергетичного підходу до проблем інформаційної безпеки, слід виокремити житомирську наукову школу І. Г. Грабара. Відома монографія «Безпекова синергетика: кібернетичний та інформаційний аспекти (2019) [2] розкриває теоретичні та практичні основи забезпечення інформаційної безпеки людини, суспільства, держави у кібернетичному та інформаційному просторах з використанням синергетичного підходу.

Методологічний контекст проблем інформаційної безпеки досліджують О. П. Дзюбань, О. Ю. Панфілов, Р. А. Чимчикаленко [4], де обґрунтовується доцільність застосування до них діалектичного, структурно-функціонального, синергетичного, системного та інших підходів.

Слід виокремити і досягнення харківської наукової школи проф. С. П. Євсеєва, зокрема, «The synergetic approach for providing bank information security: the problem formulation» [7], в якій зазначено, що на сучасному етапі розвитку науки і техніки забезпечення інформаційної безпеки повинно базуватися на новому підході — синергетичному. Його реалізація, як зазначають автори, уможливить синергетичний ефект взаємодії обраних профілів безпеки і як наслідок — продемонструє якісно нові і невідомі раніше емерджентні властивості системи безпеки.

Заслуговує на увагу дослідження групи одеських науковців Н. М. Баландіної, М. Д. Василенко та ін. стосовно доведення необхідності нового методологічного підходу до побудови моделі поведінки людини в цифровій сфері, спрямованої на захист інформації в соціальному інжинірингу [1]. Авторами запропоновано синергійно-криптографічний підхід до побудови моделі поведінкових проявів в умовах соціального інжинірингу та в інтересах захисту інформації.

Серед іноземних дослідників варто вказати на результати М. Ульеру [10], в яких авторка інтерпретує кіберпростір як самоорганізуючу систему та володіє властивостями емерджентності. М. Ульеру вважає, що такий підхід уможливить підґрунтя для

управління інформацією і ризиками в глобальних віртуальних організаціях.

Інтернаціональний колектив науковців на чолі з О. Писарчуком у праці «Bifurcation Prediction Method for the Emergence and Development Dynamics of Information Conflicts in Cybernetic Space» (2019) аналіз інформаційних загроз розглядає як багатофакторний прогрес, що відображає всі сфери життєдіяльності суспільства.

Синергетика та синергетичні ефекти в міждисциплінарних дослідженнях. Зауважимо, що терміни «синергія» та «синергетичні ефекти» останнім часом стали часто з'являтися в наукових дослідженнях, особливо міждисциплінарних. Вивченням цих феноменів займається така галузь знань, як синергетика. Як напрям міждисциплінарних досліджень, синергетика розглядає процеси самоорганізації у складних відкритих системах різної природи. Синергетика спроможна визначати загальні принципи розвитку таких систем за межами їх предметної належності. Виходячи саме із законів синергетики можна побудувати загальний методологічний каркас, який не лише розвиває загальний міждисциплінарний погляд на знання, а й допомагає під час вивчення окремих сфер наукових досліджень.

Термін «синергія» (гр. *енергія сумісної дії*) передбачає співробітництво, сприяння, співучасть, і тому більшість науковців розглядають це поняття як спільне функціонування кількох структур, що досягають такого результату, який би за їх незалежної діяльності був би недосяжним. Цей факт підтверджується і в загальній теорії систем: сумісна дія елементів деякої системи перевершує ефект кожного окремого компонента у вигляді їхньої простої суми. Терміном «синергетичний ефект» дедалі більше позиціонують міждисциплінарний напрям науки, який пояснює утворення та самоорганізацію моделей і структур у відкритих системах.

Засновник теорії синергетики Г. Хакен зазначав, що її сутність розкривається у тому, що: 1) досліджувані системи складаються з декількох чи багатьох однакових чи різнорідних частин, які перебувають у взаємодії одна з одною; 2) ці системи є нелінійними; 3) у ході розгляду хімічних, фізичних та біологічних систем йдеться про відкриті системи, які далекі від теплової рівноваги; 4) ці системи перебувають під впливом внутрішніх і зовнішніх коливань; 5) системи можуть стати нестабільними; 6) відбуваються якісні зміни; 7) у цих системах виявляються емерджентні нові якості; 8) виникають просторові, часові, та просторово — часові та функціональні структури; 9) структури можуть бути

впорядкованими чи хаотичними; 10) у багатьох випадках можлива математизація [6].

Зазначене класиком синергетичної теорії Г. Хакеном розкриває: з одного боку, її сутність, а з другого — основні закономірності дослідження складних відкритих систем, які можна використовувати в їхніх дослідженнях. Узагальнюючи, можна виокремити основні аспекти дослідження відкритих складних систем: «самоорганізацію», «відкритість», «нелінійність», «нерівноваженість», «біфуркацію», «флуктуацію», «дисипативні структури», «атрактори».

Наведені поняття використовуються здебільшого в природничих науках, хоча останнім часом ними оперують науковці і в соціальних, економічних, юридичних та педагогічних дослідженнях. Застосуємо універсальну синергетичну методологію до дослідження інформаційної безпеки.

Синергетичні ефекти у досліджені інформаційної безпеки як системи. Розглянемо інформаційну безпеку як складне системне утворення та застосуємо до його дослідження основні синергетичні закони. Це доречно зробити вже з тих позицій, що ця проблема стала не лише міждисциплінарною та загальнонауковою, а й глобальною. Таке широке розуміння інформації створює підґрунтя вважати теорію інформації наукою, яка за сутністю наближається до фундаментальних.

Досліджувана система інформаційної безпеки є цілісною, поліфункціональною, динамічною, відкритою структурою з притаманними їй ознаками, ієрархічною побудовою, системоутворюючими зв'язками і спрямована на створення нової інтегративної якості (сукупності якостей) забезпечення інформаційної безпеки на всіх рівнях забезпечення життєдіяльності суспільства (рис. 1).

Варто зауважити, що система забезпечення інформаційної безпеки являє собою підсистему національної безпеки України загалом, і тому аналіз її функціонування в сучасних умовах російсько-української війни та постійних кіберзагроз ворога набуває стратегічного значення.

За таких складних умов традиційні погляди на безпекові проблеми навряд чи уможливлять певні гарантії щодо забезпечення інформаційної безпеки. Систему забезпечення інформаційної безпеки ми вважаємо відкритою у часі та просторі, яка постійно взаємодіє з навколишнім середовищем, обмінюється з ним енергією і, власне, інформацією, отже, для неї характерними є постійна стохастичність і мінливість [8].

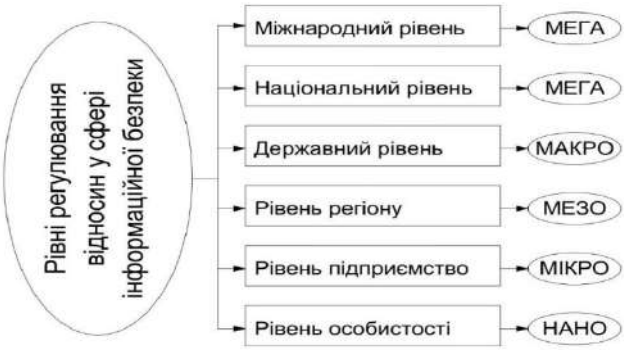


Рис. 1. Багаторівневий підхід у сфері забезпечення інформаційної безпеки

Джерело: [3].

З поняттям стохастичності тісно пов'язані явища флуктуації та біфуркації. Так, І. А. Пригожин вважає, що всі системи містять підсистеми, котрі постійно флуктуються. Іноді окрема флуктуація, або комбінація флуктуацій можуть стати настільки сильними, що попередня організація системи не витримує і руйнується. У цей переломний момент, який називають точкою біфуркації, принципово неможливо передбачити в якому напряму буде відбуватись подальший розвиток системи: чи стане ще більше хаотичним, чи перейде на новий більш високий рівень організації, який І. А. Пригожин [8] назвав дисипативною структурою.

Яскравим прикладом таких явищ слугують випадки неузгодженості складних технічних систем та інформаційних підсистем, якими вони наповнені. Іншими словами, між технологічною та інформаційною підсистемами системи безпеки в таких складних конструкціях була відсутня, як зазначається в основному принципі синергетики, взаємодія. Це часто спричиняє технічні збої та техногенні катастрофи. Останні наукові дослідження в галузі теорії синергетики стверджують, що саме синергетична концепція може стати науковим підґрунтям гармонічної взаємодії між технологічною та інформаційною підсистемами безпеки складних систем, і такою, що спроможна прогнозувати їх біфуркаційні стани, адже саме біфуркації різного виду та атрактори здебільшого призводять до катастроф та руйнування систем.

Дедалі більше науковців [5, 9] схиляються до думки, що вже саме поняття інформації тісно пов'язане з поняттям ентропії

(принцип мінімуму ентропії також основний в синергетичній теорії).

У наукових дослідженнях виокремлюється поняття — «інформаційна ентропія» — невизначеність інформаційної системи, зокрема, непередбачуваність появи деякого символу первинного алфавіту. В останньому за відсутності інформаційних втрат ентропія чисельно дорівнює кількості інформації на символ повідомлення, яке передається.

Принцип мінімуму ентропії відкритої системи (рівня її хаотичного стану) у стаціонарному стані є найважливішим результатом нерівноважної термодинаміки, оскільки пропонує цілісний критерій встановлення стаціонарного стану. Цей принцип ґрунтується, зокрема, на теорії Пригожина: у стаціонарному стані, близькому до термодинамічної рівноваги, значення швидкості продукції ентропії системи за рахунок необоротних процесів досягає відмінного від нуля постійного мінімального значення:

$$\sigma = \frac{dS}{dt} \to \min.$$

Критерієм наближення відкритої системи до стаціонарного стану слугує від'ємний знак похідної від продукції ентропії за часом.

З властивостей ентропії випливає, що вона за змістом є мірою невизначеності стану фізичної системи. Природньо, що при цьому кількість інформації можна вимірювати зменшенням ентропії системи, для уточнення стану якої і призначена власне ця інформація. Тому як об'єкт, про який передається інформація, в теорії інформації взято фізичну систему, яка має певний рівень невизначеності. Отже, інформаційна ентропія — це міра хаотичності інформації, чи міра внутрішньої невпорядкованості інформаційної системи. Ентропія збільшується у разі хаотичного розподілу інформаційних ресурсів і зменшується під час їх упорядкування. Інколи інформацію розглядають як від'ємну ентропію.

Звідси в теорії інформації рівнем апріорної невизначеності системи і застосовується ентропія та відома формула

$$H(X) = -\sum_{i=1}^{n} p_i log(p_i), \qquad (1)$$

де $H(X)$ — ентропія деякої інформаційної системи X; $x_i, i = \overline{1,n}$ — скінченна множина станів, в яких система розташована ($X \approx x_i$: подія, коли система X перебуває у стані $x_i, i = \overline{1,n}$); $p_i, i = \overline{1,n}$ — імовірність події, $\sum_{i=1}^{n} p_i = 1$.

Отже, простежується тісний зв'язок між властивостями інформаційної безпеки та основними синергетичними принципами.

Моделювання процесу забезпечення інформаційної безпеки з врахуванням ентропії системи. Розглянемо інформаційну систему як дисипативну та поставимо перед собою мету — досягти стійкого функціонування та забезпечення потрібного рівня її безпеки. Як відомо, за результатами досліджень І. Пригожина [8], саме для відкритих дисипативних систем характерним буде зменшення ентропії. Очевидно, що систему забезпечення інформаційної безпеки можна розглядати як відкриту систему.

Зауважимо, що у закритих системах процес дисипації відбувається лише як процес неперервної дезорганізації, хаотизації, руйнування початково заданої структури, що свого часу й встановила класична термодинаміка, яку ще іноді називають теорією руйнування структур.

У відкритих системах за умов стійкого обміну інформацією з навколишнім середовищем зміну ентропії можна подати у вигляді суми двох доданків: $\frac{dS_1}{dt}$ та $\frac{dS_2}{dt}$. Перший із них визначає зовнішні процеси (потік ентропії), а другий обумовлений внутрішніми процесами, які відбуваються в самій системі (виробництво ентропії):

$$\frac{dS}{dt} = \frac{dS_1}{dt} + \frac{dS_2}{dt}, \qquad (2)$$

де $\frac{dS_1}{dt}$ – потік ентропії; $\frac{dS_2}{dt}$ – виробництво ентропії.

У дослідженнях І. Пригожин зазначав, що саме у відкритих системах значення ентропії може бути довільного знаку. Справді, перший доданок: $\frac{dS_1}{dt}$ може бути більше нуля $\left(\frac{dS_1}{dt} > 0\right)$ або дорівнювати нулю $\left(\frac{dS_1}{dt} = 0\right)$. Другий же доданок може набувати як додатні, так і від'ємні значення $\left(\frac{dS_2}{dt} > 0 \text{ або } \frac{dS_2}{dt} < 0\right)$.

Звідси можна зробити висновок, що у відкритій дисипативній системі саме за рахунок другого доданку у (2) загальна зміна ентропії може бути від'ємною.

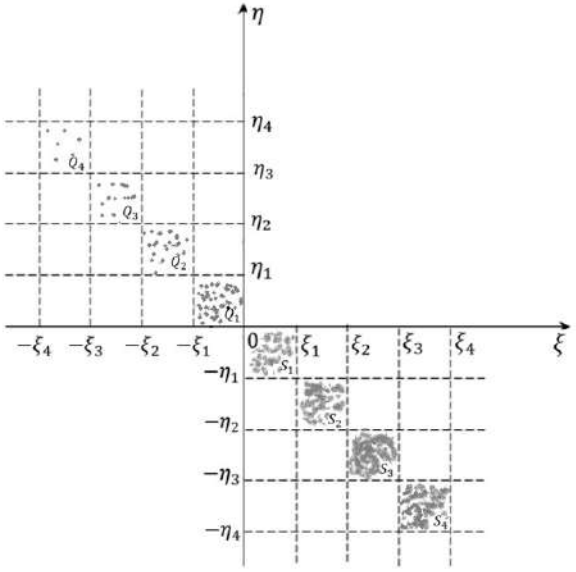
Ситуація, за якою зміна ентропії у відкритій системі $\frac{dS}{dt} < 0$, характеризує дисипативну систему.

Далі слід проаналізувати внутрішні зміни у системі, так щоб уможливити зменшення хаосу, спрогнозувати безпечні та стійкі

робочі режими її функціонування та на практиці досягнути потрібного рівня її безпеки загалом.

Для чіткого розуміння впливу процесів ентропії на рівень забезпечення захисту інформаційної системи подамо в умовних координатах (рис. 2): Oξ — вісь зміни ентропії інформаційної системи; Oη — вісь рівнів забезпечення інформаційної безпеки залежно від ступеня реалізації потенційних загроз.

Умовно, вісь Oη відділяє від'ємну та додатно ентропії інформаційної системи, а вісь Oξ — безпечні та небезпечні зони її функціонування. Можна вважати, що у точці O відбувається балансування системи від нестійкого до стійкого стану, тобто точка O — точка рівноваги системи.



$Q_1 - Q_2$: зона загроз, забезпечення ІБ
$Q_3 - Q_4$: зона безпеки
$S_1 - S_2$: зона небезпеки
$S_3 - S_4$: зона втрат та руйнувань

Рис. 2. Залежність рівня забезпечення інформаційної безпеки від процесів ентропії у системі

Джерело: розроблено авторами.

Проаналізуємо стан функціонування інформаційної системи в правій півплощині від осі Oη, коли ентропія додатна. На проміжну $[0; \xi_1]$ кількість ентропії ще недостатньо велика. Проте інформаційна система потрапляє до зони небезпеки (S_1). Це середовище підвищеного ризику та можливості загроз функціонування

системи. У цій зоні кількість ентропії може як збільшуватися, так і зменшуватися, тому розвиток системи має ймовірнісний характер. Так, зі збільшенням ентропії — небезпека наростає і система переходить в зону S_2. Поки що для функціонування системи немає катастрофічних наслідків і можна вжити заходи і протидіяти загрозам із приведенням самої системи до стану рівноваги.

Проте зі збільшенням ентропії система переходить до зони S_3 ($\xi \in [\xi_2; \xi_3]$) — зону руйнування і втрат. Наростання хаосу, у нашому випадку — невпорядкованої інформації, призводить до значних змін у структурі системи, за яких повернути систему до вихідного стану стає неможливим. Майже зруйнована, зі зміненою структурою система потрапляє в зону S_4 — зону кінцевого руйнування. Зауважимо, що саме тут, поряд з остаточним руйнуванням системи, цілком можливі й ефекти самоорганізації системи: прояви нових зародків її абсолютно нової організації, структури та властивостей, що стане предметом подальших наших досліджень.

Проаналізуємо стан функціонування інформаційної безпеки зліва від осі 0η, коли ентропія від'ємна. Зауважимо, що це буває лише у відкритих складних дисипативних структурах.

Наприклад, на проміжку $[-\xi_1; 0]$ ентропія вже від'ємна, однак система ще перебуває в зоні загроз, оскільки характер ентропії може змінитися в будь-який момент. Розташування у цій зоні вказує на рівень загроз на стан інформаційної безпеки загалом, які можуть вплинути за цілеспрямованих дій інших об'єктів. Саме ця зона вимагає найпильнішої уваги з боку суб'єктів безпеки, оскільки характер сучасних загроз в кіберпросторі має непередбачуваний асиметричний характер. Саме тут будуть найефективнішими стабілізаційні заходи, спрямовані на пом'якшення впливу дестабілізуючих на інформаційну систему вчинків. Проведення таких заходів напрямлене на те, щоб система інформаційної безпеки повинна мати таку структуру, щоб дозволило їй знищувати негативні прояви зовнішнього середовища: воно має або не пропускати зовнішні збурення, або відходити від них в безпечнішу зону Q_2, а потім у Q_3 — зону безпеки. Стан безпеки інформаційної системи зумовлює надійну її захищеність та збереження інформації. В цій зоні структурним елементам системи вже не загрожують дестабілізуючі впливи — усі показники перебувають у межах допустимих значень та мають стійку тенденцію до покращення.

Окремо варто вказати на поведінку в системі Q_4 — близької до ідеальної. За таких умов в ній повністю відсутній хаос. Це

означає, що інформація в інформаційних джерелах відсутня повністю, наприклад, — повністю зникли записи в банківських операціях, що неможливо в реальному інформаційному просторі. Можна, за таких умов, зробити припущення, що система знову стає замкненою і процес має циклічний характер. Проте, це вже тема наступних наукових розвідок.

Отже, доходимо висновку, що наведений підхід зонування залежно від кількості та знаку ентропії є, на нашу думку, необхідним для виокремлення та специфікації безпечних та стійких робочих режимів функціонування інформаційної системи, які на практиці дозволяють забезпечити потрібний рівень безпеки. Моніторинг зміни ентропії є необхідним і доцільним для підтримки стійкості і безпеки функціонування інформаційних систем загалом.

Висновки та перспективи подальших наукових розвідок. У роботі на основі системного та синергетичного підходів розвинуто методологію функціонування інформаційної системи в сучасних умовах кіберзагроз. Представлення інформаційної безпеки як відкритої, складної і дисипативної системи уможливлює використовувати в її дослідженні теорії інформаційної ентропії та моделювати зони загроз в процесі її функціонування залежно від характеру ентропії.

Подальші наукові розвідки пов’язані з вивченням процесів самоорганізації в інформаційних системах у біфуркаційних станах і математичного моделювання їх прогнозування.

Бібліографічні посилання

1. Баландіна Н.М. Підхід до моделювання поведінкових проявів у соціальному інжинірингу в інтересах захисту інформації. *Вісник Черкаського державного технологічного університету*. *Технічні науки*. 2019. С.57-66.

2. Грабар І.Г., Грищук Р.В., Молодецька К.В. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія. За заг. ред. д.т.н., проф. Р. В. Грищука. Житомир: ЖНАЕУ, 2019. 280 с.

3. Джалладова І., Батечко Н., Коломієць-Людвіг Є. Системний підхід до аналізу нормативно-правового забезпечення інформаційної безпеки. *Social development & Security*. 2018. Vol. 7. Iss. 5. С. 3–20.

4. Дзьобань О.П., Панфілов О.Ю., Чемчикаленко Р.А. Методологічний контекст дослідження проблеми інформаційної безпеки. Зовнішня торгівля: економіка, фінанси, право. 2014. № 2. С. 171-180.

5. Brillouin L. Science and Information Theory. Second Edition. *Dover Publications.* 2013. July 17. 368 p.

6. Hermann Haken. Synergetics. Springer — Verlag Berlin, Heidelberg, New York*, 1978, 383p.*

7. Hryshchuk R., Yevseiev S. The synergetic approach for providing bank information security: the problem formulation. *Ukrainian Scientific Journal of Information Security*. 2016. vol. 22. issue 1. p. 64-74.

8. Prigogine I, Stengers I, Order Out of Chaos: Man's New Dialogue with Nature by Ilya Prigogine, Isabelle Stengers, Alvin Toffler (Foreword). Heinemann. London. 1984. 432 p.

9. Shannon, Claude Elwood (July 1948). A Mathematical Theory of Communi-cation. B*ell System Technical Journal*. 27(3): 379–423p.

10. Ulieru M. (2003). Emergence in Cyberspace: Towards the Evolutionary Self-Organizing Enterprise. In: Carbonell, J.G., Siekmann, J., Kowalczyk, R., Müller, J.P., Tianfield, H., Unland, R. (eds) Agent Technologies, Infrastructures, Tools, and Applications for E-Services. NODe 2002. Lecture Notes in Computer Science, vol 2592. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-36559-1_3.

Статтю подано до редакції 29.11.2022

УДК: 004.056 DOI 10.33111/mise.102.3

Бєгун А.В., к.е.н., професор
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Шкоденко Т.В., магістр економічної кібернетики,
аспірант денної форми навчання,
Київський національний економічний університет
імені Вадима Гетьмана

Begun A.V., Philosophy Doctor,
Professor of the Department of Computer Mathematics
and Information Security,
KNEU named after Vadim Hetman
Shkodenko T.V., master of economic cybernetics,
full-time graduate student,
KNEU named after Vadim Hetman

АНАЛІЗ ОСОБЛИВОСТЕЙ СИСТЕМ ЗАХИСТУ ВЕЛИКИХ ДАНИХ В ЕЛЕКТРОННОМУ БІЗНЕСІ

ANALYSIS FEATURES OF BIG DATA PROTECTION SYSTEMS IN ELECTRONIC BUSINESS

***Анотація**. Ефективність захисту великих даних електронного бізнесу забезпечує високу конкурентоспроможність підприємницької діяльності на сучасному ринку. За останнє десятиліття термін «електронний бізнес» дістав широку популярність серед населення у сучасному світі, що і викликає певні загрози з боку зовнішніх чинників та формує актуальність розвитку сучасного програмного та технологічного забезпечення захисту великих даних електронного бізнесу в цілому. Актуальність обраної тематики обґрунтована підвищенням значимості електронної ролі комерції у сфері бізнес-діяльності, а також зростаючою потребою захисту учасників електронної комерції від шахрайських дій. У статті автори аналізують особливості систем захисту інформації бізнесових структур цифрової економіки. Висвітлено основні елементи сучасних технологій в контексті рівнів безпеки великих даних у сфері електронного бізнесу. Розглянуто основні проблеми, з якими стикається електронний бізнес у сфері захисту персональних і прихованих даних. Проаналізовано основні погляди провідних учених, які займалися і займаються питаннями захисту великих даних. Надано характеристику основним напрямам, з якими стикається електронний бізнес у сучасному середовищі. Запропоновано головні шляхи подолання проблеми підвищення рівня захисту даних. Визначено основні етапи використання сучасного програмного забезпечення, спрямованого на захист неструктурованих даних електронного бізнесу.*

***Ключові слова:** електронний бізнес, програми захисту, методи захисту, сучасний рівень, персональні дані, приватні дані, прихована інформація, системи злому, комп'ютерні технології.*

Abstract. *The effectiveness of the protection of big data of e-business ensures high competitiveness of entrepreneurial activity in the modern market. Over the last decade, the term "electronic business" has gained wide publicity and popularity among the population in the modern world, which in turn causes certain threats from external factors and shapes the relevance of the development of modern software and technological support for the protection of big data of electronic business as a whole. The relevance of the chosen topic is justified by the increasing importance of the electronic role of commerce in the field of business activities, as well as the growing need to protect participants of electronic commerce from fraudulent actions. In this article, the authors analyze the features of information protection systems of business structures of the digital economy. The main elements of modern technologies in the context of security levels of big data in the field of e-business are highlighted. The main problems faced by e-business in the field of protection of personal and hidden data are considered. The main views of leading scientists and researchers who were and are dealing with issues of big data protection are analyzed. The main directions faced by e-business in the modern environment are characterized, the main ways to overcome the problem of increasing the level of data protection are proposed, and the main stages of using modern software aimed at protecting unstructured e-business data are defined.*

Keywords: *electronic business, protection programs, protection methods, state of the art, personal data, private data, hidden information, hacking systems, computer technology.*

Постановка проблеми. Період XXI століття — особливий час переходу до цифрового ведення підприємницької діяльності, яка передбачає електронне виробництво послуг та товарів, що у свою чергу вимагає ефективного захисту особистих великих даних у сфері ведення електронного бізнесу в сучасних умовах. Ефективність захисту великих даних електронного бізнесу забезпечує високу конкурентоспроможність підприємницької діяльності на сучасному ринку. За останнє десятиліття термін «електронний бізнес» здобув широку популярність серед населення в сучасному світі, що спричинює певні загрози з боку зовнішніх чинників та формує актуальність розвитку сучасного програмного та технологічного забезпечення захисту великих даних електронного бізнесу в цілому.

Сьогодні значним попитом користується надійна та ефективна система захисту великих даних електронного бізнесу, як важлива складова та запорука успішності ведення електронної підприємницької діяльності в сучасному світі, який з кожним роком все більше розвивається та йде вперед за допомогою сучасних високотехнологічних винаходів та їх впровадженням в повсякденне життя кожної людини. Інформаційні технології та мережа Інтернет стають невід'ємною частиною життя економічних агентів, у зв'язку з цим створюються нові умови для здійснення бізнесу: розробка вебпропозицій, виникнення принципово нових ринків, формування ринку інноваційних товарів та послуг. Комерційна

діяльність активно переноситься в середовище Інтернету та залучає дедалі більше учасників електронних бізнес-операцій. Цей факт підтверджується активністю наукових публікацій про електронний бізнес та сучасних систем захисту великих даних.

Однак, незважаючи на зростання масштабів електронного бізнесу, як і під час здійснення будь-якої діяльності, можуть виникнути загрози несанкціонованого доступу, що може призвести до серйозних збитків.Отже, онлайн-бізнесу загрожують усі внутрішні та віддалені атаки, властиві будь-яку розподілену комп'ютерну систему, що взаємодіє за допомогою передачі даних по відкритих мережах. Тому потрібно відшукувати шляхи та методи вирішення проблем безпеки в електронному бізнесі. Актуальність обраної тематики обґрунтована підвищенням значимості електронної ролі комерції у сфері бізнес-діяльності, а також зростаючою потребою захисту учасників електронної комерції від шахрайських дій.

Аналіз останніх досліджень і публікацій. Серед провідних українських науковців та спеціалістів, які займалися дослідженням поставленого питання сучасних проблем та особливостей захисту великих даних електронного бізнесу, слід виділити таких, як З. І. Віновський, Р. М. Бліхарський, Д. О. Еймор [2], Т. М. Горний, Т. М. Харик, А. І. Соболевський, В. О. Заблоцький, Є. С. Єпіфанов [3], І. Р. Микитчин, А.І. Барбуляк та П. Р. Швед, М. Б. Клімковський, І. О. Кусий, Р. А. Озарків, Р. Р. Дубина, А. М. Кармінський [4], М. І. Макар, І. П. Війтишин, В. Р. Войтович та В. Л. Матвіїв, Н. М. Крейніна, Є. С. Стоянова, А. П. Манюшис [5], І. Т. Балабанов, В. М. Родіонова, А. Д. Шеремет, А. А. Паскова [6], О. В. Єфімова та інші.

Слід виділити також і зарубіжних науковців, які зробили значний внесок у розвиток і дослідження питань захисту особистих даних у системі електронного бізнесу та методів протидії за допомогою сучасного програмного забезпечення різним кібератакам для захисту даних. Серед провідних зарубіжних науковців, в більшості американських та європейських, слід виділити таких як: Akter S.I. [7], Altman, E.I., Tishaw, J.R., Taffler, A.A., Van Horn, P.R., Alvin, E.R., Bertil, O.P., Thorstein, B.W., Walras, J.M., Alfred A.O., Schumpeter, J.A., Wilson, J.N., Bunge, M.H., Gattenberger, K.C., Scheimin, J.P., Forrester, J.A., Weitzecker, E.E., Lovins, L. W, Smith AR, Griffin NR, Damodaran AD, McCarthy MW, Gruening JM, Monahan GI, Flynn JS, Griffin RR., Zaman D.H., Andersen T.R., Bedford J.D., Watson H.J. [8], Tsai C.W. [8], Lai C. F. [8], Chao H. C. [8] і низка інших науковців, які зробили значний вклад у розвиток поставленого питання.

Невирішені проблеми. Серед основних питань, які досі потребують подальшого розв'язання, слід виділити такі, як недосконаліть сучасного програмного забезпечення спрямованого на захист великих даних у сфері ведення електронного бізнесу, брак кваліфікованих кадрів, спроможних протистояти діючим проблемам ззовні та проблеми правильного використання сучасних інструментів Big Data у процесі ведення електронного бізнесу.

Цілі статті

1. Провести аналіз існуючого сучасного програмного забезпечення спрямованого на захист великих даних електронного бізнесу.

2. Описати особливості функціонування програм та технологій спрямованих на безпосередній захист великих даних електронного бізнесу від зовнішніх та внутрішніх чинників.

3. Запропонувати перспективні шляхи застосування сучасного технологічного та програмного забезпечення для безпосереднього захисту великих даних у сфері електронного бізнесу, як одного з основних та важливих важелів збереження високої конкурентоспроможності підприємницької діяльності на ринку.

Виклад основного матеріалу. Електронний бізнес як сфера цифрової економіки включає фінансові, торгові та усі пов'язані з іншими бізнес-транзакціями операції, які проводяться за допомогою Інтернету [2, с. 106]. Розвиток такого сучасного кластеру економічної діяльності, що являє собою інноваційно насичену галузь, створює нові економічні бізнес-моделі, надає сучасні умови ведення підприємницької діяльності, а також змінює підхід до традиційних способів продажів і стає однією з сфер, яка найбільш активно розвивається у різноманітних напрямах економіки [1]. Про це свідчать показники, подані на рис. 1.

У визначенні до електронної комерції відносять електронний обмін інформацією, електронний рух капіталу, електронні гроші, електронну торгівлю, електронний маркетинг, електронний банкінг [6, с. 173]. На сьогодні на українському сегменті під електронною комерцією у вузькому розумінні прийнято розуміти електронну торгівлю. За даними компанії «Statista», роздрібні продажі онлайн-торгівлі у всьому світі склали 1,3 трлн дол.

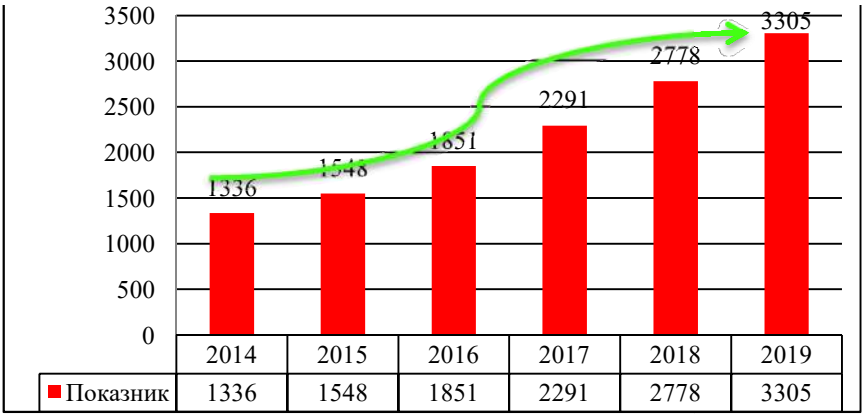


Рис. 1. Динаміка розвитку електронного бізнесу у світі, трлн дол. США

Досить поширена не до кінця правильна думка, що онлайн-бізнес почати легше, ніж традиційний. Проте це твердження дискусійного характеру, оскільки, з одного боку, немає потреби використовувати такі ресурси, як оренда приміщення (а складом для зберігання товару може бути будь-яка частина квартири, невеликого приміщення) або можна виключити користування послугами продавця та спростити логістику. Але, з другого боку, зберігають серйозність і вагомість такі види діяльності, як своєчасна та по можливості безкоштовна доставка, забезпечення оплати товару або послуги (онлайн- та офлайн-транзакції) [1, с. 43]. І тут варто приділяти увагу настройкам і забезпеченню безпеки оплати онлайн через банківські картки або електронні гаманці.

Отже, з погляду початкових інвестицій, можна виділити кілька видів електронної комерції:

1) не вимагають вкладень (дропшипінг, перепродаж за партнерською програмою);

2) які вимагають мінімальних капіталовкладень (покращений дропшипінг, продаж партнерських товарів, але на власних сайтах);

3) потребують середнього рівня інвестицій (будь-який онлайн-магазин);

4) вимагають серйозних інвестицій на введення в електронний бізнес (онлайн-магазини з великим асортиментом за суміжними лініями) [2, с. 107—108].

Між цими категоріями існують перехідні форми. Зазначимо, що онлайн-бізнес вимагає певної кваліфікації, і тут у конкурент-

ній боротьбі перемагають лише професійні гравці. Актуальність розвитку бізнесу на просторах всесвітнього павутиння вкрай висока, оскільки на даний момент кількість підприємців, задіяних у ньому, зростає в геометричній прогресії, а отже, необхідно усвідомлювати, що розвиток комерційної діяльності в Інтернеті пов'язаний як з її перевагами, так і має властиві їй ризики [6, с. 174].

Електронний бізнес пропонує низку переваг та можливостей для учасників ринку:

1) скорочення витрат з допомогою виключення чи заміни раніше значимих ресурсов. Наприклад, втрата необхідності найму штату співробітників чи оренди приміщення тощо;

2) можливість невеликих компаній досягти глобального ринку, оскільки перспективи електронної комерції настільки серйозні, що бізнес не має географічних обмежень;

3) можливість конкурувати з великими світовими компаніями;

4) можливість цілодобового зворотного зв'язку з клієнтом [2, с. 44-45].

Електронний бізнес не є єдиною можливістю для отримання прибутку, і все ж таки ніяка інша модель бізнесу не запропонує подібних переваг. До того ж надається можливість розвивати бізнес у вільний від основної роботи час або фрилансом.

Активне нарощування темпів та обсягів електронного бізнесу розширює і можливості для покупців, а саме [3, с. 220]:

• великий асортимент продукції та послуг;

• можливість цілодобової покупки;

• комфортні умови купівлі, оформлення замовлення без відвідування магазинів та супермаркетів;

• здійснення купівлі товарів із різних країн світу;

• вплив на стратегію та поведінку виробника шляхом формування відгуків та пропозицій [2, с. 109].

На тлі активного розвитку електронного бізнесу основним питанням, яке потребує підвищеної уваги з боку як вчених, так і професіоналів, залишається безпека захисту великих даних електронного бізнесу. Нині ключовою перешкодою розвитку онлайн-платежів став психологічний чинник. Так, результати опитувань показують, що розвитку інтернет-торгівлі перешкоджає недовіра безпеки онлайн-середовища та підвищені ризики потенційного шахрайства з персональними даними, зокрема і з реквізитами платіжних карток та гаманців [6, с. 175].

Прийнято виділяти кілька видів ризиків від шахрайства у віртуальній мережі:

– дублювання технічного пристрою (електронного гаманця або жорсткого диска комп'ютера);

– зміна або дублювання відомостей, повідомлень чи програм;

– крадіжка персональних даних та платіжних реквізитів;

– відмова у проведенні операцій;

– «соціальна інженерія» [3, с. 221–222].

Одним із найбільш популярних інноваційних методів підвищення безпеки систем захисту великих даних, що застосовуються учасниками електронного бізнесу, є перевірка використання сертифікованих протоколів інтернет-ритейлером. Найбільш широко застосовувані методи забезпечення безпеки онлайн-комерції можна звести до наступних [1, с. 46]:

• Secure Socket Layer (SSL) під час здійснення інтернет-банкінгу передбачає шифрування даних у разі спроби перехоплення даних, що передаються; і тут важливим стає забезпечення захисту безпосередньо сервера, у якому проводиться відповідна платіжна транзакція;

• різні способи ідентифікації власників платіжних інструментів (карт, гаманців та ін.); тут особливо виділимо перевірку кодів для карток Visa CV2, і для MasterCard — CVK2; перевірка справжності відбувається на підставі перевірки адреси (AVS);

• одноразові паролі, які отримуються в SMS або безпосередньо в банкоматі, які надсилаються на мобільний телефон для проведення конкретної транзакції;

• криптографія, що використовує асиметричні методи шифрування — системи з відкритим ключем — мають два ключі, які не можуть бути розраховані один від одного;

• ЦЕП (цифровий електронний підпис), що дозволяє легко ідентифікувати відправника запиту;

• генератори одноразових паролів, які є зовнішніми відносно комп'ютери пристрою, що підключаються за допомогою USB-порту;

• зовнішній електронний ключ, який генерується та записується на зовнішній диск при першому вході до системи та використовується надалі для здійснення платіжних транзакцій [2, с. 110].

На додаток до цього економічні агенти часто роблять додаткові заходи для забезпечення безпечного проведення інтернет-платежів під час здійснення електронного бізнесу:

1. *Обмеження використання особистого сертифіката*. Система деяких банків дозволяє використовувати електронний ключ або електронний сертифікат лише на тому комп'ютері, на якому він був створений. Через це ви можете здійснювати платежі тіль-

ки через інтернет-банкінг зі свого комп'ютера, хоча ви можете переглядати виписки на інших пристроях [3, с. 223].

2. *Віртуальна клавіатура*, щоб шахраї не могли читати дані реєстру під час набору тексту на стандартній клавіатурі з комп'ютерними вірусами.

3. Історія підключень — ця функція дозволяє користувачеві інтернет-банку визначати підключення до системи будь-кого та відстежувати несанкціоновані події.

На думку експертів, захист корпоративних інформаційних систем залежить від ряду факторів: 30 % — від технічних рішень, що застосовуються; 40 % — від інституціональних механізмів в установі; і 30 % — від морального стану суспільства та загального культурного рівня користувача [2, с. 111].

Станом на 2022 р. одними із найбільш використовуваних програм для захисту великих даих електронного бізнесу в сучасному світі є такі: «Serial Port Control», «Bitdefender», «Symantec Corporation», «TrustPort a.s.», «McAfee, Inc.» та «G DATA Software AG». Сьогодні в період XXI століття, розвитку технологій дані програми використовуються в найбільших інтернет-корпораціях сучасності [6, с. 176]. До прикладу програма для захисту великих даних «G DATA Software AG» використовується в компанії «Amazon», яка дозволяє ретельно дотримувати основні вимоги безпеки для захисту великих даних зазначенної компанії, яка є найбільшим представником сучасносі у сфері електронного бізнесу. Наприклад, одна з найбільших біотехнологічних інтернет-компаній світу «Life Technologies» використовує декілька програм захисту особлистих даних, серед яких є програма «TrustPort a.s.», яка дозволяє наперед виявляти та знешкоджувати загрози від зовнішніх чинників за допомогою раптового виявлення вірусної інформації в системі.

Висновки. На підставі проведеного дослідження зазначимо, що електронний бізнес вже тенденційно стає сучасним затребуваним та перспективним напрямом цифрової економіки, у якому економічні агенти не лише розвивають свій бізнес, але отримують можливість отримати передові знання та набути професійних навичок у різних сферах. Вихід на простори електронної комерції може забезпечити успішний старт для розвитку власного бізнесу, який пропонує комфортні умови як для продавця, так і покупця.

Однак як і будь-яка економічна діяльність, електронна комерція не захищена від загрози втручання в галузь шахраїв. Маючи широкий асортимент методів, що використовуються для забезпечення безпеки великих даних в інтернет-середовищі, учаснику

електронного бізнесу доцільно пам'ятати, що багато залежить безпосередньо від користувача. Найчастіше причиною шахрайського доступу до облікового запису учасника операції може стати його неуважність або недбалість.

Отже, щоб уникнути потенційних ризиків власнику облікового запису слід обмежити доступ до платіжних реквізитів та персональних даних шляхом регулярної зміни паролів до систем та проведення операцій лиш тільки на попередньо перевірених пристроях. Проте основне вирішення проблеми інформаційної безпеки великих даних електронного бізнесу залишається в основному за апаратним та програмним забезпеченням.

Бібліографічні посилання

1. Бєгун А.В.,Плахтій М.О., Осипова О.І., Урденко О.Г. Аналіз зовнішніх і внутрішніх загроз функціонування електронного квитка видовищних заходів. *Моделювання та інформаційні технології в економіці*. 2021. № 101. С. 20–31.
2. Еймор Д.О. Електронний бізнес. Еволюція та революція. Харків: Вільямс, 2021. 320 с.
3. Єпіфанов Є.С., Атаров Н. З. Основні етапи розвитку електронного бізнесу. *Запитання регіональної економіки*. 2020. № 3. Т. 28. С. 106-111.
4. Кармінський А.М. Інформатизація бізнесу: концепція, технології, системи захисту великих даних. Київ: Фінанс та статистика, 2020. 623 с.
5. Манюшіс А.П., Смольянінов В., Тарасов В. Віртуальне підприємство як ефективна форма організації зовнішньоекономічної діяльності. *Проблем теорії та практики управління*. 2020. № 4. С. 3-27.
6. Паскова А.А. Технології «Big Data» в автоматизації технологічних і бізнес-процесів. *Науковий огляд. Технічні науки*. 2019. № 4. С. 23-27.
7. Akter S.I. Big data analytics in E-commerce: a systematic review and agenda for future research. Shahriar Akter, Samuel Fosso Wamba. *Electronic Markets*. Vol. 26, Issue 2. Springer International Publishing AG. 2019. P. 173-194.
8. Big data analytics: a survey. Tsai C.-W., Lai C.-F., Chao H.-C. and Vasilakos A.V. *Journal of Big Data*. 2021. Vol. 2. № 1. P. 29-32.
9. Watson H.J. Tutorial: Big Data analytics: Concepts, technologies, and applications. Comm. of the Association for Information Systems. 2019. Vol. 34. Article 65. P. 1247-1268.

Статтю подано до редакції 21.11.2022

УДК: 338.1:334.7 DOI 10.33111/mise.102.4

Ващаєв С.С., к.е.н., доцент
кафедри математичного моделювання та статистики,
Київський національний економічний університет
імені Вадима Гетьмана

Джалладова І.А., д.фіз.-мат.н., професор
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Камінський О.Є., д.е.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Vashchaiev S. S., PhD in Economics,
Associate Professor of the Economic and Mathematical Modelling Department,
KNEU named after V. Hetman

Dzhalladova I. A., Doctor of Science in Physics and Mathematics,
Professor of the Department of Computer Mathematics and Information Security,
KNEU named after V. Hetman

Kaminsky O.Y., Doctor of Economics,
Associate Professor of the Department of Computer Mathematics and Information Security,
KNEU named after V. Hetman

ОПТИМІЗАЦІЯ ЛАНЦЮЖКА МЕНЕДЖЕРСЬКИХ РІШЕНЬ В ПРОЦЕСІ ПОСТВОЄННОГО ВІДНОВЛЕННЯ УКРАЇНИ

OPTIMIZATION OF THE CHAIN OF MANAGERIAL DECISIONS IN THE PROCESS OF POST-WAR RECOVERY OF UKRAINE

Анотація. *Країни Заходу розробляють комплекс заходів щодо надання економічної допомоги Україні для її відновлення після закінчення російсько-української війни. У липні 2022 р. на Міжнародній конференції в Лугано Україна презентувала Національний план відновлення. Метою статті є аналіз структури ланцюга управлінських рішень для управління повоєнною відбудовою України та розробка дизайну та структури основи для її забезпечення, яка містить багато вимірів — управлінського, організаційного та технологічного. Визначено концептуальні орієнтири потенціалу та впровадження наскрізної прозорості ланцюжка управлінських рішень для плану відновлення на основі цифрових технологій. Роз-*

роблений фреймворк містить деякі інноваційні ідеї щодо використання принципів культури DevOps для організації ланцюжка управлінських рішень та організації забезпечення наскрізної прозорості управління під час відновлення України на основі застосування цифрових технологій. Зокрема, було розроблено концептуальні вказівки щодо управління цифровим ланцюгом поставок і використання технологій для підвищення стійкості шляхом створення та використання прозорості в середовищах з бідною інформацією. На прикладі плану повоєнної відбудови України розширено аналіз цифрових застосувань, щоб забезпечити стабільність ланцюга управління від миттєвих одноразових збоїв до бойових умов. Запропоновано багатовимірну структуру, що складається з компонентів управління, організації та цифрових технологій. Визначено, що наскрізна прозорість може допомогти підвищити стійкість ланцюжка поставок ефективним чином без створення надмірних і дорогих резервів.

Визначено загальні закономірності взаємодії двох циклів осмислення рішень та формування сенсу між організаційними суб'єктами, що забезпечує постійний розвиток цифрової інфраструктури ланцюгів управління проєктами в складних умовах.

Ключові слова: *ланцюг управлінських рішень, DevOps, управління, динамічне моделювання, фреймворки*

Abstract. *Western countries are developing a set of measures to provide economic assistance to Ukraine for its recovery after the end of the war with Russia. In July 2022, at an international conference in Lugano, Ukraine presented its National Recovery Plan. The purpose of the article is to analyze the structure of the chain of managerial decisions for managing the post-war reconstruction of Ukraine and to develop the design and structure of the framework for its support, which contains many dimensions — managerial, organizational and technological. Definition of conceptual guidelines for the potential and implementation of end-to-end transparency of the chain of management decisions for the recovery plan based on digital technologies. The developed framework contains some innovative ideas regarding the use of DevOps culture principles to organize the chain of managerial decisions and the organization of ensuring end-to-end management transparency during the recovery of Ukraine based on the application of digital technologies. In particular, conceptual guidelines have been developed for digital supply chain management and the use of technology to increase resilience by creating and leveraging transparency in information-poor environments. Using the example of Ukraine's post-war reconstruction plan, the analysis of digital applications is expanded to ensure the stability of the control chain from momentary one-time failures to combat conditions. A multidimensional framework consisting of management, organization and digital technology components is proposed. It has been determined that end-to-end transparency can help improve supply chain resilience in an efficient manner without creating excessive and costly reserves.*

General patterns of interaction with two cycles of making sense of decisions and forming meaning between organizational subjects have been determined, which ensures the constant development of the digital infrastructure of project management chains in difficult conditions.

Keywords: *chain of managerial decisions, DevOps, management, dynamic simulation, frameworks*

Постановка проблеми. Західні партнери розробляють комплекс надання економічної допомоги Україні для її відновлення

після завершення російсько-української війни. План допомоги Україні вважається аналогом «Плану Маршалла» — програми економічної допомоги європейським державам після Другої світової війни, яка почала діяти у 1948 р. з ініціативи держсекретаря США Джорджа К. Маршалла.

За оцінками України, витрати на реконструкцію можуть скласти 750 млрд дол. США (760 млрд євро). ЄС оцінює ці витрати в 349 млрд дол. Обсяг різних програм відновлення варіюється від 100 до 500 млрд доларів США і передбачається реалізувати за допомогою партнерів із США та ЄС.

У липні 2022 р. на Міжнародній конференції в Лугано Україна презентувала свій Національний план відновлення. Досі демократичні партнери не відповіли на українські пропозиції з допомоги у повоєнному відновленні.

Цей документ є спробою GMF допомогти заповнити цю порожнечу та стимулювати дискусію зі значущого західного плану відновлення України. Це не повний проєкт таких зусиль, а структурована колекція рекомендацій для урядів-донорів та міжнародних установ. Він обмежується проблемами розробки та впровадження такого плану та не коментує Національний план відновлення України. Загалом планується відновлення 38 409 об'єктів, зокрема 6674 житлових будинки і 146 медичних закладів.

Першим ключовим фактором розробки «Українського плану Маршалла» є визначення ключових зацікавлених сторін фінансування.

Другим ключовим фактором для відновлення буде послідовність фаз підтримки.

Для процесу одужання слід застосовувати послідовний підхід із поступовим нарощуванням активності. Він має мати чотири етапи: допомога, реконструкція, модернізація та вступ до ЄС. *Допомога* включатиме невідкладну допомогу та базову реабілітацію, оскільки війна триває. *Реконструкція* передбачатиме швидке реагування на руйнування, спричинені війною, після припинення вогню або досягнення врегулювання, зосереджуючись на інфраструктурі та мобілізації ринкових механізмів. *Модернізація* — це фаза «відбудувати краще», яка залучає прямі іноземні інвестиції для формування нової економіки та нової країни, що є більш цифровою, більш екологічною, більш демократичною та більш орієнтованою на ЄС. *Фаза вступу* передбачає інвестиції, які більше спрямовані на приведення країни до її майбутніх партнерів по ЄС.

Міжнародні зусилля країн, які не є членами ЄС, будуть спрямовані на передній план в очікуванні того, що зацікавленість міжнародної спільноти в допомозі Україні з часом зменшиться, а політичні та фінансові зобов'язання ЄС лише зростуть.

Створення нового агентства допомоги чи централізованого трастового фонду для донорів не є ані реалістичним, ані доцільним. Натомість G7 та інші країни-партнери повинні працювати через багато донорські фонди МФО, мобілізуючи сильні сторони різних банків розвитку та використовуючи готові рішення для відповіді на цю нагальну потребу. Координатору відновлення, наділеному G7 автономією та повноваженнями, потрібно буде допомогти узгодити принципи умовності та вимоги щодо нагляду.

Допомога Україні має надаватися з певними умовами, особливо в запланованих масштабах і на користь країни з корупційною історією. Виплата коштів на реконструкцію має залежати від того, чи країна успішно запровадить і впровадить давні реформи системи управління та судової системи на початковому етапі надання допомоги. Потрібно призначити незалежного генерального інспектора, офіс якого розслідував би звинувачення у неправомірній поведінці та сприяв ефективному використанню коштів.

Але ефективність прийняття рішень політиками під час бойових дій та після воєнного відновлення значною мірою залежить від їхньої здатності інтегрувати та осмислювати інформацію. Війна ставить уряд України перед складним завданням прийняття рішень в інтересах громадської безпеки та економічного забезпечення. По суті, політики мають реагувати на загрози, рівень яких є невідомою, і вони приймають рішення в умовах обмеженого часу в умовах надзвичайної невизначеності. Ставки високі, проблеми складні і вимагають ретельного збалансування різних інтересів, зокрема, життєвого забезпечення населення, розвитку економіки та прав людини. Ці обставини роблять процеси прийняття рішень особами, які формують політику та економіку, вразливими до помилок і упереджень в обробці інформації, тим самим збільшуючи ймовірність помилкових процесів прийняття рішень.

Аналіз останніх досліджень і публікацій. Зіштовхнувшись з інформацією, яка постійно змінюється, високими ставками, обмеженням часу та необхідністю збалансувати численні проблеми та інтереси, уряди змушені приймати рішення зі складних питань за субоптимальних умов [1]. Органи влади мають реагувати на загрози, рівень яких є невідомою, та приймати рішення в умовах обмеженого часу і надзвичайної невизначеності. Ці обставини

роблять процеси прийняття рішень особами, які формують політику та економіку, вразливими до помилок і упереджень в обробці інформації, тим самим збільшуючи ймовірність помилкових рішень. Попередні дослідження показують, що ефективність прийняття рішень у дуже складних і невизначених ситуаціях, таких як війна, значною мірою залежить від здатності груп успішно здобувати, інтегрувати та обробляти інформацію [2].

Іншими словами, це залежить від якості процесу прийняття рішень, що є важливою передумовою, яка (не гарантує, але) збільшує ймовірність позитивних результатів [3]. Важливо те, що, хоча неможливо визначити, які рішення є найкращими, можна вдосконалити процеси, які використовуються для прийняття цих рішень.

Управління ланцюгом постачання включає три рівні стратегічних рішень (довгострокові рішення), тактичного рівня (середньострокові рішення) і операційного рівня (день прийняття рішення) [4]. Проєктування мережі постачання є одним із найважливіших стратегічних рішень, які необхідно прийняти на початкових етапах управління ланцюгом поставок.

Зосереджуючись на оптимальних рішеннях ланцюга поставок за участю постачальників логістичних послуг, у дослідженні Лі та ін. [5] вивчали ланцюг поставок, що складається з роздрібного продавця та виробника. Логістичні послуги можуть надаватися в чотирьох ситуаціях: роздрібний продавець, виробник, виробник, переданий третьою стороною, і роздрібний продавець, переданий третьою стороною. У роботі було проаналізовано оптимальні рішення кожного суб'єкта під керівництвом виробника.

У праці Чжана та ін. [6] було побудувано двоступеневий ланцюг поставок, що складається з онлайн-магазинів і постачальників логістичних послуг, та досліджено оптимальні роздрібні ціни на продукти, керовані роздрібними торговцями, і оптимальні рішення щодо розширення потужностей постачальників логістичних послуг.

Дослідники С. Субрата та ін. [7] побудували трирівневий ланцюг поставок за участю уряду і дослідили оптимальну стратегію державного субсидування. Система ланцюга постачання, в якій бере участь постачальник логістичних послуг з двох рівнів, складається з кількох осіб, які приймають рішення на різних рівнях, а це за змістом складний чотирирівневий ланцюг постачання.

Закупівлі, виробничі цехи, рекламні дії в багатоканальних моделях, оптимізація маршрутизації, моніторинг трафіку у режимі

реального часу та проактивне управління безпекою є одними з останніх сфер застосування аналітики даних і штучного інтелекту в ланцюжках поставок і управлінні операціями [8].

Підбиваючи підсумок, аналіз літератури показує, що для встановлення видимості наскрізного ланцюга поставок найчастіше використовуються такі цифрові технології, як смарт-аналітика, системи раннього попередження помилок, технології блокчейн та цифрові онлайн-платформи і портали.

Систематичний аналіз відповідної літератури показує, що українські та зарубіжні науковці досліджують здебільшого оптимальні рішення для ланцюга менеджерських рішень за участю одного постачальника логістичних послуг і кількох конкурентних постачальників продуктів. Однак більшість із таких досліджень базуються на управлінні виробництвом чи мережею роздрібної торгівлі і не передбачає оптимізацію ланцюга менеджерських рішень в рамках плану за участю урядів та фінансових установ для пост воєнного відновлення країн.

Мета статті — аналіз структури ланцюга менеджерських рішень для управління пост воєнним відновленням України та розробка дизайну та структури фреймворку для його забезпечення, який містить багато вимірів — управлінський, організаційний і технологічний. Визначення концептуальних орієнтирів щодо потенціалу та впровадження наскрізної прозорості ланцюга менеджерських рішень для плану відновлення на основі цифрових технологій.

Основний матеріал дослідження. У XXI ст. вже сталися технологічна революція (тобто Індустрія 4.0), глобальна пандемія та глобальна війна в Європі. Однак принципи сучасних ланцюгів менеджерських рішень були розроблені в епоху економічного управління та глобалізації, і тепер стикаються з проблемою адаптації до цих революційних тенденцій.

Вимірювання та аналіз є критично важливими для контролю правильності рішень. У цьому випадку концепція фактичного підходу до прийняття рішень залежить від використання різних інструментів якості для аналізу фактів і пов'язаних даних. Однак процесний підхід не пов'язаний із вимірюванням, тому пропонується наступна гіпотеза:

Гіпотеза 1. Фактичний підхід до прийняття рішень у рамках плану відновлення позитивно асоціюється з використанням цифрових інструментів.

Для керівних органів Європейського Союзу важливим індикатором надання фінансової допомоги є прозорість. Прозорість

можна розглядати і як здатність, і як результат. Пропонується визначити прозорість ланцюга менеджерських рішень з позицій можливостей як здатність представляти фізичний ланцюг поставок у цифровому просторі з усіма відповідними даними, які можна збирати, обробляти, оновлювати та отримувати доступ у режимі реального часу, підтримувати планування, моніторинг та контролю прийнятих рішень. Як результат, наскрізна прозорість ланцюга рішень матеріалізується як цифровий двійник фізичного ланцюга постачання.

Використовуючи класифікацію ризиків пропозиції, попиту та процесів [10], є можливим проаналізувати конкретні випадки таких ризиків під час пост воєнного відновлення, та їх ключові аспекти, які можливо забезпечити за допомогою різних цифрових технологій.

Експерти вказують на прозорість як на одну з ключових детермінантів управління ризиками ланцюжка менеджерських рішень під час війни, а також визначають наступні проблеми:

– неповна прозорість у багаторівневих організаційних конструкціях;

– вузькі місця логістики через локдауни, безпекові заходи і дефіцит потужностей як морських, так і повітряних перевезень;

– нестабільність запасів (дефіцит і надлишок), а також затримка поставок;

– часткова неготовність постачальників (через політичні аспекти).

У табл. 1 наведено комплексну таксономію ризиків прийняття рішень та технологій забезпечення наскрізної прозорості для ланцюга менеджменту.

Ураховуючи це, основною метою фреймворку забезпечення ланцюга менеджерських рішень для управління пост воєнним відновленням України є гарантування рівня прозорості ланцюга управління під час збоїв і створення пов’язаною структури розробки та реалізації, яка містить управлінські, організаційні та технологічні аспекти. Фреймворк має покривати потреби по всьому ланцюгу прийняття рішень, забезпечуючи економію витрат та доставку від основного виробництва до точок відновлення.

Фреймворк, що пропонується, подано на рис. 1, він містить управлінські, організаційні та технологічні компоненти.

Можливості управління включають резервування, наприклад резервні джерела та виробничі потужності, альтернативні маршрути транспортування, цифрову інвентаризацію для зменшення ризиків. Організаційні можливості стосуються створення органі-

заційної структури для управління стійкістю, впровадження управління стійкістю в повсякденні бізнес-процеси, а також розробки планів на випадок непередбачених ситуацій і чітких інструкцій для різних керівників і організаційних підрозділів для надзвичайних ситуацій. Нарешті технологічний вимір фреймворку включає розвиток наскрізної прозорості ланцюга поставок за рахунок цифрових платформ і смарт-аналітики, впровадження систем раннього попередження та автоматизації виробничих і логістичних процесів для підвищення їх адаптивності.

Таблиця 1

КОМПЛЕКСНА ТАКСОНОМІЯ РИЗИКІВ ЛАНЦЮГІВ МЕНЕДЖЕРСЬКИХ РІШЕНЬ

<table>
<tr><td rowspan="2">Ризики ланцюга менеджерських рішень</td><td colspan="4">Цифрові технології підвищення прозорості прийняття рішень у невизначених ситуаціях</td></tr>
<tr><td>Цифрові платформи спільних ланцюгів поставок</td><td>Динамічна симуляція</td><td>Блокчейн технології</td><td>Смарт-аналітика</td></tr>
<tr><td>Постачання:
• затримка поставок;
• часткова недоступність постачальників (через локдаун);
• повна неготовність (корупційні ризики)</td><td rowspan="3">Спільне вирішення проблем з постачальниками для зменшення ризику координації та розгортання стратегії відновлення</td><td rowspan="3">Аналіз причини збою поставок, прогнозування наслідків збою та рекомендації для політики відновлення</td><td rowspan="3">Розпізнавання корупційних ризиків в реальному часі</td><td rowspan="3">Раннє виявлення ризиків постачання</td></tr>
<tr><td>Попит:
• незбалансованість фінансових і матеріальних потоків;
• зменшення попиту</td></tr>
<tr><td>Процеси:
• недостатня швидкість прийняття рішень;
• нестабільність запасів на складах (нестачі та надлишки)</td></tr>
</table>

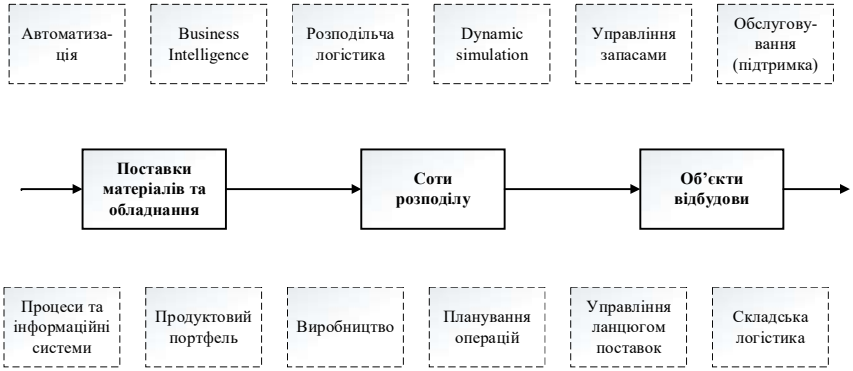


Рис. 1. Фреймворк ланцюга менеджерських рішень у процесі поствоєнного відновлення України

Джерело: розроблено авторами.

Використовуючи теорію просторової економіки, є доцільним в основу адміністративного та інституційного поділу для проєкту поствоєнного відновлення України в межах фреймворку використати стандарти Тюнена — правильний шестикутник, центр якого рівновіддалений від усіх його сторін.

Для такого шестикутника пропонується застосовувати термін — «сота», в межах якого буде знаходитися група об'єктів відновлення. Ці стандарти відповідатимуть першому рівню стандарту територіального поділу країн Європейського Союзу для статистичних цілей — Номенклатурі територіальних одиниць для статистики (NUTS) [8]. Також під час моделювання ланцюга менеджерських рішень проєкту відновлення доцільно використати сітку та ієрархію Кристаллера, оскільки вони дозволяють якісно ідентифікувати взаємозв'язки між адміністративними територіями першого, другого і третього порядків, а також ефективно визначати адміністративні межі різних замовлень для відновлення країни.

Використання якісних цифрових інструментів, вірогідно, збільшить шанси на прийняття правильних рішень і покращення ефективності організації, тобто персоналу та внутрішніх результатів [9].

Складові фреймворку ланцюга менеджерських рішень у процесі поствоєнного відновлення України подано у табл. 2.

Таблиця 2

СКЛАДОВІ ФРЕЙМВОРКУ

Складова	Призначення	Ефект	Компоненти
Автоматизація	У ланцюгах постачання всі операції, в яких регулярно повторюються рутинні дії або те, чим сьогодні займаються звичайні комп'ютерні системи, можна автоматизувати.	підвищення ефективності і продуктивності індивідуальні рішення до потреб клієнта усунення ризиків і додаткових витрат при впровадженні рішень автоматизації	автоматизовані склади автономні мобільні роботи (AMR) або конвеєри в поєднанні з автоматизованими пунктами передачі або завантаження системи сортування автоматичне розвантаження і завантаження цифровізація ланцюгів постачання автоматична ідентифікація матеріалів
Business intelligence	Компанії не можуть використовувати 75 % зібраних даних	створення «компанії, керованої даними» повністю автоматизована корпоративна звітність та забезпечення принципу «єдиного джерела правди». використання штучного інтелекту та машинного навчання в розширеній аналітиці даних	вдосконалені алгоритми машинного навчання та штучного інтелекту business intelligence- продажі business intelligence-виробництво business intelligence-логістика 5) business intelligence-фінанси 6) business intelligence-HR
Розподільча логістика	Правильна стратегія розподілу може вплинути на близько 80 % витрат на логістику	зниження логістичних витрат і підвищення рівня сервісу збільшення швидкості потоку, щоб досягти кращої зручності обслуговування за тих самих витрат	стратегія розподілу 2) оптимізація продуктового портфеля 3) аутсорсинг логістики

		підготовка дистрибуції до нових сценаріїв — зростання, зміни поведінки клієнтів, нові проєкти тощо	
Dynamic simulation	Динамічна симуляція виробництва та логістики усуває ризики, пов'язані з неправильними управлінськими рішеннями, щоб зменшити несподівані витрати під час впровадження змін. Остаточна форма системи налаштовується за допомогою динамічної 3D-моделі перед її впровадженням	усунення ризиків і невдалих рішень мінімізація множинних витрат під час впровадження рішення рекомендація оптимального рішення	виявлення та усунення вузьких місць перевірка запланованих змін у виробництві та логістиці моделювання критичних сценаріїв Digital Twin —цифрова форма реальної управлінської системи
Технічне обслуговування	Аналіз критичності запчастин, оптимізація життєвого циклу запчастин і запровадження автоматизованих процесів закупівлі запчастин	підвищення загальної ефективності обладнання (OEE), середнього часу напрацювання на відмову (MTBF) і зменшення середнього часу до ремонту (MTTR) оптимізація запасів запасних частин і усунення готових запасних частин і незареєстрованих складських приміщень або складів покращення співвідношення профілактичного та коригувального обслуговування та підвищення доступності обладнання	Мобільний додаток для фотографування запчастин і присвоєння їм інформації та вебдодаток для загального огляду ідентифікованих запчастин і перевірки їх ідентифікації

Закінчення табл. 2

Складова	Призначення	Ефект	Компоненти
Процеси та інформаційні системи	78% ефективності співробітників можуть залежати від правильної організації внутрішніх процесів	вся інформація доступна в одному місці оптимізація та автоматизація процесів = економія коштів та часу рекомендація оптимального рішення відповідно до потреб замовника	1) картографування поточної ситуації; 2) підтримка вибору ІС та оцінки Blueprint
Продуктовий портфель	Комплексний підхід, який розглядає всі відповідні аспекти (продажі, маркетинг, просування, ланцюг поставок тощо) за допомогою методології 360 градусів	збільшення прибутку на 2-3% зниження вартості запасів на 3-5% менше роботи з продуктами — автоматизація процесів	Аналіз Оптимізація Асортимент
Виробництво	Зміна способу планування виробництва може збільшити продуктивність до 30%	збільшення ефективності використання ресурсів до 30% збільшення доступності товарів на полицях до 99%+ До 25% скорочення капіталу, пов'язаного з виробництвом	динамічне моделювання (цифровий двійник) системи управління на виробництві роботизовані робочі станції візуалізація даних у вигляді інформаційних панелей
Планування продажів і операцій	Мета — стабільні, працездатні плани з дедлайнами замовників, висока завантаженість виробничого обладнання та людей	побудова сталого бізнесу послідовні та чітко визначені цілі та плани всієї організації оптимальне планування продажів і ресурсів — збільшення прибутку на 7%	Інструмент моделювання S&OP

Управління ланцюгом поставок	Стратегія управління ланцюгом поставок (SCM) є невід'ємною частиною корпоративної стратегії.	підвищення ефективності та дієвості матеріального, інформаційного та грошового обігу цілісність, надійність і гнучкість ланцюга поставок побудова сталого бізнесу та підвищення прибутковості компанії	Стратегічний план, цілі для визначених індикаторів управління запасами
Управління запасами	Програма інвестування пов'язаного капіталу, щоб у першу чергу зберегти на складі ключові товари та позбутися відстаючих	зменшення зобов'язаного капіталу на 20% підвищена доступність товарів для клієнта до 99 %+ автоматизація процесів — економія часу 50 %	Інформаційна система управління запасами
Складська логістика	80 % компаній не можуть використовувати власні склади на повну	збільшення потоку накопичувачів до 25 % збільшення обсягу зберігання до 25 % до 10 % зниження витрат на логістику	Комплексний проєкт внутрішнього і зовнішнього планування складських приміщень, включаючи відповідні технології та транспортно-розвантажувальне обладнання

Джерело: розроблено авторами.

Маючи на увазі ці системні основи, сформулюємо наступні методологічні принципи фреймворку ланцюжка менеджерських рішень в процесі пост воєнного відновлення України:

Принцип 1: підтримка прийняття рішень вважається життєздатною моделлю системи, яка складається з етапів до зриву, зриву та після зриву. Моделі динамічної симуляції забезпечують надійну конструкцію, аналіз стійкості, стрес-тестування різних альтернативних конструкцій та симуляцію політики умовного відновлення. Це лише кілька прикладів із багатьох можливих сфер застосування. Отже, пропонується використовувати цю трикрокову класифікацію як основну структуру, в рамках якого підтримку прийняття рішень забезпечує створення цифрового двійника ланцюга менеджерських рішень.

Принцип 2: інтеграція фізичних і кіберджерел даних з онлайн-моделюванням лінцюга менеджерських рішень

Моделі підтримки прийняття рішень можна збагатити даними з фізичних джерел (наприклад, системи ERP) і кіберджерел (наприклад, блокчейн, портали для співпраці з постачальниками та географічні, історичні дані про місцевість). Наприклад, історичні дані про ризики щодо попередніх збоїв або географічні дані про регіональну безпеку можуть допомогти в побудові реалістичних сценаріїв для оцінки стійкості. Це допоможе забезпечити параметричні вхідні дані для динамічних моделей, враховуючи доступні ресурси в неперерваному ланцюжку. Звідси інтеграція фізичних і кіберджерел даних з динамічними симуляціями вважається другим принципом створення цифрового двійника ланцюжка менеджерських рішень.

Принцип 3: моделі ланцюга прийняття рішень в рамках плану відновлення як інтеграція фізичних і кібермереж. У керованих даними інтегрованих системах підтримки прийняття рішень моделі ланцюгів стають ширшими та представляють як оганізаційну структуру, так і її кіберсистему.

Таким чином, третій принцип проєктування цифрового двійника системи управління проєктом відновлення полягає в розгляді фреймворку управління як інтеграції фізичних і кібермереж з точки зору кібернетики другого порядку.

Принцип 4: фреймоворк ланцюга прийняття рішень підтримує методологію використання даних для навчання та розпізнавання шаблонів збоїв. Компонент навчання є одним із нових якісних методів смарт-аналітики та забезпечує основу для ідентифікації зривів і моделей реакцій, які можна використовувати для вдосконалення як динамічних симуляцій, так і планування робіт.

Компоненти Індустрії 4.0 загалом і цифрові продукти зокрема створюють програми смарт-аналітики для досягнення нової якості та прозорості ланцюгів прийняття рішень під час керування серйозними проєктами. Поєднання динамічної симуляції, кібермереж, стандартів Тюнена, та інструментів аналізу даних утворює цифрового двійника: нову керовану даними структуру для управління проєктом повоєнного відновлення України.

Висновки та пропозиції. Основною метою цього дослідження було дослідити потенціал і розробити рекомендації щодо впровадження фреймворку для підвищення прозорості та стійкості ланцюга менеджерських рішень, щоб бути краще підготовленим до майбутніх збоїв. Розроблений фреймворк містить деякі інноваційні ідеї щодо організації ланцюга менеджерських рішень та організації забезпечення наскрізної прозорості управління під час відновлення України на базі застосування цифрових технологій. Зокрема, розроблено концептуальні вказівки щодо управління цифровим ланцюгом поставок і використання технологій для підвищення стійкості шляхом створення і використання прозорості в умовах нестатку інформації. На прикладі плану поствоєнного відновлення України розширено аналіз цифрових додатків для забезпечення стійкості ланцюга управління від миттєвих одноразових збоїв до умов бойових дій.

Висновки продемонстрували, як наскрізна прозорість може покращити управління стійкістю та допомогти компаніям справлятися зі збоями під час війни. Результати дослідження лежать в основі запропонованого багатовимірного фреймворку, що складається з компонентів управління, організації та цифрових технологій. Визначено, що наскрізна прозорість може допомогти підвищити стійкість ланцюжка поставок ефективним чином без створення надмірних і дорогих резервів.

Визначено загальні шаблони взаємодії з двома циклами надання сенсу рішень та формування сенсу між організаційними суб'єктами, що забезпечує постійний розвиток цифрової інфраструктури ланцюгів управління проєктом у складних умовах.

Післявоєнна відбудова дає шанс для України модернізувати свою економіку шляхом зміцнення бізнес-середовища (зменшення корупції, забезпечення прав приватної власності та загальне зміцнення верховенства права) та « перескоку» перед поколінням технологій.

Бібліографічні посилання

1. Otte, K. P., Knipfer, K., and Schippers, M. C. (2018). Team reflection: a catalyst of team development and the attainment of expertise. *The Oxford Handbook of Expertise*, Oxford University Press, doi: 10.1093/OXFORDHB/9780198795872.013.44.

2. Schippers, M.C., Edmondson, A.C., and West, M.A. (2014). Team reflexivity as an antidote to team information-processing failures. *Small Group Res.* 45. 731–769. doi: 10.1177/1046496414553473.

3. Wolak J. (2013). Catastrophic politics: how extraordinary events redefine perceptions of government. *Polit. Commun*. 30, 515–517. doi: 10.1080/10584609.2013.805683

4. Ganeshan, R., & Harrison, T. P. (1995). An introduction to supply chain management. *Department of Management Science and Information Systems*, 303.

5. Li X., Li Y. J., Cai X. Q. et al. Service channel choice for supply chain: who is better off by undertaking the service? *Production and Operations Management*. 2016. vol. 25, pp. 516–534.

6. Zhang J., Zhao S., Cheng T. C. E., and Hua G., «Optimisation of online retailer pricing and carrier capacity expansion during low-price promotions with coordination of a decentralised supply chain. *International Journal of Production Research*. 2019. vol. 57, no. 9, pp. 2809–2827.

7. S. Subrata, S. Majumder, and I. E. Nielsen, (2019). Is it a strategic move to subsidized consumers instead of the manufacturer? IEEE Access, vol. 7, pp. 169807–169824.

8. Choi T.-M. and Lambert, J.H. (2017), Advances in Risk Analysis with Big Data. Risk Analysis, 37: 1435-1442. URL. https://doi.org/ 10.1111/risa.12859

9. Zhang, G. (1999). Beyond ISO 9000 certification — a China experience. *Managerial Auditing Journal*. Vol. 14 Nos 1/2, pp. 75-8.

10. Christopher M., Peck H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*. Vol. 15. No. 2, pp. 1-13.

11. NUTS Homepage (2022). URL. https://ec.europa.eu/eurostat/web/ nuts/history, last accessed 2022/11/04

Статтю подано до редакції 28.11.2022

УДК: 5.519.2 DOI 10.33111/mise.102.5

Галіцин В.К., д.е.н., професор,
професор кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Жук Д.В., студент 3 курсу спеціальності «Системний аналіз»,
кафедра комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Петриченко А.В., студентка 3 курсу спеціальності «Системний аналіз»,
кафедра комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана.

Galicin V.K., Doctor of Economic Sciences,
Professor, Professor Department of Computer Mathematics
and Information Security,
KNEU named after Vadym Hetman

Zhuk D.V., Student of the 3rd year, specialization «Systems analysis»,
Department of Computer Mathematics and Information Security,
KNEU named after Vadym Hetman

Petrychenko A.V., Student of the 3rd year, specialization «Systems analysis»,
Department of Computer Mathematics and Information Security,
KNEU named after Vadym Hetman

ВИПАДКОВІ ПРОЦЕСИ В МЕТЕОРОЛОГІЇ

RANDOM PROCESSES IN METEOROLOGY

Анотація. *Зміна клімату — це спостережувані та прогнозовані довгострокові зміни середнього клімату, а також мінливість клімату, викликана діяльністю людини, включаючи такі аномалії, як посухи, сильні шторми та повені. Клімат нашої планети постійно змінювався протягом усієї геологічної історії Землі, і ці зміни супроводжувалися значними коливаннями середніх глобальних температур. Одним із головних чинників зміни глобальної середньої температури є спалювання викопного палива, вугілля, газу та нафти, що збільшило концентрацію парникових газів, таких як вуглекислий газ, у нашій атмосфері. Ця робота в першу чергу спрямована на вивчення проблем прогнозування та моніторингу такого погодного явища, як локальна зміна температури — на основі моделей часових рядів, представлених у цій роботі, можна зробити необхідні прогнози також для вимірювання рівня снігового покриву, рівень опадів. Використання моделей прогнозування температури (таких як метод Холта-Вінтера або бібліотека Пророка) має велике практичне значення, починаючи від прогнозування температури на наступний рік*

для сівби, врожайності культур тощо. У даній роботі було проведено довгостроковий аналіз середньодобової температури у Київській області мовою програмування Python та її бібліотеками для аналізу даних Pandas, Numpy, Scikit-Learn тощо за допомогою моделей експоненційного згладжування та бібліотеки Prophet. За допомогою цих моделей можна обробляти та прогнозувати різні типи даних, такі як: температура, рівень опадів, глибина снігового покриву. Крім того, прогнози можуть бути використані для різноманітних цілей людської діяльності. Матеріали статті мають науково-методичний характер.

Ключові слова: *випадковий процес; часові ряди; метеорологія; зміна клімату; модель прогнозування; навчання під наглядом; експоненціальне згладжування; метод Холта-Вінтера; бібліотека Пророк.*

Abstract. *Climate change is the observed and projected long-term changes in average climate, as well as climate variability, caused by human activity, including such anomalies as droughts, severe storms and floods. The climate of our planet has been constantly changing throughout the entire geological history of the Earth, and these changes were accompanied by significant fluctuations in average global temperatures. One of the main drivers of global average temperature change is the burning of fossil fuels, coal, gas and oil, which has increased the concentration of greenhouse gases such as carbon dioxide in our atmosphere. This work is primarily aimed at studying the problems of predicting such a weather phenomenon as a local change in temperature — based on the time series models presented in this work, it is possible to make the necessary predictions also for measuring the level of snow cover, precipitation level. The use of temperature prediction models (such as Holt-Winter's method or Prophet library) is of great practical importance, starting from predicting the temperature for the next year for sowing, crop yields, etc. In this work, a long-term analysis of the average daily temperature in the Kyiv region was carried out using the Python programming language and its data analysis libraries Pandas, Numpy, Scikit-Learn, etc. using exponential smoothing models and the Prophet library. These models can be used to process and forecast different types of data, such as: temperature, precipitation, snow depth. In addition, forecasts can be used for various purposes of human activity. The materials of the article have a scientific and methodological nature.*

Keywords: *Random process; time series; meteorology; climate change; prediction model; supervised learning; exponential smoothing; Holt-Winter's method; Prophet.*

Постановка проблеми. Зміна клімату та наслідки цього процесу для планети — один з важливих напрямів сучасних метеорологічних досліджень. Метеорологія наука про будову і властивості земної атмосфери та фізичних процесів, що в ній відбуваються. Перша офіційна згадка про цю науку належить Аристотелю, який приблизно в 340 р. до н. е. написав книгу під назвою «*Метеорологія*», що містила все, що було відомо на той час про погоду та клімат. Назва походила від грецького слова «Μετέωρο», що означало «щось високо» і стосувалося усього, що спостерігалося в атмосфері [2].

Математичні методи та моделі використовують для розв'язання побудови прогнозу погоди і загальної циркуляції атмосферних процесів, чисельних алгоритмів для їх вирішення. Рівняння гідротермодинаміки атмосферних процесів є досить скла-

дними, тому існує необхідність розробки ефективніших алгоритмів, здатних з високою точністю описати широкий спектр завдань динамічної метеорології та прогнозу погоди. Побудова алгоритмів розв'язання таких завдань тісно пов'язана з проблемою апроксимації рівнянь, генералізації даних і стійкості отриманих розв'язків, які є основними проблемами під час конструкції нових чисельних алгоритмів загалом. З наукової точки зору передбачення погоди — одне з найскладніших завдань фізики атмосфери. Удосконалення відповідного комп'ютерного обладнання дозволяє реалізовувати математичні підходи і методи дослідження атмосфери. Кожен із них дає змогу в тій чи тій мірі прогнозувати метеорологічні явища.

Аналіз останніх досліджень і публікацій. Для отримання достовірного прогнозу погоди, у міжнародних кліматичних центрах збирається інформація про поточну погоду на Землі. Вона отримується з тисяч метеостанцій, метеопостів, зондів, радіобуїв: наземних, літальних, плаваючих, що покривають необхідну територію густою сіткою. Для того щоб модель провела розрахунок прогнозу погоди, їй необхідно зібрати якомога більше даних про поточну погоду. Чим густіше на території розміщені метеостанції, тим точніше буде розрахований прогноз [4].

Статистичні моделі спостережуваних щоденних змін («Генератори погоди»), можуть заповнювати відсутні дані або створювати нескінченно довгі синтетичні — ці моделі погодних часових рядів імітують ключові властивості спостережуваних метеорологічних записів (тобто щоденні середні значення, дисперсії та коваріації, частоти, екстремуми тощо). Вони використовуються в моделюванні змін сільського господарства, екосистем чи клімату, оскільки спостережувані наземні метеорологічні дані часто є неадекватними у контексті їх тривалості, повноти чи просторового охоплення.

Щоденні симулятори погоди є, безумовно, найпоширенішими як через широку доступність даних про погоду в часовому масштабі, так і з великою кількістю моделей впливів, які керуються щоденними даними про погоду [5]. Демонстрацію роботи випадкового генератора погоди подано на рис. 1.

Існує два взаємодоповнюючі способи перегляду погодних моделей. По-перше, коли ці моделі використовуються для моделювання за методом Монте-Карло, їх можна розглядати як складні генератори випадкових чисел, результати яких статистично нагадують щоденні дані про погоду в певному місці [1].

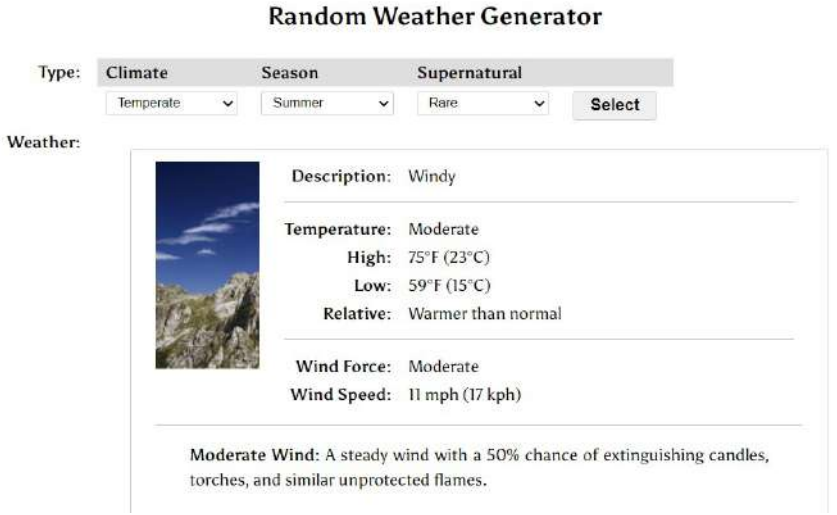


Рис. 1. Випадковий генератор погоди

Джерело: [9].

Важливо зазначити, що генератори погоди не є алгоритмами прогнозування погоди, і тому сильно відрізняються від детермінованих погодних моделей, які працюють шляхом чисельного інтегрування диференціальних рівнянь у частинних похідних, що описують потоки рідини. Приклад моделювання за вказаним методом продемонстровано на рис. 2. По-друге, це стохастичні моделі щоденних (і відповідно довготривалих) коливань погоди. З цієї позиції параметри стохастичної моделі погоди містять стислу дистиляцію певних аспектів місцевого клімату на локальній території.

Опади не лише є найважливішою метеорологічною змінною для багатьох застосувань, а й наявність або відсутність опадів також зазвичай впливає на статистику багатьох змінних без опадів, які потрібно моделювати. Дані про атмосферні опади демонструють відмінні та складні характеристики, які ускладнюють статистичні моделі, необхідні для їх опису. На додаток до кореляції між значеннями в послідовні періоди часу, яка є типовою для всіх погодних змінних, кількість опадів є унікальною за змішаним характером, оскільки це є як дискретна, так і неперервна змінна [7].

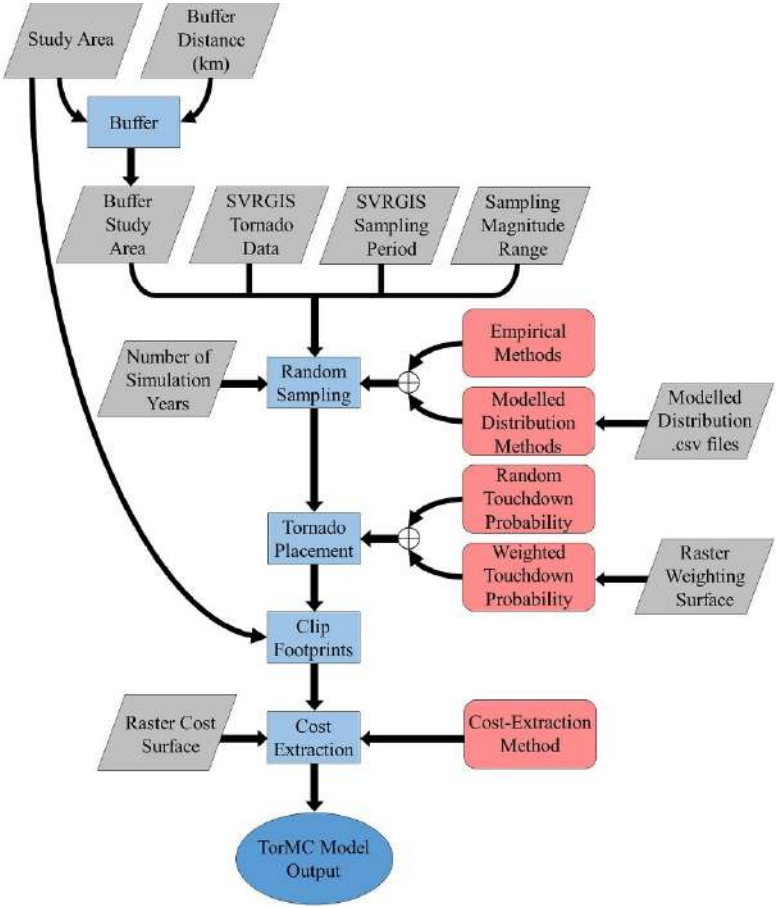


Рис. 2. Приклад моделі для розрахунку впливу торнадо за методом Монте-Карло

Джерело: [10].

Іншими словами, опади дуже часто точно дорівнюють нулю, і отже, існує розрив у розподілі ймовірностей даних про опади між нульовими та ненульовими спостереженнями. Процес випадання опадів проявляється у двох станах погоди — вологому або сухому. Ключовим аспектом стохастичних моделей погоди є представлення тенденції вологих і сухих днів виявляти стійкість або позитивну послідовну кореляцію, так що вологий і сухий цикли мають тенденцію повторюватися у часі сильніше, ніж очікується.

Процес визначення інтенсивності опадів належить до моделювання ненульової кількості опадів.

Через розвиток науково-технічного прогрес зростає не лише завчасність прогнозів, а й їхня точність — це дає можливість отримати прогностичну інформацію уже не лише для кожного пункту, а й для окремих районів міст, навіть вулиць. «Проте для того, щоб зробити такі розрахунки для України, необхідно суттєво реорганізувати існуючу мережу спостережень, адже вона уже давно не задовольняє існуючі потреби в інформації. Саме це завдання і є одним з пріоритетних для ДСНС України. Технічному переоснащенню мережі спостережень в Україні сприятиме співпраця з компанією «Baron — Critical Weather Intelligence», з якою нещодавно підписано Протокол про співробітництво у сфері гідрометеорологічної діяльності», — повідомляють у ДСНС України.

Основним методом, який використовують синоптики в усьому світі для прогнозу погоди, є синоптичний. Цей метод передбачає аналіз і прогноз атмосферних процесів і умов погоди за допомогою синоптичних карт, аерологічних діаграм, вертикальних розрізів атмосфери та інших засобів. Дані численних моделей погоди все ще є допоміжними засобами. Вони дозволяють отримати інформацію лише про основні характеристики атмосфери — температуру, тиск, вологість, швидкість вітру та їхню зміну. Використовуючи цю інформацію, синоптики можуть спрогнозувати явища погоди, їхню інтенсивність та локалізацію і попередити про них населення та відповідні органи влади.

Зміна клімату — це спостережувані та прогнозовані довгострокові зміни клімату, а також мінливість клімату, спричинена діяльністю людини, включаючи такі аномалії, як посухи, сильні шторми та повені. Удосконалення якості прогнозів погоди відбувається за двома напрямами: поліпшення справджуваності прогнозу і збільшення його завчасності. Короткостроковий прогноз визначається переважно початковим станом атмосфери. Для середньострокових прогнозів потрібне як детальне знання початкових полів метеорологічних величин, так і уміння описати впливи зовнішніх чинників, які призводять до нового стану рівноваги системи, що прогнозується. Довгостроковий прогноз меншою мірою залежить від початкового стану атмосфери і включає елементи моделювання клімату.

Мета статті — аналіз проблем прогнозування такого погодного явища, як локальна зміна температури, на основі моделей часових рядів та їх застосування також для вимірювання рівня снігового покриву, рівню опадів.

Основний матеріал дослідження. З метою довгострокового аналізу та прогнозу середнього рівня температури у Київській обл. було використано відкриті дані з сайту NOAA (National Oceanic and Atmospheric Administration). Київська обл., на якій проводиться довгостроковий прогноз та аналіз показників замірів, розташована на півночі України. Клімат помірно континентальний, помірний, з достатньою вологістю.

NOAA — це федеральне відомство в структурі Міністерства торгівлі, яке займається різними видами метеорологічних, геодезичних досліджень і прогнозів для США та інших країн, вивченням світового океану і атмосфери. На сайті NOAA розміщені відкриті дані, де за певний проміжок часу можна знайти місцеві кліматологічні дані, морські дані, річні та сезонні норми тощо. Наявні відкриті дані з вимірювань станцій 3 у Київській обл.: KIEV, UP; BORYSPIL, UP; NEMESHAEVO, UP. Сторінку з сайту з прикладом запиту на пошук денних загальних показників погоди у Київській обл. подано на рис. 3. На рис. 4 показано деякі деталі про локацію, що досліджується. Інформація про наявні станції в Київській обл. представлено на рис. 5.

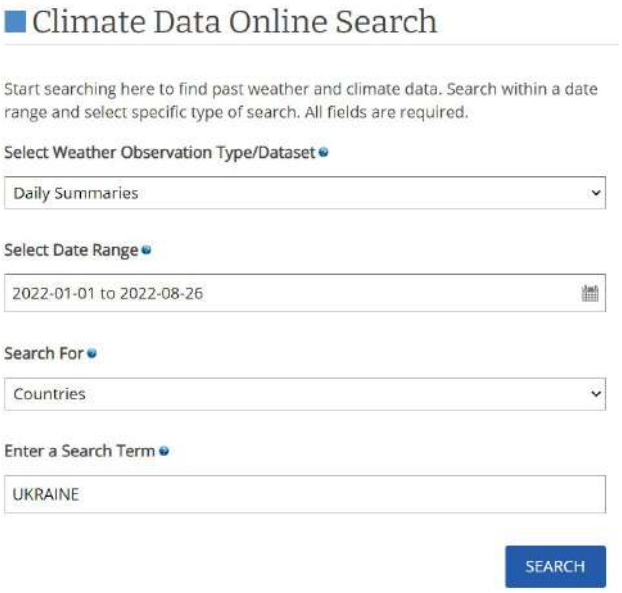


Рис. 3. Пошук денних загальних показників погоди у Київській обл.

Джерело: [11].

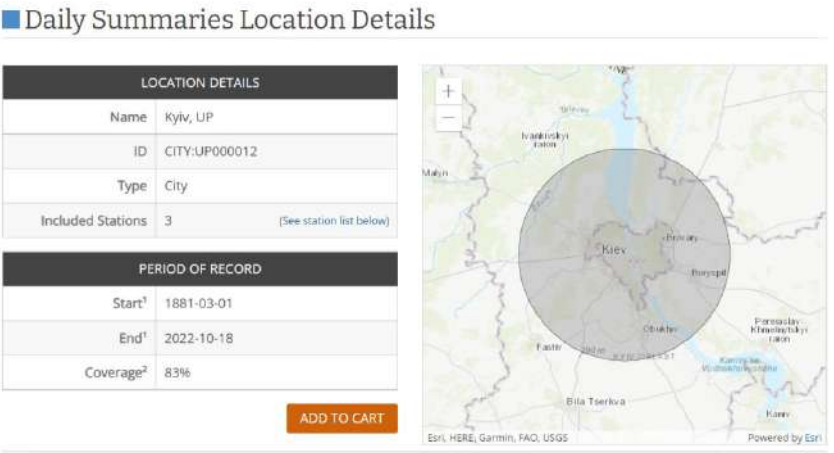


Рис. 4. Деталі шуканої локації, % покриття станцій

Джерело: [12].

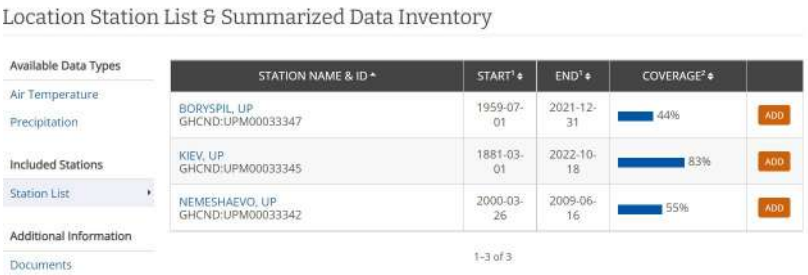


Рис. 5. Наявні станції у Київській обл., періоди замірів спостережень

Джерело: [13].

Структура отриманих даних:

- STATION — номер певної станції;
- NAME — назва певної станції;
- LATITUDE, LONGITUDE — широта, довгота;
- DATE — дата;
- TAVG — середня температура;
- TMAX — максимальна температура;

- TMIN — мінімальна температура;
- PRCP — рівень опадів;
- SNWD — глибина сніжного покриву.

Дослідження даних проводилося мовою програмування Python, включаючи бібліотеки для роботи з масивами великих даних Pandas, Numpy, засобів візуалізації Plotly, Matplotlib, статистичних моделей Statsmodels, класичного машинного навчання з вчителем Scikit-Learn. Виконавши розвідковий аналіз даних (Exploratory Data Analysis), на перший погляд можна помітити, що:

1) дозмір дата сету — 24844 записи та 11 колонок;

2) максимальні, максимальні, середні, середньоквадратичне відхилення рівнів температур, опадів, глибини сніжного покриву на 3 станціях в Київській області;

3) існує багато пропущених даних, особливо рівня глибини снігу (пояснюється сезонністю), температур максимальних та мінімальних;

4) унікальних записів на кожній станції — різна кількість, так як заміри не проводилися кожен день;

5) станція NEMESHAEVO, UP почала працювати набагато пізніше (у 2000 р.), ніж станції KIEV, UP і BORYSPIL, UP.

На рис. 6 продемонстровано статистику даних та аналіз кількості пропущених значень. На рис. 7 подано приклад перших замірів у 2000 р.

	LATITUDE	LONGITUDE	ELEVATION	PRCP	SNWD	TAVG	TMAX	TMIN
count	24884.000000	24884.000000	24884.000000	8825.000000	2468.000000	22698.000000	13534.000000	12332.000000
mean	50.391401	30.678729	129.332744	2.399127	120.184765	8.748498	13.378077	4.697389
std	0.077932	0.284881	48.803056	6.259729	127.966285	9.986619	11.164683	8.962894
min	50.333000	30.100000	0.000000	0.000000	10.000000	-26.500000	-21.700000	-43.000000
25%	50.333000	30.533100	122.000000	0.000000	30.000000	1.000000	3.800000	-1.400000
50%	50.400000	30.533100	122.000000	0.200000	79.000000	8.900000	14.000000	4.700000
75%	50.400000	30.967000	166.000000	2.200000	180.000000	17.200000	22.800000	12.200000
max	50.600000	30.967000	166.000000	255.000000	2230.000000	36.200000	94.600000	26.800000

```
STATION        0
NAME           0
LATITUDE       0
LONGITUDE      0
ELEVATION      0
DATE           0
PRCP       16059
SNWD       22416
TAVG        2186
TMAX       11350
TMIN       12552
dtype: int64
```

Рис. 6. Статистики отриманих даних, кількість пропущених значень (NaN values)

Джерело: розроблено авторами.

	STATION	NAME	LATITUDE	LONGITUDE	ELEVATION	DATE	PRCP	SNWD	TAVG	TMAX	TMIN
0	UPM00033342	NEMESHAEVO, UP	50.6	30.1	0.0	2000-03-26	NaN	NaN	NaN	NaN	12.6
1	UPM00033342	NEMESHAEVO, UP	50.6	30.1	0.0	2000-04-25	NaN	NaN	NaN	21.0	NaN
2	UPM00033342	NEMESHAEVO, UP	50.6	30.1	0.0	2000-04-26	NaN	NaN	NaN	23.1	12.6
3	UPM00033342	NEMESHAEVO, UP	50.6	30.1	0.0	2000-04-27	NaN	NaN	23.1	23.0	11.5
4	UPM00033342	NEMESHAEVO, UP	50.6	30.1	0.0	2000-04-28	NaN	NaN	23.0	24.4	15.3

Рис. 7. Приклад перших замірів на станції NEMESHAEVO, UP у Київській обл., початок замірів 2000 р.

За методом Найменших квадратів візуалізуємо лінію тренду випадкового процесу, а також сам випадковий процес, де на осі *OX* — час (дискретна величина), на осі *OY* — середньодобова температура (неперервна величина).

Випадковий процес середньодобової температури є стаціонарним у випадку замірів на станціях KIEV, UP і BORYSPIL, UP, має виражену сезонність по роках та порах року. Діаграми зображено на рис. 8–10.

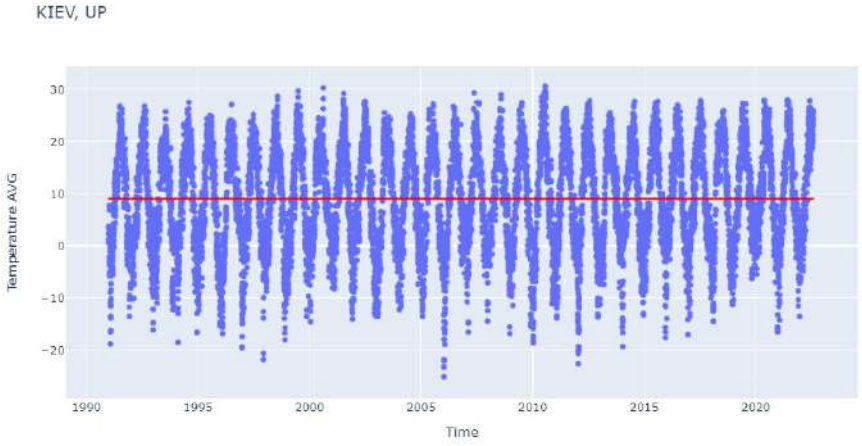


Рис. 8. Показники замірів середньодобової температури на станції KIEV, UP

Джерело: розроблено авторами.

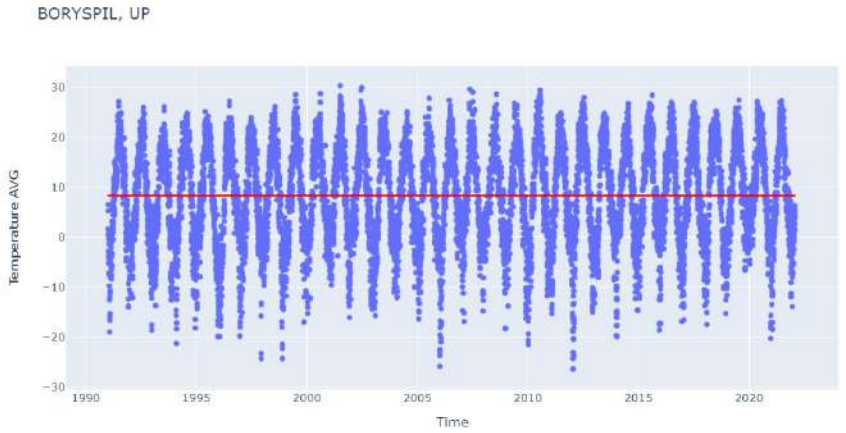


Рис. 9. Показники замірів середньодобової температури на станції BORYSPIL, UP

Джерело: розроблено авторами.

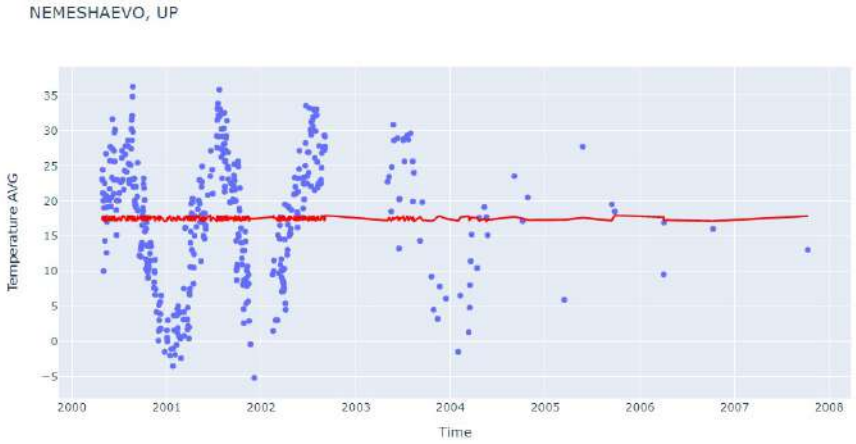


Рис. 10. Показники замірів середньодобової температури на станції NEMESHAEVO, UP

Джерело: розроблено авторами.

У випадку недостатніх і непостійних замірів на станції NEMESHAEVO, UP можна сказати, що цей процес не є стаціонарним — заміри припинилися у 2008 р. Для перевірки стаціонар-

ності випадкового процесу можна використати критерій Дікі-Фуллера та p-value. Якщо p-value менше 0,05, то нульову гіпотезу (відкинути нестаціонарність) буде відхилено, і цей випадковий процес буде стаціонарним. В іншому випадку він не буде стаціонарним [6].

Результати проведення тесту Дікі Фуллера подано на рис. 11–13.

```
adf, pval, usedlag, nobs, crit_vals, icbest =  adfuller(temp1.values) # KIEV, UP station
print('ADF test statistic:', adf)
print('ADF p-values:', pval)
print('ADF number of lags used:', usedlag)
print('ADF number of observations:', nobs)
print('ADF critical values:', crit_vals)
print('ADF best information criterion:', icbest)
```

```
ADF test statistic: -7.814145099346631
ADF p-values: 6.942206731164266e-12
ADF number of lags used: 40
ADF number of observations: 11275
ADF critical values: {'1%': -3.4309301143596738, '5%': -2.861796379231577, '10%': -2.5669064655552334}
ADF best information criterion: 52077.163820151254
```

Рис. 11. Результати тесту Дікі-Фуллера для випадкового процесу замірів станції KIEV, UP

Джерело: розроблено авторами.

```
adf, pval, usedlag, nobs, crit_vals, icbest =  adfuller(temp2.values) # BORYSPIL, UP station
print('ADF test statistic:', adf)
print('ADF p-values:', pval)
print('ADF number of lags used:', usedlag)
print('ADF number of observations:', nobs)
print('ADF critical values:', crit_vals)
print('ADF best information criterion:', icbest)
```

```
ADF test statistic: -7.752913154242219
ADF p-values: 9.91031944752788e-12
ADF number of lags used: 39
ADF number of observations: 10902
ADF critical values: {'1%': -3.4309499670139245, '5%': -2.8618051521469448, '10%': -2.5669111353567367}
ADF best information criterion: 51982.25663392912
```

Рис. 12. Результати тесту Дікі-Фуллера для випадкового процесу замірів станції BORYSPIL, UP

Джерело: розроблено авторами.

Отже, є три випадкові процеси з дискретним часом спостереження. Згідно результату статистичних тестів Дікі — Фуллера, перші два процеси мають чітку стаціонарність по роках. Останній має занадто багато відсутніх значень і є нестаціонарним, його не можна точно описати з позиції сезонності.

Декомпозиція часових рядів — це статистична задача, яка розбиває часовий ряд на кілька компонентів, кожен з яких представляє одну з базових категорій закономірностей, а саме: тренд, сезонність і залишки [8].

```
adf, pval, usedlag, nobs, crit_vals, icbest =  adfuller(temp3.values) # NEMESHAEVO, UP station
print('ADF test statistic:', adf)
print('ADF p-values:', pval)
print('ADF number of lags used:', usedlag)
print('ADF number of observations:', nobs)
print('ADF critical values:', crit_vals)
print('ADF best information criterion:', icbest)
```

```
ADF test statistic: -2.8267475129688497
ADF p-values: 0.054553482945667635
ADF number of lags used: 3
ADF number of observations: 436
ADF critical values: {'1%': -3.445437655035993, '5%': -2.8681918844944785, '10%': -2.5703132171113543}
ADF best information criterion: 2378.713320634922
```

Рис. 13. Результати тесту Дікі-Фуллера для випадкового процесу замірів станції NEMESHAEVO, UP

Джерело: розроблено авторами.

Припустимо, що у нас є дві адитивні моделі, тобто такі, що складаються з лінійного тренду та сезонного циклу з однаковою частотою та амплітудою. Сезонні та залишкові компоненти представлені на рис. 14.

Рис. 14. Сезонний компонент випадкових процесів

Джерело: розроблено авторами.

Усі спостереження мають однакову сезонну структуру: починаючи з низької середньої температури на початку року взимку, потім навесні середня температура все більше зростає, влітку —

пік середньодобової температури року, середньодобова осіння температура знижується, в кінці циклу закінчується низькою середньо добовою температурою. На рис. 15 продемонстровано залишковий компонент випадкових процесів.

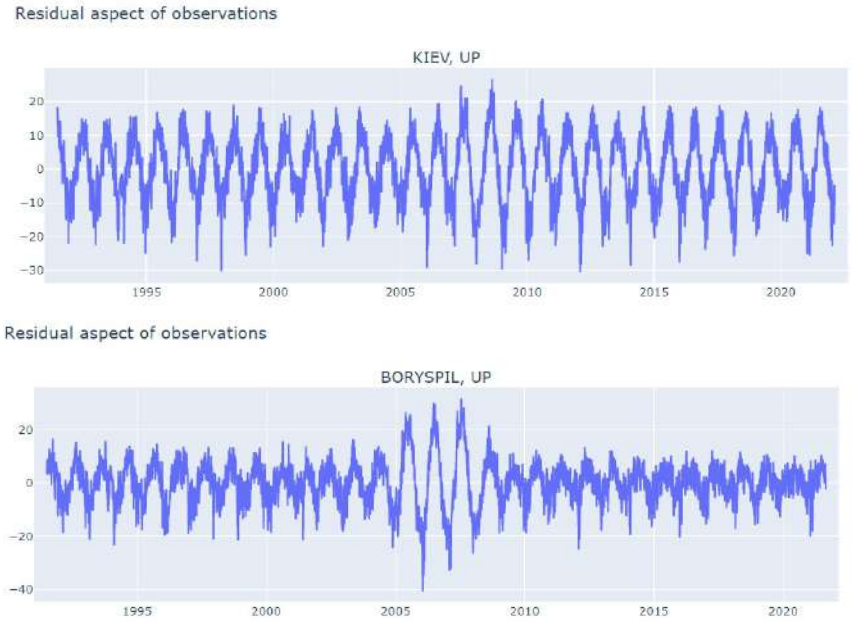


Рис. 15. Залишковий компонент випадкових процесів

Джерело: розроблено авторами.

Типи моделей прогнозування часових рядів [3]:

- *Класичні моделі часових рядів* — це сімейство моделей, які традиційно часто використовуються в багатьох областях прогнозування. Вони здебільшого базуються на часових змінах у часовому ряді та адекватно відображають залежності з однофакторними часовими рядами. Ці моделі зазвичай застосовуються лише до часових рядів і не є корисними для інших типів машинного навчання.
- *Контрольовані моделі* — це сімейство моделей, які використовуються для багатьох завдань машинного навчання. Модель машинного навчання використовує чітко визначені вхідні змінні та одну або кілька вихідних (цільових) змінних. Контрольовані моделі можна використовувати для часових рядів, за умови, що є спосіб виокремити сезонність і помістити її в змінну.

Експоненційне згладжування — це метод математичного перетворення, який застосовується при прогнозуванні часових рядів. При кожній наступній ітерації враховуються всі попередні значення ряду, але ступінь врахування зменшується за експонентою (s_t — згладжений ряд; c_t — первинний ряд; $\alpha \in (0, 1)$ — коефіцієнт згладжування, який обирається апріорі). Рекурентна формула має вигляд:

$$s_t = \begin{cases} c_1 : t = 1 \\ s_{t-1} + \alpha * (c_t - s_{t-1}) : t > 1 \end{cases}$$

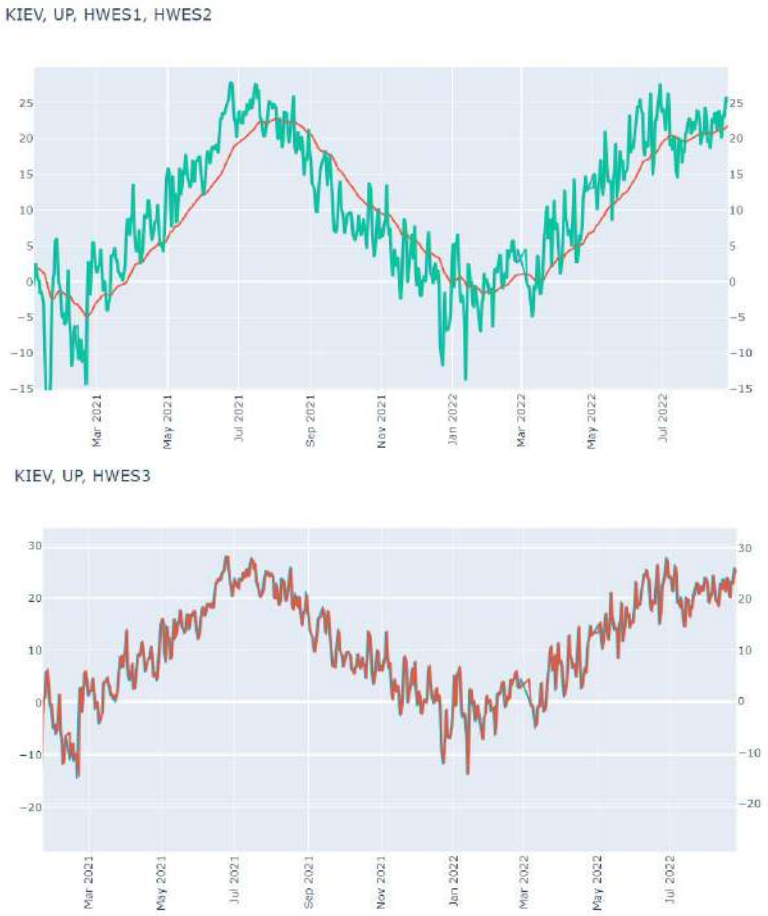


Рис. 16. Одиничне, подвійне, потрійне експоненційне згладжування

Джерело: розроблено авторами.

На рис. 16 побудовано графіки відповідно одиничного, подвійного та потрійного експоненційного згладжування. Розроблений авторами на основі потрійного експоненційного згладжування прогноз на рік вперед подано на рис. 17. Використано модель Хольта — Уінтерса. Основні характеристики отриманої моделі за методом Хольта-Уінтерса (коефіцієнта R^2, похибок MSE, MAE) подано на рис. 18.

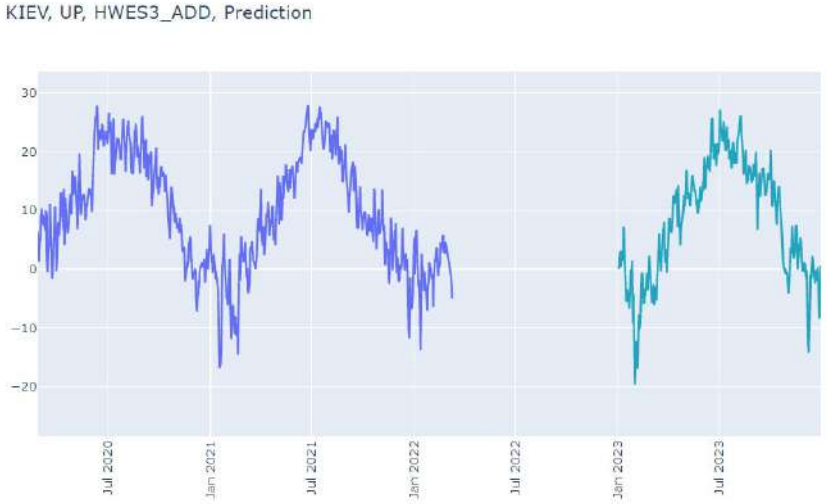


Рис. 17. Прогноз на рік вперед за допомогою потрійного експоненційного згладжування (модель Хольта — Уінтерса)

Джерело: розроблено авторами.

```
In [51]: mean_squared_error(temp1.values[365:730], data) # MSE
Out[51]: 26.316476334574727

In [52]: mean_absolute_error(temp1.values[365:730], data) # MAE
Out[52]: 4.036518487871952

In [53]: r2_score(temp1.values[365:730], data) # R^2
Out[53]: 0.7024258165900131
```

Рис. 18. Результати методу Хольта—Уінтерса (коефіцієнта R^2, похибок MSE, MAE)

Джерело: розроблено авторами.

Бібліотека Prophet — це збірка процедур для прогнозування даних часових рядів на основі адитивної моделі, де лінійні або нелінійні тренди узгоджуються з річною, тижневою та денною сезонністю.

На рис. 19 подано отриманий авторами прогноз на рік складених з використанням бібліотеки Prophet. На рис. 20 показано відповідні результативні характеристики останніх прогнозів.

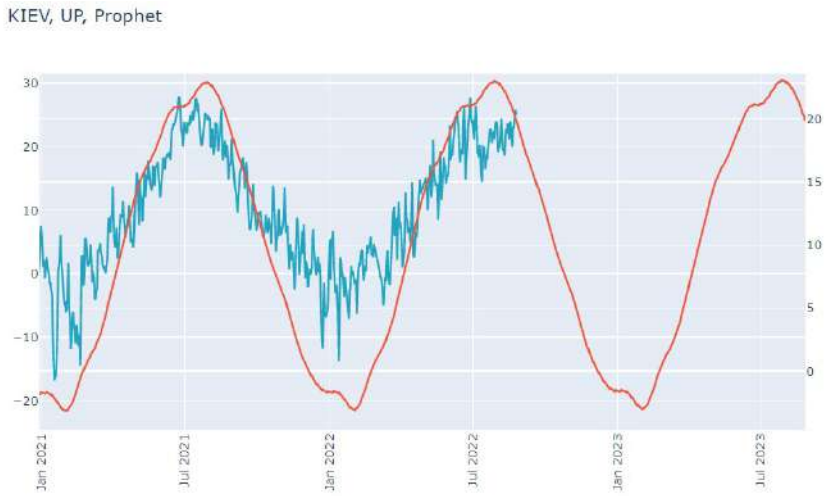


Рис. 19. Прогноз на рік вперед
за допомогою бібліотеки Prophet

Джерело: розроблено авторами.

```
In [46]: mean_squared_error(temp1.values, forecast.iloc[0:11316]["yhat"].values) # MSE
Out[46]: 17.296278436536348

In [47]: mean_absolute_error(temp1.values, forecast.iloc[0:11316]["yhat"].values) # MAE
Out[47]: 3.296445347214469

In [48]: r2_score(temp1.values, forecast.iloc[0:11316]["yhat"].values) # R^2
Out[48]: 0.8233631153055813
```

Рис. 20. Результати бібліотеки Хольта-Уінтерса (коефіцієнта R^2, похибок MSE, MAE)

Джерело: розроблено авторами.

Висновки та пропозиції. Було проведено довгостроковий аналіз середньодобової температури у Київській обл. мовою програмування Python та її бібліотеками для аналізу даних Pandas, Numpy, Scikit-Learn тощо за допомогою моделей експоненційного згладжування, бібліотеки Prophet. За результатами даної роботи можна зробити такі висновки:

- Бібліотека Prophet має вищий показник R^2 і нижчий MSE, MAE відповідно. Незважаючи на те, що Prophet є моделлю half-black box, вона досить добре прогнозує за допомогою керованих методів машинного навчання — модель генералізує дані, а також розпізнає сезонність і стаціонарність.
- Використовуючи моделі класичного прогнозування часових рядів (наприклад, експоненціальне згладжування, метод Хольта — Уінтерса), керованого машинне навчання (Prophet), стає можливим їх масштабування, прогнозування на тривалі періоди часу.
- За допомогою цих моделей можна обробляти та прогнозувати різні типи даних, такі як: температура, рівень опадів, глибина снігового покриву. Крім того, прогнози можуть бути використані для різноманітних цілей людської діяльності.

Підвищення завчасності й справджуваності прогнозів метеорологічних величин, небезпечних і стихійних явищ відкривають виняткові можливості і перспективи математичного моделювання і ще більшого його практичного застосування в задачах попередження і зменшення негативних наслідків від надзвичайних ситуацій природного і техногенного характеру. Математичне моделювання на сучасному етапі є однією з важливих і ефективних систем інформаційного забезпечення, експертного аналізу, обґрунтування організаційних рішень і підвищення рівня керування. Розробка і впровадження безперервних прогнозувальних систем наразі стають все більш актуальними у зв’язку зі впровадженням автоматизованих систем оцінки ризику, прийняття рішень і керування. Однією з таких технік уточнення прогнозу може бути використання машинного навчання.

Особливо важливим, на наш погляд, аспектом даної методології є то, що вона може використовуватись для подальшого дослідження.

Бібліографічні посилання

1. Юрченко М.Є. Прогнозування та аналіз часових рядів. Методичні вказівки до практичних занять та самостійної роботи студентів спеціа-

льності 051 «Економіка» освітня програма «Економічна кібернетика», «Економічна аналітика». Чернігів: ЧНТУ, 2018. 88 с.

2. Дорошенко А.Ю., Бекетов О.Г., Прусов В.А., Тирчак Ю.М., Яценко О.А. Формалізоване проектування та генерація паралельної програми чисельного прогнозування погоди. *Проблеми програмування*. 2014. № 2–3. С. 72–81.

3. Валєєв К.Г., Джалладова І.А. Теорія ймовірностей та теорія випадкових процесів: навч. посібник. Київ:КНЕУ, 2009. 378 с.

4. Прусов В.А., Дорошенко А.Ю. Моделювання природних і техногенних процесів в атмосфері. Київ: Наукова думка, 2006. 542 с

5. Прусов В.А., Сніжко С.І. Математичне моделювання атмосферних процесів. Київ: Ніка-Центр. 2005. 496 с.

6. Shumway, Robert H. a David S. STOFFER. Time Series Analysis and Its Applications: With R Examples. Third Edition. New York: Springer-Verlag, 2011. 606 p.

7. Grimmett, Geoffrey R. a David STIRZAKER. Probability and random processes. 3rd ed. — Oxford: Oxford University Press, 2001. xii. 596 c.

8. Hamilton, James Douglas. Time series analysis. Princeton, N.J.: Princeton University Press, 1994. xiv. 799 c.

9. Random Weather Generator. URL: https://donjon.bin.sh/d20/weather/

10. A Monte Carlo model for estimating tornado impacts. URL: https://rmets.onlinelibrary.wiley.com/doi/full/10.1002/met.1552

11. NOAA Climate Data online. URL: https://www.ncei.noaa.gov/cdo-web/

12. NOAA Climate Data search. URL: https://www.ncei.noaa.gov/cdo-web/search

13. NOAA Climate Data station list. URL: https://www.ncei.noaa.gov/cdo-web/datasets/GHCND/locations/CITY:UP000012/detail

Статтю подано до редакції 25.11.2022

УДК: 331.54 DOI 10.33111/mise.102.6

Гладка Ю.А., к.фіз.-мат.н., доцент,
доцент кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Дубецький О.В., магістр спеціальності «Системний аналіз»,
кафедра комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Gladka Yu.A., candidate of Physical and Mathematical Sciences, Associate Professor, Department of Computer Mathematics and Information Security,
KNEU named after Vadym Hetman

Dubetsky O.V., master's degree in «System Analysis»,
Department of Computer Mathematics and Information Security,
KNEU named after Vadym Hetman

СИСТЕМНИЙ АНАЛІЗ ВПЛИВУ ЦИФРОВИХ КОМПЕТЕНЦІЙ НА РИНОК ПРАЦІ УКРАЇНИ

SYSTEM ANALYSIS OF THE IMPACT OF DIGITAL COMPETENCES ON THE LABOR MARKET OF UKRAINE

Анотація. *Інтелектуальний аналіз даних є однією з ефективних сфер створення інноваційних даних, призначених для виявлення прихованої та цінної інформації. Досягнення наукової інформаційної експертизи застосовуються у різних сферах людської діяльності, однією з таких сфер є ринок праці. У статті досліджено питання впливу цифрових компетенцій на ринок праці України. Проведено інтелектуальний аналіз даних ринку праці на прикладі вакансій. Встановлено поточний стан використання цифрових компетенцій в Україні. Виявлено проблемні аспекти аналітичної інтерпретації цифрових компетенцій та забезпечення повноти розкриття інформації у сфері цифрових компетенцій в умовах цифрових трансформацій, запропоновано шляхи вирішення. Доведено, що зіставлення тегів на основі правил відповідає всім необхідним навичкам, але також виділяє інші іменники та власні іменники. Через великий шум і для видобування використано інший словник для отримання необхідних іменників (навичок). Цю проблему вирішено за допомогою інших моделей NLP, таких як тематичне моделювання, LSTM і вбудовування слів. Зроблено висновок з аналізу, що вилучення контекстних тем без шуму усе ще вивчається. Проведене дослідження дозволило визначити низький рівень застосування цифрових компетенцій у посадових вимогах. Підтверджено, що це свідчить про недостатній розвиток цифровізації і пов'язано безпосередньо з економічною ситуацією в країні, яка має місце обмеженість ресурсів.*

Ключові слова: *системний аналіз, інтелектуальний аналіз даних, цифрова компетентність, цифрові технології, вирішення проблем, цифровізація, цифрові перетворення, ефективність.*

Abstract. *Data mining is one of the effective areas of creating innovative data designed to uncover hidden and valuable information from data. Achievements of scientific information expertise find their application in various spheres of human activity, one of such spheres is the labor market. The article examines the impact of digital competencies on the labor market of Ukraine. An intellectual analysis of labor market data was carried out using the example of vacancies. The current state of use of digital competences in Ukraine is established. Problematic aspects of the analytical interpretation of digital competences and ensuring the completeness of information disclosure in the field of digital competences in the conditions of digital transformations are identified, solutions are proposed. Rule-based tagging meets all the necessary skills, but also highlights other nouns and proper nouns. There was a lot of noise and mining required another dictionary to get the required nouns (skills). This problem is interesting to solve using other NLP models, such as topic modeling, LSTM, and word embedding. The most important conclusion from the analysis is that noise-free context topic extraction is still under investigation. The conducted research made it possible to determine the low level of application of digital competencies in job requirements. This indicates the insufficient development of digitalization, which is directly related to the economic situation in the country, and there is a limitation of resources.*

Keywords: *system analysis, intelligent data analysis, digital competence, digital technologies, problem solving, digitalization, digital transformations, efficiency.*

Актуальність теми дослідження. Цифрові навички сьогодні вже не є спеціальними знаннями, якими володіють лише спеціалісти з ІКТ. Це основна компетентність сучасної людини, обов'язкові навички, без яких з кожним роком стає все важче соціалізуватися, адаптуватися, навчатися чи просуватися по кар'єрних сходах.

Дедалі частіше з'являються дослідження, в яких вчені стверджують, що в найближчому майбутньому майже кожна професія буде у різний спосіб пов'язана з цифровими навичками через швидкі зміни в технологіях.

Отже, системний аналіз впливу цифрових компетенцій на ринок праці України вбачається актуальним науковим завданням.

Постановка проблеми. Інтелектуальний аналіз даних є однією з ефективних галузей створення інноваційних даних, призначених для виявлення прихованої та цінної інформації з даних. Досягнення наукової інформаційної експертизи знаходять своє застосування в різних сферах людської діяльності, однією з таких сфер є ринок праці.

Україна, як і більшість країн світової економіки, стикається з різними суттєвими змінами: прогресивні технології, старіння населення та інші, що впливає на попит і пропозицію компетенцій. Труднощі полягають у розвитку ефективності компетенцій та їх невідповідності, недостатні інвестиції та недолік ключових компетенцій. Проблемні ситуації, такі як коронавірус і військові за-

грози, впливають на потреби в здібностях, а також на пропозиції роботи. Навички змішуються та закріплюються у нові комбінації. Вимоги до компетентності змінюються настільки швидко, що більшість наборів обов'язків не відповідають сьогоденню, не кажучи вже про шукачів роботи, постачальників освітніх послуг та роботодавців.

Як зазначено Всесвітнім економічним форумом (WEF, 2019), стає більш очевидним, що ринок праці повинен створити навички як спільну валюту, підтримувати співпрацю між роботодавцями та освітянами. Слід розглянути загальний метод оновлення і консолідації таксономії компетенцій, групування навичок та їх визначення. Такий підхід має потенціал для створення фундаменту для більш ефективного ринку для підвищення кваліфікації та перекваліфікації [2].

Ідея цього аналізу полягає в тому, щоб зібрати дані з Державного центру зайнятості (https://www.dcz.gov.ua/) зі списками вакансій, щоб витягти навички / очікування, які часто потрібні для виконання різноманітних робіт.

Аналіз останніх досліджень і публікацій. Питання інформаційно-комунікаційної або цифрової компетентності, що дозволяють опрацьовувати інформацію, забезпечивши перехід від кваліфікаційної моделі до повноцінних компетентнісних моделей, які супроводжують людей упродовж їх особистісного розвитку і професійної кар'єри, знаходиться в полі зору як теоретиків, так і практиків. Цій проблемі приділяють значну увагу як українські (Л. Боярчук [3], М. Махсма [4]), так і зарубіжні (Л. Бревер [5], Дж. Джеймс [6]) дослідники. Але незважаючи на цінність проведених досліджень, питання цифрових компетенцій в Україні залишаються невирішеними та потребують подальшого дослідження.

Постановка завдання. Мета статті полягає в інтелектуальному аналізі сучасного стану використання цифрових навичок на ринку праці України.

Виклад основного матеріалу. Згідно з Рамками цифрової компетентності для громадян України цифрова компетентність є ключовою в умовах Четвертої промислової революції. Цей термін містить впевнене, критичне, творче та відповідальне використання і взаємодію з засобами цифрових технологій для навчання, працевлаштування, роботи, дозвілля та участі у суспільному житті. Він охоплює такі поняття, як інформаційна грамотність та медіаграмотність, комунікація та співпраця, створення цифрового контенту (включаючи основи програмування), безпека (а та-

кож захист персональних даних у цифровому середовищі та кібербезпеку), а також розв'язання різнопланових проблем з використанням цифрових технологій навчання впродовж життя. Детальний опис та рівні володіння наведено в Рамці цифрової компетентності для громадян України (Опис рамки цифрової компетентності для громадян України, 2021) [7].

Після успішного збирання та форматування даних із Державного центру зайнятості (https://www.dcz.gov.ua/) дані містили чіткий ідентифікатор, назву вакансії, регіон, опис роботи, дату оголошення, рівень оплати праці та назву компанії. Дані про вакансії включають період з 2020-01-04 по 2022-12-09 та налічує 800 353 вакансії з 4920 спеціалізацій (табл. 1).

Таблиця 1

ФРАГМЕНТ ФРЕЙМУ ОТРИМАНИХ ДАНИХ

	id	name	region	description	pubdate	salary	company
60380	1044882174	склеювач	Житомирська область, Коростень	заробітна плата усього грн опис ...	2020-06-17	5000	652, КОРОСТЕНСЬКИЙ МЦЗ
194062	1058985347	бармен	Чернівецька область, Чернівці	заробітна плата усього грн у тому чис...	2021-11-03	8000	2412, Чернівецький МЦЗ (Чернівецький регіон)
278517	1062273224	продавець продовольчих товарів	Луганська область, Біловодський район, Біловодськ	заробітна плата усього грн у тому чис...	2021-06-05	6000	1215, Біловодський районний центр зайнятості
45393	1039715974	бібліотекар	Чернівецька область, Чернівці	заробітна плата усього грн у тому чис...	2020-02-19	5500	2412, Чернівецький МЦЗ (Чернівецький регіон)
299075	1051226405	оператор котельні	Миколаївська область, Доманівський район, Цвіт...	заробітна плата усього грн у тому чис...	2020-12-10	5000	1463, ДОМАНІВСЬКА РАЙОННА ФІЛІЯ МИКОЛАЇВСЬКОГО...

Після того як були зібрані дані, ми відформатували більшість стовпців у керований спосіб. Більшість роботи, яку потрібно буде виконати, — це вилучення характеристик із опису вакансій. Як початковий крок виконано всі звичайні етапи попередньої обробки, необхідні для обробки природної мови. Це і використання регулярних виразів для видалення непотрібних символів, і видалення типових та нерелевантних стоп-слів, і маркування кожного окремого опису. Розбір тексту на слова, а також приведення їх до початкової форми виконано за допомогою бібліотеки Pymorphy2 [8].

Процес, який тут застосовувався, полягав у розбитті на фрагменти — це спосіб вилучення певних фраз із документа. Спочатку планувалось використовувати спеціальний NER (Name Entity Recognition), щоб отримати навички з опису посади. Дослідивши способи впровадження цього рішення, ми вирішали використовувати класифікацію на основі фрагментації, а не NER через кількість необхідних навчальних даних. Створення навчального та тестового наборів для NER зайняло б набагато більше часу.

Серед тих слів, які потрібно розібрати, давайте подивимося на найчастіші слова, які використовуються в описах вакансій (рис. 1).

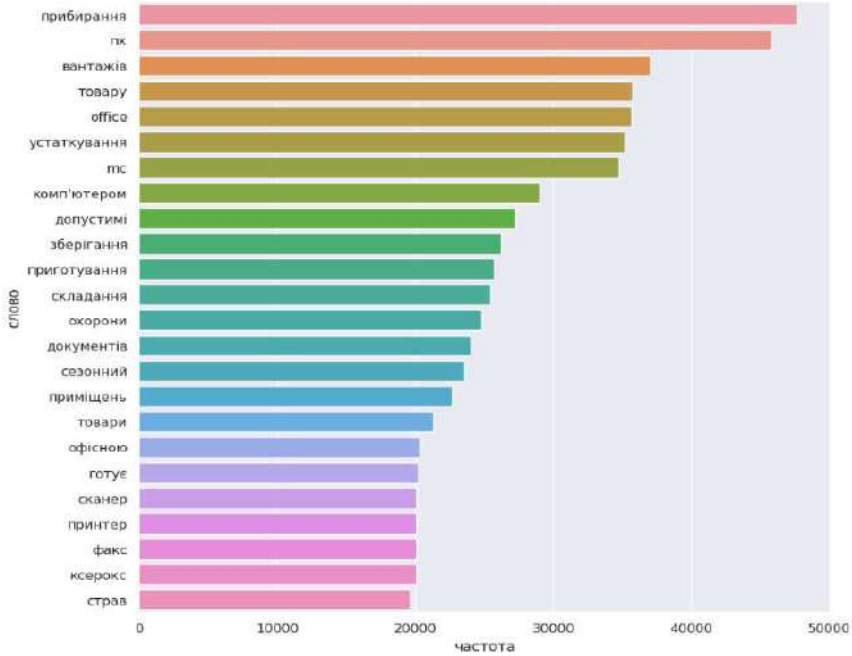


Рис. 1. Візуалізація найчастіших слів

Джерело: розроблено авторами.

Зрозуміло, що ці головні слова навряд чи є навичками. Можна очікувати, що слово «пк» буде часто зустрічатися, але навіть це слово з'являється в корпусі лише 45787 раз. Можливо, біграма (рис. 2) чи триграма (рис. 3) почнуть розкривати навички в описі вакансії? Що ж, ми бачимо деякі кращі результати, і деякі навички починають з'являтися в найчастіших даних *n*-грамів, але має бути більш ефективний спосіб ідентифікації цих навичок в описі посади.

Ми використати нейронні мережі для нашого другого підходу та спробували модель word2vec [9], щоб отримати необхідні вектори навичок. Ми навчили модель за допомогою набору токенів із вилученого опису вакансії та запустили вимірювання подібності. Наведений нижче фрагмент коду показує найбільш схожі слова у домені цифрових навичок (рис. 4). Word2vec також корисний для конкретних цифрових навичок.

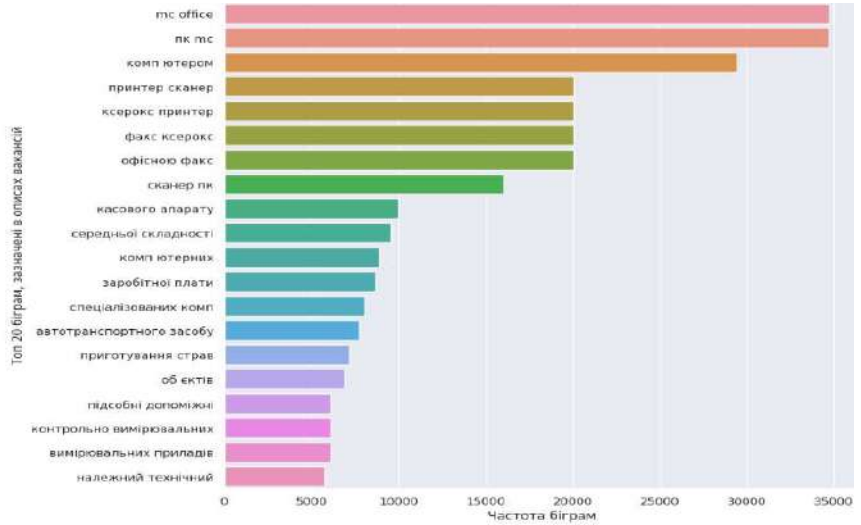


Рис. 2. Візуалізація найчастіших біграм

Джерело: розроблено авторами.

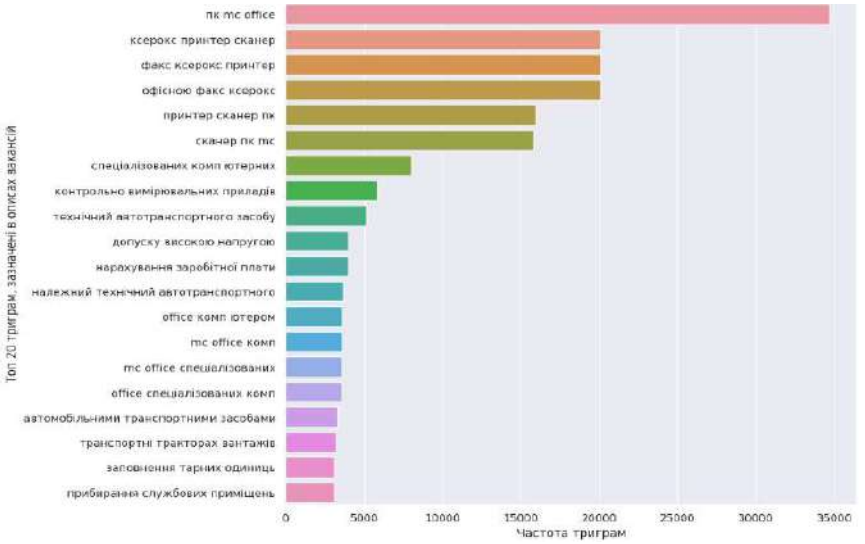


Рис. 3. Візуалізація найчастіших триграм

Джерело: розроблено авторами.

```
# digital specific skills
model.wv.most_similar(['office', 'word', 'excel', 'сканер', 'принтер', 'програмування', 'розробка',
          'програма', 'комунікація', 'співпраця'],topn=25)
```

```
[('sql', 0.6188371777534485),
 ('exel', 0.6100712418556213),
 ('server', 0.5948401689529419),
 ('windows', 0.5821477174758911),
 ('adobe', 0.581726610660553),
 ('photoshop', 0.5815576314926147),
 ('html', 0.5787284970283508),
 ('css', 0.5703566074371338),
 ('corel', 0.5607632994651794),
 ('програми', 0.5599780082702637),
 ('draw', 0.555258572101593),
 ('erp', 0.5471287369728088),
 ('point', 0.5455071926116943),
 ('linux', 0.5435844659805298),
 ('web', 0.5325785875320435),
 ('illustrator', 0.5323614478111267),
 ('mysql', 0.530738234519958 5),
 ('програміст', 0.5307325720787048),
 ('autocad', 0.5301836729049683),
 ('excel', 0.527507722377771),
 ('medoc', 0.5256964564323425),
 ('адміністрування', 0.5248759984970093),
 ('клієнт-банк', 0.519995391368866),
 ('internet', 0.5174419283866882),
 ('google', 0.517166197299957 3)]
```

Рис. 4. Візуалізація найбільш схожих слів у домені цифрових навичок

Джерело: розроблено авторами.

Ґрунтуючись на нашому аналізі, ми визначили різні набори навичок, яким надають топ 25 назв вакансій із 1544, в яких використовуються цифрові компетенції (табл. 2). З усього проаналізованого корпусу кількість назв вакансій становить 31,38 % із цифровими компетенціями.

Таблиця 2

ТОП-25 НАЗВ ВАКАНСІЙ З ЦИФРОВИМИ КОМПЕТЕНЦІЯМИ

№ з/п	Назва вакансії	Частота у корпусі
1	бухгалтер	6257
2	спеціаліст державної служби (місцевого самоврядування)	2609
3	головний бухгалтер	1513
4	фахівець	1459
5	менеджер (управитель) із збуту	1268
6	економіст	1103
7	комірник	764
8	продавець-консультант	708
9	адміністратор	693
10	інженер	687

Закінчення табл. 2

№ з/п	Назва вакансії	Частота у корпусі
11	вчитель закладу загальної середньої освіти	686
12	менеджер (управитель)	611
13	начальник відділу	599
14	оператор комп'ютерного набору	556
15	діловод	547
16	юрисконсульт	509
17	інженер-конструктор	496
18	секретар	487
19	інженер з охорони праці	471
20	оператор поштового зв'язку	463
21	продавець непродовольчих товарів	462
22	інспектор з кадрів	412
23	інженер-програміст	407
24	фахівець з публічних закупівель	398
25	начальник відділу поштового зв'язку	385

Висновок. У нашому інтелектуальному аналізі даних використовувалися подвійні алгоритми. В обох є застереження. Подібність word2vec базується на описі, який ми навчили, тому пошук навичок для кожної ролі не вдається, якщо в описі не згадується роль. Словниковий запас залежить від корпусу, тому рольовий пошук не був успішним із моделлю word2vec.

Зіставлення тегів на основі правил відповідає всім необхідним навичкам, але також виділяє інші іменники та власні іменники. Було багато шуму, і для видобування потрібен був інший словник для отримання необхідних іменників (навичок). Цю проблему цікаво вирішити за допомогою інших моделей NLP, таких як тематичне моделювання, LSTM і вбудовування слів. Найважливіший висновок із цього аналізу полягає в тому, що вилучення контекстних тем, без шуму, досі досліджується.

Проведене дослідження дозволило визначити низький рівень застосування цифрових компетенцій у посадових вимогах. Це свідчить про недостатній розвиток цифровізації, що безпосередньо пов'язано з економічною ситуацією в країні, має місце обмеженість ресурсів.

Подальші наукові дослідження доцільні в напрямах: розроблення методик з питань застосування цифрових компетентностей; підвищення ефективності роботи служби зайнятості через її цифрову трансформацію.

Бібліографічні посилання

1. Toby Segaran. Programming Collective Intelligence: Building Smart Web 2.0 Applications. O'Reilly Media, Inc, 2007. 308 c.
2. World Economic Forum. (2019). Strategies for the new economy: Skills as the currency of the labour market. URL: https://www.weforum.org/whitepapers/strategies-for-the-new-economy-skills-as-the-currency-of-the-labour-market
3. Боярчук Л.В. Застосування зарубіжного досвіду в роботі Державної служби зайнятості України. *Науковий вісник Полісся*. № 20151(1). С. 65—70.
4. Махсма М. Світові тенденції трансформації зайнятості населення в умовах глобалізації економіки. *Україна: аспекти праці*. 2007. № 4. С. 10—15.
5. Brewer L. Enhancing youth employability: What? Why? and How? Guide to core work skills. URL: https://www.ilo.org/wcmsp5/-groups/public/@ed emp/@ifp skills-/documents/publication/wcms_213452.pdf
6. James J. Heckman Hard Evidence on Soft Skills. *National Bureau of Economic Research*. 2012. June. URL: http://www.nber.org/papers/w18121
7. Опис Рамки цифрових компетентностей для громадян України. Міністерство цифрової трансформації України. 2021. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf
8. PyMorphy2. URL: https://pymorphy2.readthedocs.io/en/stable/
9. URL: https://code.google.com/archive/p/word2vec/

Статтю подано до редакції 26.11.2022

УДК:378.147 DOI 10.33111/mise.102.7

Дем'яненко В.В., к.е.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Дем'яненко О.О., к.фіз.-мат.н., доцент
кафедри математичного аналізу та теорії ймовірностей,
НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського»

Репета Л.А., к.фіз.-мат.н., доцент
кафедри математичного аналізу та теорії ймовірностей,
НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського»

Demianenko V.V. Candidate of Economik Science Associate professor of the department of Computer Mathematics and Informational Security,
KNEU named after V. Hetman

Olga O. Demianenko PhD (physical and mathematical sciences),
Associated professor of Mathematical analysis and Probability Theory Department National Technical University of Ukraine «Igor Sicorsky Kiev Politechnic Institute», Kyiv

Lesia A. Repeta PhD (physical and mathematical sciences),
Associated professor of Mathematical analysis and Probability Theory Department National Technical University of Ukraine «Igor Sicorsky Kiev Politechnic Institute», Kyiv

ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПРОЦЕСІ ВИКЛАДАННЯ МАТЕМАТИЧНИХ ДИСЦИПЛІН У ТЕХНІЧНИХ ТА ЕКОНОМІЧНИХ ЗАКЛАДАХ ВИЩОЇ ОСВІТИ

APPLICATION OF MODERN INFORMATION TECHNOLOGY IN THE TEACHING PROCESS OF MATHEMATICAL DISCIPLINES IN TECHNICAL AND ECONOMIC HIGHER EDUCATIONAL INSTITUTIONS

Анотація. *Бурхливий розвиток новітніх інформаційних та комп'ютерних технологій, які стосуються абсолютно всіх сфер діяльності людей. Їх застосування впливають на економіку країни, політику, освіту, культуру, зачіпають сфери професійної діяльності, кардинально змінюють наш побут та ін. Розвиток цих технологій стосується різних верств населення та усіх вікових категорій. Сфера освіти, яка, по-перше, пов'язана з молодим поколінням, що радо тягнеться до всього нового; по-друге, щільно пов'язана з розвитком науки і наукових досліджень, реагує на виклики, що створені розвитком новітніх технологій і, відповідно, змінюється. Пандемія covid-19 і широкомасштабний наступ у*

російсько-українській війні у 2022 р. пришвидшили процеси впровадження інноваційних комп'ютерних технологій у навчальний процес у формі дистанційного навчання. Мета статті полягає у дослідженні особливостей навчального процесу в екстремальних умовах карантину та воєнного стану, в аналізі різних форм навчання, які були запропоновані та запроваджені, в узагальненні того практичного досвіду викладання математичних дисциплін у технічному та економічному університетах, який було набуто в цей унікальний період. У роботі проведено аналіз стану освітнього процесу та динаміку його змін у законодавчій сфері. Обґрунтована необхідність розбудови дистанційної форми навчання в навчальному процесі. Розглянуто особливості проведення лекцій, практичних і семінарських занять та контролю рівня знань студентів при дистанційній формі навчання. Визначено особливості проведення занять у синхронному та асинхронному режимі. Стаття має науково-методичний характер.

Ключові слова: *дистанційна форма, інформаційно-комунікаційні технології, асинхронна форма навчання, покрокові тести, короткочасні тести, навчальний процес, засоби контролю знань.*

Abstract. *The rapid development of the latest information and computer technologies, which affect absolutely all spheres of human activity. Their application affects the country's economy, politics, education, culture, affects areas of professional activity, radically changes our everyday life, etc. The development of these technologies concerns different segments of the population and all age categories. The field of education, which, firstly, is connected with the young generation, which gladly reaches for everything new; secondly, it is closely related to the development of science and scientific research, responds to the challenges created by the development of the latest technologies and, accordingly, changes. The global pandemic of COVID-19 and the Russian-Ukrainian war of 2022 accelerated the processes of introducing innovative computer technologies into the educational process in the form of distance learning. The purpose of the article is to study the peculiarities of the educational process in the extreme conditions of quarantine and war, to analyze the various forms of education that were proposed and implemented, to summarize the practical experience of teaching mathematical disciplines in technical and economic universities, which was acquired during this unique period. The paper analyzes the state of the educational process and the dynamics of its changes in the legislative sphere. There is a well-founded need to develop a distance form of education in the educational process. Peculiarities of conducting lectures, practical and seminar classes and controlling the level of students` knowledge in the distance form of education are considered. The peculiarities of conducting classes in asynchronous mode are determined. The article has a scientific and methodological character.*

Key words: *distance learning, information and communication technologies, asynchronous learning, step-by-step tests, shot-term tests, educational process, knowledge control tools.*

Вступ. Ми живемо у час бурхливого розвитку новітніх інформаційних та комп'ютерних технологій, які стосуються абсолютно всіх сфер діяльності людей. Їх застосування впливають на економіку країни, політику, освіту, культуру, зачіпають сфери професійної діяльності, кардинально змінюють наш побут та ін. Розвиток цих технологій стосується різних верств населення та усіх вікових категорій. Зрозуміло, що сфера освіти, яка, по-перше

пов'язана з молодим поколінням, що радо тягнеться до всього нового; по-друге, щільно пов'язана з розвитком науки і наукових досліджень, реагує на виклики, що створенні розвитком новітніх технологій і, відповідно, змінюється. Пандемія covid-19 і широкомасштабний наступ у російсько-українській війні з боку рф у 2022 р. пришвидшили процеси впровадження інноваційних комп'ютерних технологій в навчальний процес у формі дистанційного навчання. Зазначимо, що до початку пандемії covid-19 дистанційна форма навчання розглядалась як додаткова можливість здобути професійні знання поряд з заочною та другою освітами і викликала певну недовіру та упереджене ставлення суспільства до одержаних у такий спосіб знань. Однозначного підходу до реалізації дистанційного навчання не було і наразі також ще нема. Але, якщо до початку пандемії covid-19 і широкомасштабного наступу рф у 2022 р. дистанційна форма була однією серед інших форм навчання, то після згаданих подій це стало чи не єдиним можливим способом продовжити навчання у ЗВО і школах. Тому досвід, що був набутий в таких екстремальних умовах, на думку авторів, є корисним і може бути застосованим надалі.

Постановка проблеми. Незавершеність реформи вищої освіти створила цілу низку проблем, з якими викладачі та студенти ЗВО змушені боротись самотужки. Перехід до різнорівневих програм в середній школі і демократичність здобуття вищої освіти, коли, фактично, кожен бажаючий має доступ до неї, створює розрив у знаннях і навичках вступників на одні й ті самі спеціальності. Першокурсники опиняються в різних стартових умовах. Уніфікація освітніх програм вищої школи призвела до скорочення годин вивчення базових курсів з математичних дисциплін, фізики, інформатики тощо і ускладнює для студентського загалу подолання цього недоліку. Вирівняти стартові умови може лише значна вмотивованість студентів до самостійної роботи, наявність необхідних матеріалів для праці і їх доступність незалежно від місцезнаходження і часу доступу. Зазначимо, що, не зважаючи на різноманіття освітніх закладів, їх форм та спеціалізацій за фахом, проблеми професійного навчання є спільними і притаманні вищий освіті України загалом. Пандемія covid-19 загострила цю ситуацію і стала справжнім викликом для всієї освітянської спільноти. У зв'язку з введенням в Україні карантину навесні 2020 р. більшість ЗВО змушені були перейти до дистанційної форми навчання з подальшим застосуванням інформаційно-комунікаційних технологій. Сталось це неочікувано, ніяких централізовано розроблених інструкцій

чи вказівок на початку дистанційного навчання не існувало. Ситуація склалась унікальна: і за рівнем складності, і за широким спектром можливостей в сенсі її вирішення. Ця проблема виявилась спільною як для студентів, так і для викладачів. Кожен лектор чи викладач практичних занять опинилися перед необхідністю створення і розповсюдження матеріалів відповідних курсів, до яких студенти мали б доступ. Практичні заняття вимагали створення умов для спілкування, виконання завдань, перевірки засвоєння поточного матеріалу.

Аналіз останніх досліджень та публікацій. Необхідність змін в освіті, інформатизації та комп'ютеризації освітнього процесу, створення електронної освіти, широке застосування інтернет-технологій у нашій державі регулюється положеннями Закону України «Про Національну програму інформатизації», прийнятому у 1998 р. На сьогодні система освіти України перебуває у стані реформування. Початкова та середня школи активно та системно реформуються на державному рівні. Структура післяшкільної освіти також зазнала змін: зникли профтехучилища та технікуми. На зміну їм прийшли коледжі. Вища освіта також змінюється. Закон України «Про вищу освіту» надав закладам вищої освіти можливість самостійно і незалежно приймати рішення з організації освітнього процесу, наукових досліджень, розвитку академічних свобод і академічної мобільності [1, 2]. Початок відчутних структурних змін у вищій школі України поклав Болонський процес (Згуровський & Якименко, 2006) та обов'язкове складання ЗНО для вступу у заклад вищої освіти. Проте фактична реформа вищої школи ще не завершена. Модернізація освіти, викликана бурхливими змінами в інформаційних технологіях, зробила актуальною розвиток дистанційного навчання, його популярність і необхідність. Застосування такої форми є дуже важливим при здобутті професійних знань, одержанні другої освіти, підвищенні кваліфікації. Також дистанційна форма навчання створює рівні можливості як для працездатних здобувачів, так і для здобувачів вищої освіти з обмеженими можливостями.

Пандемія covid-19 і подальша активна фаза бойових дій у російсько-українській війні показали, що дистанційне навчання із застосуванням сучасних інформаційних технологій стало чи не єдиним можливим способом продовжувати навчальний процес. Зауважимо, що ще у 2002 р. МОН України започаткувало експеримент з дистанційної освіти, до якого було залучено низку провідних університетів країни. В аналітичній записці «Світовий до-

свід розвитку дистанційних форм освіти у вітчизняному контексті» Національний інститут стратегічних досліджень окреслив здобутки і досягнення дистанційної освіти в розвинених країнах, широкі можливості використання таких форм і перспективи їх розвитку. На основі цього аналізу було підготовлено низку пропозицій для МОН України. Зокрема, було запропоновано створити разом із провідними ЗВО потужний проєкт дистанційного онлайн-навчання, адаптованого до умов нашої держави. У 2012 р. була розроблена стратегія розвитку освіти всієї країни на найближчі роки до 2021 р. [3]. У 2013 р. МОН України видало Наказ «Про затвердження Положення про дистанційне навчання» [4]. У цьому документі сформовано основні засади організації, мету і завдання дистанційного навчання. Підкреслено необхідність створення інформаційно-комунікаційних ресурсів і технологій для його забезпечення. Законодавче підґрунтя для розвитку дистанційного навчання із застосуванням інноваційних інформаційно-комунікаційних ресурсів і технологій було створено. Це дало потужний поштовх для досліджень у цьому напряму. Низка публікацій була присвячена аналізу проблеми дистанційної освіти загалом [8].

Специфіка такого навчання вимагає і специфічних підходів до контролю одержаних знань і їх оцінки. Широкого розповсюдження отримали різні види тестувань, як один із засобів контролю знань здобувачів освіти. Науковці почали публікувати матеріали пов’язані безпосередньо зі складанням тестів і аналізом якості цих тестів [5, 6]. Крім того, проблема дистанційного навчання досліджувалась всесторонньо, зокрема і з позицій її сприйняття як викладачами, так і студентами [7].

Мета статті полягає в дослідженні особливостей навчального процесу в екстремальних умовах карантину та війни, в аналізі різних форм навчання, які були запропоновані та запроваджені, в узагальненні того практичного досвіду викладання математичних дисциплін в технічному та економічному університетах, який було набуто в цей унікальний період.

Основний матеріал досліджень. Процес навчання у ЗВО є неперервним ланцюгом, що починається з курсу лекцій і закінчується підсумковим контролем рівня знань студентів у вигляді екзамену чи заліку. Традиційна лекція для студентів в аудиторії в умовах карантину та воєнного стану стала неможливою. На зміну їй прийшли електронні конспекти, відеолекції на YouTube-каналах чи в Гугл-класах, лекції в Zoom-конференціях та ін. Різноманітність підходів до викладання лекційного матеріалу вра-

жає. Кожний із перерахованих варіантів має як недоліки, так і переваги. Виділяти як найкращий якийсь один спосіб передачі теоретичного матеріалу студентам, мабуть, зарано і недоцільно: дуже малий досвід, і результат загалом оцінюється знаннями, що набули студенти. Об'єктивна оцінка набутих знань буде можлива лише після закінчення дистанційного навчання. Поки що кожен викладач покладається на ті можливості, що надає ВНЗ, свої уподобання, рівень обізнаності в комп'ютерних технологіях та власні технічні можливості.

Зауважимо, що завдяки дистанційній формі роботи більшість викладачів суттєво підняли свій рівень інтернет-користувачів, значно просунулись у застосуванні сучасних програмних комп'ютерних розробок і використанні різноманітних можливостей, які вони надають.

На думку авторів, найбільш ефективною є комбінована форма подачі лекційного матеріалу, що включає як безпосереднє спілкування зі студентами, так і надання матеріалів для самостійного опанування певних тем в електронному вигляді. Таке спілкування може відбуватися у вигляді консультації після перегляду чи вивчення матеріалу студентами або читання лекції в режимі реального часу в Zoom-конференції чи на інших платформах із можливістю регулювати темп лекції та відповідати на питання студентів.

Важливим фактором ефективності проведення такої лекції стає вмотивованість до навчання студентів. Робота над лекційним матеріалом в дистанційному режимі – важка праця. Без живого інтересу до предмета вивчення або без глибокого усвідомлення необхідності вивчення матеріалу, позитивний результат практично не можливий. Особливо важко це дається першокурсникам. Мало хто з них вміє самостійно опрацьовувати теоретичний матеріал. Відповідно, задача викладача не тільки передати у якийсь спосіб лекційний матеріал студентам, а й підказати як саме його опрацювати та вивчити. Зрозуміло, що є якась частина студентів, які не дивляться відеолекції, або присутні на лекції лише формально. Засобів впливу на таких студентів лектор практично не існує. Частина з них змінить ставлення до навчання з плином часу, а частина змушена буде покинути навчання у ЗВО. Беззаперечно, ця проблема була й до дистанційної форми навчання, але саме в цій формі вона надзвичайно загострилась.

Суттєвої трансформації зазнали також засоби контролю знань. Подібно до традиційних контрольних та самостійних робіт, які пишуть в аудиторії, в режимі дистанційного навчання такі роботи

виконуються також. Їх пропонують писати студентам в режимі відеоконференції або поза конференцією протягом строго обмеженого часу. Після написання студенти надсилають роботи викладачу на пошту або в групу, що створена в соцмережах. У будь-якому разі перевірка таких робіт забирає у викладача багато часу та зусиль, що зумовлено деякими об'єктивними причинами, так і якістю форми надісланих робіт, форматів файлів, можливості їх прочитання тощо.

Кардинальне полегшення в сенсі перевірки знань дають тести. У першу чергу оцінили це викладачі. Запроваджувати тестування як вид перевірки рівня засвоєння матеріалу студентами почали вже давно. Але в період дистанційного навчання проведення тестів отримало широке розповсюдження. Студенти також позитивно реагують на подібний різновид роботи. Тестова форма перевірки і контролю знань для них є відомою та звичною, бо всі здавали ЗНО. Комп'ютерні технології, що застосовуються під час тестування легко і з зацікавленням сприймається молодим поколінням. Можливість пройти тести в діапазоні широкого часового вікна також подобається і підтримує демократичний стиль в процесі навчання. Після початку війни такий спосіб проведення тестів став особливо актуальним та отримав широке застосування. Отже, переваги тестів очевидні.

Проте є й недоліки. Крім вмотивованості студенів постає проблема самостійності виконання тестових завдань. Актуальною, і чи не головною, лишається проблема академічної доброчесності. Тут перед студентами постає дилема – висока оцінка будь-якою ціною чи об'єктивний результат навчання. Хибне уявлення про «допомогу другу» спонукає когось виконувати завдання за іншого, а когось звертатись за такою допомогою. Часто зусилля, які витрачаються на те, щоб обійти правила проходження тесту більші, ніж ті, які потрібні для вивчення матеріалу. Але студенти не завжди усвідомлюють це. На жаль, заручниками такої ситуації стають доброчесні студенти. Вони опиняються в невигідному становищі. Для усунення таких недоліків і підтвердження об'єктивності оцінки знань студентів викладачам доводиться проводити додаткові заходи: захисти, додаткові опитування, тощо. Проблема слабкого усвідомлення того, що ставлення до навчання має бути відповідальним та доброчесним, насправді є наслідком багатьох загальносуспільних проблем. Доводиться сподіватися, що корекція поведінки студентської молоді в процесі навчання позитивно вплине на формування їх світогляду та продовжить створення демократичних традицій в суспільстві.

Матеріал та методи. Методи реалізації кожного окремого ланцюжка освітнього процесу в режимі дистанційного навчання заслуговують свого дослідження. Лекційний матеріал, як вже було зазначено вище, подається різноманітними способами. Викладач, спираючись на навчальну програму, керується при цьому власним досвідом, особистими уподобаннями, технічними можливостями та рівнем обізнаності в комп'ютерних технологіях.

Крім формування власних лекцій, у нього є можливість посилатись на відеоматеріали колег, викладені в YouTube, або розміщені на відповідних платформах кафедрального чи загально університетського рівня. Стосовно лекцій можна сформулювати тільки якісь загальні методи та підходи. Докладне дослідження повинне враховувати спрямованість ЗВО, особливості дисципліни та спеціальності для якої призначено курс. Так курс математичного аналізу, який читають математикам та економістам, повинен мати суттєві відмінності. Крім того, особливу увагу необхідно приділити таким важливим елементам лекційного курсу, як перша та остання лекції, лекції, що підсумовують окремі змістовні модулі курсу. Зокрема під час проведення першої лекції слід визначити мету, предмет, основні завдання курсу, вказати міждисциплінарні зв'язки, перелік компетенцій. Для стимулювання зацікавленості слухачів корисно подати історичну картину передумов виникнення та розвитку дисципліни. Наводячи зв'язки між теорією та практикою, можна висвітлити перспективи використання знань, умінь та певного досвіду після засвоєння навчальної дисципліни в практичній площині та подальшій роботі.

Практичні заняття в режимі дистанційного навчання також набули різних форм. Дехто з викладачів проводить заняття в режимі реального часу біля дошки часто придбаної власним коштом, іноді під запис. Така форма максимально наближена до традиційного заняття в аудиторії, але, нажаль, доступна не всім. Інші проводять пари в режимі конференцій із використанням інтерактивних дошок або можливостей хмарного середовища Zoom чи сервісів Google. Хтось готує презентації з максимально великою кількістю розібраних прикладів. Дуже корисними є невеличкі відеоролик'язань окремих стандартних задач. Загалом наголосимо, що записані викладачами відеолекції, практичні заняття із застосуванням різноманітних відео та анімацій, які допомагають студентам розібратися в новому матеріалі, зрозуміти розв'язання типових задач, набути та закріпити нові навички в нинішніх умовах виявились дуже корисними.

Чи не найпроблемнішим етапом освітнього процесу в режимі дистанційного навчання виявилась перевірка рівня знань студентів. Як вже було зазначено вище, широкого розповсюдження набуло тестування студентів.

Ефективним способом перевірки знань стали широкі покрокові тести, які дозволяють пропонувати комплексні задачі і перевіряти набуті знання та вміння, іноді, по цілих розділах вивченого матеріалу. Такі тести дозволяють виставити диференційовану оцінку та максимально об'єктивно оцінити роботу студента. Але не будь-яку задачу слушно перевіряти покроковим тестом. Так, наприклад, по курсу «Математична логіка та теорія алгоритмів» побудова алгоритму розв'язку задачі у відповідних алгоритмічних системах (машина Тюрінга, машина Поста, нормальні алгорифми Маркова тощо) не є однозначною. Аналогічна проблема виникає під час програмування тесту на пошук екстремумів функцій багатьох змінних у курсі математичного аналізу. Один із варіантів тесту саме на цю задачу наводимо нижче (рис. 1).

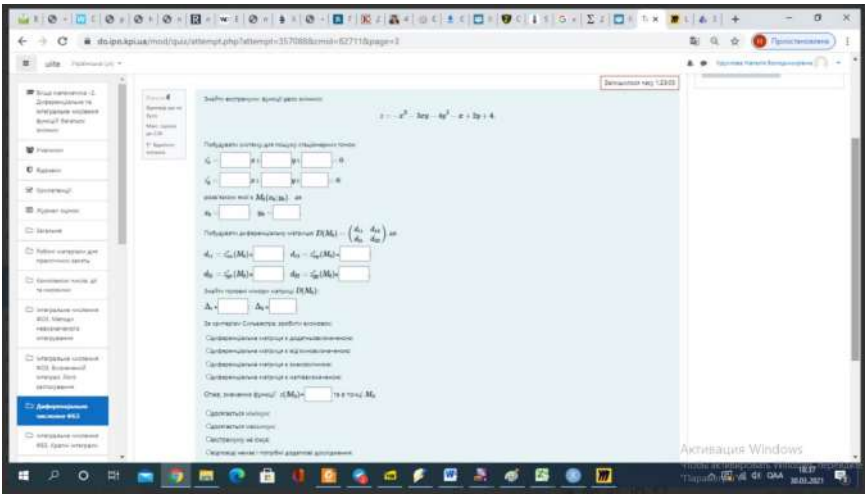


Рис. 1. Варіант тесту на знаходження екстремумів функцій багатьох змінних у курсі математичного аналізу

Пропонуючи покроковий тест, викладач змушує студента розв'язувати задачу вказаним способом і тим самим обмежує його можливість творчо підійти до дослідження. На платформі Moodle, яка використовується для розміщення дистанційних кур-

сів і в НТУУ «КПІ ім. Ігоря Сікорського», і в КНЕУ, є можливість прикріпити власний розв'язок тестової задачі у вигляді малюнка, але це додає роботи викладачу. Відповідно під час перевірки таких задач краще використати інші підходи.

Широкого застосування набули так званні *швидкі короткочасні тести*, які спрямовані на перевірку поточних теоретичних знань і набутих навичок у розв'язанні стандартних задач. Вони складаються з невеликої кількісті задач, від 3 до 5 і на їх написання відводиться час від 15 до 30 хв. Проводити їх можна часто, практично по кожній темі. Короткочасні тести не перевіряють хід розв'язання задачі, хоча допускають можливість перевірки деяких проміжних кроків. Основною перевагою короткочасних тестів порівняно з довгими покроковими є те, що, по-перше, задача сформульована без підказок про хід розв'язання; по-друге, студент може сам обрати спосіб розв'язку. Є і негативна сторона тестування. Існує велика кількість програмних засобів, таких як MATLAB, Wolfram Mathematica, online калькулятори, які дозволяють розв'язувати стандартні задачі з курсу вищої математики і студенти ними широко користуються.

Отже, у ході створення тестів ці особливості бажано враховувати. Щоб унеможливити або хоча б мінімізувати використання додаткових інформаційних ресурсів, можна чітко вивіряти час, що виділяється на проходження тесту. Він має бути достатнім для самостійного розв'язання задач середньостатистичним студентом і замалим для того, щоб використати програмні продукти.

Крім того, питання в задачі потрібно формулювати так, щоб змусити студента виконувати завдання самостійно. Наприклад, в тесті за темою «Множини» з курсу математичного аналізу, якщо запропоновано виконати якісь дії над множинами, то у відповіді можна попросити записати не саму результуючу множину, а кількість елементів з неї, які відповідають вказаним в задачі умовам. На якомусь етапі розв'язання, безумовно, можна застосовувати додаткові інтернет-ресурси, але на це потрібний час і достатній рівень кваліфікації у програмуванні та бути впевненим користувачем спеціальних програм.

Ще одна перевага цих тестів полягає у простоті форми запису відповіді, тобто питання має бути сформульовано так, щоб не було потреби писати додаткові вказівки до заповнення відповіді. Найкраще, коли відповідь можна задати натуральним числом, що легко вбивається з клавіатури комп'ютера, планшета чи телефона. На жаль, момент зручної відповіді не завжди вдається зберег-

ти. Дробові відповіді можуть бути записані у різних варіантах. У таких ситуаціях необхідно виписувати додаткові вимоги до заповнення відповіді. Але, якщо тести проводяться регулярно і складають серію, то в такій серії тестів дотримуватись одного правила не складно. Короткочасні тести, як і широкі покрокові також зручно програмуються в Moodle. Але це накладає додаткові вимоги на запис відповіді — вона має бути записана так, як запрограмована. Щоб не перевантажувати умову задачі правилами запису відповіді, можна вимагати внести у відповідь якусь її частинку, наприклад, якийсь коефіцієнт. Приміром, коли вимагається записати рівняння прямих та площин в тесті «Пряма на площині. Пряма і площина у просторі» з курсу аналітичної геометрії необхідно врегулювати питання кратності коефіцієнтів та їх знаки. Розробники можуть вказати один з коефіцієнтів, що зафіксує конкретний запис відповіді. З одного боку, це є підказка, з другого — своєрідна маленька математична задача на розуміння студентом того, що правильні рівняння прямих та площин можна задавати у різних варіантах.

Наведені прийоми стосуються тестів із вбудованими відповідями. Наводимо приклад такого тесту (рис. 2).

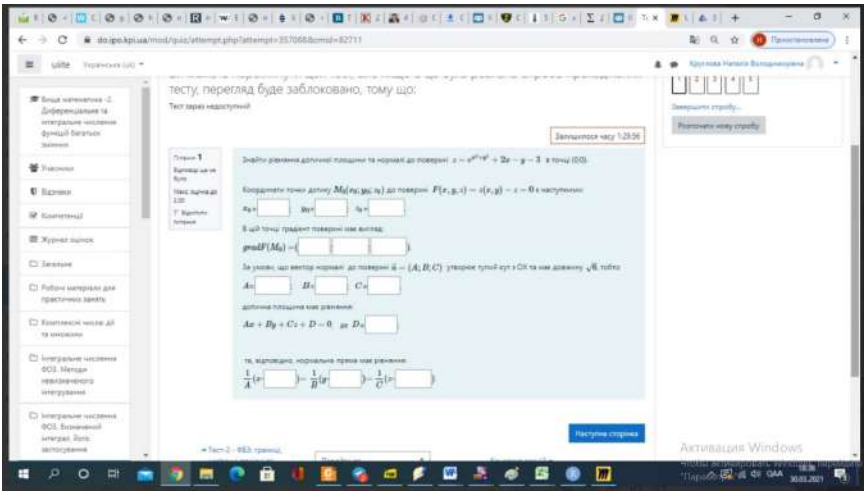


Рис. 2. Приклад тесту з вбудованими відповідями

Під час створення короткочасних тестів можна використовувати і тести на множинний вибір. Зауважимо, що розробка тестів вимагає не тільки створення самих задач з урахуванням всіх за-

значених вище особливостей, а й необхідність розмноження варіантів. Ось тут використання відповідних програмних засобів стає розробникам у нагоді. Зокрема, зручно використовувати тип питання «розрахунковий простий» у Moodle та шаблони розв'язків, що створені в Excel, Mathematica, або запрограмовані на вибраній мові програмування.

Однією зі зручних форм опитування виявились Google форми. Викладач відкриває широке вікно, наприклад, протягом доби, коли студенти можуть виконати завдання. При цьому він не пов'язаний із загально університетською платформою Moodle і ситуація суттєво не залежить від можливого перевантаження централізованої платформи і стану з електропостачанням в університеті. Студент може сам визначати коли саме він буде його виконувати в межах відкритого вікна, розуміючи скільки треба часу на виконання. Результат студент отримує одразу після закінчення своєї роботи, не чекаючи, щоб усі інші учасники опитування закінчили роботу. Створення самої Google-форми подібне до тих тестів, які у великій кількості складались викладачами за попередній період дистанційного навчання, хоча розробка досконалої Google форми потребує від викладача достатньо багато часу.

Google форма за особистою домовленістю між викладачем та студентами може виконуватись кілька разів. Це додає гнучкості системі самоконтролю рівня знань як самого студента, так і контролю зі сторони викладача, при збереженні об'єктивності оцінювання. Google форма показала себе надзвичайно ефективною, якщо комбінувати теоретичні запитання з практичними. Теоретичне запитання може бути приміром у наступному вигляді (рис. 3): означення надається у вигляді формули та пропонується вибрати всі правильні твердження що стосуються наведеної формули (завдання на множинний вибір).

Подібні завдання більше придатні для короткочасних перевірок знань, наприклад на початку чи наприкінці заняття для оцінювання рівня розуміння і опрацювання теми заняття.

Автори розглянули різні методи та підходи до реалізації основних етапів освітнього процесу в режимі дистанційного навчання. Але з початком війни саме дистанційне навчання зазнало суттєвої трансформації. Крім синхронної форми, коли заняття відбуваються в режимі реального часу додалась асинхронна форма. Синхронний режим дистанційного навчання означає, що заняття відбуваються за розкладом.

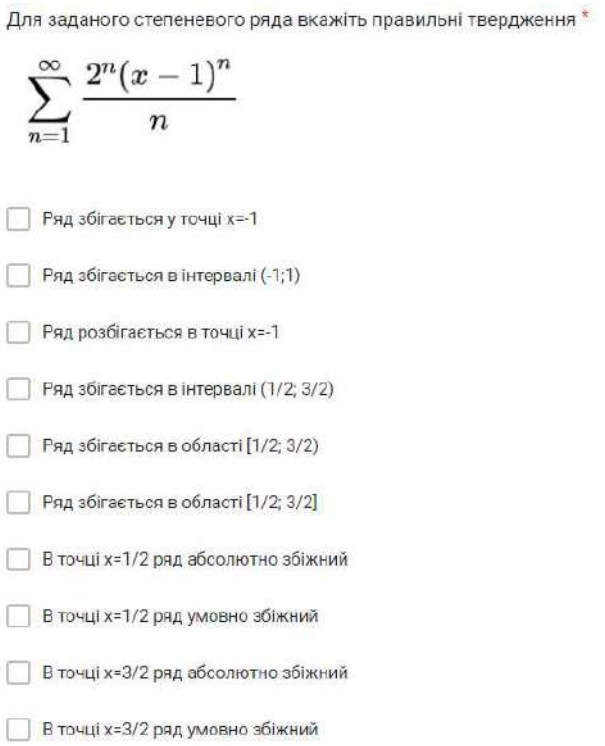


Рис. 3. Комбінування теоретичних запитань із практичними

Проте не всі студенти, зі зрозумілих причин, мають можливість відвідувати on-line заняття. Асинхронна форма навчання наразі є найбільш актуальною. Вона створює умови, коли студенти мають однакові можливості й доступ до навчальних матеріалів, незалежно від часу, місця перебування чи інших чинників Процес асинхронного навчання відбувається наступним чином: маючи на руках теоретичний лекційний матеріал і матеріал практичних занять, студент опрацьовує його самостійно. У матеріалах практичних занять частина завдань, що виносяться, умовно, для аудиторної роботи, подається з розібраними прикладами. Частина завдань, подібних до вже розібраних, залишається на самостійне виконання. Доступ до усіх матеріалів залежно від можливостей, які має викладач, і ситуації, в якій він знаходиться, подається в електронному, друкованому, прописаному вигляді або у відео запису лекцій і практичних занять. Після обговорення з викладачем обсягу завдань і термінів їх виконання, студенти ві-

дсилають виконану роботу поза розкладом занять. Можлива і комбінована форма.

За спостереженням авторів, дистанційно в синхронному режимі працюють від 20 до 30 % студентів. Близько 10 % студентів не виходять на зв'язок з викладачами. Частина з них відтермінувала, а частина, на жаль, покинула навчання. Решта обрали асинхронне навчання. Іншими словами, практика показала, що в умовах воєнного стану студенти переважно обирають асинхронну форму навчання. Наголосимо, що введення такої форми навчання суттєво розширило коло студентів, що хочуть навчатись та не мають можливості працювати систематично в режимі розкладу. Зауважимо також, що наведена статистика не є загальною, а швидше базується на власному досвіді авторів та їх колег і стосується, в першу чергу, студентів молодших курсів.

Здавалося, введення синхронної та асинхронної форм дистанційного навчання дозволить вирішити основні проблеми освіти, в умовах обставин, коли і студенти, і викладачі опинились в різних країнах, в різних областях України з різною безпековою ситуацією. Розроблені і вже апробовані дистанційні курси мали забезпечити рівні можливості навчатися всім студентам.

Проте в асинхронному режимі питання контролю і оцінювання знань студентів залишились, і навіть загострились. Звісно, безпосередня робота викладачів зі студентами в аудиторіях, коли у кожного студента є можливість обґрунтувати свою думку, з'ясувати усі тонкощі задачі тощо є найбільш інформативною. Дистанційна форма в довоєнний період дозволяла проводити тестування студентів технічних спеціальностей на платформі Moodle. Розробці відповідних дистанційних курсів і тестових завдань, як їх складової, і в КПІ, і в КНЕУ був створений широкий спектр різноманітних тестів. Такий спосіб контролю виявився дуже ефективним та зручним для усіх учасників навчального процесу. У цьому випадку студентам для виконання роботи надавався доступ до тесту в певний, обмежений, проміжок часу. Після збігання часового терміну кожен мав змогу побачити свій результат. Але стало зрозуміло, що у гарячій фазі воєнних дій ці обмеження працюють не на користь студенів. Викладачі змушені були шукати інші альтернативні способи контролю рівня знань студентів.

Ще однією особливістю освітянського процесу у воєнний період став індивідуальний підхід до навчання кожного студента. Як зазначалось вище, близько третини студентів дистанційно з'являються на лекціях, працюють на практичних заняттях, відві-

дують консультації, тобто дозволяють викладачу працювати з групою. Решта з тих, хто навчається асинхронно, працюють із викладачем фактично індивідуально. Безумовно, це кардинально змінює режим роботи викладачів, а також збільшує їх навантаження. Але хочеться відмітити, що загальним настроєм переважної більшості студентів є бажання працювати попри будь-які обставини.

Висновки. Підсумовуючи, можна наголосити, що досвід дистанційного навчання, що був отриманий під час пандемія covid-19 і воєнного стану, дозволить використати його позитивні сторони, переформатувати процес навчання, суттєво підняти його якість у подальшому і знайти ефективні способи розв'язання багатьох проблем, що накопичувалися роками.

Бібліографічні посилання

1. Про вищу освіту: Закон України (2015). URL: http://zakon1.rada.gov.ua/laws/show/1556-18/page

2. Про вищу освіту: Закон України зі змінами № 2145-VIII від 05.09 2017. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text

3. Національна стратегія розвитку освіти України на 2012–2021 роки. Затверджено розпорядженням Кабінету Міністрів України від 4 вересня 2013 р. № 686-р. *Офіційний вісник України*. 2012. № 11. С. 400.

4. Про затвердження Положення про дистанційне навчання. Наказ Міністерства Освіти і науки України від 25.04.2013 № 466. URL: http://zakon.rada.gov.ua/laws/card/z0703-13/ed20130627

5. Диховичний О.О., Дудко А.Ф. (). Комплексна методика аналізу якості тестів з вищої математики. *Науковий часопис НПУ імені М. П. Драгоманова*. Серія 2: Комп'ютерноорієнтовані системи навчання. 2015. № 15. С. 139-144.

6. Диховичний О.О., Круглова Н.В. Імітаційне моделювання й аналіз матриць первинних балів педагогічного тестування за допомогою мови R. *Інформаційні технології і засоби навчання*. 2018. № 5. Т. 67.

7. Мороз С.А., Романовський О.Г., Мороз В.М., Домбровська С.М., Грень Л.М., Помаза-Пономаренко А.Л. Дистанційна форма здобуття вищої освіти: аналіз думки студентів щодо якості, перваг і недоліків. *Інформаційні технології і засоби навчання*. 2022. № 5. Т. 79.

8. Ткачук Г.В. Особливості впровадження мобільного навчання: перспективи, переваги та недоліки. *Інформаційні технології і засоби навчання*. 2018. № 2. Т. 64. С. 13–22.

Статтю подано до редакції 28.11.2022

УДК: 519.252 DOI 10.33111/mise.100.8

Колєчкіна Л.М., д.фіз.-мат.н., професор
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Колєчкін В.О., старший викладач
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Koliechkina L.M., doctor of physical and mathematical sciences
professor of the Department of Computer Mathematics and Information Security,
KNEU named after V. Hetman

Koliechkin V.O., senior lecturer
of the Department of Computer Mathematics and Information Security,
KNEU named after V. Hetman

БАГАТОФАКТОРНА МОДЕЛЬ ЕКОНОМІЧНОЇ ЗАДАЧІ ОПТИМІЗАЦІЇ РОБОТИ ПІДПРИЄМСТВА ТА АНАЛІЗ МЕТОДІВ ЇЇ РОЗВ'ЯЗАННЯ

MULTIFACTOR MODEL OF THE ECONOMIC PROBLEM OF OPTIMIZING THE WORK OF THE ENTERPRISE AND ANALYSIS OF THE METHODS OF ITS SOLUTION

Анотація. *Різні економічні процеси часто можна описати за допомогою математичного моделюванню, тобто виразити певні залежності між економічними показниками через рівняння регресії. У процесі побудови багатофакторних регресійних моделей можуть виникнути проблема визначення закону розподілення спостережень і знаходження параметрів цього розподілу. В загальному така проблема може бути вирішена шляхом перевірки статистичних гіпотез, на основі числових статистичних тестів і критеріїв з урахуванням помилок першого і другого роду. Розглянуто економіку-математичну модель, яка може бути прикладом моделі прикладних задач. Для реалізації моделі і її застосування описано різні методи статистичного аналізу та їх порівняльні характеристики. Проведено числовий експеримент. Показано, що модель задачі носить загальний характер, але може бути використана для практичної проблеми, що пов'язана з аналізом та оптимізацією економічних показників підприємства. Під час застосування відповідного програмного забезпечення (MS Excel, GPSS World, AnyLogic і та ін.) можна швидко отримати точні показники діяльності підприємства та зробити відповідні висновки про його функціонування на даний момент, розрахувати прогнозовані значення на майбутнє.*

Ключові слова: *багатофакторна модель, оптимізація, статистичний аналіз даних, кореляційно-регресійний аналіз*

Abstract. *Various economic processes can often be described with the help of mathematical modeling, that is, express certain dependencies between economic indicators through regression equations. In the process of building multivariate regression models, the problem of determining the law of the distribution of observations and finding the parameters of this distribution may arise. In general, such a problem can be solved by testing statistical hypotheses, based on numerical statistical tests and criteria taking into account errors of the first and second kind.*

The paper considers an economic-mathematical model, which can be an example of a model of applied problems. To implement the model and its application, various methods of statistical analysis and their comparative characteristics are described. A numerical experiment was conducted. The problem model has a general nature, but can be used for a practical problem related to the analysis and optimization of the economic indicators of the enterprise. When using the appropriate software (MS Excel, GPSS World, AnyLogic, etc.), you can quickly obtain accurate indicators of the company's activity and make appropriate conclusions regarding its current functioning, calculate forecast values for the future.

Keywords: *multifactor model, optimization, statistical data analysis, correlation-regression analysis*

Постановка проблеми. Різні економічні процеси часто можна описати за допомогою математичного моделюванню, тобто виразити певні залежності між економічними показниками через рівняння регресії. При цьому під регресією розуміється залежність між величинами, що є випадковими [1–3]. Процес побудови математичних залежностей між факторами дозволяє визначити наявний тісний зв'язок між даними показниками і спрогнозувати одну залежну змінну через інші незалежні змінні. Маємо статистичний аналіз, на основі якого можемо робити висновки про розвиток економічних показників та їх зміни. Найбільш актуальними для моделювання економічних процесів є багатофакторні регресії, так як більшість економічних показників описуються як залежність від двох і більше факторів [4–7]. У процесі побудови багатофакторних регресійних моделей можуть виникнути проблема визначення закону розподілення спостережень і знаходження параметрів цього розподілу. У загальному така проблема може бути вирішена шляхом перевірки статистичних гіпотез на основі числових статистичних тестів і критеріїв з урахуванням помилок першого і другого роду.

Аналіз останніх досліджень і публікацій. Ця теорія детально розроблена, описана в літературі і є загальновідомою [6, 7]. Але слід зазначити, що з різних причин на практиці її досить рідко використовують. Досить часто для проведення статистичного аналізу користуються можливостями табличного процесору MS Excel або іншими статистичними пакетами обробки даних. При цьому важливим аспектом є урахування специфіки вихідної зада-

чі та її властивостей і особливостей. В цьому плані є доцільним використання прикладної статистики.

Цікавим є підхід, який описаний у [8, 9] на базі застосування теорії інформації для розв'язування різного класу статистичних задач.

У статтях описано [3, 5] метод найменших квадратів (МНК), який є широко відомим і користується достатньою популярністю. Разом з тим не припиняються спроби вдосконалення цього методу. Як результат, з'являються нові модифікації і версії МНК, однієї з яких є зважений метод найменших квадратів (ЗМНК). Суть ЗМНК полягає в тому, щоб надати спостереженням вагу, що обернено-пропорційна похибкам їх апроксимації. Отже, спостереження ігноруються тим більшою мірою, чим складніше їх апроксимувати [3, 5]. В результаті такого підходу формально похибка апроксимації знижується, проте фактично це відбувається шляхом часткової відмови від перегляду проблемних спостережень, що вносять велику помилку.

Під прикладної статистикою розуміють частину математичної статистики, присвячену методам обробки реальних статистичних даних, а також відповідне математичне і програмне забезпечення. Звідси суто математичні завдання і не включають у прикладну статистику.

Під статистичними даними розуміють числові або нечислові значення контрольованих параметрів (ознак) досліджуваних об'єктів, які отримані в результаті спостережень (вимірювань, аналізів, випробувань, дослідів іта ін.) певного числа ознак, у кожної одиниці, що увійшла в дослідження. Способи отримання статистичних даних та обсяги вибірок встановлюють виходячи з постановок конкретної прикладної задачі на основі методів математичної теорії планування експерименту.

Результат спостереження x_i досліджуваної ознаки X чи їх сукупності, y_i-ї одиниці вибірки відображає кількісні та якісні властивості обстеженої ознаки з номером i (де $i = 1, 2,..., n$, а n — обсяг вибірки). На основі вибраних даних слід проаналізувати вибірку та зробити висновок про подальші дослідження ознак і характеристик математичної моделі.

Результати спостережень $x_1, x_2,..., x_n$, де x_i — результат спостереження i-ї одиниці вибірки, або результати спостережень для декількох вибірок, обробляють за допомогою методів прикладної статистики, відповідно до поставленої задачі. Використовують, як правило, аналітичні методи, тобто методи, засновані на числових розрахунках. В окремих випадках допустимо застосування графічних методів візуального аналізу [5, 6].

Кількість розроблених дотепер методів обробки даних дуже велике. Вони описані в статтях і підручниках, а також в стандартах та інших нормативно-технічних та інструктивно-методичних документах. Це пов'язано з необхідністю обробки великих масивів даних і їх аналізу [1–7].

Багато методів прикладної статистики вимагають проведення трудомістких розрахунків, і тому для їх реалізації необхідно використовувати комп'ютери. Програми розрахунків на ЕОМ повинні відповідати сучасному науковому рівню. Однак для одиничних розрахунків при відсутності відповідного програмного забезпечення успішно використовують мікрокалькулятори.

Аналіз методів математичної статистики та їх порівняння. На сьогодні в математичній статистиці розроблений ряд загальних методів визначення оцінок і похибок, такі як метод моментів, метод максимальної правдоподібності, метод однокрокових оцінок, метод стійких робасних оцінок, метод незміщене оцінок і та ін. Теоретичні основи різних методів оцінювання та отримані з їх допомогою конкретні правила визначення оцінок і довірчих кордонів для тих чи інших параметрів розподілів розглянуто в [2–5].

Більшість статистичних методів належать до методів параметричної статистики, в основу яких покладено припущення, що випадковий вектор змінних утворює деякий багатовимірний розподіл. Якщо це припущення не підтверджується, слід скористатися непараметричними методами математичної статистики.

Наприклад, відомий метод моментів, що заснований на використанні виразів для моментів розглянутих випадкових величин через параметри їх функцій розподілу дає можливість отримати оцінки, підставляючи вибіркові моменти замість теоретичних в функції, що виражають параметри.

Що стосується оцінок максимальної правдоподібності, то, як правило, вони є ефективними і мають меншу дисперсію, ніж оцінки методу моментів. В окремих випадках доцільно використовувати не оцінки максимальної правдоподібності, а інші види оцінок, наприклад, однокрокові оцінки, що називаються в літературі наближені оцінки максимальної правдоподібності. При досить великих обсягах вибірок вони мають досить гарні властивості, як і оцінки максимальної правдоподібності. Тому їх слід розглядати не як «наближені», а як оцінки, отримані по іншому методу, ніж метод максимальної правдоподібності.

Під час вивчення причинно-наслідкових зв'язків показники моделі поділяють на результатні та факторні. Це групування не постійне, воно залежить від конкретних ситуацій, мети аналізу. Напри-

клад, в оцінці змін прибутку від реалізації продукції показник собівартості продукції розглядають як факторний. Водночас у ході вивчення затрат на виробництво собівартість розглядають як результатний показник, що залежить від багатьох факторів виробництва.

Слід зазначити, що у використанні статистичного показника необхідно розглядати такі задачі: опис структури економіки підприємства, опис тенденцій розвитку економіки в майбутньому, аналіз і прогнозування різних економічних явищ, вияв факторів розвитку економіки підприємства для прийняття управлінських рішень [3–5].

У процесі моделювання економічних показників підприємства засобами статистичного аналізу можуть бути застосовані такі підходи:

1. *Кореляційний аналіз* дозволяє встановити силу і напрям стохастичного взаємозв'язку між змінними (випадковими величинами).

2. *Регресійний аналіз* забезпечує моделювання взаємозв'язку однієї випадкової змінної від однієї або декількох інших випадкових змінних. При цьому перша змінна називається залежною, а решта — незалежними. Вибір або призначення залежною і незалежних змінних є довільним / умовним і здійснюється дослідником залежно від розв'язуваної ним задачі.

3. *Канонічний аналіз* призначений для аналізу залежностей між двома списками ознак (незалежних змінних), що характеризують об'єкти.

4. *Дисперсійний аналіз* можна визначити як параметричний, статистичний метод, призначений для оцінки впливу різних чинників на результат експерименту, а також для подальшого планування експериментів.

5. *Кластерний аналіз* — це метод класифікаційного аналізу; його основне призначення — розбиття множини досліджуваних об'єктів і ознак на однорідні в деякому сенсі групи, або кластери [1–6].

Одним із важливих напрямів у статистичному аналізі є багатовимірний статистичний аналіз, який застосовують під час вирішення таких завдань:

- дослідження залежності між ознаками;
- класифікація об'єктів або ознак, заданих векторами;
- зниження розмірності простору ознак.

При цьому результатом спостереження є вектор значень фіксованого числа кількісних і іноді якісних ознак, виміряних у об'єкта. Нагадаємо, що кількісна ознака — це ознака, яку можна безпосередньо виразити числом і одиницею виміру. Кількісна ознака протиставляється якісній, що визначається віднесенням до

однієї з двох або більше умовних категорій (якщо є рівно дві категорії, то ознака називається альтернативною.

Статистичний аналіз якісних ознак — це частина статистики об'єктів нечислової природи. Кількісні ознаки діляться на ознаки, виміряні в шкалах інтервалів, відносин, різниць, абсолютних похибок, а якісні — на ознаки, виміряні в шкалі найменувань і порядкової шкали. Методи обробки даних повинні бути узгоджені зі шкалами, в яких виміряні розглянуті ознаки.

Метою дослідження залежності між ознаками є доказ наявності зв'язку між ознаками і вивчення зв'язку між ними. Для доказу наявності зв'язку між двома випадковими величинами X і Y застосовують кореляційний аналіз [2, 4, 5].

Якщо спільний розподіл X і Y є нормальним, то статистичні висновки засновують на вибірковому коефіцієнті лінійної кореляції, в інших випадках використовують коефіцієнти рангової кореляції Кендалла і Спірмена, а для якісних ознак — критерій x_i-квадрат.

Регресійний аналіз застосовують для вивчення функціональної залежності кількісної ознаки. Основне завдання регресійного аналізу полягає в оцінці невідомих параметрів a і b, які задають лінійну залежність y від x. Для вирішення цього завдання застосовують розроблений К. Гаусом метод найменших квадратів, тобто знаходять оцінки невідомих параметрів моделі a і b з умови мінімізації суми квадратів по змінних a і b [2, 4–5].

Теорія регресійного аналізу описана і розрахункові формули дані в спеціальній літературі [2, 4–7]. У цій теорії розроблені методи точкового та інтервального оцінювання параметрів, які задають функціональну залежність, а також непараметричні методи оцінювання цієї залежності, методи перевірки різних гіпотез, пов'язаних з регресійної залежності. Вибір планів експерименту, тобто точок x_i, у яких будуть проводитися експерименти зі спостереження y_i — предмет теорії планування експерименту [18].

Дисперсійний аналіз застосовують для вивчення впливу якісних ознак на кількісну змінну [4–7].

Постановка та формалізація задачі

Багатофакторна лінійна регресійна модель може бути записана у такому вигляді:

$$y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \ldots + \beta_p x_p + \varepsilon,$$

де y — залежна змінна; $x_1, x_2, \ldots, x_p$ — незалежні змінні (або фактори); $\beta_0, \beta_1, \ldots, \beta_p$ — невідомі параметри, які потрібно оцінити; ε — випадкова величина.

Приклад. На основі статистичних даних показника y та факторів x_1, x_2 та x_3 провести аналіз та побудувати математичну модель залежності y від x_1, x_2 та x_3, попередньо дослідивши її на наявність мультиколінеарності. Вихідні дані приведені у табл. 1.

Таблиця 1

ВИХІДНІ ДАНІ ЗАДАЧІ

Фондовіддача, x_1, тис. грн	Продуктивність праці, x_2, тис. грн	Питомі інвестиції, x_3, тис. грн	Прибуток за місяць, y, тис. грн
12	5	15	40
17	7	18	45
13	6	16	40
14	7	17	43
16	6	20	48
15	5	15	39
14	6	16	42
17	9	18	45
12	5	19	38
18	10	20	48
20	11	22	50
17	10	21	48
18	12	21	49
19	8	20	45
20	9	22	49
22	14	23	52
24	15	24	54
21	13	20	51
25	16	24	55
27	18	25	56

Виклад основного матеріалу. На першому кроці будуємо економетричну модель за замовчуванням у пакеті SPSS, тобто модель, до якої у примусовому порядку включені усі фактори — x_1, x_2 та x_3.

При цьому отримаємо такі результати:

ВВЕДЕННЯ І ДОДАВАННЯ ЗМІННИХ

Модель	Включені змінні	Виключені змінні	Метод
1	X_3, X_2, X_1	–	Примусове включення

Таблиця 2

ЗВЕДЕННЯ ДЛЯ МОДЕЛІ 1

Модель	H	R-квадрат	Скоректований R-квадрат	Стд. похибка	Зміна статистик					Дурбін — Уотсон
					Зміна R квадрат	Зміна F	ст.св.1	ст.св.2	Знч. Зміна F	
1	,963[a]	,927	,913	1,58572	,927	67,649	3	16	,000	2,404

Коефіцієнти										
Модель		Нестандартизовані коефіцієнти		Стандартизовані коефіцієнти	t	Знч.	95,0 %% довірчий інтервал для B		Статистики колінеарності	
		B	Стд. похибка	Бета			Нижня границя	Верхня границя	Толерантність	КРД
1	(Константа)	23,309	3,548		6,569	,000	15,787	30,831		
	X1	,483	,279	,382	1,730	,103	-,109	1,074	,094	10,671
	X2	,410	,281	,302	1,460	,164	-,186	1,007	,106	9,393
	X3	,550	,272	,310	2,019	,061	-,027	1,127	,193	5,169

Отже, для отриманої моделі:

- коефіцієнт детермінації $R^2 = 0,927$; це значить, що 92,7 % вихідних даних підпорядковуються лінійній регресії;
- стандартна похибка регресії E = 1,58572. У відсотковому відношенні це складає 3,38 %; оскільки E% < 15 %, то отримана модель добре пояснюється отриманою регресією;
- значення критерію Фішера F = 67,649; порівнюючи його з критичним значенням даного критерію на рівні значимості $\alpha = 0,05$ та степенями свободи $m_1 = 3$ і $m_2 = 16$: $F_{кр} = 3,24$, можна бачити, що отримана модель буде достовірною з ймовірністю 0,95.

У другій звітній таблиці, ми бачимо, що отримана модель має вигляд:

$$y = 23{,}31 + 0{,}48x_1 + 0{,}41x_2 + 0{,}55x_3.$$

В останній колонці звіту коефіцієнтів (Статистика колінеарності), можемо бачити, що значення коефіцієнта близькі до критичного значення 10, а отже, ведуть до мультиколінеарності [2, 5, 10].

Щоб позбутися ефекту мультиколінеарності, на другому кроці будуємо модель покрокової регресії, яка дасть змогу частково усунути мультиколінеарність. Для цього у вікні регресії обираємо модель покрокової регресії і зробимо перерахунок моделі. Отримаємо:

Таблиця 3

ЗВЕДЕННЯ ДЛЯ МОДЕЛІ 2

Модель	H	R-квадрат	Скоректований R-квадрат	Стд. Помилка похибки	зміна статистик					Дурбін-Уотсон
					зміна R квадрат	зміна F	ст.св.1	ст.св.2	Знч. зміни F	
1	,943[a]	,890	,884	1,83326	,890	145,812	1	18	,000	
2	,958[b]	,917	,907	1,63766	,027	5,557	1	17	,031	2,369

Коефіцієнти										
Модель		Нестандартизовані коефіцієнти		Стандартизовані коефіцієнти	t	Знч.	95,0%% довірчий інтервал для B		Статистики колінеарності	
		B	Стд. похибка	Бета			Нижня границя	Верхня границя	Толерантність	КРД
1	(Константа)	25,336	1,828		13,858	,000	21,495	29,177		
	X1	1,192	,099	,943	12,075	,000	,985	1,399	1,000	1,000
2	(Константа)	19,970	2,802		7,128	,000	14,058	25,881		
	X1	,783	,195	,619	4,018	,001	,372	1,193	,205	4,879
	X3	,644	,273	,363	2,357	,031	,068	1,221	,205	4,879

На даному етапі ми отримали дві найкращі моделі:

- $y = 25{,}34 + 1{,}19x_1$
- $y = 19{,}97 + 0{,}783x_1 + 0{,}64x_3$

При цьому для подальшого використання підходить як перша, так і друга моделі.

Модель задачі носить загальний характер, але може бути використана для практичної проблеми, що пов'язана з аналізом та оптимізацією економічних показників підприємства. Подібні задачі, але інший підхід до розв'язання, були розглянуті в різних літературних джерелах [4, 5, 10].

Висновки. Отже, використання статистичного аналізу для моделювання економічних показників підприємства є ефективним інструментом. У разі застосування відповідного програмного забезпечення (MS Excel, GPSS World, AnyLogic і та ін.) можна швидко отримати точні показники діяльності підприємства та зробити відповідні висновки про його функціонування на даний момент, розрахувати прогнозовані значення на майбутнє. Проте при цьому слід враховувати специфіку задачі та особливості методів застосування.

Бібліографічні посилання

1. Strutz, T. (2016). Data Fitting and Uncertainty (A practical introduction to weighted least squares and beyond). Springer Vieweg.
2. Карташов М. В. Імовірність, процеси, статистика. Київ: ВПЦ Київський університет, 2007. 504 с.
3. Jaynes, E.T. (1957). "Information Theory and Statistical Mechanics". Phys. Rev. 106 (4): 620. Bibcode:1957PhRv.106.620J. doi:10.1103/ physrev.106.620.
4. Єріна А.М. Статистичне моделювання та прогнозування: навч. посібник. Київ: КНЕУ, 2001. 170 с.
5. Greene, William (2012). Econometric Analysis (7th ed.). Pearson Education. pp. 34, 41–42. ISBN 9780273753568.
6. Опря А.Т. Статистика (модульний варіант з програмованою формою контролю знань): навч. посібник. Київ: Центр учбової літератури, 2012. 448 с.
7. Wooldridge, Jeffrey (2013). Introductory Econometrics, A modern approach. South-Western, Cengage learning. ISBN 978-1-111-53104-1.
8. Burnham, K. P. and Anderson D. R. (2002) Model Selection and Multimodel Inference: A Practical Information-Theoretic Approach, Second Edition (Springer Science, New York) ISBN 978-0-387-95364-9.
9. Wolberg, J. (2005). Data Analysis Using the Method of Least Squares: Extracting the Most Information from Experiments. Berlin: Springer. ISBN 978-3-540-25674-8.
10. Колєчкіна Л.М., Литвиненко Ю.О. Економетрія: навч.-метод. посіб. для самост. вивч. дисц. Полтава: ПУЕТ, 2015. 157 с.

Статтю подано до редакції 28.11.2022

УДК: 004.4`2 DOI 10.33111/mise.102.9

Корзаченко О.В., к.е.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Korzachenko O.V., PhD, Associate Professor
of the Department of Computer Mathematics and Information Security,
KNEU named after Vadym Hetman

LOW-CODE ТА NO-CODE BPMS: СУЧАСНІ ТРЕНДИ АВТОМАТИЗАЦІЇ БІЗНЕС-ПРОЦЕСІВ ПІДПРИЄМСТВА

LOW-CODE TA NO-CODE BPMS: MODERN TRENDS IN ENTERPROSE'S BUSINESS PROCESS AUTOMATION

Анотація. *Стаття присвячена дослідженню сучасних трендів автоматизації бізнес-процесів підприємств. Наразі у відповідь на стрімку зміну ринкових вимог перед бізнесом стоїть завдання прискореного створення цифрових рішень і вибору відповідних інструментів та платформ розробки, що забезпечать безперечні конкурентні переваги. Проаналізовано особливості автоматизації бізнес-процесів шляхом проєктування або використання готових BPMS. Виявлено, що класичні BPMS мають низку недоліків, що перешкоджають вчасним цифровим трансформаціям. Альтернативою є розробка таких систем або окремих додатків на основі платформ low-code та no-code. Виявлено, що платформи з низьким кодом, які використовують для створення програмного забезпечення BPM, є економічно ефективнішими за традиційні BPM. На основі порівняльного аналіз платформ low-code та no-code визначено особливості вибору тієї чи тієї платформи для автоматизації бізнес-процесів з урахуванням специфіки діяльності компаній. Основним внеском статті є характеристика нової галузі розробки програмних продуктів на основі платформ low-code та no-code й особливостей і перспектив застосування таких платформ для проєктування систем і програмних додатків автоматизації бізнес-процесів підприємств, що ґрунтується на дослідницькій методології побудови теорії на основі огляду провідних наукових та інформаційних джерел.*

Ключові слова: *бізнес-процес, управління бізнес-процесами, система управління бізнес-процесами, BPMS, автоматизація бізнес-процесів, low-code, no-code, LCDP, NCDP.*

Abstract. *The article is devoted to the research of modern trends in enterprises' business processes automation. Currently, in response to rapidly changing market requirements, businesses are faced with the task of accelerating the development of digital solutions and choosing the appropriate development tools and platforms that will provide undeniable competitive advantages. The article analyzed the features of business processes automation by designing or using ready-made BPMS. It was found that classic BPMS have a number of disadvantages that prevent timely digital transformations. An alternative is the development of such systems or individual applications based on low-code and no-code platforms. Low-code*

platforms used to build BPM software have been found to be more cost-effective than traditional BPM. On the basis of a comparative analysis of low-code and no-code platforms, the features of choosing one or another platform for business processes automation, taking into account the specifics of the companies' activities, are determined. Based on a theory-building research methodology through the literature and other information sources review, the main contribution of the article is the description of the new field of software product development based on low-code and no-code and the features and perspective of using such platforms for designing systems and software applications for enterprises' business processes automation.

Keywords: *business process, business process management, business process management system, BPMS, business process automation, low-code, no-code, LCDP, NCDP.*

Постановка проблеми. Нині підприємствам досить часто доводиться стикатися з проблемами автоматизації діяльності через зростаючу складність внутрішніх бізнес-процесів, збільшення кількості та посилення інтенсивності зв'язків з зовнішніми стейкхолдерами і партнерами. До того ж мінливі ринкові умови вимагають від компаній швидкої та гнучкої реакції на нові вимоги зовнішнього середовища. Очевидно, що сучасні реалії мають враховувати й інформаційні технології (ІТ), які обирає окрема компанія, а автоматизовані системи управління бізнес-процесами повинні бути стійкими, щоб забезпечити можливість змінити характер діяльності, підлаштуватися до динамічного середовища і вчасно реагувати на зміни. Наразі ІТ-ринок надає різні класи програмного забезпечення для автоматизації бізнес-процесів чи побудови комплексних систем управління бізнес-процесами, що вимагає їх детального дослідження та визначення варіантів практичного застосування.

Аналіз останніх досліджень і публікацій. Свого розвитку наукова думка щодо перспектив застосування й удосконалення платформ розробки ІТ-рішень на основі концепції low-code та no-code знайшла у працях Guerra E., Kolovos D.S., Lara J., Mottu J.-M., Pierantonio A., Richardson C., Ruscio D.D., Rymer J.R., Sambandam S., Srikanth R.P., Tisi M., Wimmer M., Yan Z. та інших. Дослідники визначають сутність, переваги та наявні недоліки платформ розробки, акцентують увагу на перспективах застосування для автоматизації діяльності компаній в умовах стрімкої цифрової трансформації. В українських наукових дослідження ця тематика не знайшла належного відображення, що значною мірою стримує широке розповсюдження даної технології та може негативно позначитися на процесах ІТ-підтримки діяльності національних компаній.

Метою статті є дослідження теоретико-методичних і практичних засад використання інструментів автоматизації бізнес-

процесів підприємств, а також визначення особливостей, доцільності та перспектив розробки систем управління бізнес-процесами на основі low-code та no-code платформ.

Виклад основного матеріалу дослідження. Класичним інструментом автоматизації процесів, який широко використовується бізнесом протягом останніх десятиліть, є програмне забезпечення для управління бізнес-процесами — Busines Process Management System (BPMS). BPMS традиційно допомагали компаніям спрощувати складні процеси, усуваючи рутинну ручну роботу. Сьогодні вони використовуються для автоматизації, моніторингу та аналізу бізнес-процесів, що дає додаткові можливості для топ-менеджменту компанії, покращує продуктивність усіх інших стейкхолдерів, та сприяє розвитку бізнесу. BPMS надають особам, які приймають рішення, доступ до ключових відомостей про діяльність, дають змогу аналізувати ризики та забезпечують кращий огляд діяльності підприємства [7].

Незважаючи на те що більшість програмного забезпечення цього класу має достатньо функціональних можливостей для підтримки управління бізнес-процесами підприємства, через активізацію цифрових трансформацій процеси компаній стали більш взаємопов'язаними, що виявило певні недоліки традиційних BPMS [7].

1. Бізнес-процеси зазвичай не залежать від організаційної структури та перетинають різні департаменти або навіть локації компанії, а в їх реалізації можуть приймати участь навіть віддалені команди. Це означає, що до BPMS висувається вимога більшої гнучкості та можливості швидкого налаштування.

2. BPMS, як правило, мають круту криву навчання, особливо коли налаштовані відповідно до різних вимог підприємства, через що команди повинні постійно проходити певні тренінги та курси для того, щоб мати змогу працювати з системою.

3. Хоча BPMS може надати простий і спрощений доступ до даних для вищого керівництва, але робота з системою вимагає певних технічних знань. Для внесення незначних змін у бізнес-процес потрібна участь висококваліфікованих розробників, причому внесення змін може тривати достатньо довго.

З метою посилення стійкості підприємств, для їх швидкого та ефективного реагування на потреби ринку, зусилля в галузі науки та IT були зосереджені на розробці відповідних програмних рішень, а саме — побудові програмних додатків без повторного традиційного кодування та програмування вручну [15]. Першими результатами стали мови програмування четвертого покоління та

інструменти швидкої розробки додатків, які почали з'являтися у 1990-ті роки. Ці результати мали практичне застосування, проте не досягли домінуючого становища у галузі розробки програмного забезпечення. Нове покоління інструментів — платформи розробки low-code (Low Code Development Platforms, LCDPs). LCDPs дають можливість користувачам створювати повноцінні програми, взаємодіючи з ними за допомогою динамічних графічних інтерфейсів користувача (user interface, UI), візуальних компонентів і декларативних мов програмування, також дозволяють створити програмне забезпечення у «хмарі» через модель PaaS.

Термін «low-code» вперше введений Forrester Research у 2014 р. (Кембридж, США) [10]. Зазначалося, що для постійної швидкої розробки додатків компанії віддають перевагу low-code альтернативам. LCDPs — це екосистеми, за допомогою яких можна розробляти додатки, мінімізуючи написання коду вручну. У 2017 р. Forrester оновив визначення, за яким LCDPs — це продукти та/або хмарні сервіси для розробки додатків, які використовують візуальні, декларативні методи замість класичного програмування, і не вимагають від клієнтів значних витрат часу для навчання та початку роботи, при цьому витрати збільшуються пропорційно бізнес-вартості платформ [12].

LCDPs дозволяють бізнес-користувачам створювати власні програми під певні потреби з мінімальними знаннями із програмування та IT за рахунок використання графічного UI, компонентів перетягування (drug-and-drop) та інших зручних структур [14]. При описі LCDPs М. Росс використав порівняння з коробкою Lego, оскільки вони складаються з набору функціональних блоків та компонентів [11]. Кожен такий блок може бути використаний у різних програмах як складова для реалізації повної функціональності. Наприклад, розробникам не потрібно кодувати об'єкти інтерфейсу з нуля, коли вони можуть обрати його з попередньо вбудованих компонентів інтерфейсу. Крім того, ці компоненти можна легко налаштувати та оновлювати в міру зміни бізнес-потреб. Завдяки LCDPs, навіть citizen developers, тобто бізнес-користувачі з базовими знаннями мов програмування, можуть легко розробляти додатки, які будуть враховувати всі необхідні положення з безпеки та надавати мінорні та мажорні оновлення коду [14].

Концепція low-code припускає можливість модифікувати, адаптувати і розвивати систему безпосередньо в ході її експлуатації за мінімізації кодування та дозволяє прискорити цикл від потреби бізнес-користувачів до автоматизованого процесу. Та-

кож експерти Gartner стверджують, що LCDPs дозволяють значно підвищити продуктивність розробників і аналітиків, а також прискорити поставку вже готової функціональності користувачам [1]. Отже, основна мета LCDPs — у відповідь на перманентну зміну зовнішніх та внутрішніх вимог до діяльності дозволити підприємствам розробляти багатофункціональні IT-рішення для мобільних та настільних пристроїв без складної інженерії та більш економічним способом.

Аналітична компанія Gartner зазначає, що ринок low-code зростає значними темпами, на що впливає постійний попит на нові IT-рішення через прискорення цифрових трансформацій, та брак кваліфікованих розробників. За даними IDC, у 2021 р. в усьому світі нестача розробників становила 1,4 млн, очікується, що ця кількість буде тільки зростати [8]. Gartner прогнозують, що до 2023 р. понад 50 % середніх і великих підприємств будуть використовувати LCDPs як одну зі своїх стратегічних платформ для розробки додатків, а до 2025 р. цей показник досягне 70 % [1].

Наразі LCDPs особливо успішно використовуються для розробки IT-рішень у таких сегментах ринку: створення додатків для роботи з базами даних, мобільні додатки, технологічні програми та програми обробки запитів, IoT [15].

Проаналізуємо стан використання LCDPs на основі звіту «Стан розвитку прикладних програм» [16], який показує результати, отримані в ході опитування понад 3300 IT-фахівців на різних континентах. Для більшості респондентів впровадження low-code систем є частиною IT-стратегії, 41 % респондентів вже використовують їх у своїй діяльності, а 10 % планують їх використання найближчим часом.

За даними опитування [16], основними причинами використання LCDPs є такі:

– прискорення цифрових трансформацій та інновацій — 66 %;
– підвищення гнучкості бізнесу — 66 %;
– зниження залежності від наявності на підприємстві розробників з високим рівнем технічних знань — 45 %;
– уникнення успадковування застарілих коду, програм, технологій (Legacy Debt) — 28 %;
– захист від постійного часто необґрунтованого переходу на нові технології та системи (Technology Churn) — 22 %;
– можливість для бізнес-користувачів вдосконалювати внутрішні процеси — 20 %;
– інше — 2 %.

Незважаючи на значну кількість переваг від впровадження та використання LCDPs, слід врахувати й певні ризики, які виникають у зв'язку з цим. Так занепокоєння викликають питання масштабованості та фрагментарності IT-рішень, розроблених на LCDPs, а також залежність від вендорів і нерозуміння місця даних програмних продуктів в IT-портфелі компанії.

Основними причинами, через які підприємства не використовують LCDPs є такі [16]:

- брак знань про LCDPs — 47 %;
- занепокоєння щодо «замикання» на вендорах LCDPs — 37 %;
- відсутність віри у те, шо можна створити необхідний тип додатку — 32 %;
- занепокоєність масштабованістю створених додатків — 28 %;
- занепокоєність безпекою створених додатків — 25 %;
- інше — 10 %.

Очевидно, що LCDPs можуть стати гарною альтернативою класичним BPMS. Так, за даними [2], у 2019 р. 18 % компаній виявили інтерес до використання LCDPs як інструменту вдосконалення бізнес-процесів у контексті їх автоматизації. Взагалі різниця між BPMS і LCDPs доволі концептуальна. BPMS є певним інструментом виконання завдань з управління бізнес-процесами, тоді як LCDP можна описати як альтернативний спосіб створення програмних продуктів, зокрема й BPMS.

Програмне забезпечення на основі low-code впливає на стратегію управління бізнес-процесами, а саме [4]:

1. Прискорює швидкість оптимізації бізнес-процесів. LCDP забезпечує швидкий, більш поступовий процес розробки. Бізнес-командам не доводиться чекати, поки IT-спеціалісти змінять або автоматизують необхідні бізнес-процеси, а бізнес-користувачі мають змогу швидко оновлювати процеси у відповідь на відгуки клієнтів або дії конкурентів.
2. Спрощує стандартизацію бізнес-процесів. Неузгодженість між процесами ускладнює дотримання вимог безпеки або їх оркестрування у системі. LCDP забезпечує просту структуру розробки, яку можна адаптувати до будь-якої команди, департаменту чи випадку використання, що може гарантувати, що всі бізнес-процеси будуть організовані, оцифровані та інтегровані в загальну процесну структуру.
3. Перерозподіляє IT та/або ресурси розробників. LCDP зменшує відставання в IT і звільняє IT-команду від необхідності що-

разу вносити зміни в кожен бізнес-процес. Як наслідок, це дозволяє розробникам та IT-фахівцям переорієнтувати свій час і увагу на інші зусилля, такі як безпека чи цифрові інновації.

Порівняння класичних BPMS та BPMS, які створені на платформах з low-code наведено у табл. 1.

Таблиця 1

ПОРІВНЯННЯ LOW-CODE І КЛАСИЧНИХ BPMS

Критерій	Low-code BPMS	Класична BPMS
Час налаштування	Миттєва реєстрація (як правило, на хмарному сервісі)	До 6 місяців (майже завжди на місці / сервері компанії)
Налаштування процесів (Process Setup)	Шаблони процесів, які налаштовуються. Інтерактивний дизайн «перетягування» компонентів drug-and-drop	Потрібно запрограмувати на етапі проєктування системи. Після впровадження важко змінити логіку виконання процесів
Вартість	У середньому 10 дол. / місяць за користувача (розробника)	6-значне число за встановлення та плата за річну підписку
Досвід користувача (User Experience)	Необхідне мінімальне кодування. Програми можуть бути розроблені бізнес-користувачами або citizen deveopers	Необхідна спеціальна підготовка співробітників-розробників та IT-допомога для конфігурацій
Інтеграція	Інтеграція API з стороннім SaaS програмним забезпеченням	Рівень інтеграції залежить від конкретного рішення. Додатки можуть встановлювати тільки розробники системи

Джерело: розроблено автором на основі [5–7].

Крім значного впливу на загальну стратегію управління бізнес-процесами в компанії, використання LCDP може забезпечити низку переваг для бізнесу. Універсальними переваги, які виявляються у всіх компаніях незалежно від їх розміру чи сфери діяльності, є:

1. Зменшення ризику. Автоматизація бізнес-процесів за допомогою LCDP допомагає стандартизувати процеси, що покращує їх видимість і контроль, а також полегшує дотримання вимог безпеки.

2. Покращення взаємодії з користувачами. BPMS створені на основі LCDP інтегруються з компонентами існуючого стеку технологій, забезпечуючи загальну структуру взаємодії з користувачами. На відміну від використання розрізненого набору додатків і програм, така технологія надає єдиний уніфікований інтерфейс, у якому керування даними та зв'язок між інтегрованими системами відбувається за лаштунками.

3. Можливість автоматизації складних процесів. Використання автоматизації на основі LCDP забезпечує легкість управління наскрізними бізнес-процесами, а адаптивність таких систем робить їх унікальним рішенням для роботи з винятковими або випадковими бізнес-процесами.

4. Підвищення ефективності. З LCDP бізнес-команди, які виявляють можливості для автоматизації операцій і бізнес-процесів, можуть проводити автоматизацію самостійно.

Одним з основних критеріїв при виборі між класичною BPMS та low-code BPMS все ж таки лишається економічна ефективність. Об'єктивно, LCDPs є дешевшими і використовують моделі ціноутворення на основі користувачів. Розгортання традиційної BPMS триває місяці та передбачає витрати на адаптацію, навчання та значні трудовитрати IT-команди. На практиці платформи з низьким кодом, які використовують для створення програмного забезпечення BPM, є економічно ефективнішими за традиційні BPM.

Окремою варіацію LCDPs є платформи, в основу яких закладена концепція no-code (No Code Development Platforms, NCDPs).

Рішення на основі no-code так само, як і low-code, використовують візуальну розробку за допомогою drug-and-drop компонентів, але вони призначені для створення більш простих програмних додатків [3]. Компаніям слід чітко розуміти, які рішення: low-code чи no-code більш доречні з погляду специфіки їх бізнесу. Порівняння LCDPs та NCDPs наведено в табл. 2.

Обидві платформи для розробки додатків low-code та no-code мають багато спільних концептуальних рис, але у разі вибору слід враховувати їхні відмінності. Перша відмінність — у цільовій аудиторії платформи. LCDP більшою мірою орієнтована на розробників, її застосування дозволяє уникнути копіювання базового коду та надати можливості для реалізації більш складних задач інноваційного характеру. NCDP краще підхожа для гібридних команд, до складу яких входять бізнес-користувачі та розробники програмного забезпечення або власникам малого бізнесу та командам, які не пов'язані з IT, наприклад відділ кадрів, фінансовий або юридичний департаменти.

Таблиця 2

ПОРІВНЯННЯ LCDPS ТА NCDPS

Критерій	LCDP	NCDP
Призначення	Інструмент швидкої розробки додатків нового покоління для професійних розробників або IT-фахівців	Програма самообслуговування для бізнес-користувачів
Основна аудиторія	Професійний розробник	Бізнес-користувач
	Citizen developer	
Основні цілі та мотиви використання	Швидкість розробки програмних додатків. Використання може підвищити продуктивність розробників, оскільки вони зможуть зосередитися на стратегічних проєктах	Простота використання платформи, що дає можливість бізнес-користувачам створювати програми для своїх департаментів
Тип проєкту	Критично важливі для бізнесу рішення та складні програми	Прості програми для департаментів
Потреба у кодуванні	Низька, але необхідність написання програмного коду зберігається	Відсутня
Складність програми	Є можливість створювати складні програми	Можливо створювати тільки прості програми
Налаштування, кастомізація	Доступні повні налаштування. Розробники можуть додати кастомний код	Можна налаштувати шаблони, які вже були створені
Розширюваність платформи	Розробник може інтегруватися з будь-якою корпоративною системою або записом	Не існує
Масштабованість	Корпоративний рівень	Обмежено користувачами відділу
Економічна ефективність	Економічно вигідно для компаній з наявною командою розробників	Економічно вигідно для компаній із завантаженою IT-командою або без IT-команди та високими вимогами

Джерело: розроблено автором на основі [3, 9].

Порівнюючи сфери застосування платформ, слід зазначити, що NCDP добре підходить для створення інтерфейсних програм, наприклад, UI, який отримує дані з різних джерел та генерує звіти та аналітику, реалізує імпорт/експорт даних.

Іншими прикладами є створення внутрішніх додатків, які позбавлені широкого спектру функціональних можливостей, або невеликих бізнес-програм із малим бюджетом на розробку. На противагу цьому, програми, створені на LCDP, можуть реалізовувати складну бізнес-логіку та розширюватися до рівня підприємства. Крім того, для інтеграції з іншими програмами та зовнішніми API, підключення до багатьох джерел даних і створення систем із комплексним захистом, LCDP є кращою альтернативою.

У контексті швидкості LCDP вимагає більше часу для навчання, адаптації, розробки та розгортання системи, оскільки вона пропонує більше можливостей для налаштування. Але це все одно значно швидше, ніж традиційна розробка. Розробка на NCDP, оскільки вона має широку конфігурацію та працює як «plug and play», займає менше часу порівняно з LCDP. Час тестування також скорочується, оскільки існує мінімальний ризик потенційних помилок, які зазвичай виникають під час ручного кодування.

Аналізуючи відкритість систем, LCDP дозволяє користувачам розширювати функціональність за допомогою кастомного коду, що надає їй більшої гнучкості та можливості багаторазового використання. Наприклад, користувачі можуть створювати власні модулі та конектори джерел даних у відповідності до власних варіантів використання, а потім застосовувати їх повторно.

Але слід відзначити, що оновлення платформи та модифікації слід тестувати з новим кастомним кодом. NCDP — більш закрита система, яку можна розширити тільки за допомогою шаблонних наборів функцій, що обмежує варіанти її використання. Проте у цьому випадку легше забезпечити зворотну сумісність, оскільки немає написаного вручну коду, який міг би зламати майбутні версії NCDP.

З архітектурної позиції підтримка масштабованості та кросплатформної сумісності є кращою у LCDP. Додавання користувацьких плагінів і власного коду відкриває можливість ширшого діапазону реалізацій і роботи з кількома платформами. NCDP має обмежений потенціал для підключення до застарілих систем або інтеграції з іншими платформами. Таким чином, він стосується

вузького набору варіантів використання та має знижену здатність до масштабування.

Висновки. У відповідь на мінливі вимоги ринку підприємства змушені стрімко змінювати власні бізнес-процеси, оскільки їх ефективність є вирішальною для успіху бізнесу. Використання класичних BPMS для автоматизації бізнес-процесів має низку недоліків, що перешкоджає швидкій цифровій трансформації. LCDPs та NCDPs стають в нагоді у разі створення користувацьких рішень у сфері управління бізнес-процесами, що надає компаніям безперечних переваг. Розробка BPMS або окремих додатків для автоматизації бізнес-процесів на таких платформах дозволяє істотно заощадити час та вартість проєктування, розробки, впровадження та їх модифікації. Та й взагалі, такий підхід до розробки може стати стандартом у майбутньому.

Рішення про вибір LCDP або NCDP для автоматизації бізнес-процесів має ґрунтуватися на визначенні поточних вимог до майбутньої системи. На це впливають: цілі використання платформи; особливості бізнес-користувачів та наявний досвід програмування; обсяг та масштаб задачі автоматизації або проблеми, яку треба вирішити; необхідність інтеграції створюваної системи із внутрішніми або зовнішніми програмами; час на розробку; необхідність роботи з конфіденційними даними та врахування аспектів інформаційної безпеки. Якщо сценарії використання складні, вимагають інтеграції з іншими локальними або хмарними програмами, висуваються вимоги, орієнтовані на клієнтів або критичні для бізнесу, або їх потрібно розгортати на всьому підприємстві, — кращим варіантом є NCDP. У цьому випадку, навіть якщо користувачі не мають необхідного досвіду в мовах програмування, партнерство з IT-командами або навчальні програми можуть вирішити ці проблеми.

Бібліографічні посилання

1. 2019 Gartner Critical Capabilities for Enterprise Low-Code Application Platforms: Key Takeaways. *Solutions Review*. URL: https://solutionsreview.com/business-process-management/gartner-critical-capabilities-for-enterprise-low-code-application-platforms-key-takeaways/

2. BPTrends State of Business Process Management — 2020 Report. *BPTrends.* URL: https://www.bptrends.com/bptrends-state-of-business-process-management-2020-report/

3. Difference Between Low-Code and No-Code Platform. *Kissflow*. URL: https://kissflow.com/low-code/low-code-vs-no-code/
4. How to Build a Low-Code BPM Strategy. *Pipefy*. URL: https://www.pipefy.com/blog/low-code-bpm-strategy/
5. Low-Code vs BPM Software: What's the Difference? *Tallyfy*. URL: https://tallyfy.com/low-code-bpm/
6. Low-Code Vs. BPM. *Kissflow*. URL: https://kissflow.com/low-code/low-code-vs-bpm/
7. Low-code vs. BPM: Are they comparable? *Decode.* URL: https://www.zoho.com/creator/decode/low-code-vs-bpm
8. Low-Code vs. No-Code Development. *Outsystems.* URL: https://www.outsystems.com/glossary/low-code-no-code/
9. Low-Code vs. No-Code Development. *Outsystems.* URL: https://www.outsystems.com/glossary/low-code-no-code/
10. Richardson C., Rymer J.R. New Development Platforms Emerge For Customer-Facing Applications. *Forrester:Cambridge*. MA. USA. 2014. URL: https://docplayer.net/28404932-New-development-platforms-emerge-for-customer-facing-applications.html
11. Ross M. 4 essential features of modern low-code development platforms. InfoWorld.com. URL: https://www.infoworld.com/ article/3287146/4-essential-features-of-modern-low-code-development-platforms.html
12. Rymer J. Vendor Landscape: A Fork in The Road for Low-Code Development Platforms. *Forrester*. URL: https://cdn2.hubspot.net/hubfs/-2096695/Vendor-%20Landscape_A%20Fork%20In%20The%20Road%20For%20Low_Code%20Development%20Platforms.pdf?submissionGuid=83c10178-9f4a-4980-8d27-2f20a0fcdaa1
13. Sambandam S. Where low-code development works—and where it doesn't. InfoWorld.com. URL: https://www.infoworld.com/article/3295882/where-low-code-development-works-and-where-it-doesnt.html
14. Srikanth R. P. Will Low Code platforms be the next Excel? *Express Computer*. URL: https://www.expresscomputer.in/columns/will-low-code-platforms-be-the-next-excel/29082/
15. Tisi M., Mottu J.-M., Kolovos D.S., Lara J., Guerra E., Ruscio D.D., Pierantonio A. and Wimmer M. Lowcomote: Training the Next Generation of Experts in Scalable Low-Code Engineering Platforms. *STAF 2019 Co-Located Events Joint Proceedings: 1st Junior Researcher Community Event, 2nd International Workshop on Model-Driven Engineering for Design-Runtime Interaction in Complex Systems, and 1st Research Project Showcase Workshop co-located with Software Technologies: Applications and Foundations (STAF 2019), Eindhoven, The Netherlands, July 15 — 19, 2019.* Volume 2405 of CEUR Workshop Proceedings. P 73-78. URL: http://ceur-ws.org/Vol-2405/13_paper.pdf
16. Top Application Development Trends in 2019. *Outsystems.* URL: https://www.outsystems.com/-/media/E0A6E7121AAD4A4C975828265B3639ED.ashx?mkt_tok=eyJpIjoi

T1RsbU56azNNakJsWVRaaiIsInQiOiIyNlBCdGlrRnVHclVEY2c3TWtSSEUwNWtTU3FBVVE0M2gwK0xoSW0xaktSZ3dWS2t6amQxOFU2WlFCRllwR256aUhMTHVWa0ROSnZrU2tRUlZ4cTV5RFJXb2o5Wlphc21jaFR4bXY4ZmU3U3BrTkFNMm1BZm9MWkNsRHg0YjlzayJ9

17. Yan. Z. The Impacts of Low/No-Code Development on Digital Transformation and Software Development. URL: https://www.researchgate.net/publication/357417399_The_Impacts_of_Low_No-Code_Development_on_Digital_Transformation_and_Software_Development

Статтю подано до редакції 22.11.2022

УДК: 005.8:004 DOI 10.33111/mise.102.10

Лазарєва С.Ф., к.е.н.,
професор кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Кордунов С.Ю., старший викладач
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана
Lazerieva S.F., Candidate of Economic Science,
Professor Department of Computer Mathematics and Information Security
KNEU named after V. Hetman

Kordunov S.Yu.,
Senior Lecturer, Department of Computer Mathematics and Information Security
KNEU named after V. Hetman

МОДЕЛЬ ПРОЄКТНОГО ОФІСУ В СИСТЕМІ УПРАВЛІННЯ ОРГАНІЗАЦІЄЮ

PROJECT OFFICE MODEL IN THE CORPORATE IT MANAGEMENT SYSTEM

Анотація. *Питання проєктного менеджменту останнім часом викликає значну увагу як науковців, так і практиків, що обумовлене набуттям ознак проєкту більшості видів економічної діяльності та пошуком шляхів підвищення ефективності. Метою статті є аналіз існуючих підходів до створення ОУП, їх типів та моделей на сучасному етапі розвитку проєктного менеджменту в умовах диджиталізації й посилення впливу інформаційних технологій і систем управління IT на прийняття рішень щодо стратегії розвитку організації, а також визначення того, до яких нових викликів слід готуватися проєктним офісам у майбутньому. Проаналізовано концепцію розвитку офісу управління проєктами (ОУП) і розглянуто найбільш поширені організаційні моделі ОУП. Також досліджено міжнародні стандарти управління проєктами, а саме — серія ISO 21500, а також стандарти де-факто PMBOK, PRINCE2, P2M та ін. Визначено та з'ясовано основні тренди розвитку ОУП та виклики, з якими стикаються організації в умовах цифрової революції та цифровізації. Встановлено основні сучасні еволюційні ознаки ОУП та розглянуто їх різновиди, напрями подальшого розвитку та перехід до моделі трансформації. Наведено ключові фактори щодо вибору моделі PMO, яка найкраще відповідатиме бізнес-стратегії та дозволить компанії отримати максимальну вигоду. З метою систематизації та поглиблення розуміння місця проєктного офісу в системі управління організацією проведено їх класифікацію.*

Ключові слова: *управління проєктами, офіс управління проєктами, управління портфелем, модель проєктного офісу, види проєктних офісів, трансформація проєктного офісу.*

Abstract. *The issue of project management has recently attracted considerable attention of both scientists and practitioners, which is due to the acquisition of project features of most types of economic activity and the search for ways to increase efficiency. The purpose of the article is to analyze the existing approaches to the creation of the PMU, their types and models at the current stage of the development of project management in the conditions of digitalization and the strengthening of the influence of information technologies and IT management systems on decision-making regarding the organization's development strategy, as well as to determine what new challenges should be faced to prepare for project offices in the future. The article analyzes project management office (PMO) development concept and considers the most common PMO organizational models. Project management international standards, i.e., the ISO 21500 series, as well as the de facto standards of PMBOK, PRINCE2, P2M, etc. were analyzed too. The main PMO development trends and the challenges faced by organizations in the conditions of the digital revolution and digitization have been identified and clarified. The key modern evolved PMO features are defined and their varieties, further development directions and the transition to a transformation model are considered. Key factors regarding the choice of the PMO model, which will fit the business strategy best and will allow company to get the maximum benefit, are given. In order to systematize and deepen the understanding of the place of the project office in the management system of the organization, their classification was carried out.*

Keywords: *project management, project management office, portfolio management, project office model, types of project offices, project office transformation.*

Постановка проблеми у загальному вигляді. Сучасний етап розвитку систем управління економічними об'єктами можна назвати етапом бурхливого розвитку технологій не лише технічних, а й гуманітарних технологій загального менеджменту і проєктного зокрема.

Передумовою розвитку концепції проєктного менеджменту є створенням організацій, діяльність яких, розвиток і зміна діяльності може бути представлена як сукупність різних проєктів, що забезпечують досягнення стратегічних цілей організації. Такі організації стають більш конкурентоспроможними порівняно з підприємствами, які мають функціональну організацію діяльності. Разом із тим досягнення очікуваних переваг у разі переходу до проєктно-орієнтованого управління наражається на необхідність розв'язання цілої низки проблем, пов'язаних із затримкою проєктів, їх невідповідністю якості та специфікаціям, перевищенням витрат та ін., а також пошуком способів уникнення конфліктів між проєктами, покращення використання ресурсів, узгодження з цілями організації.

Одним з організаційних рішень для розв'язання цих проблем є створення в системі управління компанією спеціальної структури для надання підтримки керівникам проєктів.

Аналіз останніх досліджень і публікацій. Питання проєктного менеджменту останнім часом викликає значну увагу як науко-

вців, так і практиків, що обумовлене набуттям ознак проєкту більшості видів економічної діяльності та пошуком шляхів підвищення ефективності.

Бурхливе поширення ідей проєктного менеджменту розпочалось від 1990-х років, коли професійні стандарти та сертифікати з управління проєктами стали визнаними галузевими стандартами. У середовищі науковців і практиків набули популярності такі стандарти де факто, як Project Management body of Knowledge (PMBOK Guide), 5–7 видання [1, 2, 3] і Project Management Competence Development Framework [4], розроблені Американським Інститутом управління проєктами (Project Management Institute — PMI); методологія управління проєктами PRINCE/PRINCE2 (Projects In Controlled Environents), розроблена Управлінням урядових комерційних проєктів Великобританії [5]; Individual Competence Baseline for Project, Programme & Portfolio Management (ICB-4.0) [6], розроблені Міжнародною асоціацією управління проєктами (International Project Management Association — IPMA; рамкові стандарти практичної компетентності проєктних менеджерів категорії GL1 і GL2 [7], розроблені Міжнародним об'єднанням з розробки Стандартів управління проєктами (Global Alliance for Project Performance Standards — GAPPS); Керівництво з управління інноваційними проєктами і програмами організацій (P2M) [8], розроблене Японською асоціацією управління проєктами (Project Management Association of Japan — PMAJ), та ін.

Відносно недавно технічним комітетом Міжнародної організації зі стандартизації ISO/TC 258, «Project, programme and portfolio management» була розроблена серія стандартів ISO 21500, зокрема стандарт ISO 21500:2021 «Управління проєктами, програмами та портфоліо — контекст і концепції» [9], який разом із ISO 21502:2020 [10] скасовує та замінює 1 видання (ISO 21500:2012 «Керівництво по управлінню проєктами»), яке було технічно переглянуте. Оновлена версія стандарту містить огляд середовища для управління проєктами, програмами та портфелями, управління ними та загальні фактори, що впливають на ширше середовище. Цей документ дає загальне уявлення про взаємозв'язки між стандартами щодо управління проєктами, програмами та портфоліо. Подальші вказівки щодо управління проєктами, програмами та портфоліо, а також керування ними наведені в таких стандартах: ISO 21502:2020 Project, programme and portfolio management — Guidance on project management; ISO 21503:2022 Project, programme and portfolio management —

Guidance on programme management; ISO 21504:2022 Project, programme and portfolio management — Guidance on portfolio management та ISO 21505:2017(en) Project, programme and portfolio management — Guidance on governance.

Саме стан розвитку методології проєктного менеджменту і потреба створення скоординованого і стандартизованого підходу до управління проєктами всередині організації стали ключовим фактором створення, розвитку та поширення сучасної концепції офісу управління проєктами (ОУП) / Project Management Office (PMO).

Невирішені раніше частини загальної проблеми. На сьогодні об'єктом гарячих дискусій у галузі управління проєктами є офіс управління проєктами ОУП/PMO. Що це за структура? Які її основні цілі, завдання, функції? Які типи і моделі ОУП існують. Чим вони відрізняються? Де він має бути розміщений в організації? І взагалі, наскільки потрібний такий підрозділ для проєктно-орієнтованої організації? Як вибрати модель офісу, що відповідає потребам організації?

Основною метою статті є аналіз існуючих підходів до створення ОУП, їх типів та моделей на сучасному етапі розвитку проєктного менеджменту в умовах диджиталізації й посилення впливу інформаційних технологій і систем управління ІТ на прийняття рішень щодо стратегії розвитку організації, а також визначення того, до яких нових викликів слід готуватися проєктним офісам у майбутньому.

Для цілей цієї статті під моделлю проєктного офісу будемо розуміти структуру, створену в межах організації для реалізації проєктів і надання послуг.

Така структура може бути подана через єдиний постійний офіс (наприклад, Офіс управління проєктами) або через кілька взаємопов'язаних офісів (Портфельні, Програмні та Проєктні), як постійних, так і тимчасових, поєднуючи як централізовані, так і локалізовані послуги. Це своєрідний центр прийняття рішень щодо проєктів і бізнес-змін в організації [11].

Виклад основного матеріалу дослідження. Ефективне функціонування проєктно-орієнтованої організації неможливе без створення системи управління проєктами. У свою чергу для системного використання проєктного управління необхідний спеціальний підрозділ — офіс управління проєктами (ОУП), який буде розвивати корпоративну методологію управління проєктами.

У контексті 6 і 7 видання стандарту де факто з проєктного менеджменту PMBOK [2, 3] ОУП розглядається як структура

управління, яка стандартизує процеси управління проєктами та сприяє спільному використанню ресурсів, методологій, інструментів і методів, а також бере участь в узгодженні роботи за проєктом зі стратегічними цілями організації, зокрема, залучення та співпраця зі стейкхолдерами, отримання цінності від інвестицій у проєкти тощо. За змістом ця організаційна структура централізує, координує та контролює управління проєктами та програмами, хоча може і відрізнятися як за назвою, так і за функціями в різних організаціях і навіть усередині однієї організації.

З метою систематизації та поглиблення розуміння місця проєктного офісу в системі управління організацією доцільно провести їх класифікацію. Класифікація дозволить досліджувати виконувані ним функції, й на основі цього побудувати відповідні моделі проєктного офісу для кожної з груп.

Слід зазначити, що класифікація ОУП є одним з найбільш дискусійних питань серед проєктних менеджерів та команд. Єдиного офіційного стандарту чи шаблону, що визначає, який саме тип ОУП повинен впроваджуватись в організації, немає. Існують різні способи класифікації ОУП залежно від рівня контролю над проєктами, зрілості проєктного менеджменту в компанії, а також від організації, яка, власне, ці типи виокремлює.

Одним із найпоширеніших підходів є класифікація ОУП за такими ознаками:

1) вплив на проєкти, що виконуються в організації; та

2) позиція, яку вони займають в організації [1, 13].

За першою ознакою виділяють такі типи ОУП: Допоміжний (Supportive); Контролюючий (Controlling); Директивний (Directive).

Розглянемо відмінності кожного із них.

Допоміжний (*Supportive*) *ОУП* виконує консультативну роль у проєктах, надаючи шаблони, найкращі практики, тренінги, доступ до інформації та уроків, отриманих з інших проєктів. Такий ОУП має низький рівень контролю над проєктами і здебільшого працює як база знань і репозиторій даних, надаючи необхідну підтримку і навчання членам проєктних команд.

Місце допоміжного ОУП в системі управління організацією наведено на рис. 1.

Контролюючий (*Controlling*) *ОУП* здійснює різними засобами підтримку та помірний контроль за відповідністю прийнятій в організації методології управління проєктами. Відповідність може передбачати контроль використання конкретних шаблонів, форм, методів та інструментів тощо.

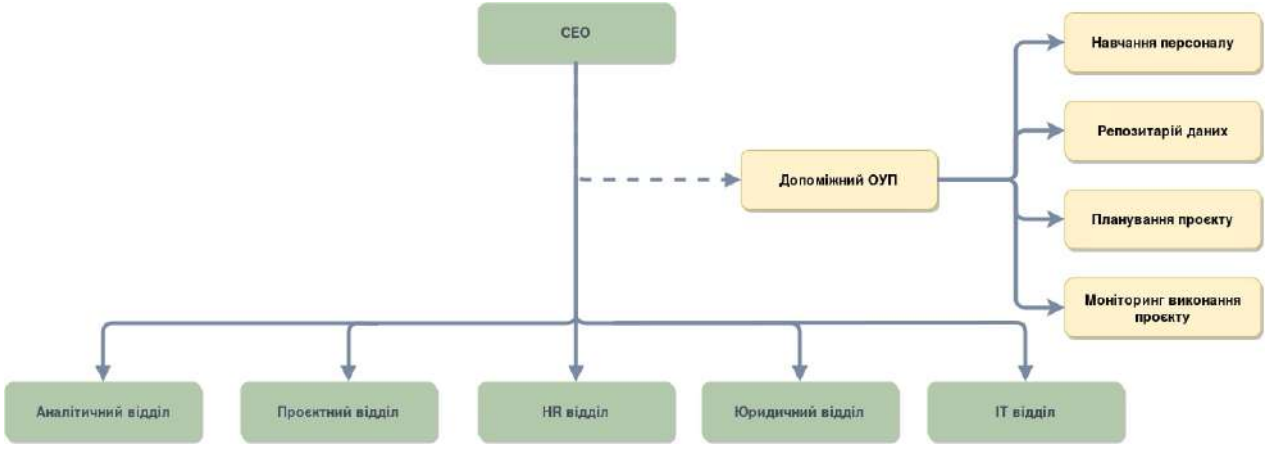


Рис. 1. Місце допоміжного ОУП в організаційній моделі підприємства

Джерело: розроблено авторами.

Рис. 2. Місце контрольного ОУП в організаційній моделі системи управління підприємством

Джерело: розроблено авторами.

Контролюючий ОУП впроваджується в організаціях, які хочуть мати вищий рівень дисципліни щодо всіх дій, процедур, методів, документації, пов'язаних зі своїми проєктами. Контролюючий ОУП може виконувати ті ж функції, що й допоміжний ОУП, але, маючи вищий рівень контролю над проєктами, також забезпечує дотримання і виконання певних організаційних практик, вказівок і методів, що узгоджені у статуті проєкту. У такий спосіб відбувається контроль над дотриманням нормативних вимог та використанням стандартизованої методології членами проєктних команд.

Місце ОУП з контрольними функціями в організаційній моделі системи корпоративного управління наведено на рис. 2.

Директивний (*Directive*) *ОУП* бере під контроль проєкти, безпосередньо керуючи ними. Маючи повний контроль над проєктами, директивний ОУП часто безпосередньо бере участь у контактуванні з клієнтами, стейкхолдерами, а також звітує напряму вищому керівництву компанії. Завдяки цьому досягається високий рівень узгодженості між проєктами. Разом з тим директивний ОУП розділяє всі ризики і несе повну відповідальність за результат виконання проєкту. Основною метою впровадження директивного ОУП є гарантування найвищого рівня послідовності практики управління проєктами в усіх проєктах, зменшення витрат шляхом централізації проєктних послуг, пряме призначення менеджерів проєктів, які стають важливою частиною планування та управління проєктами організації протягом усього життєвого циклу з точки зору ресурсів, бюджету та часових рамок.

Приклад директивного ОУП в організаційній моделі корпоративного управління зображено на рис. 3.

Як розглянуті вище типи ОУП пов'язані з рівнем зрілості проєктного менеджменту в організації подано на рис. 4.

За другою ознакою — позиція, яку ОУП займають в організації, виділяють такі типи проєктних офісів: Індивідуальний (Individual); Департаментський (Departmental); Корпоративний (Corporate).

Розглянемо особливості кожного з них.

ОУП Індивідуального (*Individual*) типу, або «Project Management Office — PMO», зазвичай надає функціональну підтримку (наприклад, інфраструктуру, управління документами, навчання тощо) окремому комплексному проєкту чи програмі. Вони встановлюють базові стандарти та здійснюють нагляд за діяльністю з планування та контролю для окремого проєкту.

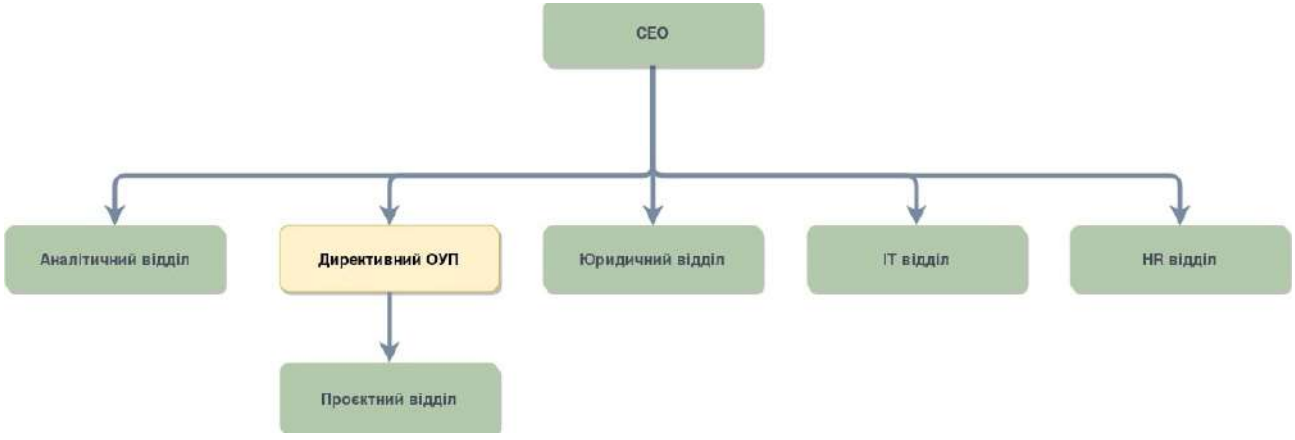


Рис. 3. Місце директивного ОУП в організаційної моделі підприємства

Джерело: розроблено авторами.

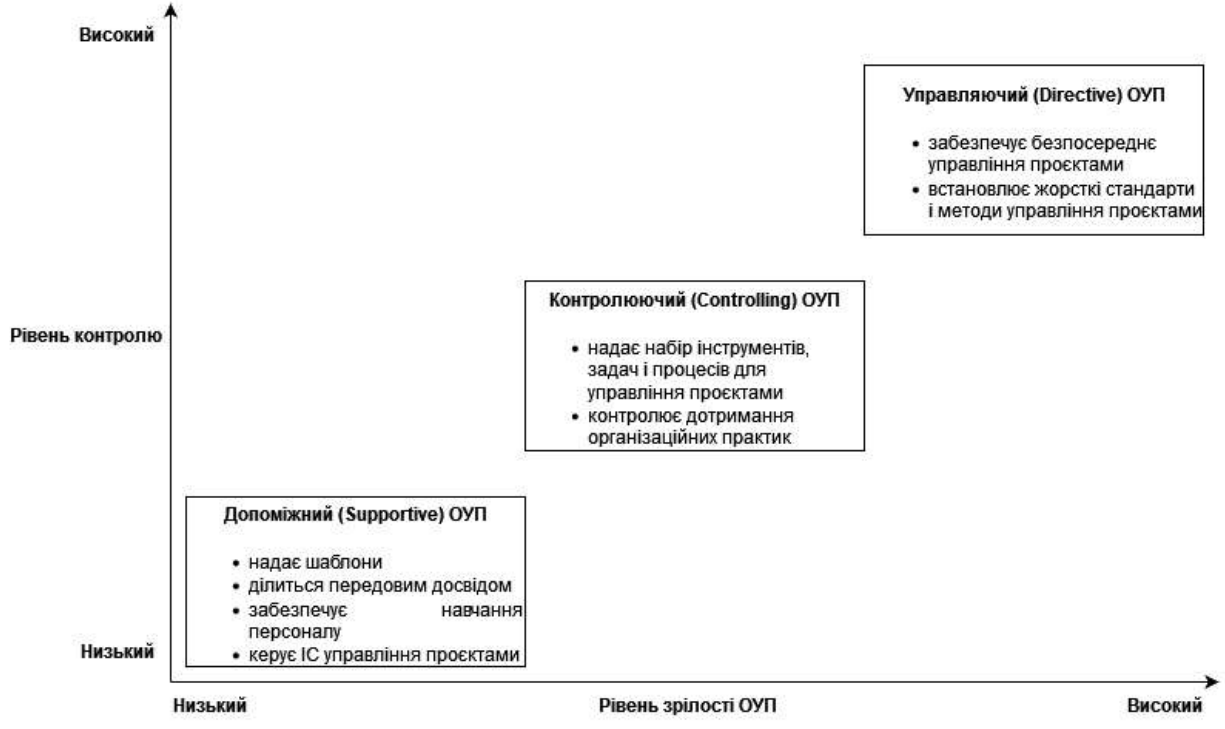


Рис. 4. Типи ОУП залежно від рівня зрілості та контролю над проєктами в організації

Джерело: розроблено авторами.

Департаментський (*Departmental*), або «Business Unit PMO», *ОУП* підтримує кілька проєктів на рівні відділу чи бізнес-підрозділу. Їхнє головне завдання полягає в тому, щоб інтегрувати проєкти різного розміру в рамках підрозділу (наприклад, IT, фінанси) від невеликих короткострокових ініціатив до багаторічних програм із багатьма ресурсами та комплексною інтеграцією технологій.

Корпоративні (*Corporate*), або «Enterprise PMO», офіси створюють стандарти, процеси та методології для покращення ефективності проєктів в організації, зазвичай відповідають за розподіл ресурсів на різні проєкти.

У табл. 1 наведено, яка головна мета створення кожного з зазначених типів ОУП.

Таблиця 1

МЕТА ОУП СТВОРЕНИХ ЗА ОЗНАКОЮ: ПОЗИЦІЯ В ОРГАНІЗАЦІЇ

№	Тип ОУП	Мета створення
1	Індивідуальний (Individual)	Підтримка управління окремими проєктами
2	Департаментський (Departmental)	Підтримка управління проєктами одного функціонального підрозділу
3	Корпоративний (Corporate)	Підтримка управління усіх проєктів компанії

У роботі [16] автори зазначають, що здебільшого ОУП скеровують роботу в одному з двох напрямів: зменшення витрат або підвищення продуктивності під час виконання проєктів.

Перший підхід спрямований на ефективне використання ресурсів і контроль виконання бюджетів. Основним способом розв'язання проблем управління проєктів за цього підходу є посилення контролю та жорстке дотримання існуючих стандартів. ОУП більшу частину своїх зусиль витрачає на збір інформації й використання владних повноважень для покарання порушників.

Другий підхід націлений, насамперед, на істотне скорочення тривалості виконання проєктів, забезпечення можливості виконання їх більшої кількості і формування портфеля проєктів, що найкраще відповідає цілям і завданням організації. У результаті опосередковано також відбувається скорочення зайвих проєктних витрат завдяки зменшенню кількості неефективних проєктів.

У рамках зазначених вище двох основних підходів автори виділяють чотири моделі побудови й функціонування ОУП:

1. *ОУП-Репозиторій* (у цій моделі в результатах роботи офісу відсутня взагалі або слабо виражена економічна складова). За цієї моделі ОУП, слугує сховищем і джерелом інформації про проєкти, методи й стандарти управління проєктами. Ця модель припускає наявність на підприємстві комплексу погоджених між собою методів і засобів виконання проєктів, управління ними й звітності. Така модель найчастіше застосовується на підприємствах з розподілом владних функцій, слабким центральним управлінням або у разі закріплення за підрозділами відповідальності за виконувані проєкти.

2. *ОУП-Наставник* (тактична модель роботи ОУП, що здатний протягом короткого часу приносити деяку економію витрат). Ця модель є розвитком моделі репозиторію й відображає наміри підприємства поширювати серед своїх функціональних служб і підрозділів методологію управління проєктами, причому ОУП приділяється роль координуючого центру комунікацій між ними. Він відповідає за документальне оформлення передового досвіду й активний моніторинг ходу виконання й характеристик проєктів. За моделі наставника обов'язковою є підтримка вищого керівництва, яке є головним споживачем його послуг. Інакше ОУП приречений завжди перебувати на других ролях.

3. *ОУП підприємства* (стратегічна модель, орієнтована на встановлення централізованого контролю за всіма основними проєктами). За цієї моделі ОУП зосереджує у своїх руках у найбільш концентрованій формі всю роботу з експертизи й оцінювання управління проєктами, має чітко встановлені цілі, задачі й права, а також підтримку з боку керівництва. Реалізація цієї моделі вимагає значно більших інвестицій. Найчастіше в рамках цієї моделі ОУП займається збором даних, необхідних для формування портфеля проєктів підприємства й утримує інформацію про всі важливі проєкти, запуск яких санкціонований керівництвом, здійснює управління проєктними ризиками в процесі ініціації й виконання проєктів, відіграє провідну роль в управлінні багатьма, одночасно виконуваними проєктами, виявляючи й усуваючи вузькі місця, по цих проєктах. Отже, на підприємстві реалізується модель «розподіленого обслуговування проєктів».

4. *ОУП, націлений на негайний результат* (стратегічна модель ОУП, орієнтована на підвищення продуктивності при виконанні проєктів, на скорочення тривалості їхнього виконання, на правильний вибір змісту портфеля проєктів. Забезпечує високу еконо-

мічну ефективність офісу). За цієї моделі ОУП орієнтований на всі проєкти організації, на ув'язування проєктів з її цілями та стратегією. Фактично, ОУП за цієї моделі, орієнтований не лише на реалізацію проєктів, а й насамперед на підтримку менеджменту у розв'язанні бізнес-завдань і досягненні стратегічних цілей компанії.

Розглянемо ще один підхід, що заслуговує на нашу увагу. Компанія Gartner, яка є одним із лідерів галузі консалтингу та IT-досліджень, виділяє такі типи ОУП [13]:

• **ОУП Активіст** (Activist PMO). За цієї моделі основною функцією ОУП є перевірка бізнес-кейсів та проєктних пропозицій, інформаційна підтримка тих, хто приймає рішення щодо проєктів, та нагляд за ходом виконання проєктів.

• **ОУП Доставки** (Delivery PMO) також відомий як офіс проєкту. Такий офіс здійснює планування та контроль виконання проєкту відповідно до очікувань бізнесу. Його задачею також є створення повторюваних процесів і методів, які працюватимуть для створення культури, орієнтованої на результати. Офіси цього типу є найпоширенішими. За даними Gartner, принаймні 40 % є головним чином ОПУ з доставки.

• *ОУП Відповідності* (Compliance PMO). За цією моделлю основним завданням ОУП є встановити стандартні практики для вимірювання ефективності проєктів та розвитку здатності розуміти статус ключових ініціатив в організації. Ця модель найбільш прийнятна для організацій з низьким рівнем зрілості проєктного менеджменту, де документація, процеси, процедури та методології відсутні або непослідовні.

• *ОУП Централізований* (Centralized PMO) створюється як місце, де нових співробітників можна швидко ознайомити з тим, як найкраще виконувати проєктну роботу в організації. Створений за цією моделлю ОУП є методичним центром для поширення та обміну передовим досвідом управління проєктами. Його завдання підвищити рівень зрілості проєктного менеджменту в організації, встановити надійні процеси для відстеження проєктів та звітності.

Підхід, що дістав назву «Офіс портфоліо, програм і проєктів» і відомий під абревіатурою P3O (Program Portfolio Project Ofice), розроблений Управлінням урядової торгівлі UK [14], має на меті допомогти організаціям побудувати структури підтримки, які забезпечать успішну реалізацію їхніх портфоліо програм і проєктів змін. P3O може бути одним або кількома пов'язаними офісами,

які виконують стратегічні функції, функції контролю та забезпечення.

РЗО описує фактори, які впливають на проєктування та побудову правильних структур для оптимізації прийняття рішень вищим керівництвом. Модель РЗО включає:

Проєктні, або програмні, офіси — тимчасові офіси, які в основному займаються управлінням виконанням конкретного проєкту(ів).

Портфельний офіс, або Центр передового досвіду (Center of excellence/CoE), — постійний офіс із наглядом за всіма проєктами / програмами в межах відділу / секції бізнесу, включаючи управління інвестиціями та стандарти, управління знаннями, навчання персоналу (CoE).

Корпоративний РМО (Enterprize PMO/ePMO) — постійний офіс, який контролює всі проєкти та програми в межах усього бізнесу та може виступати як Центр передового досвіду для встановлення стандартів на рівні підприємства.

На рис. 5 представлено високорівневу модель РЗО.

Рис. 5. Високорівнева модель РЗО

Джерело: [14].

В основу моделі проєктного офісу покладено три базові елементи / функціональні області [14]:

– Функції / послуги стратегічного планування або підтримки портфеля — вони зосереджені на підтримці управлінських рішень і можуть включати узгодження зі стратегією, визначення пріоритетів, управління реалізацією вигід, звітування через інформаційні панелі управління тощо.

– Функції / послуги підтримки доставки — вони зосереджені на підтримці впровадження змін і можуть надаватися через центральний гнучкий пул ресурсів персоналу доставки з плануванням потужностей і процесами управління персоналом.

– Функції Центру передового досвіду послуг — вони зосереджені на розробці стандартних методів і процесів, розробці послідовних робочих практик і забезпеченні їх належного застосування.

Сучасний етап часто називають ерою цифрової революції. Ця ера розпочалася у 1990-х роках і досі триває. Нині кожна організація, в якій би галузі вона не працювала, якщо хоче бути конкурентоспроможною, повинна мати рівень інформаційних технологій із акцентом на інноваційних та творчих технологіях. Це спонукає організації підтримувати цифрові/інформаційні технології. У результаті, ІТ-проєкти та програми набувають більшої актуальності, ніж у минулому. Для них організації відволікають від звичайної та функціональної діяльності значні ресурси. Тому ці проєкти мають бути правильно розставлені за пріоритетами та повністю узгоджені зі стратегією організації. Крім того, у сучасному стрімкому бізнес-середовищі організації постійно змушені пристосовуватися до мінливих ринкових умов і, відповідно, мають швидко реагувати на зміну бізнес-пріоритетів.

Тому вага і вплив ОУП стають все більш значущими у прагненні організацій підвищити конкурентоспроможність у мінливому диджиталізованому світі.

На рис. 6 показано вплив цифрової революції на еволюцію ОУП.

Щоб залишатися актуальними та розширювати свій вплив в організації, ОУП мають розвивати нові можливості. Такі удосконалені / розвинені ОУП також можуть бути різноманітними залежно від, наприклад, галузі, виду діяльності, масштабу організації, ступеня інтеграції ІТ в основні операційні процеси, рівня організаційної зрілості менеджменту в компанії та, зокрема, стратегічного планування тощо.

Рис. 6. Від цифрової революції до «розвиненого» ОУП

Джерело: [12].

Не зупиняючись на детальному аналізі різних підходів до класифікації розвинених PMO, зазначимо, що один із найбільш вдалих і системних підходів, на нашу думку, є підхід, запропонований в роботі [12]. За цим підходом ключовими для удосконаленого / розвиненого ОУП є характерними такі ознаки: підтримка; стратегічне планування; центр передового досвіду; диджиталізація / інновації; вирівнювання до стратегії; гнучкість.

На нашу думку, варто доповнити цей перелік такими характеристиками, як лідерство, культура безперервного навчання й економне управління портфелем проєктів.

Основою ***лідерства*** є бачення вищим керівництвом переваг, які приносить проєктний офіс для компанії.

Культура безперервного навчання має бути спрямована на те, щоб дати співробітникам можливість досліджувати та розкривати майбутні цінності, постійно вдосконалювати рішення, процеси і продукти.

Економне управління портфелем означає оптимізувати роботу в портфелі проєктів через встановлення пріоритетів у фінансуванні та виконанні саме тим проєктам, які додають цінності бізнес-пріоритетам.

Ключові можливості різних моделей ОУП представлено у табл. 2.

Таблиця 2

ПОРІВНЯННЯ КЛЮЧОВИХ МОЖЛИВОСТЕЙ РОЗВИНЕНОГО ОУП З ІНШИМИ МОДЕЛЯМИ

Можливості / Модель ОУП	Підтримка (Delivery Support)	Стратегічне планування (Strategic Planning)	Центр передового досвіду (Centre of Excellence)	Діджиталізація/інновації (Digital/Innovation)	Вирівнювання до стратегії (Alignment to Strategy)	Гнучкість (Agility)	Лідерство (**Leadership**)	Культура безперервного навчання (**Continuous-Learning Culture**)	Економне управління портфелем (**Lean Portfolio Management**)
Традиційний (Traditional PMO)	+								
Сучасний (Modern PMO)	+	+	+						
PMO 2.0	+	+	+	+	+				
Розвинений (Evolved PMO)	+	+	+	+	+	+	+	+	+

Джерело: адаптовано на основі [12, 15].

За класифікацією, запропонованою в [15], група розвинених ОУП також не є однорідною, і розділяється залежно від домінування тієї чи іншої характеристики на цифрові ОУП, корпоративні ОУП та гнучкі ОУП.

Цифрові (Digital) PMO — це ОУП, які мають можливість надавати інформацію про проєкти будь-якій зацікавленій стороні в будь-який час, з будь-якого місця. Цифрові ОУП використовують нові технології для полегшення співпраці та обміну інформацією всередині та за межами команд проєкту. Це обробка даних у режимі реального часу, доступна у форматі, зручному для Інтернету та мобільних пристроїв.

Корпоративні (Corporate) ОУП — це централізоване та скоординоване управління програмами та/або проєктами для досягнення стратегічних переваг і цілей. Вони створюються на корпоративному / стратегічному рівні та мають повноваження ініціювати / визначати пріоритети проєктів з корпоративної точки зору.

Маючи підтримку керівництва, ОУП підприємства впливають на стратегію, керують ключовими ініціативами та контролюють зміни в організації. Порівняно з традиційними ОУП, корпоративні ОУП виконують стратегічну місію в організації.

Гнучкі (Agile) ОУП використовує гнучкі інструменти звітності та проактивні моделі управління для підтримки гнучких проєктів в організації. Вплив гнучкого мислення виходить за рамки визначення конкретних тактичних практик, гнучкі ОУП більш готові швидко адаптуватися до змін у потребах бізнесу та вимогах проєкту / програми, ніж традиційні ОУП.

Ключовими атрибутами гнучкого ОУП є: швидке реагування на зміни, щоб зберегти зосередженість на результатах і перевагах у бурхливій економіці; балансування гнучкості і стабільності; відстеження та контроль продуктивності проєкту на основі гнучких показників.

Гнучкі практики заохочують проєктні команди постійно перевіряти свою діяльність і ефективно реагувати на зміни замість виконання попередньо встановленого довгострокового плану.

Необхідність трансформації ОУП тісно пов’язана з посиленням тиску зовнішнього бізнес-середовища на організації, що змушує їх часто змінювати пріоритети, використовувати новітні технології, шукати шляхи для прискорення та підвищення віддачі від своїх проєктів та ініціатив. У результаті ОУП має переключити увагу з виконання проєкту, керованого методологією, на бізнес-результати, орієнтовані на цінність, гнучкість і постійне вдосконалення діяльності. Драйвери еволюції ОУП зазвичай пов’язані з такими ключовими потребами:

- розвиток здатності і навичок для розвитку;
- швидке реагування на виклики;
- інноваційність проєктів, що реалізуються.

Швидкі інновації є критично важливими особливо для тих компаній, чия бізнес-стратегія орієнтована на цифрові технології. Тому багато далекоглядних ОУП зробили головним пріоритетом впровадження гнучких (Agile) методів і розширення своїх можливостей для досягнення очікуваного значного підвищення вартості / цінності.

Завдання полягає в переході від застарілої моделі ОУП, що відстежує проєкти, до ОУП, орієнтованого на бізнес-результат, а далі до гнучкого «трансформаційного ОУП», орієнтованого на клієнта. Такий перехід вимагає застосування нових структур, методологій та інструментів співпраці, а також значні інвестиції в навчання людей і впровадження гнучкого мислення в масштабах підприємства. На рис. 7 проілюстровано процес трансформації ОУП.

Причини створення ОУП в організації можуть бути різними, але основною метою завжди залишається отримання вигоди через покращення управління проєктами з погляду розкладу, вартості, ризиків та отримання цінності від інвестицій у проєкти.

Що ж до підпорядкування, воно може бути різним, залежно від основних завдань, що стоять перед таким підрозділом. Наприклад, якщо це лише створення єдиної методології, то, швидше за все, підпорядкування має бути в рамках директора з розвитку (CBDO / Chief Business Development Officer). Якщо це контрольні функції конкретного напряму, то ОУП підпорядковується відповідному заступнику, що курирує цей напрямок. Наприклад, у разі IT це може бути IT-директор (CIO / Chief Information Officer). А якщо завданнями ОУП є питання портфельного управління чи контролю всіх проєктів організації, тоді він підпорядковується, зазвичай, першій особі — виконавчому директору (CEO / Chief Executive Officer).

Для правильної побудови організаційної структури та підпорядкування ОУП потрібно чітко уявляти два моменти: основні функції підрозділу й основні споживачі інформації.

Яку ж модель краще вибрати? На вибір моделі ОУП впливає багато чинників і перш за усе це:

– рівень організаційної зрілості загального менеджменту і проєктного зокрема;

– організаційна структура управління, підпорядкування та розподіл повноважень;

– усвідомлення вищим керівництвом та іншими учасниками проєктної діяльності місії, завдань і функцій, що мають бути покладені на ОУП;

– розуміння того, хто є стейкхолдерами і основними споживачами послуг проєктного офісу;

– готовність керівників окремих функціональних підрозділів вибудовувати спільну роботу з ОУП;

– стан технічного, фінансового і фахового (наявність навченого персоналу) забезпечення проєктного офісу;

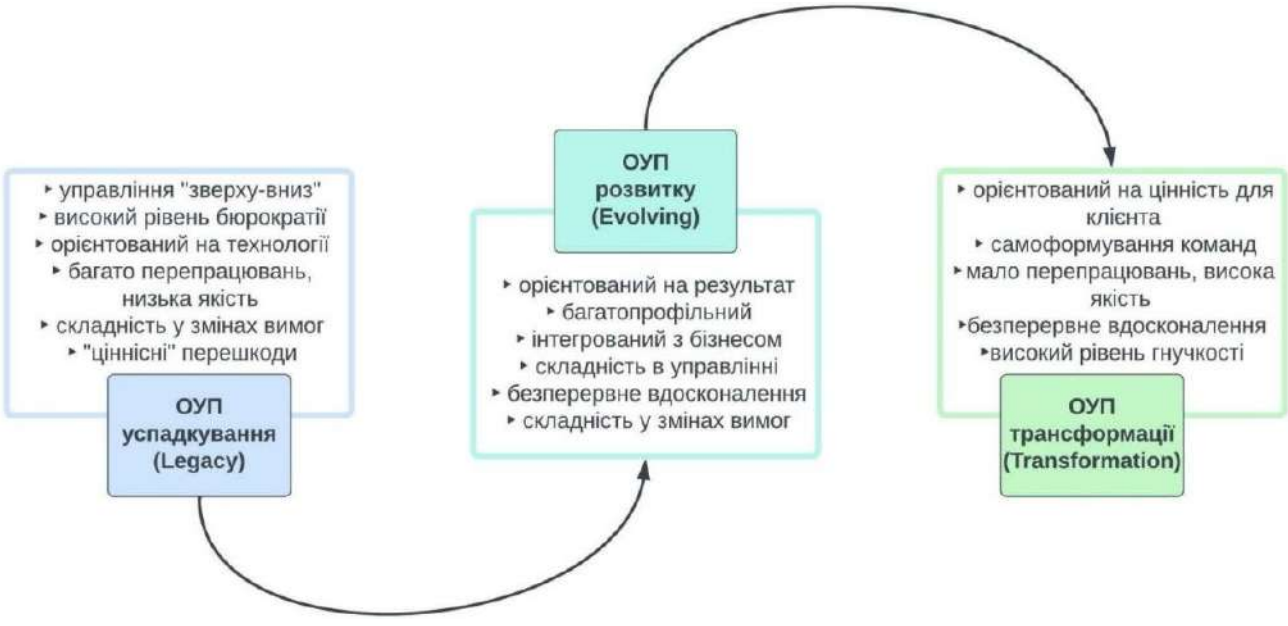


Рис. 7. Шлях трансформації ОУП

Джерело: [15].

– типи ключових проблем у галузі проєктного менеджменту в організації та «рівномірність» їх прояву в проєктах компанії;

– рівень компетенцій, лідерських якостей, авторитетності керівника ОУП та наявність кваліфікованих фахівців, здатних розв'язувати неординарні проблеми під час управління кризовими проєктами.

– Найкращим типом ОУП буде той, який зможе забезпечити підтримку потреб і задач компанії, на тому рівні, який вона може охопити й отримати максимальну вигоду.

Висновки та перспективи подальших досліджень. Розвиток концепції ОУП є одним із сучасних трендів розвитку проєктного менеджменту. Аналіз найпоширеніших організаційних моделей ОУП показав, що:

– сучасний ОУП стає більш стратегічним і для цього зміцнює зв'язки з вищим керівництвом, бере участь у стратегічному плануванні та, як наслідок, несе відповідальність за реалізацію стратегічних цілей. З організаційної позиції найбільш вигідно, якщо ОУП створюється як виконавчий відділ із прямим доступом до вищого керівництва;

– ОУП розширює рівень впливу на результативність організації, відходить від створення виключно стандартів з проєктного менеджменту і формування звітів по проєктах. Разом із керівниками груп і менеджерами проєктів бере на себе координацію використання ресурсів, розподілу їх між проєктами з урахуванням їх пріоритетності з погляду стратегічних цілей;

– посилює участь в управлінні портфелем проєктів, бере участь у прийнятті рішень щодо припинення неефективних проєктів. Цілеспрямована відмова та зупинка таких проєктів дозволить вчасно звільнити співробітників для проєктів з вищим пріоритетом;

– розвиває гнучке використання методів проєктного управління. Здійснює індивідуальне керівництво та підтримку для керівників проєктів у традиційних, гнучких або гібридних процесах і методах. Перспективним є не лише застосування гнучких методів управління, а й створення гібридних і гнучких робочих середовищ, правильно поєднуючи віддалену роботу і роботу на робочому місці;

– здійснює належне управління навичками персоналу, бере участь у формуванні проєктних команд, проводить навчання проєктних менеджерів для їх активного залучення до стратегічно цінних проєктів;

– застосовує передові практики, методології та методи проєктного менеджменту; використовує сучасні інструменти проєктного менеджменту, зокрема «хмарні» рішення, для управління проєктними командами, а саме ремоут-командами;

– активно інтегрує цифрову трансформацію в власну організаційну модель, що розширює можливості ОУП робити прямий внесок в стратегію розвитку підприємства, підвищує статус у системі управління, дає можливості і вивільняє персонал для виконання роботи більш цікавими методами. Завдяки цифровій трансформації процеси спрощуються, а ресурси звільняються, більше людей хочуть робити більше речей новими та цікавими способами, а ОУП стає інтелектуальним лідером в баченні можливостей підвищення вартості / цінності організації.

– ОУП стає драйвером для привнесення змін. Управління змінами є ключовим фактором успіху проєктів у майбутньому, що у свою чергу ставить нові завдання перед ОУП, перетворюючи його в офіс управління трансформаціями.

Питання, які, на нашу думку, є проблемними і потребують подальшого дослідження, стосуються визначення подальших напрямів трансформації та використання нових інструментів управління проєктами через диджиталізацію ОУП.

Бібліографічні посилання

1. A Guide to the Project management body of knowledge (PMBOK® guide) — Fifth edition. Newtown Square, Project Management Institute. (2013).
2. A Guide to the Project management body of Knowledge (PMBOK guide) Sixth edition Newtown Square, PA: Project Management Institute, 2017.
3. A Guide to the Project management body of Knowledge (PMBOK guide) Сьоме видання Newtown Square, PA: Project Management Institute, 2021. 216 с. Переклад укр. із залученням волонтерів та експертів громадського представництва PMI Ukraine та міжнародної служби перекладів «Філін». Спонсор підготовки українського перекладу до публікації Intellias.
4. Cartwright, C.&Yinger, M. (2007). Project management competency development framework—second edition. Paper presented at PMI® Global Congress 2007—EMEA, Budapest, Hungary. Newtown Square, PA: Project Management Institute.
5. Susan Tuttle. PRINCE2 in Action: Project management in real terms. ITGP (April 12, 2018). 254 p.

6. Individual Competence Baseline for Project, Programme & Portfolio Management — ICB v.4.2018 p.
7. GAPPS (2006) A Framework for Performance Based Competency Standards for Global Level 1 and 2 Project Managers Sydney: Global Alliance for Project Performance Standards, 55 p. URL: https://www.projectmanagement.com/content/attachments/Primus1_20101102 3434.pdf (дата звернення: 26.11.2022)
8. Керівництво з управління інноваційними проєктами і програмами організацій: Монографія. Пер. укр. під ред. проф. Ф. О. Ярошенка. Київ: Новий друк, 2010. 160 с.
9. ISO 21500:2021. Project, programme and portfolio management — Context and concepts. URL: https://www.iso.org/standard/75704.html (дата звернення 26.11.2022)
10. ISO 21502:2020. Project, programme and portfolio management — Guidance on project management.
11. URL: http://hmoftakhari.com/userfiles/ISO%2021502/ISO%2021502_2020(en)-%20PQP.pdf (дата звернення 26.11.2022)
12. Axelos Limited, Eileen J. Roden. Portfolio, Programme and Project Offices: P3O. TSO, The Stationery Office; Second edition (September 13, 2013). 232 p.
13. Giraudo, L. & Monaldi, E. (2015). PMO evolution: from the origin to the future. Paper presented at PMI® Global Congress 2015–EMEA, London, England. Newtown Square, PA: Project Management Institute.
14. Christy Pettey (March 28, 2019). 4 Types of Project Management Offices That Deliver Value. URL: https://www.gartner.com/smarterwithgartner/4-types-of-project-management-offices-that-deliver-value (дата звернення 28.11.2022)
15. Fahrenkrog, S. L., Haeck, W., Abrams, F., & Whelbourn, D. (2003). PMI's organizational project management maturity model. Paper presented at PMI® Global Congress 2003–North America, Baltimore, MD. Newtown Square, PA: Project Management Institute.
16. Seven Key Factors to a Successful PMO Transformation. URL: https://blog.protiviti.com/2020/10/27/seven-key-factors-to-a-successful-pmo-transformation/ (дата звернення 27.11.2022)
17. Kendall G., Rollins S. (2003). Advanced Project Portfolio Management and the PMO. Multiplying ROI at Warp Speed. 448 p.

Статтю подано до редакції 28.11.2022

УДК: 004.9 DOI 10.33111/mise.102.11

Лютий О.І., к.тех.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Калганова В.І., старший викладач
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Стець К.М., магістрант ННІ «ІІТЕ»,
Київський національний економічний університет
імені Вадима Гетьмана

Liutyj O.I., Candidate of Technical Sciences, Associate Professor
of the Computer Mathematics and Information Security Department,
KNEU named after V. Hetman

Kalganova V.I., lecturer
of the Computer Mathematics and Information Security Department,
KNEU named after V. Hetman

Stets K.M., graduate student,
Institute of Information Technologies in Economics,
KNEU named after V. Hetman

МЕТОДИ ВИЗНАЧЕННЯ ВИТРАТ НА КІБЕРБЕЗПЕКУ

METHODS FOR DETERMINING CYBERSECURITY COSTS

Анотація. *У статті обговорюється проблема вартості збереження секретної інформації, а отже, проблема витрат на кібербезпеку в організації бізнесу в цілому. Звернено увага на фінансовий аспект організації системи кібербезпеки навколо бізнес-даних та інформації. Для того щоб ефективно вести бізнес у конкурентному середовищі, необхідно правильно керувати інформацією та даними підприємства. Особливо, якщо ця інформація є секретною і приносить підприємству велику користь у його діяльності. Для ефективного використання секретної інформації потрібно створити систему захисту і режим обмеження доступу до інформації чи її вільного розповсюдження, за якого ефект від використання інформації з урахуванням позитивних і негативних наслідків досягатиме максимального значення. Для порівняння інформації у контексті необхідності обмеження доступу до неї пропонується оцінювати інформацію за рівнем прояву всієї сукупності загроз у разі їх вільного поширення та можливих витрат на обмеження доступу до них та визначити ваги загроз, переваг і витрат для отримання єдиного показника, що характеризує інтегральний ефект від обмеження поширення інформації. Авторами запропоновано модель розрахунку значення інтегрального показника обра-*

ного способу розповсюдження інформації, який включає потенційно можливий розмір шкоди у разі поширення інформації, потенційно можливий розмір вигоди під час вільного розповсюдження інформації, ймовірність шкоди та користі протягом життєвого циклу інформації, витрати на захист інформації. Висвітлено зв'язок між витратами на захист інформації та потрібним рівнем захисту секретної інформації. Запропоновано авторську класифікацію витрат на забезпечення кібербезпеки підприємства.

Ключові слова: *інформація, витрати, кібербезпека, підприємство, секретність*

Abstract. *The article discusses the problem of cost for maintaining secret information and therefore, problematic of cybersecurity costs throughout business organization overall. Attention is drawn to the financial aspect of organization of cybersecurity system around business data and information. In order to effectively conduct business in a competitive environment, you need to properly manage the information and data of the enterprise. Especially if this information is secret and brings great benefits to the enterprise in its activities. In order to effectively use secret information, it is necessary to create a system of protection and a regime of restriction of access to information or its free distribution, in which the effect of using information, taking into account the positive and negative consequences, would reach the maximum value. To compare information from the point of view of the need to restrict access to it, it is proposed to evaluate the information by the degree of manifestation of the entire set of threats in case of their free dissemination and possible costs of restricting access to them and to determine the "weights" of threats, benefits and costs in order to obtain a single measure that characterizes the integral effect of restricting the dissemination of information. The author proposes a model for calculating the value of the integral indicator of the chosen mode of information dissemination, which includes the potentially possible amount of damage during the dissemination of information, the potentially possible amount of benefit during the free dissemination of information, the probability of harm and benefit during the life cycle of information, the cost of protecting information. Thus, the relationship between the costs of information protection and the required level of protection of classified information is highlighted. The author also proposes a classification of costs for ensuring cybersecurity of the enterprise.*

Keywords: *Information, costs, cybersecurity, enterprise, secrecy*

Постановка наукової проблеми та її значення. Питання наявності секретності інформації, усіх пов'язаних з цим технічних процесів та скорочення витрат на всіх видах підприємств, як державних, так і приватних, постає доволі гостро у реальності повномасштабної війни та постійних кібератак і маніпуляцій. В час, коли рішення повинні ухвалюватися достатньо швидко, система має бути вибудована ефективно. В стані постійного примусового зниження витрат, першочергово постає питання про оптимізацію процесів. Класифікація витрат, створення режимів поширення інформації у зв'язку з матеріальними ризиками щодо її поширення дозволять будь-яким підприємствам створити оптимальну систему захисту секретної інформації та оптимізувати фінансових аспект роботи служби кібербезпеки всередині організації.

Аналіз останніх досліджень і публікацій. Над розв'язанням проблеми економічного аспекту кібербезпеки на підприємстві працювали наступні вітчизняні науковці: М. Г. Романюков, О. А. Лаптієв, В. В. Собчук, А. В. Собчук, С. О. Лаптієв, Т. О. Лаптієв. Проте питання саме витратної частини системи захисту інформації залишається мало дослідженим.

Мета і завдання статті. Метою статті є осмислення проблематики витрат бізнесу на кіберзахист інформації з позицій рівня секретності інформації та потенційних втрат в разі її розповсюдження. Також теоретичне узагальнення та класифікація витрат на кіберзахист даних і створення моделі прорахунку інтегрального показника обраного режиму розповсюдження інформації. Досягнення поставленої мети передбачає вирішення таких завдань: класифікувати витрати підприємства на кіберзахист даних, проаналізувати взаємозалежність між фінансовими результатами та режимом розповсюдження інформації, створити якісну модель оцінки параметрів захисту інформації.

Виклад основного матеріалу. Секретність у ринковій економіці — економічна категорія. Інформація, яка захищається, повинна приносити певну користь її власнику і виправдовувати кошти, які витрачаються на її захист. Рівень секретності зазвичай з часом зменшується і рідше (історичні документи) збільшується. Тому рівень секретності має переглядатися. Інформація повинна залишатися конфіденційною доти, доки цього вимагають інтереси національної безпеки або комерційної діяльності підприємства.

Для найбільш ефективного використання інформації за час її життєвого циклу, протягом якого вона є актуальною, необхідно обрати такий режим її розповсюдження, за якого ефект від використання інформації з урахуванням позитивних та негативних наслідків досягав би максимальної величини. За такого підходу обмеження поширення інформації на певний час є одним із способів керування інформаційним ресурсом власника на користь досягнення максимального ефекту від його використання.

Слід враховувати, що оцінка позитивних і негативних наслідків від обмеження поширення інформації становить значні труднощі. Ці наслідки можуть виявлятися у різних сферах діяльності підприємства, оцінюватися у різних шкалах та одиницях виміру.

Для порівняння відомостей з позицій необхідності обмеження доступу до них пропонується:

• оцінити ці відомості за ступенем прояву всієї сукупності загроз у разі їх вільного поширення та можливих витрат (або втраченої вигоди) у разі обмеження доступу до них;

• ранжувати чи визначити ваги загроз, вигід і витрат з тим, щоб отримати єдину міру, яка характеризує інтегральний ефект від обмеження поширення відомостей (для вирішення цього завдання необхідно визначити переліки можливих загроз від несанкціонованого поширення інформації, вигід / переваг вільного поширення інформації та статей витрат на її захист);

• з урахуванням усіх цих факторів необхідно обрати такий режим розповсюдження інформації, який би на кінець періоду її активного життєвого циклу забезпечував би максимальний ефект від використання інформації.

Для визначення вагів збитків, вигід і витрат доцільно звернутись до допомоги експертів, які добре розуміють цінність відомостей та їх взаємозв'язок із зазначеними факторами. Можливість прояву різних факторів у динаміці життєвого циклу інформації оцінюється суб'єктивною ймовірністю.

На основі порівняльних оцінок окремих факторів з урахуванням можливості їх прояву обчислюється значення інтегрального показника обраного режиму розповсюдження інформації

$$W = U \times p - V \times q - Z, \qquad (1)$$

де U — потенційно можлива величина шкоди під час поширення відомостей; V — потенційно можлива величина вигоди при вільному розповсюдженні відомостей; p — ймовірність прояву шкоди під час життєвого циклу відомостей; q — ймовірність прояву вигоди в період життєвого циклу при вільному поширенню відомостей; Z — величина витрат за захист відомостей.

Якщо розраховане значення інтегрального показника виявляється більше від нуля, то включення аналізованої інформації до переліку відомостей, віднесених до інформації обмеженого доступу, доцільно.

Віднесення інформації до інформаційних ресурсів, що підлягають захисту від несанкціонованих і ненавмисних впливів, доцільно, якщо величина шкоди, яка запобігається при цьому, перевищує величину витрат на її захист.

Наочною ілюстрацією залежності параметрів та характеристик, що визначають умови захисту засекреченої інформації, може бути така модель (рис. 1).

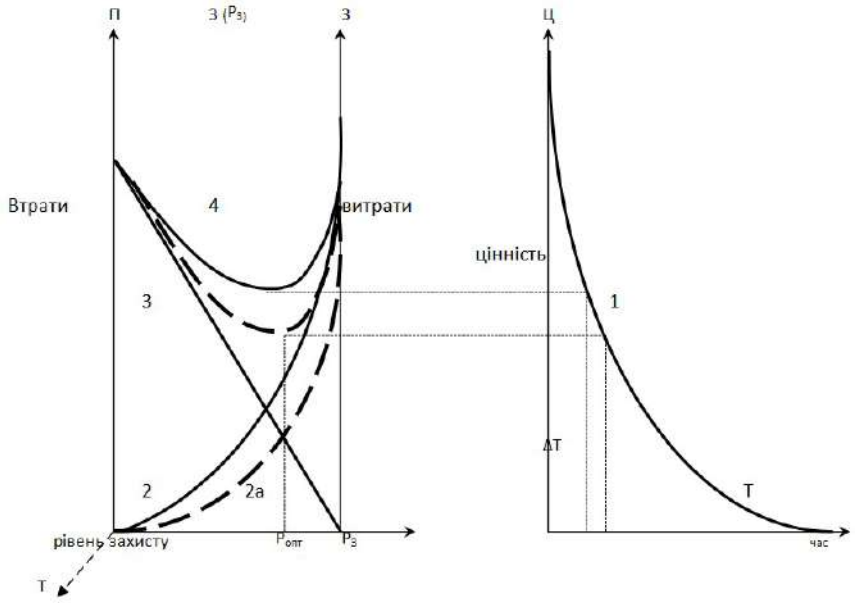


Рис. 1. Якісна модель завдання оцінки параметрів захисту інформації

На цій моделі показано якісний взаємозв'язок параметрів інформації, що охороняється, таких, як її цінність, необхідний рівень захисту, час збереження секретності, з одного боку, та економічних характеристик захисних заходів, таких як витрати на забезпечення захисту та можливі втрати внаслідок недосконалості системи захисту інформації, з другого. На рис. 1 показано, що Ц — цінність інформаційного ресурсу — об'єкта засекречення (наприклад, науково-технічного звіту, що містить опис нової перспективної технології); Т — час; Ц(Т) — характеристика старіння інформації — зменшення цінності інформаційного ресурсу з часом; РЗ — рівень (ймовірність) забезпечення захисту. На практиці РЗ <1, оскільки абсолютно надійний захист інформації навряд чи здійсненний; З(РЗ) — витрати на захист інформації як функція від необхідного рівня її захисту. Ці витрати зростають у разі підвищення вимог до рівня захисту. Прагнення досягти дуже високого рівня захисту зазвичай тягне за собою різке зростання витрат, які можуть перевищити цінність самої інформації, що захищається. П — ймовірні втрати внаслідок недосконалості захисту, які є функцією цінності інформації та реалізованого рівня її

захисту. У нульовому наближенні ці втрати апроксимуються добутком цінності інформації на ймовірність її витоку. Ймовірність витоку інформації перебуває у зворотній залежності до досягнутого рівня захисту. За такого допущення П ~ Ц(1 – р3).

Якщо сума З(Р3) + П(Р3) визначає витрати, пов'язані з засекречуванням інформації, то рівень захисту Ропт(З,П) відповідний на рис. 1 мінімум суми витрат на захист і ймовірнісних втрат внаслідок неповноти захисту інформації можна розглядати як оптимальний. Прагнення перевищити його призведе до різкого зростання витрат на забезпечення захисту інформації; зниження ж рівня захисту може призвести до збільшення втрат внаслідок її недосконалості.

Якщо вважати, що ΔТ — тимчасовий інтервал, протягом якого засекречення інформації може бути економічно виправдане (при цьому величина витрат на захист інформації в сумі з імовірнісними втратами менша за вартість засекречуваної інформації з урахуванням її старіння), то, як показано на рис. 1: ΔТmax = = ΔТ (Ц, Ропт(З, П)). Для спрощення ми нехтуємо залежністю З(ΔТ) — зростанням сумарних витрат на захист інформації, що засекречується, з часом, що можна було б легко проілюструвати, представивши ліву частину рис. 1 у тривимірних координатах.

Внаслідок того, що значення величини досягнутого рівня захисту інформації Р3 залежить як мінімум від двох параметрів: Rзі — використовуваних ресурсів (зокрема матеріальних витрат на забезпечення захисту) та Емзі — ефективності механізму захисту (використання цих ресурсів), у рамках цієї моделі можлива оптимізація.

Фактично Емзі — показник досконалості створеної та функціонуючої системи захисту інформації. За більш якісного проєктування та практичної реалізації механізму захисту — максимально ефективного залучення всіх ресурсів — той самий рівень забезпечення захисту інформації може бути досягнутий за менших матеріальних витрат. На рис. 1 це ілюструє крива 2*а*. Відповідно, при цьому про оптимальний рівень захисту інформації може бути вищим, а економічно виправдана тривалість засекречування ΔТ — більшою.

Витрати на забезпечення кібербезпеки підприємства можна поділити на одноразові та систематичні.

Одноразові витрати включають:

1) витрати формування ланки управління системою захисту інформації та інші організаційні витрати;

2) витрат на придбання та встановлення засобів захисту.

Систематичні витрати включають:

1. Витрати обслуговування системи кібербезпеки:

– витрати на здійснення технічної підтримки виробничого персоналу під час впровадження засобів захисту інформації;

– витрати на організацію системи допуску виконавців та співробітників конфіденційного діловодства;

– витрати на обслуговування та налаштування програмно-технічних засобів захисту, операційних систем, мережевого обладнання;

– витрати на організацію безпечного використання інформаційних систем;

– витрати на забезпечення безперебійної роботи системи захисту інформації.

2. Витрати на контроль роботи системи безпеки:

• витрати на контроль змін стану інформаційного середовища підприємства;

• витрати на контроль за діями персоналу;

• витрати на планові перевірки та випробування програмно-технічних засобів захисту інформації;

• витрати на проведення перевірок навичок персоналу підприємства з експлуатації засобів захисту;

• витрати на контроль правильності введення даних до прикладних систем;

• оплата праці інспекторів з контролю вимог, які пред'являються до захисних засобів, що забезпечують управління захистом комерційної таємниці.

3. Витрати на забезпечення належної якості інформаційних технологій та їх відповідності вимогам стандартів:

– витрати на забезпечення відповідності вимогам якості інформаційних технологій;

– витрати на забезпечення відповідності прийнятим стандартам та вимогам достовірності інформації, дієвості засобів захисту;

– витрати на доставку та обмін конфіденційної інформації;

– Витрати задоволення суб'єктивних вимог користувачів: стиль, зручність інтерфейсів.

4. Витрати на підвищення кваліфікації персоналу у питаннях використання наявних засобів захисту, виявлення та запобігання загрозам безпеки.

5. Витрати, пов'язані з переглядом політики кібербезпеки підприємства:

• витрати на ідентифікацію загроз безпеки;

• витрати на пошук вразливості системи захисту інформації;

• оплата роботи фахівців, які виконують роботи з визначення можливої шкоди та переоцінки ступеня ризику;

• витрати на використання додаткових засобів захисту інформації.

6. Витрати на ліквідацію наслідків порушення режиму кібербезпеки:

– витрати на відновлення системи безпеки до відповідності вимогам політики безпеки.

– витрати на придбання нових технічних засобів;

– витрати на утилізацію ресурсів, що прийшли в непридатність;

– витрати на відновлення баз даних та інших інформаційних ресурсів;

– витрати на проведення заходів щодо контролю достовірності даних, які зазнали атаки на цілісність;

– витрати на проведення додаткових випробувань та перевірок інформаційних систем;

– витрати на проведення розслідувань порушень безпекової політики;

– витрати на юридичні спори та виплати компенсацій;

– витрати, що виникли внаслідок розриву ділових відносин із партнерами.

7. Витрати, що виникають внаслідок втрати новаторства:

• витрати на проведення додаткових досліджень та розробки нової ринкової стратегії для підприємства у зв'язку з відмовою від організаційних, науково-технічних, комерційних рішень, які стали неефективними внаслідок витоку відомостей;

• витрати, що виникли через зниження пріоритету в наукових дослідженнях та неможливість патентування та продажу ліцензій на науково-технічні досягнення.

Класифікація витрат умовна, оскільки детальна розробка переліку залежить від особливостей конкретної організації та її систем захисту кібербезпеки.

Зазвичай неминучі витрати, які необхідно враховувати навіть тоді, коли рівень загроз безпеки досить низький, включають такі статті:

– обслуговування технічних засобів захисту;

– конфіденційне діловодство;

– функціонування та аудит системи безпеки;

– мінімальний рівень перевірок та контролю із залученням спеціалізованих організацій;

– навчання персоналу методам кібербезпеки.

За дотримання політики безпеки та проведення профілактичних заходів можна виключити або суттєво знизити такі витрати:

• на відновлення системи безпеки до відповідності вимогам політики безпеки;

• на відновлення ресурсів інформаційного середовища підприємства;

• на переробки всередині системи безпеки;

• на юридичні спори та виплати компенсацій;

• на виявлення причин порушення політики безпеки.

Вихідні постановки завдань захисту державної та комерційної таємниці можна подати, як показано в табл. 1.

Таблиця 1

ВИХІДНІ УМОВИ ЗАВДАНЬ ЗАХИСТУ ДЕРЖАВНОЇ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Параметри				
Об'єкти захисту	Цінність інформації	Необхідний рівень захисту інформації	Витрати захисту засекреченої інформації	Тривалість секретності
Державна таємниця	Визначається державою	Встановлюється державою (високий)	Визначаються безумовною необхідністю забезпечення необхідного рівня захисту інформації	Визначаються у відповідності з нормами законодавства про державну таємницю
Комерційна таємниця	Суб'єктивна оцінка власника інформації	Оптимальний	Гранично допустимі для власника комерційної таємниці з обліком прийнятного для нього ризику	Може бути змінена власником

В умовах стабільної економіки державне замовлення для підприємця із засекречення інформації виглядає пріоритетним, оскільки воно не пов'язане з ринковим ризиком реалізації продукції. Фінансування витрат на здійснення діяльності, пов'язаної з державною таємницею, в бюджетних установах і організаціях здійснюється за рахунок Державного бюджету України, бюджету Автономної Республіки Крим та місцевих бюджетів. Кошти на зазначені витрати передбачаються у відповідних бюджетах окремим рядком. Зазначені витрати інших установ і організацій, а також підприємств відносяться до валових витрат виробника продукції, виготовлення якої пов'язано з державною таємницею.

Витрати на здійснення заходів щодо віднесення інформації до державної таємниці, засекречування, розсекречування та охорони матеріальних носіїв такої інформації, її криптографічного та технічного захисту, інші витрати, пов'язані з державною таємницею, на недержавних підприємствах, в установах, організаціях фінансуються на підставі договору з замовником робіт, пов'язаних з державною таємницею. Підприємствам, установам і організаціям, які провадять діяльність, пов'язану з державною таємницею, можуть надаватися податкові та інші пільги в порядку, встановленому Законом України «Про державну таємницю» [1].

Вимоги до умов та рівня захисту задаються державними нормативними документами та є імперативними.

Власник комерційної таємниці зацікавлений у максимально високому рівні захисту своєї комерційної таємниці та мінімізації витрат на її захист. Це вимагає визначення їм допустимого ризику та пошуку оптимального рішення.

Висновки та перспективи подальшого дослідження. Нині питання оптимального використання фінансових ресурсів постає достатньо важливим за умови постійного скорочення фінансування та зменшення бюджетів. Також в реаліях повномасштабної російсько-української війни потрібно зважено вибирати режим розповсюдження і надання доступу до секретних даних та матеріалів як на приватному підприємстві, так і в державних структурах. Хоча загалом зараз на всіх підприємствах існують служби кібербезпеки, або працюють хоча б кілька спеціалізованих фахівців, втім загального підходу для менеджменту взаємодії між витратами на захист інформації та необхідним рівнем захисту інформації з обмеженим доступом немає серед індустрії.

Класифікація витрат, створення режимів поширення інформації у зв'язку з матеріальними ризиками щодо її поширення дозволять будь-яким підприємствам створити оптимальну систему захисту секретної інформації та оптимізувати фінансових аспект роботи служби кібербезпеки всередині організації.

Бібліографічні посилання

1. Про державну таємницю: Закон України. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text

2. Про основні засади забезпечення кібербезпеки України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. Про затвердження Зводу відомостей, що становлять державну таємницю: наказ Центрального управління Служби безпеки України від

23 грудня 2020 р. № 383. URL: https://zakon.rada.gov.ua/laws/show/z0052-21#n7
4. Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету міністрів України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#n8
5. Про інформацію: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text
6. Про електронні документи та електронний документообіг: Закон України. URL: https://zakon.rada.gov.ua/laws/show/851-15#Text
7. Про національну безпеку України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
8. Контроль за законністю заходів із кібербезпеки України. Ст. 15 КУ. URL:https://protocol.ua/ua/pro_osnovni_zasadi_zabezpe_vid_05_10_2017_2163_viii_stattya_15/
9. Меморандум про взаємодію та співробітництво в сфері кібербезпеки та кіберзахисту, спрямовану на попередження, виявлення, ефективне реагування та протидію актуальним кіберзагрозам, підвищення рівня інформаційної безпеки та ситуаційної обізнаності у сфері кібербезпеки та кіберзахисту. URL: https://interacademy.info/ekspert-mizhnarodnoi-akademii-informatsii-vziav-uchast-u-pidpysanni-memorandumu-pro-vzaiemodiiu/
10. ISO/IEC27000:2019 — Інформаційні технології — Методи і засоби забезпечення безпеки — Системи управління інформаційною безпекою — Загальні відомості і словник.
11. ISO/IEC 27001:2013 — Інформаційні технології — Методи захисту — Системи управління інформаційною безпекою — Вимоги
12. ISO/IEC 27002:2013/COR 2:2015 — Інформаційні технології — Методи захисту — Звіт рекомендованих правил для управління інформаційною безпекою
13. ISO/IEC 27005:2018 — Інформаційні технології — Методи безпеки — Управління ризиками інформаційної безпеки
14. ISO 27035 — Управління інцидентами
15. Рекомендація КОМІСІЇ (ЄС) 2017/1584 від 13 вересня 2017 року про скоординоване реагування на великомасштабні інциденти і кризи в області кібербезпеки
16. Постанова 2019/881 Європейського Парламенту і Ради від 17 квітня 2019 р. про ENISA (Агентство Європейського Союзу з кібербезпеки) і про сертифікацію кібербезпеки інформаційних і комунікаційних технологій і скасування Регламенту (ЄС) № 526/2013 (Закон про кібербезпеку)
17. Валюшко І.О. Кібербезпека України: наукові та практичні виміри сучасності. URL: http://visnyk-psp.kpi.ua/article/view/140496/137578
18. Laptiev, O., Sobchuk, V., Sobchuk, A., Laptiev, S., & Laptieva, T. (2021). Удосконалена модель оцінювання економічних витрат на систему захисту інформації в соціальних мережах. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/249

Статтю подано до редакції 29.11.2022

УДК: 004.4`2 DOI 10.33111/mise.102.12

Мамонова Г.В., к.фіз.-мат.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Годунова К.М., магістрант ННІ «ІІТЕ»
Київський національний економічний університет
імені Вадима Гетьмана

Mamonova H.V. PhD of Physical and Mathematical Sciences,
Associate Professor of the Computer Mathematics
and Information Security department
KNEU named after V. Hetman

Hodunova K.M., graduate student,
Institute Information Technologies in Economics
KNEU named after V. Hetman

РЕТРОСПЕКТИВНИЙ АНАЛІЗ СИСТЕМ УПРАВЛІННЯ БІЗНЕС-ПРОЦЕСАМИ

RETROSPECTIVE ANALYSIS OF BUSINESS PROCESS MANAGEMENT SYSTEMS

Анотація. *Управління бізнес-процесами — це систематичний підхід до запису, проєктування, виконання, документування, вимірювання, моніторингу та контролю як автоматизованих, так і неавтоматизованих процесів для досягнення цілей компанії та бізнес-стратегій. Управління бізнес-процесами охоплює свідоме, комплексне та дедалі більш технологічне визначення, вдосконалення, інновації та підтримку наскрізних процесів. Завдяки такому систематичному управлінню компанії досягають кращих результатів швидше та гнучкіше. За допомогою BPM процеси можна узгодити з бізнес-стратегією, допомагаючи покращити загальну продуктивність компанії шляхом оптимізації процесів у бізнес-підрозділах або навіть за їх межами. Мета статті полягає у дослідженні та аналізі розвитку менеджменту бізнес-процесів і виокремленні дослідницьких підходів під час його вивчення. Досліджено історію розвитку концепції управління бізнес-процесами. Визначено основні методології вдосконалення бізнес-процесів, які відрізняються за масштабами, місією та основними підходами. Проаналізовано розвиток досліджень, що стосувалися процесного менеджменту шляхом вивчення відповідної літератури. Розглянуто та систематизовано статті про менеджмент бізнес-процесів із провідних журналів про інформаційні системи. Стаття має науково-методичний характер.*

Ключові слова: *управління, бізнес-процес, бізнес-процес підрозділу, наскрізний бізнес-процес, системи управління бізнес-процесами*

Abstract. *Business Process Management is a systematic approach to recording, designing, executing, documenting, measuring, monitoring, and*

controlling both automated and non-automated processes to achieve company goals and business strategies. Business process management encompasses the conscious, comprehensive and increasingly technological definition, improvement, innovation and support of end-to-end processes. Thanks to this systematic management, companies achieve better results faster and more flexibly. With BPM, processes can be aligned with business strategy, helping to improve overall company performance by streamlining processes across business units or even beyond. The purpose of the article is to research and analyze the development of business process management and to identify research approaches in its study. This paper examines the history of the development of the concept of business process management. The main methodologies for improving business processes, which differ in scope, mission and main approaches, are defined. The development of research related to process management was analyzed by studying the relevant literature; articles on business process management from leading journals on information systems were reviewed and systematized. The article has a scientific and methodological character.

Keywords: *management, business process, division business process, end-to-end business process, business process management systems*

Постановка наукової проблеми та її значення. Управління бізнес-процесами (Business Process Management) як наукова дисципліна існує досить давно. Зусилля багатьох дослідників були присвячені вдосконаленню методологій, методів та інструментів BPM. Незважаючи на постійний розвиток протягом багатьох років, мало уваги приділялося розумінню еволюційного процесу досліджень систем з управління бізнес-процесами. У цій статті проаналізовано розвиток досліджень, що стосувалися процесного менеджменту шляхом вивчення відповідної літератури; розглянуто статті про менеджмент бізнес-процесів із провідних журналів про інформаційні системи. Програми управління бізнес-процесами набули поширення за останнє десятиліття у відповідь на попит на більш ефективні та гнучкі бізнес-процеси.

Аналіз останніх досліджень і публікацій. Історія наукової теорії управління бізнес-процесами бере початок із 1911 р., коли Фредерік Тейлор опублікував роботу під назвою «Принципи наукового менеджменту», в якій детально описано способи підвищення продуктивності шляхом застосування наукового методу [1]. Мета його наукової теорії полягає у збільшенні продуктивності всередині організаційної структури за рахунок підвищення продуктивності кожного індивіда. Дослідження Тейлора були зосереджені не на вирішенні комплексних проблем, а на повторюваних, рутинних завданнях. Кожне з таких завдань було ретельно уточнено та виміряно. Такі види діяльності піддаються стандартизації та із застосуванням відповідних технологій можуть бути автоматизовані.

У 1960-х роках технології стали рушійною силою бізнесу та прискорили зміни. Це започаткувало першу хвилю процесної орі-

єнтації під назвою Кайдзен. Японські компанії стали більш конкурентоспроможними завдяки зосередженості на програмах підвищення якості. Нещодавно TQM перетворився на «Шість сигм». Ці філософії управління були присвячені здебільшого виробництву [2].

У 1980-х роках компанія FileNet розробила цифрову систему керування документообігом, призначену для маршрутизації відсканованих документів через заздалегідь визначений процес. Цю ранню систему — пізніше придбану IBM — часто називають попередницею сучасного програмного забезпечення BPM, за словами Френка Дж. Ваятта, автора інструментів керування бізнес-процесами та автоматизації робочих процесів та проєктів.

Парадигма бізнес-процесів виникла у 1990-х роках після публікації основоположних статей Томаса Девенпорта (Thomas Davenport) в Sloan Management Review і Майкла Хаммера (Michael Hammer) у Harvard Business Review.

У той час дослідження у сфері бізнес-процесів були описані у книзі «Реінжиніринг корпорації. Маніфест революції в бізнесі» Майклом Хаммером та Джеймсом Чемпі (James A. Champy). Автори зазначали, що «фундаментальне переосмислення та радикальне перепроєктування бізнес-процесів необхідне для досягнення різких покращень у сучасних критичних показниках ефективності, таких як вартість, якість, сервіс та швидкість». Хаммер стверджував, що звичайні методи підвищення продуктивності не призводять до покращень, необхідних для роботи підприємств у 1990-х роках. У результаті підприємства були погано підготовлені для досягнення успіху під час швидкої зміни технологій, зростаючих очікувань клієнтів та глобальної конкуренції. Крім того, інформаційні технології не змогли покращити продуктивність або обслуговування клієнтів, оскільки їх використовували для автоматизації існуючих несправних процесів [3].

У 2000-х роках компанія Gartner вперше ввела термін «пакет управління бізнес-процесами» (BPMS) для позначення широкого спектра програмних додатків, які мають справу з процесами.

Спочатку BPMN розшифровувався як нотація моделювання бізнес-процесів. Перша версія була розроблена BPMN була розроблений Ініціативою управління бізнес-процесами на чолі зі Стівеном А. Уайтом з IBM, перш ніж вона була опублікована в 2004 р. Business Process Management Initiative (BPMI). З самого початку метою було створити стандартизовану графічну нотацію процесу, яку також можна було б використовувати для автоматизації процесу. У 2005 році Object Management Group (OMG) при-

дбала BPMI разом із подальшим розвитком BPMN. Перша версія BPMN була опублікована OMG у лютому 2006 р.

OMG є важливою інституцією у світі інформаційних технологій: він особливо відомий своєю уніфікованою мовою моделювання (UML), стандартом моделювання для розробки програмного забезпечення. Злиття BPMI з OMG також стало початком глобального тріумфу для BPMN, оскільки надало стимул для багатьох компаній змінитись.

У лютому 2011 р. OMG розробила поточну версію BPMN версії 2.0. Версія 2.0 прийшла з новим визначенням BPMN: модель бізнес-процесу та нотація, оскільки версія 2.0 визначила не лише нотацію, але й так звану формальну метамодель.

У 2012 р. Gartner також ввів термін «Інтелектуальне управління процесами» (iBPM) для позначення пакетів BPM, які включають штучний інтелект, розширену аналітику та звітність.

12 березня 2012 р. компанія Gartner опублікувала перший звіт «Магічний квадрант для інтелектуальних пакетів управління бізнес-процесами» (Gartner, 2012), у якому чітко висвітлено появу нового класу систем, відмінних від традиційних пакетів BPM.

Потім у вересні 2013 р. BPMN був опублікований як стандарт ISO Міжнародною організацією зі стандартизації відповідно як ISO/IEC 19510:2013. Відтоді нотація навмисно зберігається без змін, оскільки поширення різних версій нівелювало переваги від застосування нотації. Як наслідок, наприклад, кожен інструмент підтримував би різні версії або документація повинна була б враховувати відмінності кожної версії.

12 березня 2015 р. компанія Gartner опублікувала звіт «Магічний квадрант для систем управління справами на основі BPM-платформи», а через шість днів — інший звіт під назвою «Магічний квадрант для інтелектуальних пакетів управління бізнес-процесами», який значною мірою базувався на продуктах тих самих виробників.

Мета дослідження полягає у тому, щоб описати розвиток менеджменту бізнес-процесів та виокремити дослідницькі підходи при його вивченні.

Виклад основного матеріалу. У парадигмі BPM організація розглядається як система взаємопов'язаних процесів. Отже, бізнес-процес — це набір однієї або кількох пов'язаних процедур або дій, які спільно реалізують бізнес-цілі або цілі політики, як правило, у контексті організаційної структури, що визначає функціональні ролі та відносини. Подібним чином, згідно з Хікманом, бізнес-процес — це логічний ряд залежних дій, які викорис-

товують ресурси організації для створення результату, такого як продукт або послуга [4]. BPM розглядається як будь-який систематичний, структурований підхід до аналізу, вдосконалення та управління процесами з метою покращення якості продуктів і послуг. На операційному рівні BPM підтримує бізнес-процеси «[…] за допомогою методів, методів і програмного забезпечення [інструментів] для проєктування, впровадження, контролю та аналізу [процесів] із залученням людей, організаційних програм, документації та інших джерел інформації» (Веске, 2004).

BPM та його похідні постійно обговорюються та досліджуються як в наукових колах, так і в промисловості. Хоч цей термін часто плутають з іншими процесно-орієнтованими методологіями вдосконалення, такими як інновації бізнес-процесів, реінжиніринг бізнес-процесів, редизайн бізнес-процесів і вдосконалення бізнес-процесів, загалом їх можна розглядати як набір зусиль щодо вдосконалення процесів, які відрізняються за місією, масштабом та підходами. BPM охоплює усі вище зазначені методології та забезпечує загальний метод для вивчення та вдосконалення бізнес-процесів (Elzinga, et al, 1995) [5].

Цикл BPM починається з ідентифікації процесу, де він визначається та поділяється на декілька завдань. Далі моделюється та розробляється його архітектура за допомогою відповідного програмного забезпечення BPM. Потім здійснюється відкриття процесу, запуск системи та його виконання. Наступним етапом є аналіз для виявлення та оцінки проблем та можливостей для вдосконалення процесу, потім — перепроєктування процесу для визначення змін у вирішенні проблеми. Після цього новий процес буде впроваджено на етапі, на якому відстежуватиметься та керуватиметься в системах моніторингу. Загальний життєвий цикл BPM показано на рис. 1.

Успіх впровадження BPM пов’язаний із застосуванням ключових практик. Інформаційні технології розглядаються як основний фактор, що сприяє розвитку сучасних практик.

Як зазначає Девенпорт, цінність інформаційних технологій у BPM є наслідком її здатності автоматизувати, інформувати, впорядковувати, відстежувати, аналізувати, інтегрувати та виключати ресурси та дії процесів. Інформаційні технології також використовуються для подолання географічних та інтелектуальних кордонів, які заважають організаціям орієнтуватися на процеси.

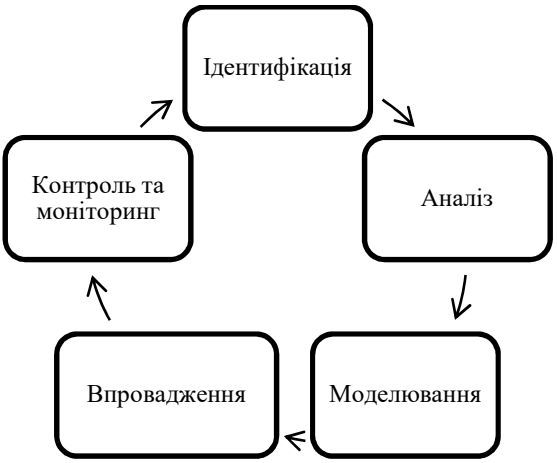


Рис. 1. Життєвий цикл BPM

Джерело: [6].

Таблиця 1

КЛЮЧОВІ ПРАКТИКИ BUSINESS PROCESS MANAGEMENT

Автор	Беннер Ташман, 1993	Харрінгтон, 1995	Кеттінгер Гуха, 1997	Ван дер Алст, 2003
Сфера дослідження	Управління процесами	Удосконалення бізнес-процесів	Реінжиніринг бізнес-процесів	Управління бізнес-процесами
Пропоновані ключові практики	1. Відображення процесу 2. Удосконалення процесу 3. Дотримання систем вдосконалених процесів	1. Організація якості 2. Розуміння процесу 3. Оптимізація процесу 4. Реалізація 5. Вимірювання і контроль 6. Постійне покращення	1. Проєктування 2. Ініціація 3. Діагностика 4. Редизайн 5. Реконструкція 6. Оцінка	1. Діагностика 2. Проєктування процесу 3. Системна конфігурація 4. Оформлення процесу

Джерело: розроблено автором.

Отже, різні інформаційні системи розроблені для сприяння виконанню практик BPM, колективно чи незалежно. Інформаційні системи як такі називаються «системами управління бізнес-процесами», «управлінськими інформаційними системами, керованими процесами» або «інформаційними системами, орієнтованими на процес (Process Aware Information System)». Залежно від сприйняття BPM для їхнього впровадження пропонуються різні фокуси управління або «ключові практики». Наприклад, з точки зору Беннера Ташмана (2003), BPM передбачає три основні практики: відображення процесів, вдосконалення процесів і дотримання систем покращених процесів. Ван дер Алст та його колеги-дослідники [7,8] пропонують чотири сфери управління, які слід розглядати як процесний менеджмент: діагностика, проєктування процесу, конфігурація системи та впровадження процесу. У табл. 1 наведені ключові практики застосування BPM.

Щоб змоделювати та описати виконувані бізнес-процеси переважна більшість BPM-систем застосовують такі інструменти:

– BPMN (Business Process Model and Notation) — міжнародний стандарт для моделювання і документування бізнес-процесів, фундаментальна частина процесного менеджменту, зрозуміла для усіх учасників бізнесу;

– BPEL (Business Process Execution Language) — мова на основі XML, яка дозволяє вебсервісам, API і людським процесам у сервісно-орієнтований архітектурі з'єднуватися та обмінюватися даними у бізнес-процесі [9];

– XPDL (XML Process Definition Language) — стандартизований формат WfMC (Workflow Management Coalition), щоб визначення бізнес-процесів можна було переключити між багатьма продуктами робочого процесу.

Еволюція програмних систем підтримки BPM почалася з двох протилежних припущень:

1) системи управління справами — підтримка процесів із непередбачуваним потоком і не зовсім відомою, але потенційно високою інтенсивністю знань;

2) традиційний BPMS — підтримка процесів відомого і суворо повторюваного характеру завдяки наявності всіх знань, необхідних для виконання процесів перед виконанням.

Загалом виокремлюють наступні види бізнес-процесів:

- такі, що виконуються в межах одного підрозділу;
- такі, що виконуються в межах одного підрозділу, а ресурси для виконання перебувають в іншому;

- такі, що виконуються в декількох суміжних структурних підрозділах (міжфункціональні);
- такі, що виконуються різними функціональними підрозділами [10].

У рамках сучасного бізнесу доцільно використовувати поняття наскрізних бізнес-процесів. Для автоматизованого управління процесами такого виду існують спеціалізовані системи управління бізнес-процесами — Business Process Management Systems (BPMS).

Огляд існуючих BPM-систем. Сучасні BPM-системи наділені функціями з управління наскрізними процесами, що включає їх моделювання, впровадження, контроль, моніторинг та аналіз), та підтримують взаємодію зацікавлених осіб з інформаційним середовищем. Такі системи здатні автоматизувати повну послідовність процесу, шлях якого пролягає через декілька функціональних підрозділів, що у свою чергу дозволяє здійснювати збір та аналіз потрібних показників ефективності. Наразі ринок BPM-систем проходить етап становлення [11]. Станом на сьогодні на ринку представлені системи відомих компаній, які пропонують підтримку бізнес-процесів протягом усього життєвого циклу та забезпечують інтеграцію зовнішніх додатків. Наприклад, такими BPM-системами є:

Bizagi BPM Suite. Моделювання в Bizagi здійснюється в нотації BPMN. Порівняно з іншими BMP-рішеннями Bizagi підтримує найвищий рівень відповідності до специфікації BPMN. Також існує функція колективного проєктування. Після створення моделі процесу користувач може завантажити її та визначити інформацію, необхідну для автоматизації процесу (визначення даних, виконавців, користувацький інтерфейс, задання бізнес-правил тощо). Процес завантажується на сервер та стає доступним для виконання. Виконання користувацьких задач здійснюється через інтерфейс. Будь-які зміни у процесі призводять до негайних змін на сервері, усі запущені екзмепляри процесу одразу починають працювати за новою моделлю.

Bonita Open Solution. Характерною особливістю програмного рішення є наявність opensource-версії, тому дана версія не є повноцінною BPM-системою, оскільки в ній відсутні засоби моніторингу процесів. Opensource-версія надає лише базову функціональність, необхідну для управління бізнес-процесами, що дозволяє розробляти процеси і виконувати їх. BOS має можливість взаємодіяти з великою кількістю додатків та сервісів, таких як бази даних, поштові сервіси, вебсервіси тощо. У системи відсутня під-

тримка динамічних змін бізнес-процесу, що уповільнює оптимізацію процесів, що є суттєвим недоліком.

Camunda Service. Сервіс має модульну конструкцію, яка дозволяє працювати у загальнодоступній, приватній та гібридній хмарі, поєднуючись з технологіями Kafka та іншими потоковими ресурсами. Конструкція opensource надає можливість адаптувати будь-який варіант використання, включаючи змішані автоматизовані / ручні робочі процеси. При застосуванні Camunda не потрібна інтерфейсна робзробка, оскільки вона дозволяє інтегрувати готовий графічний інтерфейс.

Oracle BPM Suite. Сервіс забезпечує інтегроване середовище для розробки, адміністрування та використання бізнес-додатків, зосереджених навколо бізнес-процесів. Він також дозволяє створювати моделі процесів на основі стандартів за допомогою зручних програм. Це забезпечує співпрацю між розробниками процесів і аналітиками процесів. Oracle BPM підтримує BPMN 2.0 і Business Process Execution Language (BPEL) від моделювання та реалізації до часу виконання та моніторингу. Власники процесів можуть налаштовувати гнучкі й неструктуровані бізнес-процеси за допомогою попередньо визначених компонентів. Об'єднує різні етапи життєвого циклу розробки додатків, задовольняючи наскрізні вимоги до розробки додатків на основі процесів. Oracle BPM об'єднує етапи проєктування, реалізації, виконання та моніторингу на основі інфраструктури архітектури компонентів обслуговування. Це дозволяє різним особам брати участь на всіх етапах життєвого циклу програми [12].

Висновки. У даній роботі досліджено історію розвитку концепції управління бізнес-процесами. Визначено основні методології вдосконалення бізнес-процесів, які відрізняються за масштабами, місією та основними підходами. Незважаючи на розвиток технологій, сучасні системи управління бізнес-процесами все ще обмежені у своїй здатності підтримувати найкращі практики BPM. На сьогодні існує досить невелика кількість систем, які підтримують збір та інтерпретацію даних від екземплярів бізнес-процесу в реальному часі.

Варто зауважити, що традиційні системи не пропонують інструментів підтримки для діагностики бізнес-процесів, тому часто організації змушені самостійно впроваджувати програмні рішення, попередньо стикаючись із проблемами інтеграції існуючих систем у власну організаційну структуру. Отже, є багато напрямів для подальших досліджень BPM.

Бібліографічні посилання

1. Dumas M., Rosa M., Mendling JL., Reijers HA. Fundamental of Business Process Management. Second ed. ed. s.l.: Springer (2013).
2. Dumas, M., ver der Aalst, W.M.P. and ter Hofstede, H.M. (2005) Process-aware information systems: Bridging people and software through process technology, John Wiley & Sons, Inc., Hoboken, NJ.
3. Hammer, C. and Champy, J. (1993) Reengineering the corporation: A manifesto for business revolution, HarperBusiness, New York, NY.
4. Hickman, L.J. (1993) Technology and Business Process Re-engineering: Identifying opportunities for competitive advantage, British computer Society CASE Seminar on Business Process Engineering, 29, London
5. Enzinga, D.J., Horak, T., Chung-Yee, L. and Bruner, C. (1995) Business process management: Survey and methodology, IEEE Transactions on Engineering Management, 24, 2, 119-28.
6. Kumar, A, et al. (2002) Dynamic Work Distribution in Workflow Management Systems: How to balance quality and performance, Journal of Management Information Systems, 18, 3, 157-193.
7. O'Neal, P., Sohal, A.S. (1999) Business process reengineering: a review of recent literature, Technovation, 19, 571-581.
8. Palvia, P., Pinjani, P., Sibley, E.H. (2007) A profile of information systems research published in Information & Management, Information & Management, 44, 1, 1-11
9. Специфікація мови BPEL версії 1.1. URL: http://www.ibm.com/developerworks/webservices/library/wsbpel
10. BPM — управління бізнес-процесами. URL: https://www.it.ua/knowledge-base/technology-innovation/business-process-management-bpm
11. Сорока А.М. Інформаційні технології в управлінні бізнес-процесами на підприємствах. *Економіка. Менеджмент. Бізнес*. 2018. № 2(24). С. 76–81.
12. Oracle SOA Suite 11g. URL: http://www.oracle.com/technologies/soa/soa-suite.html

Статтю подано до редакції 22.11.2022

УДК: 519.7, 005 DOI 10.33111/mise.102.13

Мамонова Г.В., к.фіз.-мат.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Лисенко М.Ю., магістрант, ННІ «ІІТЕ»
Київський національний економічний університет
імені Вадима Гетьмана

Mamonova H.V., PhD of Physical and Mathematical Sciences, Associate Professor
of the Computer Mathematics and Information Security department
KNEU named after V. Hetman

Lysenko M.Y., graduate student,
Institute Information Technologies in Economics
KNEU named after V. Hetman

ІСТОРІЯ СТВОРЕННЯ ТА РОЗВИТКУ 3DS-ТЕХНОЛОГІЇ

HISTORY OF CREATION AND DEVELOPMENT OF 3DS-TECHNOLOGY

Анотація. *Питання безпеки платежів завжди було одним із найважливіших завдань будь-якої платіжної системи. Інженери та криптографи постійно працюють над створенням нових алгоритмів і систем безпеки, а хакери шукають уразливі місця в цих системах. Запровадження стандарту EMV для фізичних карток і технології 3D Secure для онлайн-платежів значно обмежило можливості шахраїв викривати та фальсифікувати дані карток і використовувати вкрадені реквізити. Стаття містить загальний огляд історії створення даної техніки, принцип її дії та шлях розвитку. Перехід платіжних програм на роботу з інтегрованим SDK (software development kit) підвищить швидкість та зручність процесу підтвердження операції. Доведено, що завдяки передачі відбитка пристрою також значно підвищиться рівень «впізнавання» емітентом свого клієнта. Частка операцій, що вимагають підтвердження, стрімко зменшуватиметься з поширенням таких додатків та їх активним використанням власниками карток для оплати товарів та послуг. Показано, що платіжна автентифікація для merchant-initiated платежів також підвищить конверсію платежів за підписками на регулярні сервіси, які стають особливо затребуваними останніми роками разом із переходом на сервісну модель споживання. Стаття має науково-методичний характер.*

Ключові слова: *стандарт EMV; 3D Secure; дані картки; оплата; система оплати; онлайн оплата.*

Abstract. *The issue of payment security has always been one of the most important tasks of any payment system. Engineers and cryptographers are*

constantly working to create new algorithms and security systems, while hackers are looking for these systems' vulnerabilities. The introduction of the EMV standard for physical cards and the 3D Secure technology for online payments had significantly limited the fraudsters' opportunities to expose and falsify card data and exploit stolen details. This article contains a general overview of the history of the creation of this technology, the principle of its operation and the path of development. The transition of payment programs to work with an integrated SDK (software development kit) will increase the speed and convenience of the transaction confirmation process. At the same time, thanks to the transfer of the device's fingerprint, the level of "recognition" by the issuer of its client will also significantly increase. The share of transactions requiring confirmation will rapidly decrease with the spread of such applications and their active use by cardholders to pay for goods and services. Payment authentication for merchant-initiated payments will also increase the conversion of payments for subscriptions to regular services, which have become especially popular in recent years with the transition to a service consumption model. The article has a scientific and methodological character.

Keywords: *EMV standard; 3D Secure; card data; payment; payment system; online payment.*

Постановка наукової проблеми та її значення. Питання безпеки під час проведення платежів було і залишається одним із найголовніших завдань будь-якої платіжної системи. Інженери та криптографи працюють над створенням нових алгоритмів та систем захисту, а зловмисники шукають у цих системах вразливі місця.

Період значного підвищення безпеки платежів припадає на 2000–2010 рр., коли впровадження стандарту EMV для фізичних карток і технології 3D Secure для інтернет-платежів суттєво обмежило можливості шахраїв у викритті та підробці карткових даних та експлуатації вкрадених реквізитів [1, 3]. Ця стаття містить загальний огляд історії створення даної технології, принцип її роботи та шлях розвитку.

З технічного боку платіжні картки виявилися захищеними настільки добре, що найслабшою ланкою при здійсненні платежів залишилась людина. В той самий час реальний досвід показав, що впровадження додаткових ступенів захисту може знизити зручність користування для кінцевого користувача і зменшити конверсію — частку платежів, що успішно завершуються. Втрата конверсії означає, наприклад, що магазин недоотримає прибуток, а власник картки не здійснить бажану покупку.

Аналіз останніх досліджень і публікацій. Наприкінці 1990-х років Інтернет почав стрімко проникати у повсякденне життя людини. Канал продажів через мережу відкрив нову сторінку в історії торгівлі і викликав дуже швидке зростання дистанційних платежів банківськими картами. Так само стрімко почала збільшуватись частка шахрайства з інтернет-картами, оскільки для здійснення платежу достатньо було мати лише номер картки та термін її дії.

Платіжні системи зреагували на нову загрозу введенням нового захисного параметра — CVV коду, який друкується на звороті картки. Він має гарантувати, що платіж здійснює саме власник картки. Однак через малу довжину коду (3 символи) існує можливість підглянути його під час оплати товарів на касі або отримати шляхом крадіжки фізичної картки.

Так гостра необхідність захистити дистанційні платежі сприяла появі першого стандарту безпеки — 3D Secure. Він додає для онлайн-платежів ще один крок — аутентифікацію держателя, що дозволяє банку переконатися, що платіж ініціював саме держатель картки, аби захиститися від шахрайських операцій.

Вперше розроблена у 1999 р. для Visa Inc., технологія 3D Secure вже понад 20 років забезпечує безпеку інтернет-платежів [2, 4].

Схема роботи 3D Secure 1.0.2. Протокол описує взаємодію трьох сторін (доменів), що і відображено у назві «3D». Ухвалення рішення про можливість здійснення операції з залученням трьох незалежних доменів стало основною ідеєю технології.

Виділимо ці домени та зони їхньої відповідальності [4, 8].

- *Домен емітента* містить власника картки та банк, який випустив цю картку (банк-емітент). У зоні відповідальності цього домену лежить автентифікація власника картки, тобто підтвердження факту легітимного володіння карткою особою, яка здійснює операцію. Основним 3DS-компонентом у домені емітента є ACS (Access Control Server).
- *Домен еквайра* включає інтернет-магазин і банк, що обслуговує його рахунок та операції (банк-еквайр). Цей домен відповідає за вибудовування комерційних відносин із покупцем, а також за проведення фінансової складової операції через платіжну систему. Саме з домену еквайра ініціюється проведення платіжної операції. Основним 3DS-компонент у домені еквайра є MPI (Merchant Plugin Interface).
- *Домен взаємодії* — це платіжна система (ПС). Платіжна система забезпечує взаємодію між доменом еквайра та доменом емітента, встановлює правила цієї взаємодії, визначає вимоги до безпеки, а також надає можливість здійснення фінансової частини операції. Основним 3DS-компонент у домені ПС є DS (Directory Server).

Після визначення основних складових перейдемо до технічної реалізації. Протокол 3D Secure побудований поверх HTTPS протоколу з використанням повідомлень у форматі XML для передачі між доменами. Спрощену схему роботи подано на рис. 1.

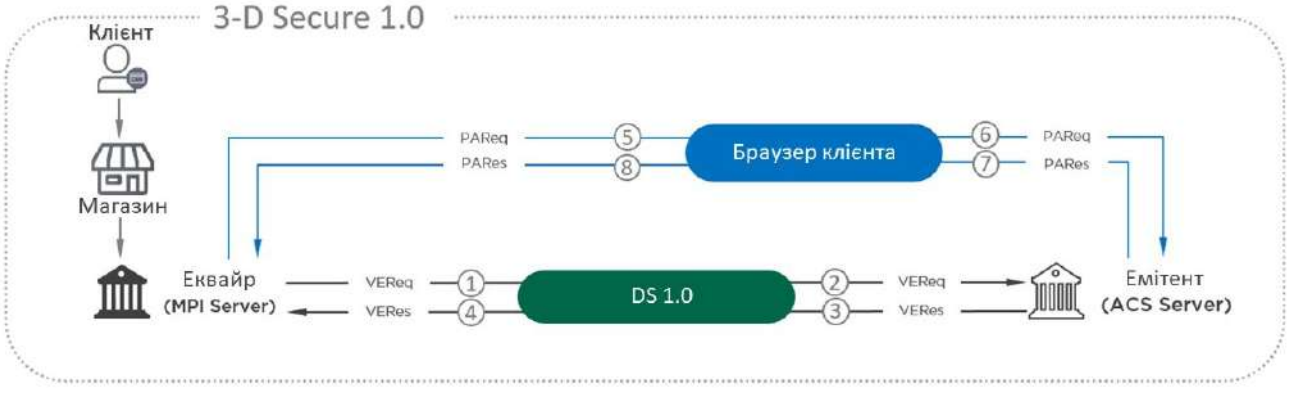


Рис. 1. Загальна схема роботи протоколу 3DS 1.0

Джерело: розроблено авторами.

Виконання платежу складається з таких кроків [8].

1. Утримувач картки оформляє замовлення в інтернет-магазині з оплатою онлайн, на платіжній сторінці вводить реквізити картки та натискає кнопку «Сплатити».

2. Дані з платіжної сторінки передаються до MPI.

3. MPI надсилає до DS повідомлення VEReq (Verification Request) (1) з номером картки та даними про інтернет-магазин.

4. DS перевіряє VEReq-повідомлення, визначає банк-емітент картки та відправляє повідомлення VEReq (2) до ACS.

5. ACS перевіряє VEReq-повідомлення та визначає можливість проведення автентифікації покупця за 3D Secure, після чого формує повідомлення VERes (Verification Response) (3). Якщо проведення автентифікації можливе, в VERes передається URL сторінки ACS, на яку повинен бути перенаправлений користувач. Повідомлення VERes передається до DS.

6. DS перевіряє повідомлення VERes і повертає його назад до MPI (4).

7. MPI формує повідомлення PAReq (Payment Request) (5) з інформацією про операцію та технічними даними від ACS. Повідомлення передається через браузер на URL-адресу ACS, отриману в VERes.

8. ACS у відповідь на запит браузера PAReq (6) повертає форму автентифікації власника картки. Утримувач бачить поле введення одноразового пароля.

9. Утримувач вводить отриманий за sms/push код і натискає кнопку «Підтвердити», код відправляється в ACS;

10. ACS перевіряє код та формує повідомлення PARes (Payment Response) з результатом автентифікації та даними для виконання фінансової складової операції. Повідомлення PARes (7) передається через браузер на адресу MPI.

11. MPI отримує від браузера PARes (8), перевіряє повідомлення, включаючи підпис, а у разі успішної перевірки — ініціює проведення фінансової частини операції (авторизації).

12. MPI отримує результат проведення авторизації та перенаправляє браузер назад в інтернет-магазин, власник картки бачить результат проведення платежу.

Як бачимо, у процесі 3DS-автентифікації відбувається обмін технічною інформацією між декількома залученими сторонами і при цьому процес виглядає досить просто.

Етапи розвитку 3D Secure в Україні. Технологія 3DS стала принципово новим явищем у платіжному просторі країни, тому її входження на український ринок було непростим. Як наслідок,

використання 3DS спочатку сильно підірвало транзакційний потік (конверсію).

Згадаємо, які методи використовували банки для перевірки клієнта [1, 4].

– *Статичний пароль* — найбільш простий спосіб, який було впроваджено одним із перших. При першому платежі з інтернет-магазину клієнт переадресовувався на ACS, де мав вигадати пароль і заповнити форму. Створений пароль прив'язувався до карти і під час наступних платежів з'являлася сторінка автентифікації, де потрібно було його вводити. Перевагами цього способу була відносна простота і можливість швидко змінити пароль за необхідності, тому деякий час цей спосіб автентифікації вважався безпечним та зручним. Але незабаром безпека статичних паролів почала падати і через кілька років після запуску вони перестали вважатися безпечними, тому платіжні системи не рекомендують використовувати їх для 3DS-автентифікації.

– *Скретч карта* — це карта, на якій інформація знаходиться під шаром, що стирається. Для 3D Secure випускалися подібні карти, на кожній знаходилося кілька одноразових паролів. Клієнти отримували ці картки у відділеннях банків. У разі чергового платежу на сторінці ACS потрібно було ввести один із паролів зі скретч-картки. Такий підхід забезпечував більш високий рівень безпеки, але виникали інші проблеми: одноразові коди на карті закінчувалися або, якщо карта губилася, доводилося йти у відділення банку за новою. Клієнти забували про це і стикалися з проблемою вже під час проведення платежу. У результаті падала і конверсія, і задоволеність клієнта.

– *Коди на чеку* — підхід, схожий із попереднім варіантом, але тут одноразові коди друкувалися на чеку під час операції в банкоматі, де отримувати їх було зручніше, ніж у відділеннях. Але чеки також можна було вкрасти, а в банкоматах з'явився інший спосіб: маючи дублікат карти, зловмисник міг зняти гроші, отримати коди та розплатитись в інтернеті.

– *CAP-ридер* (*Chip Authentication Program*) — пристрій, схожий на сучасні мобільні термінали, при отриманні картки видавався клієнту. У нього вставлялася карта, вводився код доступу і на екрані генерувався одноразовий пароль. Такий підхід забезпечував високий криптографічний захист, але не отримав масового поширення через високу вартість CAP-ридера та незручність використання.

– *Display Card* — банківська картка з генератором випадкових паролів. Такі карти були зручні і безпечні, оскільки генератор паролів завжди був під рукою і мав стійкий криптографічний захист. Але були й серйозні мінуси, які не дозволили подібним

картам поширитися масово. Насамперед це вартість, яка не розрахована на масового клієнта. Крім того, у карті було присутнім автономне джерело живлення, яке могло розрядитися раніше закінчення терміну дії картки, і в цілому подібні карти були більш вразливі до механічних впливів.

Сьогодні багатьма банками використовується гібридна система з push- та sms-повідомлень. Такий підхід виправданий, оскільки додаток банку може бути не встановлений, працювати некоректно або ж клієнт може не мати доступу до інтернету. У цьому випадку використовується SMS. Проте спосіб автентифікації за допомогою OTP (одноразовий пароль) перестає задовольняти сучасним вимогам зручності при здійсненні платежів, а шахраї знаходять все нові шляхи та можливості отримання OTP у клієнтів.

Виклад основного матеріалу. Понад двадцять років перша версія протоколу 3DS вирішує поставлене перед нею завдання забезпечення безпеки дистанційних платежів. Проте будь-яка технологія застаріває, і з часом виявилися деякі особливості 3DS 1.0, які зажадали таких поліпшень [4, 5]:

- *Підвищення конверсії*. Який би спосіб автентифікації не використовувався, будь-яке додаткове підтвердження платежу клієнтом створює бар'єр для завершення оплати, від чого страждає і сам клієнт, і магазин. Причини, з яких платіж не завершується, можуть бути різними:

– недовіра клієнтів до спливаючих вікон і введення в них кодів, страх бути обдуреним;

– нерозуміння що саме потрібно зробити для підтвердження оплати;

– помилки при введенні, введення іншого значення;

– погане інтернет-з'єднання, проблеми переадресації на ACS або назад із ACS до магазину;

– відсутність доступу до телефону, прив'язаного до картки;

– проблеми з відправкою SMS на стороні банку або з доставкою SMS на телефон клієнта.

- *Адаптація до мобільних пристроїв*. Платіжні системи при сертифікації емітентів за технологією 3D Secure 1.0 накладали певні вимоги щодо розміру та змісту сторінки автентифікації. Дані вимоги сильно обмежують веброзробника у верстці цих сторінок. У разі використання мобільного пристрою, частка оплат з яких зростає щороку, користувач стикається з наступною проблемою: надавана емітентом HTML-форма виглядає сторонньо в GUI мобільного додатка, її масштаб і розміщення можуть бути незручними для користувача.

- *Підвищення рівня захисту від шахрайства* із застосуванням соціальної інженерії. Жоден метод автентифікації за 3DS 1.0 не забезпечує дійсно надійного захисту платежу від методів шахрайства, відомих за загальною назвою «соціальна інженерія». Одноразовий код шахраї можуть дізнатися безпосередньо у клієнта, ввівши його в оману. Наприклад, шахрай представляється співробітником служби безпеки банку та повідомляє про здійснення підозрілої операції по картці клієнта. Для її скасування необхідно назвати код, який прийде за SMS або PUSH. У цей час за скомпрометованими реквізитами картки шахраєм здійснюється операція грошового переказу, для якої і запитується код підтвердження.
- *Поліпшення користувацького досвіду*. За останні 20 років банки привчили клієнтів, що введення OTP — це нормально. Але насправді менше як 0,05 % всіх операцій є шахрайськими. Тобто майже по всіх операціях із введенням OTP пароль насправді не потрібен, оскільки операцію проводить легітимний власник картки.

Для вирішення цих завдань була розроблена наступна версія протоколу — EMV 3DS 2.0.

Народження EMV 3D Secure. У середині 2010-х моральне та технічне старіння 3DS 1.0.2 підштовхнуло консорціум EMVCo (організація, що займається розробкою стандартів у сфері платіжних технологій) до розробки нової версії протоколу, який отримав назву EMV 3D Secure 2.0. Він схожий на попередника, але має низку істотних покращень [6, 8].

Перша чорнова версія специфікації EMV 3DS мала номер 2.0.1. Перша робоча версія має номер 2.1.0. Перерахуємо її основні можливості та особливості:

- *Frictionless-автентифікація*. За допомогою ризикового аналізу протокол дозволяє (Risk-based analysis, або RBA) виконати Frictionless-аутентифікацію, тобто підтвердження належності картки платнику відбувається без його безпосередньої участі. Це одне з найважливіших нововведень, яке і спричиняє основні переваги нового протоколу: зручність для клієнта та підвищення рівня конверсії для торгівельно-сервісних підприємств (ТСП).
- *Підтримка кількох каналів проведення автентифікації*:

– браузерний (browser-based, або BRW) — звичний канал оплати з інтернет-магазину через браузер на десктопі, мобільному пристрої тощо;

– з програми (application-based, або APP) — 3DS-автентифікація виконується безпосередньо з мобільного додатку, при цьому за реалізацію функцій EMV 3DS відповідає спеціальна

інтегрована у програму бібліотека. Це дозволяє поліпшити користувацький досвід, оскільки автентифікація проходить у нативному оточенні платіжного додатку. При цьому збираються додаткові дані про пристрій, що важливо для впізнавання ризиковою машиною клієнта і підвищує безпеку операції, що проводиться;

– ініційований ТСП (3DS requestor initiated (3RI)) — ініціюється магазином самостійно без запиту власника. Цей канал може бути використаний для передплат, регулярних платежів тощо.

- *Підтримка двох категорій автентифікації*:

– платіжна (Payment, або PA) — власник автентифікується для того, щоб провести оплату товару чи послуги, здійснити грошовий переказ;

– неплатіжна (Non-Payment, або NPA) — власник автентифікується під час здійснення операції, яка не передбачає подальшого руху коштів. Це може бути прив'язка карти до сервісу, перевірка при токенізації картки тощо.

- *Захищеність інформаційних потоків*. На відміну від першої версії 3DS 1.0.2, в якій прикладні дані передаються через браузер, усі значущі дані в EMV 3DS передаються через захищене середовище безпосередньо між компонентами платіжної 3DS-інфраструктури. Пристрій користувача використовується лише для виконання технічних запитів при взаємодії з ACS емітента;
- *Підтримка гнучкої системи ризикового аналізу*, яка, крім виконання Frictionless, може також реагувати на загрози. Якщо система фіксує нетиповий для даного клієнта грошовий переказ, наприклад, з незнайомого пристрою або з іншої країни, то така операція може бути заблокована або вимагати посилених методів автентифікації. Для підтвердження може знадобитися не тільки введення одноразового пароля, але й відповіді на додаткові питання контролю або введення біометричних даних. Очевидно, стовідсоткового захисту від соціальної інженерії не існує, але дана технологія знижує можливість успішного шахрайства порівняно з першою версією 3DS [7].

Як бачимо, наявні проблеми 3DS 1.0.2 значною мірою вирішуються EMV 3DS 2.0. Крім того, протокол активно розвивається, платіжні системи та банки займаються впровадженням його наступної версії — 2.2.0.

Схема роботи EMV 3D Secure 2.0. Протокол 3D Secure 2.0 побудований поверх HTTPS протоколу з використанням повідомлень у форматі JSON. Склад доменної моделі не змінився порівняно з 3DS 1.0. Основні зміни стосуються саме схеми роботи, спрощена модель якої представлена на рис. 2.

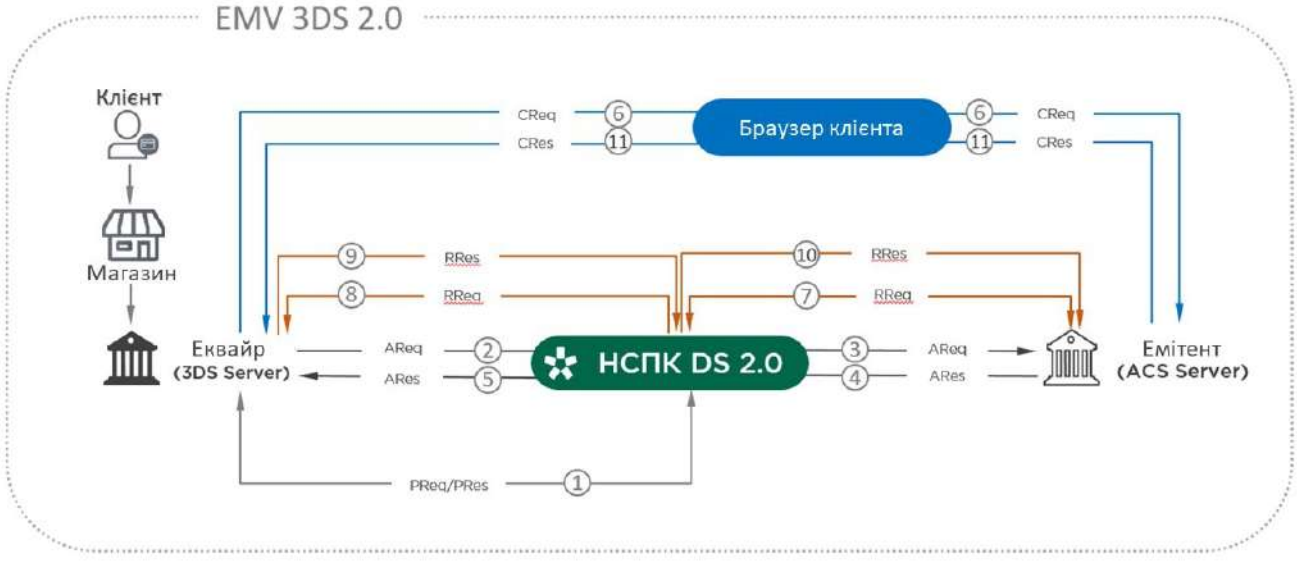


Рис. 2. Загальна схема роботи протоколу 3DS 2.0

Джерело: розроблено автором.

У EMV 3DS доданий новий інформаційний потік між 3DS Server (MPI у минулій версії) та DS. У ньому 3DS Server періодично отримує з DS запитом PReq (1) інформацію про підписані на протокол карткові діапазони емітентів та їх параметри. У повідомленні PRes компонент DS для кожного карткового діапазону повертає підтримувану версію протоколу, додаткові опції, а також адресу 3DS Method URL. 3DS Method URL — це URL-адреса компонента ACS, яка має викликатися 3DS Server-ом у браузері перед автентифікацією користувача. Завдяки цьому виклику ACS може виконати ідентифікацію пристрою, зібрати його параметри та при отриманні запиту на автентифікацію зв'язати його з цими даними.

Нові можливості в EMV 3DS 2.2.0. Випущена наприкінці грудня 2018 року версія специфікації 2.2.0 містить важливі нововведення та покращення [4][8]:

Платіжна автентифікація у 3RI каналі. У 2.1.0 версії для 3RI була можлива лише неплатіжна автентифікація (NPA), доречна при прив'язці карти до особистого кабінету, електронного гаманця тощо, що не є затребуваним для операцій, які ініціюються ТСП без участі власника. У 2.2.0 стала можлива реалізація платіжної автентифікації (PA) у рамках 3RI. Причому сценарій автентифікації можливий як Frictionless, і Challenge. В останньому випадку використовується новий підхід до автентифікації — Decoupled Authentication.

Decoupled Authentication або відкладена автентифікація — це підхід, при якому перевірка власника картки може бути відкладена у часі. Метод автентифікації, який використовуватиметься при цьому, залишається на розсуд емітента. Наприклад, це може бути дзвінок з банку у зручний для клієнта час, запит підтвердження електронною поштою або через мобільний додаток. Ключовим аспектом відкладеної автентифікації є те, що підтвердження необов'язково потрібне в конкретний момент проведення операції, а може бути виконано протягом тривалого часу (до 7 днів).

Whitelisting. Ще одне нововведення специфікації 2.2.0 — можливість для клієнта додати ТСП (інтернет-магазин чи іншу компанію, на адресу якої здійснюється оплата) до списку довірених (whitelist) на стороні емітента. На сторінці автентифікації власник має можливість підтвердити додавання до білого списку даного ТСП. Обов'язковою умовою додавання до білого списку є успішно проведена автентифікація за challenge-сценарієм. При цьому ACS додатково може проінформувати 3DS Server про успішне

додавання цього магазину до білого списку. За підсумками емітент може проводити наступні операції з цього ТСП по тій самій карті без додаткового звернення до власника картки, тобто по frictionless-сценарію, оскільки клієнт дав на це усвідомлену згоду. Крім того, банк-еквайр при наступних сплатах також може вимагати проведення операції за frictionless-сценарієм на підставі того, що ТСП знаходиться в білому списку. Утримувач картки отримує контроль над тим, у яких магазинах він дозволяє оплату без додаткового підтвердження, що у результаті покращує користувацький досвід. Магазинотримує збільшення конверсії, оскільки прибирається зайвий бар'єр у вигляді обов'язкового підтвердження операції. За змістом whitelisting є простим і дешевим способом реалізувати переваги EMV 3DS 2.0 без створення складної RBA-машини.

Висновки. Подальше проникнення EMV 3DS 2.0 у платіжну інфраструктуру призведе до ширшого використання RBA та зниження частки операцій, які потребують підтвердження від клієнта. Робота з поліпшення якості даних і збагачення їх опціональними реквізитами платежу ще більше посилять цю тенденцію [1, 9].

Сьогодні відсутність підтвердження операції одноразовим кодом усе ще викликає стурбованість пересічного користувача. Однак протягом кількох років ситуація зміниться, і питання викликатиме вже запит банком додаткового підтвердження під час здійснення типового платежу. Найбільш технологічні та сучасні гравці ринку вже сьогодні перестають вимагати додаткове підтвердження операцій, які відповідають типовому купівельному профілю власника картки.

Впровадження нових можливостей, таких як відкладена автентифікація та білі списки, ще більше ускладнить 3DS-інфраструктуру, але при цьому запропонує кінцевому користувачеві банківської картки гнучкість та можливість змінювати платіжні налаштування під себе, що ще більше покращить зручність карткових платежів.

Перехід платіжних програм на роботу з інтегрованим SDK (software development kit) підвищить швидкість та зручність процесу підтвердження операції. При цьому завдяки передачі відбитка пристрою також значно підвищиться рівень «впізнавання» емітентом свого клієнта. Частка операцій, що вимагають підтвердження, стрімко зменшуватиметься з поширенням таких додатків та їх активним використанням власниками карток для оплати товарів та послуг.

Платіжна автентифікація для merchant-initiated платежів також підвищить конверсію платежів за підписками на регулярні сервіси, які стають особливо затребуваними останніми роками разом із переходом на сервісну модель споживання.

Отже, у найближчі кілька років ми припускаємо вирішення більшої частини проблем, пов'язаних зі спадщиною технології 20-річної давності, 3D Secure 1.0.2, і зміну на краще користувацького досвіду при здійсненні інтернет-платежів банківськими картками.

Бібліографічні посилання

1. Конверсія вища, ризики нижчі: як технологія 3ds 2.1 підніме дохід інтернет-магазину. *Finance.ua.* URL: https://web.archive.org/web/20200929063156/https://news.finance.ua/ua/news/-/479051/konversiya-vyshha-ryzyky-nyzhchi-yak-tehnologiya-3ds-21-pidnime-dohid-internet-magazynu
2. Технологія 3D Secure — безпечні розрахунки картками в інтернеті / ОТП Банк Україна. URL: https://www.otpbank.com.ua/privateclients/pay-cards/3dsecure/
3. 3D Secure. *Вікіпедія — вільна енциклопедія*. URL: https://uk.wikipedia.org/wiki/3-D_Secure
4. 3D Secure. *Wikipedia*. URL: https://en.wikipedia.org/wiki/3-D_Secure
5. Card authentication and 3D Secure. URL: https://stripe.com/docs/payments/3d-secure
6. Burdett, D. FRC 2801: Internet Open Trading Protocol — IOTP. Version 1.0E. April 2000, 290 p.
7. Murdoch, Steven J.; Anderson, Ross, Sion, R. (ed.). Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication (PDF). URL: https://www.cl.cam.ac.uk/~rja14/Papers/fc10vbvsecurecode.pdf
8. Verified by Visa Implementation Guide (PDF). URL: https://usa.visa.com/dam/VCOM/download/merchants/verified-by-visa-acquirer-merchant-implementation-guide.pdf
9. What is 3D Secure? And Its Advantages for E-commerce. MONEI. URL: https://monei.com/blog/what-is-3d-secure-and-its-advantages-for-e-commerce/

Статтю подано до редакції 22.11.2022

УДК: 330.46 DOI 10.33111/mise.102.14

Щедріна О.І., к.е.н., доцент
кафедри комп'ютерної математики та інформаційної безпеки,
Київський національний економічний університет
імені Вадима Гетьмана

Shchedrina O.I., PhD Candidate of Economic Sciences, Associate Professor
of the Computer Mathematics and Information Security department
KNEU named after V. Hetman

ЦИФРОВА ТРАНСФОРМАЦІЯ ЧЕРЕЗ ХМАРНІ ОБЧИСЛЕННЯ

DIGITAL TRANSFORMATION THROUGH CLOUD COMPUTING

Анотація. *З початком епідемія коронавірусу, а згодом і воєнного стану в Україні, перехід на віддалену роботу збільшив попит на хмарні сервіси. Звичайні користувачі застосовують хмарні сервіси щодня, зберігають важливу для них інформацію в хмарних сховищах, працюють в online-редакторах або завантажують додатки для смартфона. Найбільше можливостей відкривають хмарні сервіси для бізнесу, організацій та підприємств. Хмарні провайдери забезпечують високий рівень зручності експлуатації та інформаційної безпеки, а також надають інструменти для того, щоб отримувати з корпоративної інформації найбільшу користь. Трансформація IT-ресурсів у хмару складний процес, який вимагає системного підходу. Немає однакових планів міграції. Хоча цілі міграції можуть бути схожими, кожна організація або компанія повинна адаптувати свій план на основі бізнес-цілей, ресурсів, термінів, вимог та можливостей. Для багатьох компаній найскладнішим питанням, пов'язаним із міграцією, це «з чого почати формулювати свій план?». Для переходу до «хмари» у статті висвітлено основні питання міграції в хмару, етапи та проблеми реалізації планів. У статті дано трактування понять трансформація та міграція в «хмару». Поданий зміст процесу трансформації в «хмару» і проаналізовані наявні стратегії міграції. Сформовано зовнішні та внутрішні чинники, які впливають на трансформацію в хмару. Автором запропоновано етапи хмарної трансформації на основі проєктного підходу. Матеріали статті мають науково-методичний характер. Розглянуто методичні підходи та методи до розв'язання проблем в трансформації бізнесу до хмар.*

Ключові слова: *Хмара, трансформація, міграція, стратегія міграції, аудит, постачальник хмарних послуг, рехостинг, реплатформинг.*

Abstract. *With the beginning of the coronavirus epidemic, and later the martial law in Ukraine, the transition to remote work increased the demand for cloud services. We, as ordinary users, use cloud services every day, store important information for us in cloud storage, work in online editors or download smartphone applications. Cloud services open up the most opportunities for business, organizations and enterprises. Cloud providers provide a high level of*

ease of use and information security, and also provide tools to get the most out of corporate information.

The transformation of IT resources into the cloud is a complex process that requires a systematic approach. No migration plans are the same. Although migration goals may be similar, each organization or company must tailor its plan based on business goals, resources, timelines, requirements, and capabilities. For many companies, the most difficult question related to migration is "where to start formulating your plan?". For the transition to the cloud, the article highlights the main issues of migration to the cloud, the stages and problems of implementing plans. The article provides an interpretation of the concepts of transformation and migration to the cloud.

The content of the process of transformation into the cloud is presented and the available migration strategies are analyzed. The external and internal factors that affect the transformation into the cloud have been formed.

The author proposed stages of cloud transformation based on a project approach.

The materials of the article have a scientific and methodological nature. Methodical approaches and methods for solving problems in the transformation of business to clouds are considered in the article.

Keywords: *Cloud, transformation, migration, migration strategy, audit, cloud service provider, rehosting, replatforming, rehosting.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими і практичними завданнями. Актуальність теми обумовлена тим, що застосування хмарних технологій дає можливість ефективно розв'язувати завдання бізнесу. Використання хмарних технологій буде найближчими роками повсюдним, а не просто популярним.

Аналітики Gartner [1] заявили, що до 2025 р. понад 85 % організацій перейдуть на принцип хмарних технологій та не зможуть повною мірою реалізувати свої цифрові стратегії без використання хмарних архітектур і технологій.

У 2022 р. глобальний дохід від хмарних обчислень оцінюється в 474 млрд дол. порівняно з 408 млрд дол. у 2021 р. [1]. За оцінками аналітиків Gartner, протягом наступних кількох років прибутки від хмарних обчислень перевищать хмарні прибутки на відповідних корпоративних IT-ринках.

У зв'язку з цим виникає необхідність уточнення теоретико-методологічних засад цифрової трансформації через технології хмарних обчислень.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання проблеми, що висвітлюється, і на які спирається автор. Проблемам теорії та практики міграції в хмару присвячено роботи закордонних і вітчизняних дослідників, а саме: M. Daconta [2], V. Dantas [3], P. Reznik, J. Dobson, M. Gienow [4], О. Є. Камінського [5] та інших. При цьому на сьогодні не існує єдиної точки зору на зміст поняття «хмарна трансфо-

рмація», «хмарна міграція» та її моделі та інструменти. Рівень наукової опрацьованості проблеми визначається новизною її виникнення і пов'язаної з цим поки її слабкою науковою розробкою процесів хмарної трансформації.

Виділення неневирішених раніше частин загальної проблеми, яким присвячується стаття. Механізми функціонування та способи управління хмарною трансформацією залишаються недостатньо вивченими.

Метою статті є дослідження міграції інфраструктури компанії в хмару та розробка практичних рекомендацій для прийняття оптимальних управлінських рішень.

Виклад основного матеріалу дослідження. Одним зі шляхів до цифрової трансформації є впровадження хмарних обчислень, які допомагають створювати інтелектуальні підприємства. Сучасний бізнес розглядає трансформацію в хмару не як тренд, а як інструмент збереження конкурентної спроможності та підвищення ефективності роботи. Для того щоб зберігати конкурентоспроможність компаніям необхідно не тільки уважно стежити за тенденціями розвитку нових технологій, але і застосовувати їх. До таких технологій належить хмарні обчислення.

Хмарні технології ─ це модель надання повсюдного і зручного доступу до загальних обчислювальних ресурсів, які можуть бути швидко надані і звільнені з мінімальними експлуатаційними затратами або звернення до провайдера. Сутність хмарних технологій полягає в наданні віддаленого доступу до послуг, обчислювальним ресурсам і інтернет-додаткам.

Міграція в хмару — це процес переміщення програм та даних з одного розташування (зазвичай це приватні сервери компанії, локальні сервери) на сервери постачальників загальнодоступних служб хмар, а також між різними хмарами.

Мігрують в хмару бази даних, вебсайти, сховища, сервери, додатки і встановлені налаштування. Існує декілька видів перенесення IT-інфраструктури: повна і часткова міграція, і створення гібриду, переміщення між хмарами, переміщення із хмари в локальне середовище.

Компанія може виконувати різні типи хмарних міграцій. Однією з поширених моделей є передача даних і додатків із локального центру обробки даних у загальнодоступне середовище. Однак міграція в хмару може також призвести до переміщення даних і додатків з однієї хмарної платформи або постачальника на інших; ця модель відома як міграція з хмари в хмару. Існує зворотна хмарна міграція, репатріація хмари або вихід із хмари,

коли дані або додатки переміщуються з хмари навпаки в локальний центр обробки даних

Повна міграція. При повної міграції в хмару повністю переміщують інформація, використовувані додатки і сервіси та інше. Такий варіант міграції може бути зручним для малого і середнього бізнесу.

Часткова міграція. При часткової міграції частина ресурсів переноситься в хмару, а частина залишається в локальному середовищі. Такий варіант переходу підходить великим організаціям з декількома офісами.

Створення гібриду. За такого варіанту комбінуються можливості приватної і публічної хмар, а також локальної інфраструктури. Частина сервісів може перебувати в локальному (корпоративному) середовище, частина — в приватній хмарі, а решту необхідних додатків і даних — в публічній. Між хмарами встановлюється захищений канал для безпечного перенесення даних між хмарами.

При міграції з хмари в хмару організації переміщують додатки або дані з одного хмарного середовища до іншого. Великі постачальники хмарних послуг пропонують інструменти управління міграцією в хмару.

Багато організацій використовують декілька хмар і переміщують ресурси між загальнодоступними хмарами шляхом міграції з хмари до хмар. Крім того, такий тип міграції корисний, коли організації потрібні переваги продуктів, служб та цін, що надаються хмарними платформами. Хоча управління ресурсами у кількох хмарах може бути складним процесом, ними можна легко управляти з одного розташування, використовуючи засіб централізованого управління.

Зворотна міграція в хмару, також відома як репатріація в хмару, передбачає переміщення додатків назад до інфраструктури або приватної хмари. Як правило, організації переміщують частину або всі свої бізнес-компоненти із загальнодоступної хмари до локального центру обробки даних, який є більш безпечним та забезпечує більший контроль над обчислювальним середовищем.

Одним із рішень для змінних потреб є поява гібридних рішень для зберігання даних, які поєднують у собі локальне (або приватне хмарне сховище) та загальнодоступне хмарне сховище. Разом вони поєднують у собі продуктивність та масштабованість пропозицій загальнодоступної хмари з безпекою та налагодженістю приватних чи локальних розгортань. Але щоб гібридні рішення були життєздатними, два рішення (локальна та загальнодоступна хмара) мають бути сумісні.

Міграція в хмару може бути простим або складним процесом залежно від того, куди компанія хоче перенести свій бізнес у хмару. Перша частина цієї складності полягає у нескінченних термінах.

Такі терміни, як хмарна стратегія, хмарна трансформація, хмарна міграція та служби хмарної міграції, частково збігаються. Вони є частиною одного цілого, а також означають різні речі. Під цими термінами мають на увазі наступне, з погляду як один термін впливає на інший:

Хмарні обчислення — доставка IT-ресурсів на вимогу через інтернет з оплатою за фактом використання. Купувати, розміщувати та обслуговувати фізичні центри обробки даних та сервери не потрібно. Натомість компанія отримує доступ до технологічних сервісів: обчислювальних сервісів, сховищ та баз даних, якими можна користуватися за необхідності завдяки постачальнику хмарних послуг, такому як, наприклад, Amazon Web Services (AWS).

• *Хмарна стратегія* — це те, що компанія хоче, щоб хмара зробила для бізнесу з точки зору операційних результатів.

• *Хмарна трансформація* — це процес використання хмари для досягнення цих результатів з часом.

• *Хмарна міграція* — це метод актуалізації зміни міграції вибраних додатків, робочих навантажень та сховищ у хмару, щоб зробити ці операційні результати реальними та активними.

• *Послуги та інструменти хмарної міграції* спрощують процес хмарної міграції шляхом автоматизації, яка спрощує, організовує та стандартизує виконання кроків у процесі міграції.

• *Постачальники хмарних послуг* (CSP) надають хмарні середовища, архітектурні стандартні блоки, послуги та інструменти для планування, міграції, управління та оптимізації додатків та робочих навантажень у хмарі.

Єдиного визначення термінів «хмарна трансформація» і «хмарна міграція» не існує. Це пов’язано з тим, що кожне перетворення хмари та кожна міграція у хмару є унікальним досвідом. Вони обидва глибоко впливають на взаємодію людей, процесів і технологій, що працюють разом з додатками, даними та сховищем.

Хмарна трансформація полягає в тому, як локальні додатки, робочі навантаження та сховища змінюється у разі їх переміщення до хмари. Хмарна трансформація ніколи не буває одиничною подією з єдиним результатом, а є безперервною серією подій з потенційно безліччю певних результатів.

Хмарна трансформація є безперервністю, стійкістю та гнучкістю, які необхідні бізнесу компанії для адаптації та процвітання в

цифрову епоху. Компанії потрібно побудувати свою стратегію хмарної трансформації задля досягнення конкретних цілей за допомогою перенесення додатків та робочих навантажень у хмару. Переваги роботи у хмарі, як правило, включає: перевагу у витратах та безпеці, експлуатаційні переваги.

Для досягнення цих цілей необхідна розробка стратегії до переходу до хмарної трансформації, яка потребує активного партнерства в рамках усієї компанії. Потрібно сфокусувати стратегію на виконанні чотирьох етапів поточної трансформації хмари за допомогою міграції, які включають:

- планування;
- доставлення та міграція;
- управління;
- оптимізація.

Для того щоб зрозуміти, чого компанія хоче досягти в хмарі, необхідно починати з розуміння її поточного стану, щоб вибрати правильний шлях для досягнення певних бізнес-результатів за допомогою хмарної трансформації. Аналіз поточного середовища (людські процеси, мережі, додатки, робочі навантаження та сховище) є основою визначення того, що, де і як перенести в хмару. Бізнес-результати або цілі компанії є деякою комбінацією економії витрат, масштабованості, доступу, безпеки та гнучкості бізнесу у найширшому сенсі. Порівнюючи ці цілі з повним уявленням про поточне середовище, можна визначити:

- які програми, робочі навантаження, сховища та їх залежність від додатків принесуть найбільшу віддачу від міграції;
- що з цього потрібно перемістити, коли, як і куди.

Усі програми, які використовує компанія, потрібно розділити на чотири категорії:

Програми не можна перемістити до хмари. якщо перенесення програми в хмару неможливе, то найкращий спосіб для таких програм ─ зберегти та використовувати програми локально;

2. Коригування додатків. До цієї категорії потрібно віднести додатки, які мають цінність для бізнесу, але потребують поліпшення та коригування;

3. Не потребують змін — належать додатки, які мають цінність і не вимагають змін.

4. Припинення експлуатації програми. Програми, які не становлять жодної цінності для бізнесу, у цьому випадку програми перестають експлуатувати.

Під час аналізу необхідно також відповісти на питання, які подані в табл. 1.

Таблиця 1

ПЛАНУВАННЯ ПЕРЕХОДУ ДО ХМАРИ

Аналіз	Яке обладнання, додатки, сховища компанія має нині? Як вони використовуються для бізнесу? Скільки з них зберігають, взаємодіють зі конфіденційною інформацією? Як можна консолідувати, завершити експлуатацію, мігрувати, адаптувати, трансформувати їх? Що потрібно вивести з експлуатації, замінити, повторно розмістити, перебудувати, залишити локально? Що і скільки компанія заощадить у плані витрат або навантаження, перейшовши в хмару? Як вимірювати витрати? Чи може компанія перенести сховища даних, які стосуються конфіденційної інформації, у хмару? Яка користь для користувача від будь-якої програми (робочого навантаження)? Які моделі витрат компанія використовує для визначення заощаджень? Як компанія аналізує витрати, щоб довести успіх міграції? Чи може компанія перенести сховища даних, які містять конфіденційну інформацію, у хмару? Яка користь для продуктивності користувача від будь-якої програми (робочого навантаження)?
Оцінка витрат	Щоб оцінити реальну цінність міграції для компанії, необхідно оцінити поточні витрати та які додаткові тимчасові витрати можуть бути понесені у рамках проєкту міграції. Щоб забезпечити максимально ефективну міграцію, компанія повинна проаналізувати та порівняти потенційні витрати, які будуть пов'язані з переходом додатків до різних хмарних провайдерів. Терміни, тривалість, вартість запланованих сервісів і порядок міграції всі програми можуть збільшити вартість міграції
План міграції	Які хмарні сервіси провайдеру будуть використовуватися для додатків та сховищ? Як команди (провайдера, компанії) співпрацювати під час міграції? Якими будуть витрати? Якою буде ціна тривалих затримок? Які фактори, що затримують, можемо врахувати до того, як почнемо міграцію? Як компанія буде навчати користувачів? Чи будуть користувачі та ІТ-відділ готові до роботи одночасно?
Тестування, пілотування, налаштування	Що вимагатиме дубльованого чи гібридного стану для тестування? Що можна тимчасово протестувати у хмарі? Як захищатиметься конфіденційна інформація? Як впроваджуватиметься та вдосконалюватиметься механізми контролю витрат? Як необхідно отримувати відгуки кінцевих користувачів про покращення для всіх змінених процесів? Як можна спланувати та перепланувати фінансове становище компанії для подальших покращень під час та після міграції

Відповіді на ці запитання залежать від того, чи володіє компанія внутрішнім IT-досвідом і готовністю розробляти та реалізовувати стратегію трансформації та міграції.

За результатами аудиту необхідно отримати оцінку поточної ситуації в IT-інфраструктурі компанії, з рекомендаціями щодо модернізації наявної інфраструктури (капітальні витрати), і доцільності міграції в хмару (операційні витрати).

Слід розпочати з аудиту та оцінки всіх додатків, які використовує компанія на можливість їх міграції у хмару. Потрібно відповісти на такі запитання: Яке програмне забезпечення використовує компанія? Від яких додатків компанія може відмовитись, оскільки вони застаріли або не мають цінності для компанії? Аналізуючи результати, потрібно встановити, що робити з кожним компонентом системи, необхідно оцінити цінність компанії кожного компонента систем.

Метою планування стратегії міграції у хмару є допомога у формулюванні відповідей на безліч питань, пов'язаних із тим, що, куди, чому, як і коли переміщати. Кожна стратегія міграції у хмару має бути спрямована на узгодження потреб бізнесу з варіантами міграції додатків, робочого навантаження та сховища, які забезпечують:

- зниження капіталовкладень;
- підвищення масштабованості;
- появу нових послуг та збільшення доходів;
- покращення доступу до додатків для віддалених співробітників;
- підвищення безпеки та контролю;
- оптимізація бізнесу та аварійне відновлення.

Першим етапом у розробці докладної стратегії міграції у хмару є точне розуміння того, що таке стратегія міграції у хмару. Більшість організацій розуміють, що стратегія міграції у хмару є основою їхніх найближчих та довгострокових планів підвищення ефективності роботи та бізнес-інновацій. Стратегія визначає, як хмара поміняє поточні та майбутні бізнес-операції та результати.

Важливо розуміти, що стратегія міграції у хмару — це довгостроковий документ, у якому поточні та майбутні міграції додатків розглядаються через бізнес-стратегію міграції у хмару. Бізнес-стратегія міграції в хмару — це більш докладне уявлення компанії загальної стратегії щодо хмари та того впливу, який міграція вплине на покращення бізнес-операцій та результатів. Це має допомогти компанії створити економічне обґрунтування міграції, тобто це означає чітке уявлення про те, що компанія очікує отримати в результаті міграції.

Визначення витрат на трансформацію у хмару, до яких відносяться сукупна вартість володіння (TCO) та окупність інвестицій (ROI), капіталовкладення та експлуатаційні витрати, вплинуть на стратегію. Необхідно довести розрахунками і показати, що сукупна вартість володіння загальнодоступних хмарних сервісів менша, ніж сукупна вартість володіння локальними альтернативами. Не завжди просто визначити витрати та окупність інвестицій у хмарну міграцію, наприклад, для гібридних або мультихмарних середовищ між кількома постачальниками хмарних послуг.

Успіх стратегії міграції в загальнодоступну хмару буде залежати від безлічі факторів, які взаємопов'язані і можуть бути реалізовані за допомогою низки етапів (кроків) стратегії міграції в хмару:

• Підготовка співробітників компанії до змін міграції до хмар (розробка плану навчання).

• Картування додатків та оцінка інфраструктури. (Карти бізнес-процесів — це метод, розроблений для схематичного проєктування процесу, щоб кожен член команди досяг однієї і тієї ж ідеї та виконував процес у точній відповідності до методу. Кінцевою метою картування процесів є надання докладної інформації про процеси, що допомагають організації, і про те, як вони підтримують її у досягненні її бізнес-цілей.).

• Варіанти перенесення додатків.

• Терміни міграції (коли і що мігрувати).

• Модернізація мережі та міркування продуктивності.

• Пропускна здатність та затримка.

Підготовка інфраструктури компанії до змін варто розпочати з детального розуміння корпоративного портфеля додатків. Необхідно порівняти програми, щоб визначити, які програми будуть переміщені в хмару. Це також допоможе визначитися з використанням поетапного чи масштабного підходу до міграції у хмару, щоб можна було встановити терміни та графіки таких переміщень.

У 2010 р. компанія Gartner опублікувала п'ять стратегій міграції в хмару, пізніше компанія AWS змінила цей список і ввела свої так звані «6R», зараз визначають «7R».

Процес міграції для кожної програми зводиться до одного з шести підходів:

• *Рехостинг* (Rehosting) — переміщення додатків у хмару «як є». Зазвичай його використовують великі організації, які потрібно швидко перенести велике число додатків. За допомогою цієї стратегії легко переміщають локальні програмні компоненти в

хмару, нічого не змінюючи. Таке рішення, як правило, є короткостроковим. Оскільки програми не оптимізовані та не модифіковані для хмарного середовища, такі програми можуть зіткнутися з проблемами продуктивності.

• *Рефакторинг* (Refaktoring) — зміна архітектури. Змініть код програми для кращої підтримки хмарного середовища. Рефакторинг має на увазі повний реінжиринг програм для створення його хмарної версії. Ця стратегія є найбільш трудомісткою та витратною, але вона забезпечує довгострокову економію завдяки відповідності фактичних потреб у ресурсах хмарної інфраструктури. Хмарні програми дозволяють компанії швидко адаптуватися до нових вимог клієнтів, оскільки розробники легко додають або змінюють наявні функції.

Метод рефакторингу або повторної архітектури включає переписування додатків з нуля, щоб зробити їх хмарними. Ця стратегія дозволяє реалізувати весь потенціал хмарних технологій, таких як архітектура мікросервісів, безсерверні рішення, контейнери, функція як послуга та балансування навантаження.

• *Реплатформа* (Replatforma) — зміна платформи, перенесення хмарних програм без істотних змін, але з використанням переваг хмарного середовища. Розробники роблять незначні оптимізації перед міграцією. Це не призводить до змін у базовій архітектурі програми.

• *Replace* (Замінити) — припинення підтримки програми та заміна її новою хмарною програмою.

• *Retain* (Залишити) — зберегти локальні додатки, які важко перенести.

• *Retire* — виведення з експлуатації: робота деяких додатків може бути припинена, і їх слід припинити експлуатувати, а не мігрувати в хмару.

• *Reimagine* — переосмислення бізнес-процесів для використання переваг хмари.

У табл. 2 подана характеристика основних стратегій міграцій.

Внутрішня мережа відіграє велику роль у процесі міграції у хмару від попередньої до наступної міграції, оскільки вона повинна буде підтримувати процеси міграції, балансування навантаження та інші аспекти, пов’язані з доступом до додатків, затримкою, пропускною здатністю та оптимізацією. Для визначення поточного стану потрібна оцінка мережі для порівняння трафіку додатків та пристроїв. Оптимізація мережі є важливою ланкою при міграції у хмару, де доступ до програм та безпека мають першорядне значення.

Таблиця 2

ХАРАКТЕРИСТИКА ОСНОВНИХ СТРАТЕГІЙ МІГРАЦІЙ

Назва стратегії	Рехостинг	Реплатформинг	Рефакторинг
Короткий опис	Програми та дані переносяться у хмару практично без змін	Додатки та дані зазнають деяких змін, необхідних для більш ефективного використання хмарної архітектури та сервісів	Програми і дані перевіряються та перекодуються для ефективної роботи у хмарному середовищі.
Інтеграція з хмарною архітектурою	мала	середня	висока
Складність реалізації	низька	середня	від середнього до високого
Переваги	Не потрібно жодних змін у коді. Простота перенесення основних сервісів. Дуже низькі початкові витрати. Не потрібний додатковий аудит безпеки або відповідності вимогам	Надає доступ до більшості власних хмарних функцій. Потребує помірних навичок розробки програмного забезпечення. Може бути масштабовано пізніше.	Програми та бази даних будуть спочатку працювати в хмарі. Підвищена продуктив-ність та надійність. Спрощення внесення подальших змін. Поліпшена масштабованість. Найкраща економічна ефективність у довго-строковій перспективі
Недоліки	Не можна отримати всі можливості та переваги хмари. Можуть виникнути проблеми з оптимізацією. Програми можуть працювати не так, як передбачалося	Пізніше може знадобитися великий рефакторинг. Для ефективного функціонування потрібна автоматизація. Не використовується весь спектр хмарних послуг	Для застосування потрібні досвід та час. Потрібні великі початкові інвестиції. Залежить від прив'язки до постачальника послуг

Після порівняння програм, визначення залежності одних додатків від інших, потреби в інфраструктурі та мережі, можна розпочати проєктування та налаштування хмарної архітектури, спочатку оцінивши витрати на інфраструктуру на основі потреб у зберіганні даних, трафіку та використання пам'яті (ресурсів ЦП).

Програми, робочі навантаження та пов'язані з ними бази даних постійно змінюються через введення нових даних, оновлень та змін, які є частиною їхнього звичайного повсякденного використання. У процесі міграції центру обробки даних компанія обов'язково повинна мати можливість відстежувати ці зміни.

Крім того, компанія також повинна мати можливість безпомилково оновлювати ці зміни в режимі реального часу протягом усього процесу міграції, особливо на етапах тестування та переходу. Відстеження цих незначних змін вручну без інструменту автоматизації, який може постійно відстежувати та реплікувати свіжі зміни у міру проходження процесу міграції, практично неможливе.

Після перенесення додатків та робочих навантажень вони існують одночасно з локальними робочими навантаженнями до повного переходу у хмару. Компанія повинна тестувати систему таким чином, щоб вона представляла кінцеве виробниче середовище.

Тестування. Перш ніж переносити робочі навантаження, потрібно протестувати та порівняти роботу однієї й тієї ж програми локально й у хмарі. За необхідності оптимізувати ресурси для забезпечення прийнятних значень. Зазвичай параметри роботи програм включають:

- швидкість запуску;
- швидкість відгуку;
- продуктивність у періоди високого та низького навантаження;
- зручність використання на різних платформах.

Після тестування робочі навантаження та додатки переносяться в хмару. Однак на цьому процес не закінчується. Після завершення міграції необхідно протестувати навантаження, оцінити показники та перевірити хмарну інфраструктуру на наявність вразливостей.

Висновки. Застосування хмарних технологій на сьогодні актуально в усіх галузях і типах бізнесу. Хмарна міграція ― це не просто перехід у хмару; це ітеративний процес оптимізації, спрямований на зниження витрат та повне розкриття потенціалу хмари. Це впливає на всі організаційні аспекти, включаючи людей, процеси та технології. Але завдяки гнучким моделям споживання

та ціноутворення хмара може підтримувати високу масштабованість, продуктивність, гнучкість, віддалену роботу та економічність.

Бібліографічні посилання

1. Gartner Says Cloud Will Be the Centerpiece of New Digital Experiences. URL: https://www-gartner-com.translate.goog/en/newsroom/press-releases/2021-11-10-gartner-says-cloud-will-be-the-centerpiece-of-new-digital-experiences?_x_tr_sl=en&_x_tr_tl=ru&_x_tr_hl=ru&_x_tr_pto=sc#:~:text=By%202025%2C%20Gartner%20estimates%20that,up%20from%2030%25%20in%202021

2. Daconta M. The Great Cloud Migration: Your to Cloud Computing, Big Data and Linked Data. Publisher: Outskirts Press, 2013. 218 p.

3. Dantas V. Architecting Google Cloud Solutions: Learn to design robust and future-proof solutions with Google Cloud technologies. Publisher: Packt Publishing, 2021. 472 p.

4. Reznik P., Dobson J., Gienow M. Cloud Native Transformation. Publisher: O'Reilly Media, 2019. 540 p.

5. Камінський О.Є. Хмарні технології в парадигмі інформаційної економіки: монографія. Київ: КНЕУ, 2018. 230 с.

Статтю подано до редакції 21.11.2022

УДК 330.46:004.49

Фролов Д.І.,
кафедра математичного моделювання та статистики
Київський національний економічний університет
імені Вадима Гетьмана

Матвійчук А.В., д.е.н., професор
кафедри математичного моделювання та статистики
Київський національний економічний університет
імені Вадима Гетьмана

Frolov D.I.,
Department of Mathematical Modeling and Statistics,
Kyiv National Economic University named after Vadym Hetman

Matviychuk A.V., Doctor of Economic Sciences,
Professor of Department of Mathematical Modeling and Statistics,
Kyiv National Economic University named after Vadym Hetman

КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО РОЗПІЗНАВАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА ОСНОВІ ТЕХНОЛОГІЙ МАШИННОГО НАВЧАННЯ

CONCEPTUAL APPROACH TO MALWARE RECOGNITION BASED ON MACHINE LEARNING TECHNIQUES

Анотація. *Україна протягом останніх років знаходиться в стані неоголошеної кібервійни. За останнє десятиліття аналіз та методи виявлення шкідливих програм пройшли значні зміни, що віддзеркалює відповідний розвиток різноманітних технік з розробки шкідливого програмного забезпечення. Системи виявлення шкідливих програм (MDS) — це перша лінія захисту від зловмисних атак. Тому для таких систем критично важливим є максимально точне й ефективне виявлення загроз. Зазвичай MDS використовують традиційні алгоритми машинного навчання, які потребують вибору та видобування ознак, що займає багато часу та може викликати помилки. В даній статті представлений концептуальний підхід до розпізнавання шкідливого програмного забезпечення з використанням новітніх моделей машинного навчання, розроблених для опрацювання зображень. Техніка конвертації файлів шкідливого програмного забезпечення в зображення у відтінках сірого відкриває можливості використання нейромережевих архітектур, розроблених для їх розпізнавання та класифікації. Згорткові нейронні мережі, а також найновітніші трансформери Swin 1-ої та 2-ої версій, разом із гібридною нейронною мережею CoAtNet, виступають перспективними кандидатами для проведення дослідження з визначення найбільш ефективної моделі для виявлення та класифікації шкідливого програмного забезпечення. Дана стаття може стати важливим підґрунтям для майбутніх дослідників у міждисциплінарній області використання методів та технік машинного (та глибинного) навчання в сфері кібербезпеки.*

Ключові слова: *кібербезпека, MDS, розпізнавання шкідливого програмного забезпечення, глибинне навчання, згорткова нейронна мережа, CoAtNet, Swin трансформер*

Abstract. *Ukraine has been in a state of undeclared cyberwar for several years. Over the past decade, malware analysis and detection methods have undergone significant changes, reflecting the corresponding development of various techniques for developing malicious software. Malware Detection Systems (MDS) are the first line of defense against malicious attacks. Therefore, it is critically important for such systems to accurately and effectively detect threats. Typically, MDS use traditional machine learning algorithms, which require feature selection and extraction, a process that is time-consuming and error-prone. This article presents a conceptual approach to recognizing malicious software using state-of-the-art machine learning models developed for image processing. The use of the technique of converting malicious software files into grayscale images opens up opportunities for the use of neural network architectures developed for image recognition and classification. Convolutional neural networks, as well as the latest Swin transformers of the 1st and 2nd versions, along with the CoAtNet hybrid neural network, are promising candidates for further research to determine the most effective model for recognition and classification of malicious software. This article could be an important milestone for future researchers in the interdisciplinary field of using machine (and deep) learning methods and techniques in cybersecurity.*

Keywords: *cybersecurity, MDS, malware detection, deep learning, convolutional neural network, CoAtNet, Swin transformer*

Постановка проблеми. У 2022 році в Україні почалася повномасштабна війна. Для того, щоб завдати найбільшої шкоди нашій країні, з боку агресора використовується різноманітна зброя. Особливе місце в цьому займають кібератаки. При цьому, в Україні фактично вже декілька років триває повномасштабна кібервійна.

Зростання кількості випадків атак зловмисного програмного забезпечення (написаного як досвідченими злочинцями, так і початківцями за допомогою загальнодоступних моделей машинного навчання, таких як ChatGPT), зниження вартості процесорної потужності та прогрес, досягнутий у цій галузі, сприяють появі нових досліджень та пропозицій щодо покращення аналізу шкідливого програмного забезпечення (ШПЗ). Так, протягом останніх років машинне, зокрема глибинне навчання, активно використовуються в світі як підхід до виявлення та аналізу шкідливих програм.

У зв’язку з цим, тематика дослідження теоретичних та технологічних аспектів інтелектуальних систем [1], використання методів та технік штучного інтелекту в сфері кібербезпеки, а також, як результат, проблематика вибору найбільш ефективних моделей машинного навчання для розпізнавання та класифікації шкідливого програмного забезпечення є особливо актуальною в цей час.

Системи виявлення шкідливих програм (Malware Detection System або MDS) — це перша лінія захисту від зловмисних атак [2]. Тому для таких систем критично важливим є максимально точне й ефективне виявлення загроз. Зазвичай MDS використовують традиційні алгоритми машинного навчання, які потребують вибору та видобування ознак, що займає багато часу та може викликати помилки. В даній статті представлений концептуальний підхід до розпізнавання шкідливого програмного забезпечення з використанням новітніх моделей машинного навчання, розроблених для опрацювання зображень.

На початкових етапах застосування машинного навчання до проблеми розпізнавання зловмисного програмного забезпечення застосовувалися алгоритми кластеризації. Однак ці підходи, здебільшого, не вирішують проблему, коли в наборі даних, що аналізується, присутній широкий спектр класів шкідливих програм.

Аналіз останніх досліджень і публікацій. За останні два десятиріччя проводилось багато досліджень у сфері виявлення та класифікації шкідливого програмного забезпечення із застосуванням методів та технік машинного навчання, деякі з котрих заслуговують на особливу увагу [3-10].

Отримані за результатами зазначених досліджень показники точності варіюються та, за певних умов, досягають 99 %. Так, в дослідженні [3] представлені результати застосування декількох модифікованих алгоритмів перцептрона для виявлення шкідливого програмного забезпечення — було досягнуто точності від 69,90 % до 96,18 %, при цьому більш точні моделі мали також більшу кількість помилкових спрацювань.

Разом з цим, в науковій роботі [4] досліджувався метод виявлення шкідливого програмного забезпечення, що базується на модифікованому алгоритмі випадкового лісу (random forest) в поєднанні з коефіцієнтом інформаційного приросту для кращого представлення ознак. Такий підхід забезпечив точність 97 % за низького рівня помилкових спрацювань, що робить його придатним для захисту корпоративних мереж.

В рамках комплексної роботи з дослідження різних методів машинного навчання для класифікації статичних характеристик 32-бітних зловмисних виконуваних файлів (portable executable або PE32) для Windows [6], автори видобули n-граму байтів, n-граму коду операції, виклики API та PE32 із виконуваного файлу Windows і застосували алгоритми на основі статистики (наївний Байєс), методу опорних векторів (support vector machine або SVM) і методу найближчих сусідів (k-nearest neighbors або k-NN).

Також було виявлено, що у більшості випадків класифікаційний алгоритм C4.5 та k-NN виявляють кращу ефективність, ніж інші методи, в той час як SVM та штучні нейронні мережі (artificial neural network або ANN) на деяких наборах ознак показали гарну продуктивність. З іншого боку, мережа Байєса та наївний Байєс мають погану ефективність порівняно з іншими методами машинного навчання. Отримані результати підтверджують тезу, що машинне навчання допомагає в аналізі шкідливих програм та може використовуватися в рамках діяльності з кіберзагрозами для автоматизації виявлення індикаторів компрометації. Незважаючи на те, що в результаті цього дослідження були отримані всі статистичні характеристики з виконуваного файлу, жоден із алгоритмів, які використовувались, не зміг досягнути рівня точності 96 %.

Результати новітнього дослідження з аналізу та виявлення шкідливих програм за допомогою алгоритмів машинного навчання [10] показали, що згорткові нейронні мережі (Convolutional Neural Networks або CNN) мають точність розпізнавання 98,76 %, опорно-векторні машини (SVM) — 96,41 %, а дерева рішень (decision trees або DT) — 99 %, таким чином, перевершуючи інші класифікатори за цим показником. Було проведено порівняння ефективності алгоритмів DT, CNN та SVM щодо виявлення шкідливого програмного забезпечення на тестовому наборі даних за умови низького рівня помилкових спрацювань (false positive rate або FPR). Помилкові спрацювання склали: 2,01 % для DT, 3,97 % для CNN та 4,63 % для SVM, відповідно. Таким чином, метод машинного навчання DT показав найкращі показники на наборі даних від Канадського інституту кібербезпеки. Представлені результати мають особливе значення в поточних умовах, коли програмне забезпечення стає все більш поширеним і складним для виявлення зловмисного коду.

Шкідливі програми також постійно еволюціонують і стають все складнішими. Внаслідок цього, виявлення та розуміння їх внутрішніх механізмів також становить задачу з високим рівнем складності. Крім того, зростаюча динаміка та різноманітність сучасних технологій зв'язку та обчислення дозволяють одній шкідливій програмі проявлятися в семантично та структурно різних формах. Як результат, процес її ефективного виявлення та класифікації потребує, відповідно, застосування найбільш сучасного інструментарію. Враховуючи ризики, які створює ШПЗ, в тому числі для критичної інфраструктури, точність його розпізнавання має прямувати до 100 %.

Разом з цим, ще у 2011 році в статті «Зображення шкідливого програмного забезпечення: візуалізація та автоматична класифікація» колективом авторів [11] було запропоновано підхід до оцінювання та класифікації ШПЗ на основі його візуалізації у вигляді зображень у відтінках сірого. За результатами зазначеної роботи був створений набір даних Malimg, який буде більш детально розглянутий далі у цій статті.

Метод Натараджа та співавторів [11] зосереджений на виконуваних файлах, що містять код шкідливого програмного забезпечення. Вони використовували необроблені двійкові дані з таких файлів в процесі побудови байтових зображень, зрештою генеруючи зображення в градаціях сірого для класифікації (рис. 1).

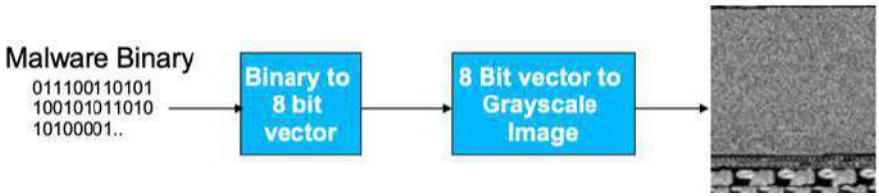


Рис. 1. Візуалізація зловмисного програмного забезпечення як зображення [11]

Процес отримання зображення з виконуваного файлу містить такі етапи:

- попередня обробка — очищення зразків ШПЗ для видалення непотрібної інформації, такої як заголовки та залишкові дані; як результат, зображення зосереджуються на основній функціональності такого програмного забезпечення;
- побудова байтових зображень — цей метод перетворює необроблені двійкові дані шкідливого програмного забезпечення (послідовність байтів) на двомірне зображення в градаціях сірого, коли кожному значенню байта у вихідних даних відповідає певна інтенсивність пікселя на зображенні (наприклад, нижчі значення байтів відображаються темнішими пікселями, ближче до чорного, а вищі значення — світлішими пікселями, ближче до білого);
- зміна розміру зображення — для налаштування зображення до розміру, придатного для подальшої обробки та аналізу, використовуються такі методи, як інтерполяція;
- стандартизація — додаткова стандартизація зображень для покращення ефективності алгоритмів класифікації можлива за

допомогою методів обробки зображень, таких як нормалізація або гістограмне вирівнювання.

Підхід [11] не обмежується певним типом формату виконуваного файлу. Конкретний тип файлу може змінюватися залежно від того, який зразок шкідливого програмного забезпечення аналізується.

Переформувавши масив 8-бітних елементів коду у матрицю та розглянувши його як зображення у градаціях сірого, авторам [11] вдалося виявити важливі візуальні кореляції в текстурі зображення шкідливих програм, що належать до того самого сімейства. Це може бути наслідком широкого розповсюдження методу створення нових варіантів шкідливого ПЗ через повторне використання коду в програмі зборки.

Виконуваний файл (наприклад, з розширенням .exe для Windows файлів) складається з трьох основних розділів:

– .data (initialized data) — розділ даних використовується для оголошення ініціалізованих даних або констант, які не змінюються під час виконання, таких як константні значення, імена файлів або розмір буфера;

– .bss (block started by symbol) використовується для оголошення змінних, наприклад, неініціалізованих даних;

– .text (code) — у текстовій частині розміщено фактичний машинний код програми.

Крім перелічених, можуть бути наявні такі додаткові розділи, як:

– .rsrc (resources) — містить усі ресурси для програми (наприклад, .ico, .rc, .dialog);

– .rdata (read-only data) — використовується для зберігання даних, які не належать до розділу .data або .bss (це також дані, які доступні лише для читання та містять літеральні рядки, константи та інформацію про каталог налагодження);

– .idata (import data) — містить інформацію про імпорт, наприклад, DLL програми, включно з каталогом імпорту та таблицею адрес імпорту;

– .edata (export data) — містить інформацію про імена та адреси експортованих функцій, а також каталог експорту, який надає адресу та зміщення функцій програмам, які імпортують DLL;

– .reloc (relocation) — містить таблицю базових переміщень (базове переміщення — це зміна інструкції або ініціалізованого значення змінної, яка потрібна, якщо завантажувач не може завантажити програму).

Графічне зображення формату виконуваного файлу представлене на рис. 2.

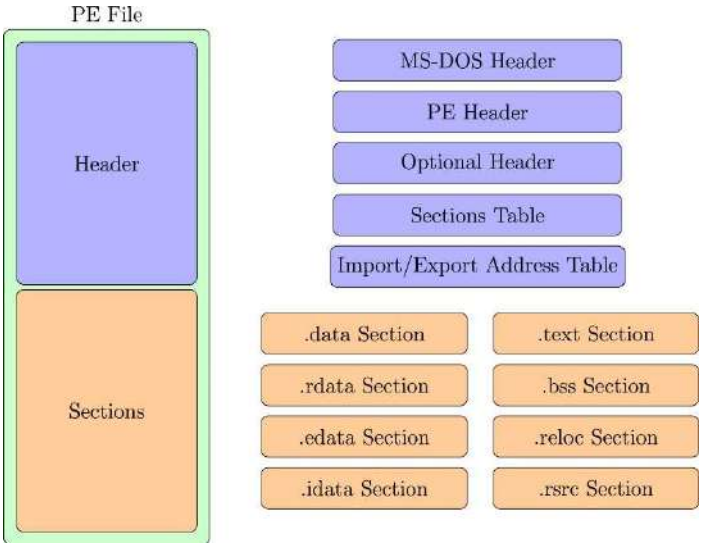


Рис. 2. Графічне представлення формату виконуваного файлу [12]

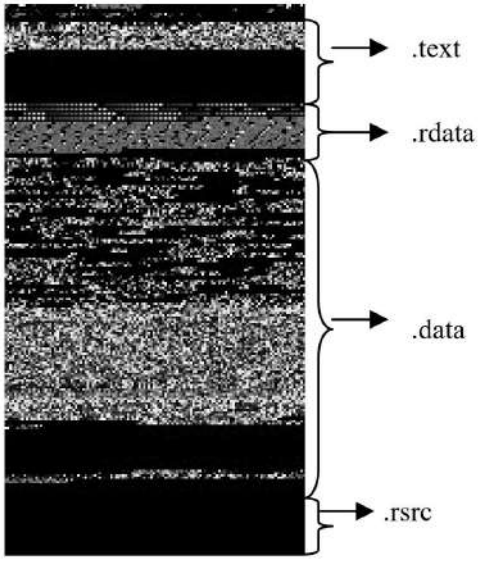


Рис. 3. Зображення бінарних фрагментів зразка ШПЗ (троян Dontovo.A) [11]

Інші розділи виконуваного файлу також можуть з'явитися в результаті використання поліморфних або метаморфічних методів, щоб приховати фактичний код ШПЗ. У деяких трансформаціях зловмисного програмного забезпечення можна побачити різні бінарні фрагменти, а секцію складання зловмисного програмного забезпечення можна ідентифікувати за різними текстурами на зображеннях.

Підхід, запропонований у [11], дозволяє зафіксувати незначні зміни, зберігаючи глобальну структуру, та допомагає виявити варіації ШПЗ.

На рис. 3 представлений зразок результату перетворення файлу на прикладі шкідливого програмного забезпечення троян Dontovo.A.

Набір даних Malimg. Оригінальний набір даних Malimg був створений в рамках проєкту з обробки сигналів для аналізу шкідливих програм на кафедрі електротехніки та комп'ютерної інженерії університету Каліфорнії (США). Метою цього проєкту було дослідження методів обробки сигналів та зображень для аналізу шкідливого програмного забезпечення [13].

Двійкові файли шкідливого програмного забезпечення були візуалізовані у вигляді зображень у сірій шкалі. При цьому спостерігалося, що для багатьох сімейств шкідливих програм зображення (які належать до одного сімейства), їх зображення виглядають дуже схожими за макетом і текстурою. Як зазначалось раніше за текстом, більшість нових шкідливих програм є модифікаціями вже існуючих. Таким чином, варіанти такого ШПЗ мають майже однаковий вміст.

Протягом реалізації вказаного проєкту, колективом дослідників було зроблено два основних спостереження [13]:

1. Існує візуальна схожість у варіантах шкідливого програмного забезпечення в межах сімейств.

2. Існує візуальна несхожість між варіантами шкідливого програмного забезпечення різних сімейств.

Для подальшої роботи були використані ці візуальні подібності та відмінності й запропоновано функції, засновані на схожості зображень, для вирішення проблем класифікації, виявлення, пошуку шкідливого програмного забезпечення та інших завдань.

При цьому, набір даних Malimg використовується вже більше десяти років в різних роботах із розпізнавання шкідливого програмного забезпечення і, де-факто, став бенчмаркінг стандартом для дослідження ефективності використання різних методів і моделей машинного навчання.

Відповідно, у нашому дослідженні з розпізнавання (класифікації) шкідливого програмного забезпечення також використаємо загальнодоступний набір даних Malimg, який розміщений на інтернет платформі Kaggle [14].

Розподіл зображень з даного набору даних, що містить 25 сімейств (класів) шкідливого програмного забезпечення, представлений на рис. 4.

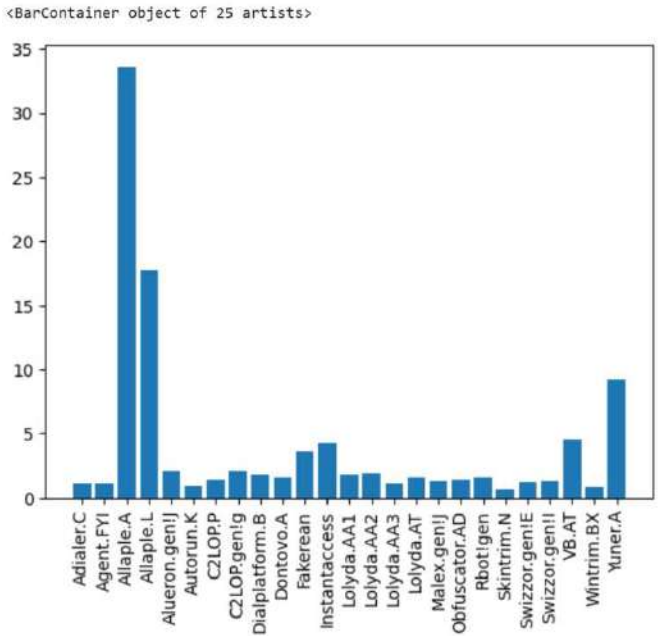


Рис. 4. 25 класів ШПЗ в наборі даних Malimg

Даний набір містить 9340 зображень байт-плотів шкідливих програм з 25 різних сімейств, а саме: Adialer.C, Agent.FYI, Allaple.A, Allaple.L, Alueron.gen!J, Autorun.K, C2LOP.P, C2LOP.gen!g, Dialplatform.B, Dontovo.A, Fakerean, Instantaccess, Lolyda.AA1, Lolyda.AA2, Lolyda.AA3, Lolyda.AT, Malex.gen!J, Obfuscator.AD, Rbot!gen, Skintrim.N, Swizzor.gen!E, Swizzor.gen!I, VB.AT, Wintrim.BX, Yuner.A.

На приведених нижче зображеннях шкідливого програмного забезпечення (рис. 5) візуально можна прослідкувати незначні модифікації. В той саме час, у зразків, що належать до одного сі-

мейства, загальна структура зображення зберігається. Однак вони візуально відрізняються від зразків зловмисних програм інших сімейств.

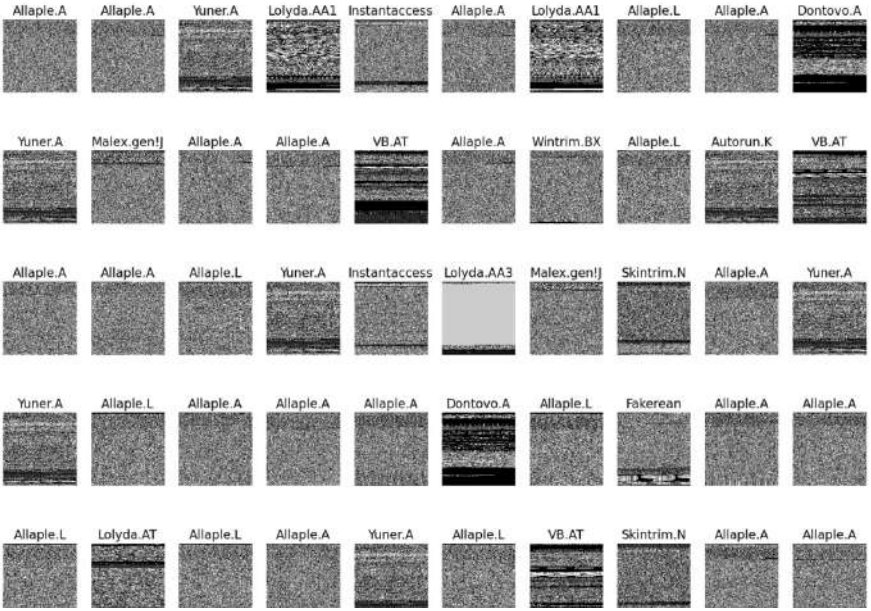


Рис. 5. Зразки зображень шкідливого програмного забезпечення різних класів у наборі даних Malimg

Важливо зазначити, що набір даних Malimg має певні обмеження, такі як нерівномірність розподілу, що потенційно впливає на навчання моделей машинного навчання. При цьому, набір даних Malimg має визнану цінність для виконання завдань з розпізнавання ШПЗ при порівнянні моделей машинного навчання, розроблених для опрацювання зображень.

Використання інтелектуальних методів аналізу даних. За останні десятиліття сфера машинного навчання пережила прорив у вирішенні багатьох завдань.

Для обчислення особливостей текстури в зображеннях зловмисного програмного забезпечення успішно застосовувався алгоритм GIST (Global Image Structure Tensor) [15], який використовує вейвлет-розкладання для видобування ознак із глобальної структури зображення. Отримані елементи використовуються для порівняння з раніше ідентифікованими шкідливими шабло-

нами. Хоча таке зображення, що відтворене на основі функцій глобальної структури, є вразливим до структурних змін, кіберзлочинці, які знають про таку техніку розпізнавання, можуть уникнути виявлення, перемістивши розділи коду або додавши фіктивні дані (наприклад, через обфускацію).

У 2015 році в рамках задачі класифікації зображень ImageNet було запропоновано використання функції активації PReLU (Parametric Rectified Linear Unit), яка за результатами дослідження перевершила людську продуктивність [16].

Винахід згорткових нейронних мереж (CNN) став важливою віхою у розвитку розпізнавання зображень. CNN є формою штучної нейронної мережі, яка імітує спосіб опрацювання зображень зоровою корою головного мозку. Так, було запропоновано підхід до протидії контрзаходам, які використовують кіберзлочинці, через використання згорткових нейронних мереж для вилучення локальних та інваріантних характеристик із зображення, а також знаходження шаблонів незалежно від їхнього розташування у файлі [17].

Так, використання CNN дозволяє виявляти шаблони відомого шкідливого програмного забезпечення, присутнього на зображенні. Далі за текстом представлена структура згорткової нейронної мережі Гіберта (Gibert's CNN), яка використовується для класифікації зловмисного програмного забезпечення, представленого у вигляді зображень у відтінках сірого (див. рис. 6).

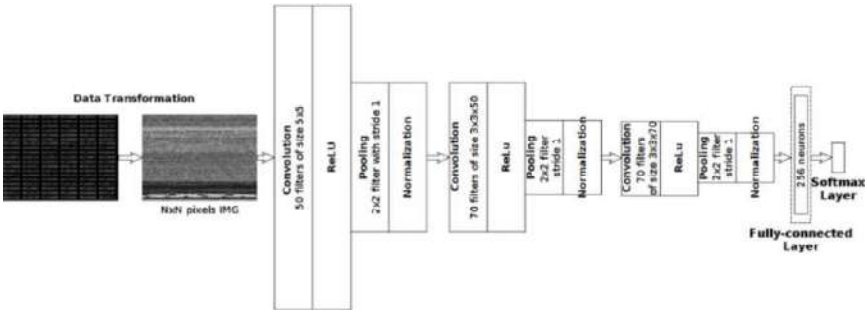


Рис. 6. Згорткова нейронна мережа Гіберта [17]

Як зазначалось раніше, за допомогою аналізу зображень у градаціях сірого, отриманих у результаті перетворення бінарного коду відомих зразків зловмисного програмного забезпечення, було зроблено висновок, що зображення з одного сімейства зловмисного програмного забезпечення схожі між собою [11]. З вве-

денням підходу щодо використання згорткових нейронних мереж можна було видобувати локальні та інваріантні особливості із зображення, знаходячи шаблони незалежно від їхнього положення. Таким чином, нейронна мережа давала змогу виявляти зразки відомого зловмисного програмного забезпечення на зображенні.

Хоча запропоноване рішення має ряд переваг, які дозволяють ефективно виявляти шкідливі програми, ця стратегія має проблеми з певними зразками, які були стиснуті або зашифровані, а також з тими, які можуть мати зовсім іншу загальну структуру.

Зазначені обставини обумовлюють подальший пошук та валідацію більш новітніх моделей машинного навчання з метою визначення найбільш ефективного рішення задачі розпізнавання та класифікації шкідливого програмного забезпечення, представленого як зображення.

Альтернативна до CNN архітектура штучної нейронної мережі, названа трансформерами зору (vision transformer або ViT), була представлена у 2020 році [18]. Це ознаменувало собою появу нового сімейства штучних нейронних мереж. Архітектура трансформеру створена для вивчення контексту і відстеження взаємозв'язків у послідовних даних. Вперше трансформери були використані з великим успіхом у програмах машинного навчання, пов'язаних з мовою та перекладом [19]. Однак, виникнення даної технології викликало значний інтерес до неї в задачах комп'ютерного зору (computer vision). У 2021 році було представлено, що трансформери, які застосовуються в задачах комп'ютерного зору, за наявності достатньої кількості навчальних даних демонструють ефективність, порівнянну з CNN, а в деяких випадках навіть вищу за них [20]. У зв'язку з цим, більшість програм, що використовують трансформери, навчаються на великих масивах даних.

Використання традиційних трансформерів зору для обробки зображень має квадратичну складність обчислень відносно розміру зображення через глобальні обчислення самоуваги [21]. Так, глобальний механізм самоуваги на зображеннях з використанням згорткових нейронних мереж детально демонструється в статті [22].

Одним із підходів до більш ефективного вилучення ознак із зображень став розроблений у 2021 р. Swin трансформер [21, 23].

Swin трансформер — це трансформерна модель глибинного навчання з найбільшою на даний момент продуктивністю в задачах зору. Swin трансформер має вищу точність порівняно з трансформером зору [18], який йому передує. Завдяки цим властивос-

тям Swin трансформери використовуються як основа в багатьох моделях розпізнавання зображень.

Прикладом такого використання є модель CoAtNet, яка була представлена у дослідженні «CoAtNet: Поєднання згортки та уваги для всіх розмірів даних» [24] у 2021 р. У наведеній роботі колектив авторів показав рішення проблеми гібридизації згортки та уваги з точки зору двох фундаментальних аспектів машинного навчання — узагальнення та потужності моделі. Назва CoAtNet походить від об'єднання слів Convolution та self-Attention. Ця гібридна модель, яка поєднала ознаки згорткової мережі та трансформеру, була виділена у нове сімейство моделей. Як заявлено авторами, CoAtNet має сильні сторони як згорткових мереж, так і трансформерів.

Разом з цим, у 2022 році була опублікована наукова робота, яка представила другу версію Swin трансформеру (Swin v.2) [25]. Першу версію було масштабовано до 3 мільярдів параметрів, що є найбільшою та найефективнішою моделлю щільного бачення станом на 2022 рік. Крім того, адаптована версія використовує в 40 разів менше мічених даних і потребує в 40 разів менше часу на навчання, ніж попередні моделі. Як результат, її використання в задачах розпізнавання зображень має більший потенціал та потенційно більшу ефективність, ніж у першої версії Swin трансформеру.

Для забезпечення кращої ефективності навчання пропонується до застосування технологію передавального навчання (Transfer Learning або TL). TL — це техніка машинного навчання, яка використовує знання, отримані з попередньо навчених моделей для покращення продуктивності моделей, що навчаються на інших, але пов'язаних завданнях. Разом з цим, передавальне навчання визначають як повторне використання моделей (навчених на попередньо існуючих наборах даних) для вирішення нових актуальних цільових завдань. TL є інструментом оптимізації, який підвищує продуктивність моделювання. До його ключових характеристик відносяться повторне використання знань, отриманих з попередніх завдань, що призводить до покращення продуктивності моделей машинного навчання та, в результаті, до економії часу та ресурсів, потрібних для навчання таких моделей [26]. TL може бути корисним у багатьох ситуаціях, коли доступні дані для попереднього навчання та нове завдання подібне до попереднього.

В підході до розпізнавання шкідливого програмного забезпечення, який пропонується в даній роботі, набір даних Malimg ви-

користовується для попереднього навчання обраних моделей з їх подальшим навчанням на іншому наборі зображень в градаціях сірого, отриманих з виконуваних файлів, які потенційно містять ШПЗ (з метою визначення та класифікації можливих загроз). Таким чином, за результатами проведеного мета-аналізу наукових публікацій з виявлення та класифікації ШПЗ, концептуальний підхід до розпізнавання шкідливого програмного забезпечення (представленого як зображення у відтінках сірого) з використанням найсучасніших моделей машинного навчання, побудованих для опрацювання зображень, можна формалізувати в двох складових: практичній та дослідницькій (див. рис. 7).

Рис. 7. Концептуальний підхід до розпізнавання шкідливого програмного забезпечення на основі технологій машинного навчання

Наведемо деталізацію етапів концептуального підходу, представленого на рис. 7, які відносяться до практичної та дослідницької складових:

1. **Отримання зображень з виконуваних файлів та підготовка набору даних (практична складова)** — формування набору зображень в градаціях сірого з виконуваних файлів, які потенційно містять ШПЗ (в тому числі: перетворення зразків шкідливого програмного забезпечення на зображення в градаціях сірого; зменшення розміру зображень для подальшого підвищення ефективності їх опрацювання; розділення отриманого первинного набору даних на тренувальну, валідаційну та тестову вибірки).

2. **Специфікація моделей (дослідницька складова)** — вибір найбільш адекватного поставленій задачі та наявному набору даних математичного інструментарію (моделей глибинного навчання) для розпізнавання/класифікації ШПЗ на основі візуальних патернів.

3. **Налаштування моделей на наборі даних Malimg (дослідницька складова)** — попереднє навчання обраних моделей та обрання найбільш ефективної моделі (моделей) для подальшого використання в реальному середовищі (в тому числі: оптимізація обраних моделей на тренувальному наборі даних; оцінювання ефективності та вдосконалення моделей на тестовому наборі даних; верифікація моделей на валідаційному наборі даних; порівняння адекватності побудованих моделей).

4. **Підготовка моделей (практична складова)** — додаткове навчання моделей на наборі даних з реального середовища (а саме: оптимізація обраних моделей на тренувальному наборі даних; оцінювання та вдосконалення моделей на тестовому наборі даних; оцінка точності та ефективності моделей на валідаційному наборі даних; вибір найкращої моделі нейромережевої архітектури).

5. **Вдосконалення моделей (практична складова)** — використання методів регуляризації, додаткові експерименти з наборами даних та моделями (за можливості розширення/зміна тренувального набору даних та проведення експериментів з різними архітектурами та параметрами моделей).

6. **Розгортання та удосконалення в реальному середовищі (практична складова)** — подальший розвиток рішення з виявлення та класифікації ШПЗ на основі візуальних патернів (в тому числі: використання обраної моделі (моделей) для виявлення та класифікації шкідливого програмного забезпечення; постійне удосконалення системи через використання нових даних та най-

сучасніших моделей нейромережевих архітектур, розроблених для опрацювання зображень).

Висновки та перспективи подальшого дослідження. В результаті проведеного мета-аналізу наукових публікацій за останні роки виявлено, що для вирішення завдань класифікації зображень високу ефективність демонструє згорткова нейронна мережа, а також найбільш сучасні моделі машинного навчання, такі як:

– трансформер Swin v.1 (2021 р.) [21, 23];

– гібридна згорткова нейронна мережа CoAtNet (2021 р.) [24];

– трансформер Swin v.2 (2022 р.) [25].

У зв'язку з цим, використання техніки конвертації файлів шкідливого програмного забезпечення в зображення у відтінках сірого відкриває можливості використання зазначених архітектур нейронних мереж для розпізнавання та класифікації такого ШПЗ. Найбільш відомим набором даних з таких зображень шкідливих програм є Malimg, що обумовлює його використання в подальшому дослідженні.

На підставі хронологічної послідовності зазначених наукових публікацій, а також заявлених дослідниками характеристик нейромережевої архітектури Swin трансформерів другої версії [25], логічно висунути гіпотезу про те, що модель машинного навчання, побудована на базі цього типу нейронної мережі, буде досягати вищої точності в розпізнаванні шкідливого програмного забезпечення порівняно з іншими архітектурами (згорткової нейронної мережі, трансформеру Swin першої версії, а також гібридної нейромережі CoAtNet).

Враховуючи зазначене, в даній роботі для підтвердження цієї гіпотези щодо ефективності класифікації шкідливого програмного забезпечення рекомендується проведення подальшого дослідження (як дослідницької складової представленого концептуального підходу), яке включатиме імплементацію зазначених чотирьох нейромережевих архітектур. Також для вирішення цього завдання доцільним є використання набору даних Malimg.

Проведене в даній статті дослідження дозволило сформулювати концептуальний підхід до розпізнавання шкідливого програмного забезпечення з використанням найсучасніших нейромережевих архітектур, розроблених для опрацювання зображень. Згідно даного підходу згорткові нейронні мережі, а також найбільш новітні архітектури Swin трансформерів 1-ої та 2-ої версій, разом із гібридною нейронною мережею CoAtNet, ви-

ступають перспективними кандидатами для проведення подальшого дослідження з визначення найбільш ефективної моделі машинного навчання для класифікації шкідливого програмного забезпечення.

Дана стаття може стати важливим підґрунтям для дослідників у міждисциплінарній області використання методів та технік машинного (зокрема глибинного) навчання в сфері кібербезпеки.

Бібліографічні посилання

1. Frolov, D., Radziewicz, W., Saienko, V., Kuchuk, N., Mozhaiev, M., Gnusov, Y., & Onishchenko, Y. (2021). Theoretical and Technological Aspects of Intelligent Systems: Problems of Artificial Intelligence. *International Journal of Computer Science and Network Security, 21*(5), 35-38. https://doi.org/10.22937/IJCSNS.2021.21.5.6

2. He, K., & Kim, D.-S. (2019). Malware detection with malware images using deep learning techniques. In *Proceedings of the 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)* (pp. 95-102). IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2019.00022

3. Gavriluţ, D., Cimpoeşu, M., Anton, D., & Ciortuz, L. (2009). Malware detection using machine learning. In *Proceedings of the 2009 International Multiconference on Computer Science and Information Technology* (pp. 735-741). IEEE. https://doi.org/10.1109/IMCSIT.2009.5352759

4. Singhal, P., & Raul, N. (2012). Malware Detection Module using Machine Learning Algorithms to Assist in Centralized Security in Enterprise Networks. *International Journal of Network Security & Its Applications, 4*(1), 61-71. https://doi.org/10.5121/ijnsa.2012.4106

5. Arp, D., Spreitzenbarth, M., Hübner, M., Gascon, H., & Rieck, K. (2014). DREBIN: Effective and explainable detection of Android malware in your pocket. In *Proceedings of the Network and Distributed System Security Symposium* (Article 23247). The Internet Society. https://doi.org/10.14722/ndss.2014.23247

6. Shalaginov, A., Banin, S., Dehghantanha, A., & Franke, K. (2018). Machine Learning Aided Static Malware Analysis: A Survey and Tutorial. In A. Dehghantanha, M. Conti, T. Dargahi (Eds.), *Advances in Information Security: Vol. 70. Cyber Threat Intelligence* (pp. 7–45). Springer. https://doi.org/10.1007/978-3-319-73951-9_2

7. Zhang, X., Wu, K., Chen, Z., & Zhang, C. (2021). MalCaps: A Capsule Network Based Model for the Malware Classification. *Processes, 9*(6), Article 929. https://doi.org/10.3390/pr9060929

8. Hemalatha, J., Roseline, S. A., Geetha, S., Kadry, S., & Damaševičius, R. (2021). An efficient DenseNet-based deep learning model for malware detection. *Entropy, 23*(3), Article 344. https://doi.org/10.3390/e23030344

9. Lin, W.-C., & Yeh, Y.-R. (2022). Efficient Malware Classification by Binary Sequences with One-Dimensional Convolutional Neural Networks. *Mathematics, 10*(4), Article 608. https://doi.org/10.3390/math10040608

10. Akhtar, M. S., & Feng, T. (2022). *Malware Analysis and Detection Using Machine Learning Algorithms*. *Symmetry, 14*(11), Article 2304. https://doi.org/10.3390/sym14112304

11. Nataraj, L., Karthikeyan, S., Jacob, G., & Manjunath, B.S. (2011). Malware images: Visualization and automatic classification. In *Proceedings of the 8th International Symposium on Visualization for Cyber Security* (Article 4). ACM. https://doi.org/10.1145/2016904.2016908

12. Gibert, D., Mateu, C., & Planes, J. (2020). The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. *Journal of Network and Computer Applications, 153*, Article 102526. https://doi.org/10.1016/j.jnca.2019.102526

13. Department of Electrical and Computer Engineering, University of California. (n.d.). Signal Processing for Malware Analysis. Retrieved from https://vision.ece.ucsb.edu/research/signal-processing-malware-analysis

14. Sunkari, M. (2022). *Malimg_dataset9010* [Data set]. Kaggle. Retrieved from https://www.kaggle.com/datasets/manaswinisunkari/malimg-dataset9010

15. Oliva, A., & Torralba, A. (2001). Modeling the shape of the scene: A holistic representation of the spatial envelope. *International Journal of Computer Vision, 42*(3), 145-175. https://doi.org/10.1023/A:1011139631724

16. He, K., Zhang, X., Ren, S., & Sun, J. (2015). *Delving deep into rectifiers: Surpassing human-level performance on ImageNet classification*. arXiv. https://doi.org/10.48550/arXiv.1502.01852

17. Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2019). Using convolutional neural networks for classification of malware represented as images. *Journal of Computer Virology and Hacking Techniques, 15*(1), 15-28. https://doi.org/10.1007/s11416-018-0323-0

18. Dosovitskiy, A., Beyer, L., Kolesnikov, A., Weissenborn, D., Zhai, X., Unterthiner, T., Dehghani, M., Minderer, M., Heigold, G., Gelly, S., Uszkoreit, J., & Houlsby, N. (2020). *An image is worth 16x16 words: Transformers for image recognition at scale*. arXiv. https://doi.org/10.48550/arXiv.2010.11929

19. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). *Attention is all you need*. arXiv. https://doi.org/10.48550/arXiv.1706.03762

20. Liu, Y., Zhang, Y., Wang, Y., Hou, F., Yuan, J., Tian, J., Zhang, Y., Shi, Z., Fan, J., & He, Z. (2021). *A survey of visual transformers*. arXiv. https://doi.org/10.48550/arXiv.2111.06091

21. Liu, Z., Lin, Y., Cao, Y., Hu, H., Wei, Y., Zhang, Z., Lin, S., & Guo, B. (2021). *Swin transformer: Hierarchical vision transformer using shifted windows*. arXiv. https://doi.org/10.48550/arXiv.2103.14030

22. Zhang, H., Goodfellow, I., Metaxas, D., & Odena, A. (2018). *Self-attention generative adversarial networks*. *arXiv.* https://doi.org/10.48550/arXiv.1805.08318

23. Loy, J. (2022, May 20). A Comprehensive Guide to Microsoft's Swin Transformer. In-depth Explanation and Animations. *Towards Data Science*. https://towardsdatascience.com/a-comprehensive-guide-to-swin-transformer-64965f89d14c

24. Dai, Z., Liu, H., Le, Q.V., & Tan, M. (2021). *CoAtNet: Marrying Convolution and Attention for All Data Sizes*. ArXiv. https://doi.org/10.48550/arXiv.2106.04803

25. Liu, Z., Hu, H., Lin, Y., Yao, Z., Xie, Z., Wei, Y., Ning, J., Cao, Y., Zhang, Z., Dong, L., Wei, F., & Guo, B. (2022). Swin Transformer V2: Scaling Up Capacity and Resolution. In *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 11999-12009). IEEE. https://doi.org/10.1109/CVPR52688.2022.01170

26. Hosna, A., Merry, E., Gyalmo, J., Alom, Z., Aung, Z., & Azim, M. A. (2022). Transfer learning: A friendly introduction. *Journal of Big Data*, *9*, Article 102. https://doi.org/10.1186/s40537-022-00652-w

Наукове видання

Моделювання та інформаційні системи в економіці

Збірник наукових праць

Заснований у 1965 р.

№ 102

Головний редактор *О. Є. Камінський*

Редактор *В. Македон*
Художник обкладинки *Т. Зябліцева*
Верстка *О. Федосенко*

Підписано до друку 24.02.23. Формат 60×84/16. Папір офсет.
Гарнітура Тип Таймс. Друк офсетний. Ум. друк. арк. 10,69.
Обл.-вид. арк. 12,17. Наклад 50 пр. Зам. № 23-5758.

Київський національний економічний університет імені Вадима Гетьмана
03680, м. Київ, проспект Перемоги, 54/1
E-mail: litera_kneu@ukr.net