

E%D0%BF%D0%B0%D0%B4%D0%B0%202021%20%D1%80%D0%BE%D0%BA%D1%83).

5. *Проблеми теорії та методології бухгалтерського обліку, контролю і аналізу [Електронний ресурс] // Державний університет «Житомирська політехніка. – 2024. – Режим доступу до ресурсу: <https://eztuir.ztu.edu.ua/bitstream/handle/123456789/8476/12.pdf?sequence=1&isAllowed=y>*

УДК 004.8:657.37

Герасименко Андрій Анатолійович,
*керівник департаменту R&D,
ISpro,
м. Київ, Україна*

ШТУЧНИЙ ІНТЕЛЕКТ У ERP-СИСТЕМАХ: СИНЕРГІЯ ТЕХНОЛОГІЙ ДЛЯ ПРОЗОРОГО ОБЛІКУ В ПРОЦЕСІ ВІДБУДОВИ УКРАЇНИ

Відбудова України після руйнівних наслідків війни є завданням безпрецедентного масштабу та складності. Це колосальний обсяг роботи, що потребує не просто фінансування, але й інноваційних підходів до управління ресурсами.

Одним із ключових викликів масштабної відбудови є розрізненість даних між різними відомствами, організаціями та проектами. Різні стандарти даних, неоднорідні системи обліку та відсутність єдиної методології оцінки збитків і потреб створюють ситуацію, коли навіть за наявності всієї необхідної інформації, її ефективне використання для прийняття комплексних рішень стає практично неможливим без додаткових технологічних рішень для інтеграції та аналізу.

Серед громадян України існує високий рівень занепокоєння щодо недостатнього контролю над процесами відбудови, що може призвести до розкрадання коштів та використання неякісних матеріалів. Міжнародний досвід також свідчить, що масштабні проекти відбудови часто стають об'єктами корупційних схем та нецільового використання ресурсів.

Для міжнародних донорів та інвесторів прозорість використання коштів є критично важливою умовою їх залучення до процесу відбудови. Відсутність ефективних механізмів контролю та прозорості може значно обмежити доступ до міжнародного фінансування та інвестицій, необхідних для відновлення країни.

Традиційні методи планування та управління проектами виявляються недостатньо ефективними для завдань такого масштабу та складності, особливо в умовах постійних змін та невизначеності, характерних для післявоєнної відбудови.

Одним із найбільш ресурсоємних аспектів управління проектами відбудови є обробка величезної кількості документів та транзакцій. AI-інтегровані ERP-

системи можуть автоматизувати цей процес.

Це дозволить не лише значно прискорити обробку документів, але й мінімізувати ризики помилок та зловживань завдяки послідовному застосуванню встановлених правил та стандартів.

AI-алгоритми особливо ефективні у виявленні аномалій та нетипових патернів, що можуть свідчити про потенційні зловживання або шахрайство. На відміну від традиційних систем аудиту, що часто виявляють проблеми постфактум, AI-системи можуть виявляти потенційні зловживання в режимі реального часу, дозволяючи вжити превентивних заходів.

Прозорість є ключовою вимогою для забезпечення довіри до процесу відбудови з боку громадян, міжнародних донорів та інвесторів. AI-інтегровані ERP-системи сприяють прозорості через: автоматичне формування детальних аудиторських слідів для всіх операцій; генерацію комплексних звітів про використання ресурсів та прогрес проєктів; візуалізацію даних у доступній формі для різних зацікавлених сторін.

Підвищена прозорість не лише зменшує ризики корупції, але й сприяє залученню додаткових ресурсів та підвищенню ефективності управління.

Одним із ключових викликів у процесі відбудови є необхідність ефективної співпраці між різними відомствами, організаціями та секторами при збереженні конфіденційності чутливих даних. Федеративне навчання пропонує інноваційне рішення цієї проблеми.

Федеративне навчання — це підхід до машинного навчання, який дозволяє навчати алгоритми на розподілених наборах даних без необхідності їх централізації. Замість передачі даних до центрального сервера, модель навчається локально на кожному вузлі (наприклад, окремій організації), а потім лише оновлення моделі (параметри, ваги) передаються для агрегації.

Ключові переваги федеративного навчання в контексті міжвідомчої співпраці: збереження конфіденційності даних – чутливі дані залишаються під контролем організацій, що їх створюють та використовують; мінімізація ризиків порушення безпеки – відсутність централізованого сховища даних значно зменшує ризики масштабних витоків інформації; відповідність нормативним вимогам – спрощується дотримання законодавчих вимог щодо обробки персональних та конфіденційних даних; можливість включення даних приватного сектору – приватні компанії можуть долучатися до спільних аналітичних проєктів без розкриття комерційної інформації.

Різні державні відомства, банки, страхові компанії та інші учасники процесу відбудови можуть спільно навчати моделі для виявлення потенційних шахрайських схем без необхідності ділитися деталями конкретних транзакцій чи персональними даними.

Такий підхід дозволяє використовувати колективний досвід та дані різних організацій для більш ефективного виявлення потенційних зловживань, зберігаючи при цьому конфіденційність інформації кожного учасника.

Ефективна відбудова вимагає координації складних ланцюгів постачання, що включають державні органи, міжнародних донорів, приватних

постачальників та логістичні компанії: учасники ланцюгів постачання можуть спільно навчати моделі для прогнозування потреб, оптимізації запасів та планування закупівель без розкриття комерційно чутливої інформації; федеративне навчання дозволяє створити «колективний інтелект» для управління ланцюгами постачання, зберігаючи при цьому комерційні таємниці та конкурентні переваги учасників.

Компанія ISpro активно працює над впровадженням технологій штучного інтелекту в свої ERP-рішення для підтримки процесів відбудови України.

ISpro впроваджує ряд технологій для забезпечення достовірності облікових даних, що є критично важливим для прозорості процесу відбудови: автоматичне формування аудиторських слідів – система фіксує детальну інформацію про всі операції, включаючи хто, коли і які зміни вніс, забезпечуючи повну простежуваність; інтелектуальна валідація даних – AI-алгоритми перевіряють дані на відповідність бізнес-правилам, історичним патернам та зовнішнім джерелам інформації; система контролю доступу на основі AI – аналізує поведінку користувачів та адаптивно регулює рівні доступу для запобігання несанкціонованим діям.

Ці технології забезпечують високий рівень достовірності даних, мінімізуючи ризики помилок, маніпуляцій та шахрайства.

На середньостроковому горизонті ISpro планує впровадження більш складних та інноваційних рішень: розширена аналітика ризиків – розробка комплексних моделей для оцінки та управління ризиками на різних рівнях (проект, програма, портфель), з урахуванням взаємозалежностей між різними факторами; розробка базової платформи для федеративного навчання – створення технологічної основи для безпечної співпраці між різними організаціями без обміну чутливими даними; мультимодальний AI для аналізу комплексних даних – розробка систем, здатних аналізувати та інтегрувати дані різних типів (текст, зображення, відео, часові ряди) для створення цілісної картини процесів відбудови; AI-асистенти для підтримки прийняття рішень – розробка спеціалізованих інтелектуальних систем для підтримки різних категорій користувачів (від керівників проектів до фінансових аналітиків та аудиторів).

У довгостроковій перспективі ISpro бачить створення комплексної AI-екосистеми для підтримки не лише відбудови, але й подальшого сталого розвитку України. ISpro прагне стати ключовим партнером у цифровій трансформації України, забезпечуючи технологічну основу для ефективної та прозорої відбудови.

Закликаємо бізнес, державні установи, науково-освітні заклади та міжнародних партнерів до активної співпраці у: створенні єдиних стандартів обміну даними та протоколів взаємодії; розробці спеціалізованих AI-рішень, адаптованих до потреб української економіки; формуванні регуляторного середовища, що стимулюватиме інновації та забезпечуватиме захист даних; розвитку освітніх програм для підготовки спеціалістів з впровадження та підтримки AI-інтегрованих ERP-систем; реалізації спільних проектів з

міжнародними організаціями для обміну досвідом та залучення передових технологій.

Лише спільними зусиллями ми зможемо побудувати сучасну, прозору та ефективну цифрову економіку, що стане основою для успішної відбудови та подальшого розвитку України.

Список використаних джерел:

1. Akinadewo, Israel S. «Artificial intelligence and accountants' approach to accounting functions.» *Covenant University Journal of Politics & International Affairs (Special Edition)* (2021).
2. Huang, Wei, et al. «Multimodal federated learning: Concept, methods, applications and future directions.» *Information Fusion* 112 (2024): 102576.
3. Khaled AlKoheji, Aysha, and Abdalmuttaleb Al-Sartawi. «Artificial intelligence and its impact on accounting systems.» *European, Asian, Middle Eastern, North African Conference on Management & Information Systems. Cham: Springer International Publishing, 2022.*

УДК 351.74

Гриненко Юлія Ігорівна,
доктор філософії,
старший аналітик Бюро економічної безпеки України,
м. Київ, Україна

ВИКОРИСТАННЯ OSINT-ІНСТРУМЕНТІВ У РАМКАХ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ ПРАВООХОРОННИХ ОРГАНІВ

Сучасний орган правопорядку повинен використовувати сучасний інструментарій управління безпекою, який враховує впливи людського чинника, надійність системи, зовнішні фактори небезпек на загальний рівень безпеки. В основі управління безпекою лежить системний підхід до виявлення джерел небезпеки і контролю чинників ризику на користь зведення до мінімуму людських жертв, матеріального збитку, а також фінансових, екологічних і соціальних втрат.

Комплексний стратегічний план реформування органів правопорядку як частини сектору безпеки і оборони України на 2023–2027 роки, схвалений Указом Президента України від 11 травня 2023 року № 273/2023, передбачає комплексні зміни в системі органів правопорядку, які мають стосуватися всіх аспектів їх функціонування, зокрема, впровадження в їх діяльність ризик-орієнтованих підходів [4].

Метою застосування ризик-орієнтованого підходу є ідентифікація ризиків вчинення кримінальних правопорушень у певній сфері та розроблення й здійснення за результатами їх оцінювання заходів щодо мінімізації та усунення таких ризиків.

Застосування ризик-орієнтованого підходу здійснюється шляхом аналізу та зіставлення даних, що містяться в банках (базах) даних органу правопорядку, та