

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2025. № 5.

DOI: <http://doi.org/10.32702/2307-2105.2025.5.32>

УДК 338.2:004.8

О. М. Світовий,

д. е. н., професор, професор кафедри маркетингу, менеджменту та управління бізнесом, Уманський державний педагогічний університет імені Павла Тичини

ORCID ID: <https://orcid.org/0000-0002-0675-559X>

С. В. Вилегжанін,

аспірант, Уманський державний педагогічний університет імені Павла Тичини

ORCID ID: <https://orcid.org/0009-0002-6760-4653>

ЗАСТОСУВАННЯ ЕЛЕМЕНТІВ ШТУЧНОГО ІНТЕЛЕКТУ В УПРАВЛІННІ РИЗИКАМИ ІТ-ПРОЄКТІВ В КОНТЕКСТІ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ПІДПРИЄМСТВ

O. Svitovyi,

*Doctor of Economics Sciences, Professor,
Professor of the Department of Marketing and Business Management,
Pavlo Tychyna Uman State Pedagogical University*

S. Vyliezhzanin,

Postgraduate student, Pavlo Tychyna Uman State Pedagogical University

APPLICATION OF ARTIFICIAL INTELLIGENCE ELEMENTS IN RISK MANAGEMENT OF IT-PROJECTS IN THE CONTEXT OF DIGITAL TRANSFORMATION OF ENTERPRISES

В статті проведений аналіз сучасного стану цифрової трансформації існуючих бізнес-процесів та застосування штучного інтелекту в управлінні ризиками IT-проєктів. Зазначено, що програми з впровадження цифрових систем, хмарних обчислень, аналітики даних стають невід'ємною частиною бізнес-процесів. Цифрові системи, як правило, пов'язані з інноваційністю та опираються на передові технології, проте існує складність їх інтеграції в існуючі інфраструктурні та інші системи.

Наголошено на необхідності контролювати ризики IT-проєктів та планувати протидію їх появі, щоб запобігти значних фінансових та репутаційних втрат. Дієвим інструментом у цьому питанні може стати штучний інтелект, який за останній час дістав значний розвиток в частині можливостей практичного застосування. З'явилося значна кількість інтернет-платформ штучного інтелекту, які дають можливість виявляти закономірності на основі яких можна робити прогностичні висновки та контролювати поточний стан проєктів.

Доведено необхідність забезпечення кібербезпеки та безпека даних, яка, зокрема базується на потоковому відстеженні дій програм або користувачів. Це багато в чому залежить від побудови структури сховища під можливість застосування машинного навчання та побудові тенденцій з спрацювання тригерів для повідомлень або автоматичних дій систем в реальному часі.

Обґрунтовано, що для зменшення ризиків із матеріально-технічними ресурсами виникає потреба в аналізі ланцюжків постачання та ефективності управління постачальниками. До прикладу, уніфікована програмна платформа GEP SMART застосовує елементи штучного інтелекту в частині комплексу для управління закупівлею необхідних ресурсів підприємства. Також акцентовано увагу на тому, що до впровадження програмного продукту він повинен обов'язково проходити етап тестування для визначення ступеня його готовності. Автоматизація тестування допомагає оптимізувати процеси та виявляти критичні сектори для

перевірки складних аспектів тестування. Аргументовано, що інтеграція систем інформаційної безпеки з інструментами, де застосовується штучний інтелект, вже є не тільки елементом інформаційного контролю, а й необхідністю.

Запропоновано заходи щодо удосконалення управління ризиками IT-проектів, зокрема, щодо інтеграції елементів штучного інтелекту в системи ризик-менеджменту, створення програм машинного навчання та контролю виконання алгоритмів та процесів.

The article analyzes the current state of digital transformation of existing business processes and the use of artificial intelligence in risk-management of IT-projects. It is noted that programs for the implementation of digital systems, cloud computing, and data analytics are becoming an integral part of business processes. Digital systems are usually associated with innovation and rely on advanced technologies, but there is a difficulty in integrating them into existing infrastructure and other systems.

The need to control the risks of IT-projects and plan to counteract their emergence in order to prevent significant financial and reputational losses is emphasized. An effective tool in this matter can be artificial intelligence, which has recently undergone significant development in terms of practical application possibilities. A significant number of artificial intelligence Internet platforms have appeared, which make it possible to identify patterns on the basis of which predictive conclusions can be drawn and the current state of projects can be monitored.

The need for cybersecurity and data security, which is based in particular on streaming monitoring of program or user actions, has been proven. This largely depends on building a storage structure for the possibility of applying machine learning and building trends from triggering triggers for messages or automatic actions of systems in real time.

It is substantiated that in order to reduce risks with material and technical resources, there is a need to analyze supply chains and the effectiveness of supplier

management. For example, the unified software platform GEP SMART uses elements of artificial intelligence in the part of the complex for managing the procurement of necessary resources of the enterprise. It is also emphasized that before implementing a software product, it must necessarily undergo a testing stage to determine the degree of its readiness. Testing automation helps to optimize processes and identify critical sectors for checking complex aspects of testing. It is argued that the integration of information security systems with tools that use artificial intelligence is no longer only an element of information control, but also a necessity.

Measures are proposed to improve risk management of IT-projects, in particular, to integrate elements of artificial intelligence into risk management systems, create machine learning programs and control the execution of algorithms and processes.

Ключові слова: *управління ризиками, ресурси, бізнес-процеси, ефективність, IT-проекти, цифрова трансформація, штучний інтелект.*

Keywords: *risk management, resources, business-processes, efficiency, IT projects, digital transformation, artificial intelligence.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В сучасному світі домінує тенденція залежності бізнесу від цифрових технологій. Передумов до зміни цього становища найближчим часом не прогнозується. Цифровізація грає ключову роль в оптимізації бізнес-процесів, масштабуванні та підвищенні їх ефективності. Впровадження цифрових систем, хмарних обчислень, аналітики великих даних (ВД) стають невід'ємною частиною бізнес-процесів. Подібні проекти хоч і є загалом частиною ширшого поняття загального проєктного менеджменту, але мають і свої особливості. Найбільшими із них є ті, які пов'язані з інноваційністю, швидкою зміною технологій та використовують великий ступінь

невизначеності вимог на старті. Також неабияку роль відіграє складність інтеграції в існуючі інфраструктурні системи та взаємодія з іншими системами. Їх взаємовплив та синергетичні ефекти можуть привести до незапланованих результатів, або взагалі до втрати проєкту. Дослідження Gartner опубліковані у 2024 році [18] показало, що лише 48% цифрових ініціатив виявляються успішними. Це, звичайно, не лише недоліки, допущені в управлінні проєктами, але й нехтування принципами ризик-менеджменту, що суттєво підвищує негативний відсоток. Тому не дивно, що останнім часом виникає все більше й більше запитів на застосування методик ризик-менеджменту, які адаптовані в частині управління ІТ-проєктами.

Аналіз останніх досліджень і публікацій. Використання інструментів штучного інтелекту в управлінні ризиками ІТ-проєктів вивчали такі вітчизняні вчені як Коваль В.В., Міхно І.С., Метіль Т.К., Рябчиков О.М. та ін. Впровадження елементів штучного інтелекту та комп'ютерних технологій, які зменшують ризик помилкових дій в організації виробничого процесу, сприяють зниженню витрат, підвищенню продуктивності, оптимізації процесу прийняття управлінських рішень, оперативності та здатності швидко реагувати на зміну факторів зовнішнього і внутрішнього середовища та забезпечують різні підходи до управління ризиками, розглядалися у наукових працях Борисевич Є.Г., Галан Л.В., Вербівської Л. В., Ковтуненка Ю.В. та ін. Проте, недостатньо дослідженими є питання складності інтерпретації вхідної інформації та визначення функцій людського та штучного інтелекту в управлінні ризиками ІТ-проєктів.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування необхідності та висвітлення деяких аспектів застосування елементів штучного інтелекту в управлінні ризиками ІТ-проєктів в контексті цифрової трансформації підприємств.

Виклад основного матеріалу дослідження. Більшість ризиків із якими стикаються ІТ-проєкти, пов'язані із такими проблемами як: перевищення строків реалізації, збільшення вартості проєкту, низька кінцева ефективність,

завелика вартість подальшої підтримки та модернізації, неможливість масштабування, критичне накопичення технічного боргу та врешті решт – незадоволеність кінцевих споживачів. Якщо ці ризики не контролювати, та не планувати протидію їх появі, то це може призвести до значних фінансових та репутаційних втрат, тобто до зворотного ефекту ніж той, заради якого звичайно плануються впровадження проєктів напряму ІТ.

Таким чином, зважаючи на значущість впливу ризиків на реалізацію ІТ-проєктів, важливим стає постійна робота над впровадженням та удосконаленням системи ризик-менеджменту, для того, щоб планово та превентивно не допускати, або якомога швидше ідентифікувати та нівелювати наслідки виникнення таких ризиків. Передовим напрямком на цьому напрямку, на нашу думку, є впровадження можливостей штучного інтелекту (ШІ), який останнім часом зробив значний стрибок в частині можливостей практичного застосування. Згідно з останнім звітом McKinsey «State of AI Report 2025» [23, с. 15], більш ніж три чверті респондентів (78%) використовують ШІ хоча б для однієї бізнес-функції, причому найбільший відсоток спостерігається у сфері ІТ (рис.1).

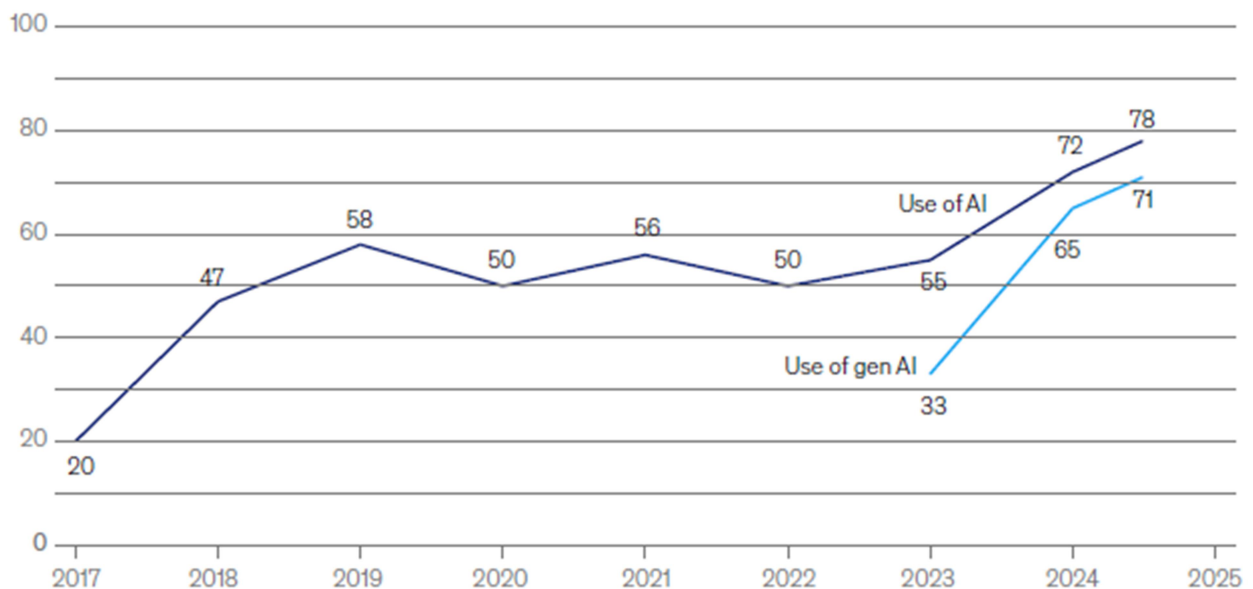


Рис. 1. Організації, які використовують ШІ принаймні в одній бізнес-функції, % респондентів

Джерело: Систематизовано та узагальнено авторами за даними [23, с. 15].

Найбільш притаманною задачею для ШІ є робота з ВД, і тому цілком закономірним є впровадження його елементів в інструменти для ризик-менеджменту, які призначені для аналізу історичних даних. Ці інструменти застосовуються для виявлення закономірностей на прикладі яких можна робити прогностичні висновки або навіть контролювати поточний стан проєктів. Як приклад, можна привести продукти від MetricStream [11], де ШІ використовується для сортування спостережень, оцінки та пошуків політик зменшення ризиків. AI Insights в Power BI [24] та Tableau AI [7] допомагають виявляти приховані закономірності та аномалії, прогнозувати тенденції, автоматизувати аспекти аналізу даних. В продуктах LogicGate [15] ШІ використовується при автоматизованій оцінці ризиків на базі історичних або потокових даних та відповідає за їх ідентифікацію, категоризацію та пріоритизацію.

Аналіз історичних даних є базою для ШІ для цілей прогнозування інфраструктурних збоїв та відмов. Predictive AIOps [19] від платформи штучного інтелекту для трансформації бізнесу ServiceNow, наприклад, використовує елементи ШІ для прогнозування та запобігання збоїв, фокусування, зниження витрат і підвищення продуктивності по технічному супроводу внаслідок використання машинного навчання для фільтрації шумів та пріоритизації подій. Також базуючись на історичних даних програмне забезпечення Oracle Primavera [14] за допомогою модуля ШІ дозволяє оцінити ризики зриву графіку, передбачає ризики затримок проєкту, міжпроєктні суперечки серед проєктів загального портфеля.

Кібербезпека та безпека даних, яка покладається на аналіз історичних даних, майже цілком базується на логуванні із поточним відстеженням дій програм або користувачів. В цьому випадку багато що залежить від побудови структури сховища з можливістю застосування машинного навчання для виокремлення аномалій та побудові тенденцій з використанням тригерів для повідомлень або автоматичних дій систем вже в реальному часі. Прикладом може бути використання платформи CrowdStrike Falcon [16] для мінімізації

кіберзагроз стороннього втручання, або роботи шкідливого програмного забезпечення та мережових атак. Ще одним прикладом застосування ІІІ в управлінні безпекою даних є відомий постачальник рішень щодо захисту даних Varonis [8], елементи якого використовуються для класифікації безпосередньо видів захищених даних, автоматизованого відновлення, виявлення загроз несанкціонованого доступу та витоку інформації, створення журналів безпеки для розслідування.

Використання штучного інтелекту у виробництві дозволяє найбільш ефективно, швидко та якісно керувати всіма процесами підприємства. Впровадження комп'ютерних технологій зменшує ризик помилкових дій в організації виробничого процесу [4, с. 93]. Вчені також стверджують, що операційна діяльність на кожному підприємстві реалізується завдяки основним наявним ресурсам, які можуть бути систематизовані у чотири групи: матеріально-технічні, фінансові, трудові та інформаційні [5, с. 99]. В цьому випадку не є виключенням й ІТ-проекти. Тому в ризик-менеджменті виокремлюється напрям оцінки ресурсного забезпечення ІТ-проектів. ІІІ, який застосовується в цих інструментах, допомагає аналізу та оцінці потреби в ресурсах, виявленні ризиків їх недостатності. Прикладом інструментів для застосування ІІІ може бути ресурс Forecast [9], який допомагає в створенні прогностичних моделей, використовується для планування ресурсів та повідомляє про відхилення в їх застосуванні, задіяний в процедурах розподілення завдань між виконавцями та командами, враховуючи об'єктивні показники останніх.

Для зменшення ризиків, зокрема із матеріально-технічними ресурсами, виникає потреба в аналізі ланцюжків постачання та ефективності управління постачальниками. Подібні елементи ІІІ застосовує уніфікована програмна платформа GEP SMART [21] в частині комплексу для управління закупівельними процесами підприємства. ІІІ в системі SAP Business For Procurement [22] допомагає формувати аналітику витрат та надає детальну інформацію, яка допомагає передбачати ринкові тенденції, мінімізувати

затримки в постачанні і створювати стійкість до інфляції. Трім того, вчені справедливо вважають, що інструменти штучного інтелекту надають цінні можливості для управління конкурентоспроможністю підприємства, що призводить до зниження витрат, підвищення продуктивності, оптимізації процесу прийняття управлінських рішень, оперативності та здатності швидко реагувати на зміну факторів зовнішнього та внутрішнього середовища, оптимізації бізнес-процесів [1].

Ризики достатності забезпечення інформаційними ресурсами в основному розподіляються за декількома напрямками: фізична достатність потужностей обчислювальних ресурсів (локальних чи хмарних) та достатність рівня доступу до ресурсів шляхом ліцензування та різного виду підписок, їх своєчасність. Протермінування ліцензій, підписок або невчасне створення необхідних доступів, як і недостатність обчислювальних потужностей, суттєво впливає на ризики зриву строків виконання та перевищення проєктних бюджетів. Ресурс AWS Cost Explore [12] за допомогою ШІ прогнозує майбутні витрати на хмарні ресурси. ШІ на платформі ServiceNow IT Asset Management [19] допомагає контролювати витрати та мінімізувати ризики ліцензування та оренди. Інша інтернет-платформа VMware [26] застосовує елементи ШІ із машинним навчанням для аналізу та прогнозування потреб в обчислювальних ресурсах проєктів з розміщення апаратної інфраструктури для програмного забезпечення.

Однією із найбільш значущих особливостей розробки програмних продуктів є високі приховані ризики, які можуть бути закладені одночасно зі створенням програмного забезпечення. Мова йде про помилки в кодовій базі, помилки логіки, архітектури, виникнення технічних боргів та проблематики сумісності та залежності. Ці помилки проявляються вже на етапах впровадження або експлуатації рішень, що призводить до неуспіху проєктів в цілому. Для різних етапів розробки існують різні інструменти, де ШІ може суттєво поліпшити ефективність управління ризиками. За умови своєчасного виявлення відхилень і проведення необхідних змін, як констатують вчені,

можливо мінімізувати ризики, які можуть виникнути на фінальній стадії проєкту [3, с. 391].

Для підвищення якості та безпеки програмного забезпечення ІІІ допомагає систематично аналізувати кодову базу, виявляти потенційні ризики та вразливості, оптимізувати процес розробки, а також вимірювати та управляти технічним боргом, що знижує ризики збоїв, вразливостей та високих витрат на підтримку у майбутньому. Наприклад, ІІІ Autofix AI на інтернет-ресурсі DeepSource [20] виконує постійний аналіз коду, який виконується навіть локально. Аналіз SAST (Static Application Security Testing), який працює у фоновому режимі, виявляє понад 5000 проблем із якістю коду і безпекою та дає методичні вказівки по кожному питанню, яке заздалегідь перевірене спеціалістами. Предиктивна аналітика на інтернет-інструменті Kiuwan Code Quality & Software Governance [13] із застосуванням ІІІ допомагає завчасно керувати технічною заборгованістю та зменшувати її, виявляючи дефекти коду, неефективність продуктивності та інші проблеми, які впливають на масштабування та перспективу подальшої технічної підтримки та розвитку проєкту.

Для визначення ступеня готовності програмного продукту, або змін до нього, до впровадження цього продукту він повинен обов'язково проходити етап тестування. Цей етап призначений для визначення ступеня готовності програмного продукту. Автоматизація тестування допомагає оптимізувати процеси, виявлення критичних областей для перевірки та автоматизації складних аспектів тестування. Використання елементів ІІІ дозволяє більш ефективно розподіляти ресурси на тестування та зосереджуватись на областях з високим ризиком. Наприклад, платформа синтетичних тестових даних GenRocket [25] створює синтетичні тестові дані, які гарантують відповідний обсяг, різноманітність і формат для навчання систем ІІІ та машинного навчання. Автоматизована система тестування Eggplant Test від Keysight [17] використовує ІІІ для тестування інтерфейсів з погляду досвіду користувача, побудови тестових сценаріїв та мультиплатформного

тестування. Ми погоджуємося із дослідниками, які вважають, що при традиційному підході до управління проєктами, рівень ризику має тенденцію до зростання на завершальних етапах проєкту, зокрема під час тестування та інтеграції [6, с. 103–104].

Після впровадження програмний продукт передається на етап технічної та програмної підтримки. Цей етап супроводжує його до кінця життєвого циклу. В будь-який момент може виникнути потреба внесення змін або додавання нового функціоналу. В такому разі виникає ризик порушень роботи продукту в частинах безпосередньо не пов'язаних із тими частинами, де саме планувались зміни, а зв'язок із тією частиною, що змінюється існує лише опосередковано та через довгий ланцюг залежностей. Всі такі частини попередньо потрібно проаналізувати та піддати тестуванню після проведення змін. ІІІ в цьому випадку допомагає виявляти, аналізувати та керувати різними типами залежностей в ІТ-системах. Це дозволяє знизити ризики каскадних збоїв, вразливостей та проблем сумісності, оптимізувати процеси внесення змін та експлуатацію в цілому. Прикладом можуть бути елементи ІІІ в Code Assurance програмного продукту SonarQube [10], який допомагає мінімізувати ризики залежності від ланцюжка зовнішніх бібліотек або інших модулів.

Таким чином застосування елементів ІІІ в ризик-менеджменті трансформує підходи до управління та надає численні переваги. Проте водночас є й проблеми, які не слід ігнорувати. Не дивлячись на те, що ІІІ досяг успіхів у визначенні та класифікації подій, одним із головних обмежень в застосуванні його на практиці є складність інтерпретації вхідної інформації для прийняття автоматичного рішення щодо розуміння рівня серйозності або її суті. Також не є сильною його стороною розпізнавання нових даних, сигналів, закономірностей, які не були враховані при навчанні, чи вже були накопичені в історичних даних. Не слід забувати й можливу упередженість, яка є наслідком суб'єктивної складової при формуванні навчальних вибірок та масиву даних.

Окремо потрібно згадати й проблематику конфіденційності даних. Неправомірне використання конфіденційної інформації разом із ризиками витоку та несанкціонованим доступом не додає популярності інструментам, які працюють із великими масивами даних. Не є виключенням і бази даних, із якими працює ІІІ. Тому інтеграція систем інформаційної безпеки з інструментами, де застосовується ІІІ є вже не тільки елементом інформаційної гігієни, але й необхідністю.

Вітчизняні дослідники акцентують увагу на тому, що успішне впровадження ІІІ в управління ризиками вимагає спільного підходу, який передбачає поєднання сильних сторін ІІІ з людським судженням, наглядом та етичними нормами [2, с. 450]. Звичайно, принаймні на даному етапі розвитку, ІІІ не зможе повноцінно замінити людський фактор в управлінні ризиками. Проте, деяку вагому частку рутинних завдань та завдань із чіткою логікою процесів або завдань, пов'язаних з обробкою великих даних, ІІІ взяти на себе цілком спроможний.

Висновки та перспективи подальших розвідок у даному напрямі. Отже, щодо подальшого розвитку застосування ІІІ в ризик-менеджменті ІТ-сфери, то на нашу думку, воно полягає в тісній співпраці з людиною. В цьому сенсі людині будуть відведені ролі більш стратегічного характеру та виконання завдань, які пов'язані із новими викликами, та з тими, які мають не чітку логіку, або базуються на етичних або соціальних нормах, досвіді та потребами в застосуванні знань із суміжних галузей. Також за людиною залишається завдання інтерпретації даних та дії, пов'язані зі змінами чинних інтеграцій ІІІ в системи ризик-менеджменту, створення програм машинного навчання та контролю виконання алгоритмів та процесів. Тому, використання ІІІ не замінює можливості людини, а значно їх розширює. Синергія людського та штучного інтелекту вже зараз гарантує підвищену ефективність та адаптивність систем управління ризиками ІТ-проектів і в цілому робить їх більш стійкими до викликів сьогодення. Подальші наші

дослідження будуть спрямовані на оптимізацію використання штучного інтелекту в управлінні ризиками ІТ-проектів.

Література

1. Вербівська Л.В. Застосування інструментів штучного інтелекту при управлінні конкурентоспроможністю підприємства. *Проблеми сучасних трансформацій. Серія: Економіка та управління*. 2023. № 10. DOI: <https://doi.org/10.54929/2786-5738-2023-10-04-06>.
2. Галан Л.В., Борисевич Є.Г. Застосування штучного інтелекту в управлінні ризиками організації як інноваційна стратегія її розвитку. *Успіхи і досягнення у науці*. 2025. № 2(12). С. 442–451. DOI: [https://doi.org/10.52058/3041-1254-2025-2\(12\)](https://doi.org/10.52058/3041-1254-2025-2(12))
3. Коваль В.В., Міхно І.С., Метіль Т. К. Комплексні технології управління проектними ризиками в ІТ-компаніях. *БІЗНЕСІНФОРМ*. 2023. № 10. С. 389–396. DOI: <https://doi.org/10.32983/2222-4459-2023-10-389-396>.
4. Ковтуненко Ю.В. Застосування штучного інтелекту у системі управління підприємством: проблеми та переваги. *Economic journal Odessa polytechnic university*. 2019. № 2(8). С. 93–99. DOI: <https://doi.org/10.5281/zenodo.4171114>.
5. Кулиняк І.Я., Боцман Ю.С. Ризики ресурсного забезпечення операційної діяльності промислових підприємств: оцінювання та регулювання. *Науковий вісник НЛТУ України*. 2017. т. 27, № 7. С. 98–102. DOI: <https://doi.org/10.15421/40270718>.
6. Рябчиков О.М. Використання штучного інтелекту при управлінні ризиками в проєктах за методологією СКРАМ. *Економіка. Менеджмент. Бізнес*. 2024. № 1(44). С. 102–109. DOI: <https://doi.org/10.31673/2415-8089.2024.010015>.
7. AI in Tableau Accelerate your data culture with AI-powered insights. Офіційний сайт Tableau from Salesforce. URL:

<https://www.tableau.com/products/artificial-intelligence> (дата звернення: 25.04.2025).

8. AI Security. Офіційний сайт Varonis. URL: <https://www.varonis.com/solutions/ai-security> (дата звернення: 25.04.2025).

9. AI that optimizes your revenue and operations. Офіційний сайт Forecast. URL: <https://www.forecast.app/features/ai> (дата звернення: 25.04.2025).

10. AI-assisted & quality-assured code. Vibe, then verify. Офіційний сайт SonarSource SA. URL: <https://www.sonarsource.com/solutions/ai> (дата звернення: 25.04.2025).

11. AI-Powered Insights and Recommendations: Transform Your Risk and Compliance Programs. Офіційний сайт MetricStream. URL: <https://info.metricstream.com/ai-powered-insights-and-recommendation.html> (дата звернення: 25.04.2025).

12. AWS Cost Explorer Features. Офіційний сайт Amazon Web Services. URL: <https://aws.amazon.com/ru/aws-cost-management/aws-cost-explorer/features> (дата звернення: 25.04.2025).

13. Code Quality & Software Governance. Офіційний сайт Kiuwan. URL: <https://www.kiuwan.com/quality-governance> (дата звернення: 25.04.2025).

14. Construction Intelligence Cloud solutions. Офіційний сайт Oracle. URL: <https://www.oracle.com/ro/construction-engineering/construction-intelligence-cloud/#rc30p3> (дата звернення: 25.04.2025).

15. Cyber Risk Management Application. Офіційний сайт LogicGate. URL: <https://www.logicgate.com/applications/cyber-risk-management-application> (дата звернення: 25.04.2025).

16. Cybersecurity's AI-native platform for the XDR era. Офіційний сайт CrowdStrike. URL: <https://www.crowdstrike.com/platform> (дата звернення: 25.04.2025).

17. Eggplant Test. Deliver faster with model-based, AI-powered test automation. Офіційний сайт Keysight Technologies. URL:

<https://www.keysight.com/us/en/products/software/software-testing/eggplant-test.html> (дата звернення: 25.04.2025).

18. Gartner Survey Reveals Only 48% of Digital Initiatives Are Successful. Офіційний сайт Gartner. URL: <https://www.gartner.com/en/newsroom/press-releases/2024-11-06-gartner-survey-reveals-only-48-percent-of-digital-initiatives-are-successful> (дата звернення: 25.04.2025).

19. IT Asset Management (ITAM). Офіційний сайт. ServiceNow. URL: <https://www.servicenow.com/products/it-asset-management.html> (дата звернення: 25.04.2025).

20. Let Autofix AI clean up your code. Офіційний сайт DeepSource Corp. URL: <https://deepsource.com/platform/ai> (дата звернення: 25.04.2025).

21. Protect Your Business With Intelligent Risk Management. Офіційний сайт GEP. URL: <https://www.gep.com/software/gep-smart/third-party-risk-management-solution> (дата звернення: 25.04.2025).

22. SAP Business AI for procurement. Офіційний сайт SAP SE. URL: <https://www.sap.com/products/artificial-intelligence/procurement.html> (дата звернення: 25.04.2025).

23. The state of AI: How organizations are rewiring to capture value / Alex Singla та ін. McKinsey Global Publishing, 2025. 23 с.

24. Use AI Insights in Power BI Desktop. Офіційний сайт Microsoft. URL: <https://learn.microsoft.com/en-us/power-bi/transform-model/desktop-ai-insights> (дата звернення: 25.04.2025).

25. Using GenRocket Synthetic Test Data for AI and ML Applications. Офіційний сайт GenRocket, Inc. URL: <https://www.genrocket.com/ai-and-ml> (дата звернення: 25.04.2025).

26. VMware Cloud Infrastructure. Офіційний сайт VMware by Broadcom. URL: <https://www.vmware.com/solutions/cloud-infrastructure> (дата звернення: 25.04.2025).

References

1. Verbivska, L.V. (2023), “Application of artificial intelligence tools in managing the competitiveness of an enterprise”, *Problemy suchasnykh transformatsij. Seriya: ekonomika ta upravlinnia*, vol. 10. DOI: <https://doi.org/10.54929/2786-5738-2023-10-04-06>.
2. Galan, L.V. and Borysevich, E.G. (2025), “Application of artificial intelligence in risk management of the organization as an innovative strategy for its development”, *Uspikhy i dosiahnennia u nauksi*, vol. 2(12), pp. 442–451. DOI: [https://doi.org/10.52058/3041-1254-2025-2\(12\)](https://doi.org/10.52058/3041-1254-2025-2(12)).
3. Koval, V.V. Mikhno, I.S. and Metil, T.K. (2023), “Complex technologies for project risk management in IT companies”, *BIZNESINFORM*, vol. 10, pp. 389–396. DOI: <https://doi.org/10.32983/2222-4459-2023-10-389-396>.
4. Kovtunencko, Y.V. (2019), “Application of artificial intelligence in the enterprise management system: problems and advantages”, *Economic journal Odessa polytechnic university*, vol. 2(8), pp. 93–99. DOI: <https://doi.org/10.5281/zenodo.4171114>.
5. Kulinyak, I.Ya. and Botsman, Yu.S. (2017), “Risks of resource provision of operational activities of industrial enterprises: assessment and regulation”, *Naukovyj visnyk NLTU Ukrainy*, vol. 27, no. 7, pp. 98–102. DOI: <https://doi.org/10.15421/40270718>.
6. Ryabchikov, O.M. (2024), “Using artificial intelligence in risk management in projects using the SCRAM methodology”, *Ekonomika. Menedzhment. Biznes*, vol. 1(44), pp. 102–109. DOI: <https://doi.org/10.31673/2415-8089.2024.010015>.
7. The official site of Tableau from Salesforce (2025), “AI in Tableau Accelerate your data culture with AI-powered insights”, available at: <https://www.tableau.com/products/artificial-intelligence> (Accessed 25 April 2025).
8. The official site of Varonis (2025), “AI Security”, available at: <https://www.varonis.com/solutions/ai-security> (Accessed 25 April 2025).

9. The official site of Forecast (2025), “AI that optimizes your revenue and operations”, available at: <https://www.forecast.app/features/ai> (Accessed 25 April 2025).

10. The official site of SonarSource SA (2025). “AI-assisted & quality-assured code”, available at: <https://www.sonarsource.com/solutions/ai> (Accessed 25 April 2025).

11. The official site of MetricStream (2025), “AI-Powered Insights and Recommendations: Transform Your Risk and Compliance Programs”, available at: <https://info.metricstream.com/ai-powered-insights-and-recommendation.html> (Accessed 25 April 2025).

12. The official site of Amazon Web Services (2025), “AWS Cost Explorer Features”, available at: <https://aws.amazon.com/ru/aws-cost-management/aws-cost-explorer/features> (Accessed 25 April 2025).

13. The official site of Kiuwan (2025), “Code Quality & Software Governance”, available at: <https://www.kiuwan.com/quality-governance> (Accessed 25 April 2025).

14. The official site of Oracle (2025), “Construction Intelligence Cloud solutions”, available at: <https://www.oracle.com/ro/construction-engineering/construction-intelligence-cloud/#rc30p3> (Accessed 25 April 2025)

15. The official site of LogicGate (2025), “Cyber Risk Management Application”, available at: <https://www.logicgate.com/applications/cyber-risk-management-application> (Accessed 25 April 2025).

16. The official site of CrowdStrike (2025), “Cybersecurity’s AI-native platform for the XDR era”, available at: <https://www.crowdstrike.com/platform> (Accessed 25 April 2025).

17. The official site of Keysight Technologies (2025), “Eggplant Test. Deliver faster with model-based, AI-powered test automation”, available at: <https://www.keysight.com/us/en/products/software/software-testing/eggplant-test.html> (Accessed 25 April 2025).

18. The official site of Gartner (2025), “Gartner Survey Reveals Only 48% of Digital Initiatives Are Successful”, available at: <https://www.gartner.com/en/newsroom/press-releases/2024-11-06-gartner-survey-reveals-only-48-percent-of-digital-initiatives-are-successful> (Accessed 25 April 2025).

19. The official site of ServiceNow (2025), “IT Asset Management (ITAM)”, available at: <https://www.servicenow.com/products/it-asset-management.html> (Accessed 25 April 2025).

20. The official site of DeepSource Corp (2025), “Let Autofix AI clean up your code”, available at: <https://deepsources.com/platform/ai> (Accessed 25 April 2025).

21. The official site of GEP (2025), “Protect Your Business With Intelligent Risk Management”, available at: <https://www.gep.com/software/gep-smart/third-party-risk-management-solution> (Accessed 25 April 2025).

22. The official site of SAP SE (2025), “SAP Business AI for procurement”, available at: <https://www.sap.com/products/artificial-intelligence/procurement.html> (Accessed 25 April 2025).

23. Singla, Alex (2025), The state of AI: How organizations are rewiring to capture value, McKinsey Global Publishing, NY, USA.

24. The official site of Microsoft (2025), “Use AI Insights in Power BI Desktop”, available at: <https://learn.microsoft.com/en-us/power-bi/transform-model/desktop-ai-insights> (Accessed 25 April 2025).

25. The official site of GenRocket, Inc (2025), “Using GenRocket Synthetic Test Data for AI and ML Applications”, available at: <https://www.genrocket.com/ai-and-ml> (Accessed 25 April 2025).

26. The official site of VMware by Broadcom (2025), “VMware Cloud Infrastructure”, available at: <https://www.vmware.com/solutions/cloud-infrastructure> (Accessed 25 April 2025).

Стаття надійшла до редакції 06.05.2025 р.