

УДК 005.6:004.8:658.5

DOI: 10.31732/2663-2209-2026-83-274-282

Дата надходження: 18.08.2026

Дата прийняття до друку: 22.09.2026

Дата публікації: 30.09.2026



Ця робота ліцензується відповідно до [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/)

РИЗИКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ МЕНЕДЖМЕНТУ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ ВИРОБНИЧИХ ПІДПРИЄМСТВ В УКРАЇНІ

Ігор Ковальчук¹, Ольга Орлова-Курилова²

¹ Аспірант освітньо-наукової програми «Менеджмент», кафедра управлінських технологій, Університет "КРОК", Київ, Україна, e-mail: KovalchukIS@krok.edu.ua, ORCID ID: <https://orcid.org/0009-0008-7827-6804>

² Д-р екон. наук, доцент, професор кафедри інформаційного менеджменту, математики та статистики Університету "КРОК", м. Київ, Україна, e-mail: orlovakov@krok.edu.ua, ORCID ID: <https://orcid.org/0000-0001-8382-8070>

RISKS OF USING ARTIFICIAL INTELLIGENCE TECHNOLOGY FOR QUALITY MANAGEMENT SYSTEM MANAGEMENT IN MANUFACTURING ENTERPRISES IN UKRAINE

Igor Kovalchuk¹, Olga Orlova-Kurilova²

¹ Postgraduate student of the Educational and Scientific Program "Management", Department of Managerial Technologies, "KROK" University, Kyiv, Ukraine, e-mail: KovalchukIS@krok.edu.ua, ORCID ID: <https://orcid.org/0009-0008-7827-6804>

² Doctor of Science in Economics, Associate Professor, Professor of the Department of Information Management, Mathematics and Statistics "KROK" University, Kyiv, Ukraine, e-mail: orlovakov@krok.edu.ua, ORCID ID: <https://orcid.org/0000-0001-8382-8070>

Анотація. Актуальність дослідження зумовлена поширенням технологій штучного інтелекту у виробничих системах управління якістю та необхідністю контролювати специфічні ризики, пов'язані з якістю даних, надійністю моделей, кібербезпекою, кадровими компетенціями й нормативною відповідністю. Метою статті є розроблення та практична апробація підходу до оцінювання ризиків інтеграції ШІ в систему управління якістю виробничого підприємства. Об'єктом дослідження є процес управління ризиками під час інтеграції ШІ в СУЯ на прикладі ТОВ «КСЕНКО АВТОПРОДАКШН». Теоретичну основу сформовано положеннями ISO 9001:2015, ISO 31000:2018, ISO 13485:2016, ISO/IEC 23894:2023 та ISO/IEC 42001:2023. Використано аналіз і синтез наукових джерел, системний і процесний підходи, експертне оцінювання та напівкількісну матрицю «ймовірність-вплив». Експертну групу сформували п'ять фахівців, пов'язаних з управлінням, якістю, виробництвом, ІТ та роботою з даними; оцінювання проведено у 2026 р. на основі матеріалів проекту, даних про виробничі й контрольні процеси та професійних суджень експертів. Ідентифіковано 29 ризиків і згруповано їх за технічними, організаційними, кадровими, інформаційно-кібербезпечними, регуляторними та соціально-етичними ознаками. Для кожної події визначено нормовані оцінки ймовірності та впливу від 0 до 1, після чого сформовано ризик-профіль. До критичних за прийнятими порогоми віднесено 7 ризиків; найвищі оцінки отримали відключення інтернету та енергосистем, мобілізація ключових фахівців і низька якість даних для навчання моделі. Запропоновано превентивні та коригувальні заходи, що охоплюють аудит даних, резервування інфраструктури, калібрування моделей, крос-навчання персоналу та формалізацію вимог. Практичне значення результатів полягає у можливості використання підходу як відтворюваного інструменту пріоритизації ризиків і планування заходів у межах СУЯ без застосування складних статистичних моделей. Наукова новизна полягає в узгодженні ризик-орієнтованої логіки стандартів систем менеджменту з оцінюванням специфічних для ШІ загроз та її апробації на конкретному виробничому підприємстві. Запропонований підхід забезпечує прозорість критеріїв, порівнюваність оцінок і можливість повторного моніторингу залишкового ризику після впровадження управлінських заходів.

Ключові слова: штучний інтелект; система управління якістю; ризик-менеджмент; виробниче підприємство; експертне оцінювання; матриця ризиків; ISO/IEC 23894.

Формул: 0; **рис.:** 0; **табл.:** 4; **бібл.:** 17

Abstract. *The relevance of the study is driven by the increasing use of artificial intelligence technologies in manufacturing quality management systems and by the need to control specific risks associated with data quality, model reliability, cybersecurity, staff competencies, and regulatory compliance. The purpose of the article is to develop and practically test an approach to assessing the risks of integrating AI into the quality management system of a manufacturing enterprise. The object of the study is the risk management process during AI integration into the QMS, using Ksenko Auto Production LLC as a case. The theoretical basis combines ISO 9001:2015, ISO 31000:2018, ISO 13485:2016, ISO/IEC 23894:2023, and ISO/IEC 42001:2023. The study applies analysis and synthesis of scientific sources, systems and process approaches, expert assessment, and a semi-quantitative probability–impact matrix. The expert group included five specialists representing management, quality, production, IT, and data-related functions; the assessment was conducted in 2026 using project materials, information on production and control processes, and professional expert judgments. Twenty-nine risks were identified and grouped into technical, organizational, human-resource, information and cybersecurity, regulatory, and socio-ethical categories. For each event, normalized probability and impact scores from 0 to 1 were determined and used to construct the risk profile. Under the adopted thresholds, seven risks were classified as critical; the highest scores were assigned to internet and power-system outages, mobilization of key specialists, and poor-quality data used for model training. Preventive and corrective measures were proposed, including data audits, infrastructure redundancy, model calibration, cross-training of personnel, and formalization of requirements. The practical value of the results lies in the possibility of using the approach as a reproducible tool for risk prioritization and action planning within a QMS without complex statistical models. The scientific novelty consists in aligning the risk-based logic of management-system standards with the assessment of AI-specific threats and testing this combination in a manufacturing setting. The approach improves transparency of criteria, comparability of assessments, and repeated monitoring of residual risk after management actions are implemented.*

Keywords: artificial intelligence; quality management system; risk management; manufacturing enterprise; expert assessment; risk matrix; ISO/IEC 23894.

Formulas: 0; **fig.:** 0; **tab.:** 4; **bibl.:** 17

Вступ. Інтеграція штучного інтелекту у виробничі системи управління якістю розширює можливості прогнозування дефектів, автоматизованого контролю та аналізу технологічних даних, але водночас створює нові джерела невизначеності. До традиційних виробничих ризиків додаються ризики низької якості даних, помилок моделей, недостатньої пояснюваності, кіберінцидентів, дефіциту компетенцій і регуляторної невідповідності. Застосування ШІ в СУЯ потребує не лише технічної валідації, а й системного ризик-орієнтованого управління. Методичною основою такого підходу є ISO 9001:2015 та ISO 31000:2018, а специфічні ризики ШІ додатково охоплюють ISO/IEC 23894:2023 та ISO/IEC 42001:2023. Для підприємств, пов'язаних із медичними виробами, важливими залишаються вимоги ISO 13485:2016, що зумовлює потребу в методиці, яка поєднує менеджмент якості, загальний ризик-менеджмент і особливості алгоритмічних систем.

Аналіз останніх досліджень. Українські дослідники розглядають ризики ШІ переважно через управлінські,

організаційні, кібербезпекові та соціально-економічні наслідки. Дашко і Никончук (2025) акцентують на впливі інтелектуальних систем на управлінські рішення та потребі аудиту моделей, якості даних і підготовки персоналу. Кривда і Кашпуренко (2023) систематизують ризики впровадження ШІ на підприємствах, а Скіцько та ін. (2023) деталізують загрози непрозорості, кібербезпеки й алгоритмічних помилок. Трикуліч (2025) аналізує підприємницькі ризики застосування ШІ, тоді як Крискун і Орлова-Курилова (2025) та Ковальчук і Орлова-Курилова (2025) пов'язують цифрові інструменти з управлінням ризиками та якістю.

У міжнародних дослідженнях особлива увага приділяється управлінню ризиками протягом життєвого циклу та забезпеченню контрольованості систем ШІ. Raji et al. (2020) пропонують наскрізний внутрішній аудит алгоритмічних систем, Morley et al. (2020) – перехід від загальних етичних принципів до практичних процедур контролю, а Ashmore et al. (2021) розглядають забезпечення надійності машинного навчання на всіх етапах

життєвого циклу. Для виробничого середовища особливо релевантні дослідження Escobar et al. (2021), які описують проблеми Quality 4.0 та промислових даних, і Tercan і Meisen (2022), які систематизують застосування машинного та глибокого навчання для прогнозування якості.

Отже, наукова база достатньо повно описує окремі групи ризиків, пов'язаних із ШІ, аудит моделей, якість даних і технології прогнозування якості. Водночас недостатньо опрацьованим залишається прикладний підхід, який би поєднував вимоги систем менеджменту якості, загального ризик-менеджменту та специфічних для ШІ ризиків у єдиній процедурі оцінювання на рівні конкретного виробничого підприємства. Саме ця методична прогалина визначає напрям дослідження.

Постановка завдання. Метою статті є розроблення та апробація напівкількісного підходу до оцінювання і пріоритизації ризиків інтеграції ШІ в систему управління якістю виробничого підприємства.

Дослідницьке припущення полягає в тому, що поєднання вимог ризик-орієнтованих стандартів із експертною матрицею «ймовірність–вплив» дає змогу отримати відтворюваний ризик-профіль навіть за відсутності достатньої статистики інцидентів. Теоретичну основу сформуvalи ISO 9001:2015, ISO 31000:2018, ISO 13485:2016, ISO/IEC 23894:2023 та ISO/IEC 42001:2023. Використано аналіз і синтез наукових праць, системний і процесний підходи, експертне оцінювання та напівкількісне ранжування.

Практичну апробацію проведено на ТОВ «КСЕНКО АВТОПРОДАКШН», що виготовляє автомобілі швидкої медичної допомоги та іншу спеціалізовану техніку (КСЕНКО Авто Продакшн, n.d.). До експертної групи увійшли п'ять фахівців: представник керівництва, фахівець із СУЯ, представник виробництва, IT-фахівець і фахівець з цифрових рішень та даних. Інформаційну базу становили внутрішні

проектна документація, дані про виробничі й контрольні процеси, зафіксовані організаційні та інфраструктурні обмеження та результати експертного обговорення за 2026 р. Підсумкові Р та І визначали консенсусом експертів.

Для кожного ризику визначали нормовані оцінки ймовірності Р та впливу І в інтервалі від 0 до 1. Їх трактували як напівкількісні експертні бали, а не як статистично встановлені ймовірності. Інтегральний ризик-індекс визначали як $R = P \times I$. Для інтерпретації використано пороги: $R \geq 0,40$ – критичний рівень; 0,24–0,39 – суттєвий; 0,11–0,23 – помірний; $R \leq 0,10$ – низький. Вплив оцінювали з урахуванням якості й безпеки продукції, безперервності процесів, витрат, строків, інформаційної безпеки та нормативної відповідності.

Результати дослідження.

Узагальнення положень міжнародних стандартів і наукових праць дало змогу систематизувати ризики інтеграції ШІ в СУЯ за шістьма групами: технічні; організаційні; кадрові; інформаційні та кібербезпекові; регуляторні; соціально-етичні. Зазначена класифікація дає змогу не обмежувати аналіз лише помилками алгоритмів, а враховувати організаційне середовище, дані, інфраструктуру, компетенції персоналу та вимоги до відповідності.

Теоретично інтеграцію ШІ у систему управління якістю доцільно розглядати як трансформацію механізму прийняття рішень у СУЯ. У традиційній моделі контроль ґрунтується на регламентованих перевітках, нормативних межах і професійному судженні персоналу, тоді як алгоритмічні системи частково перебирають функції виявлення відхилень, прогнозування та підтримки управлінської реакції. Через це змінюється сама структура ризику: поряд із виробничими й організаційними загрозами виникають ризики якості даних, помилок моделі, алгоритмічної упередженості, втрати пояснюваності та некоректного перенесення результатів на нові виробничі

умови. Отже, управління ризиками, пов'язаними із ШІ має охоплювати весь життєвий цикл рішення – від постановки задачі й підготовки даних до валідації, експлуатації, моніторингу та повторного навчання моделі.

Класифікація ризиків у СУЯ повинна враховувати не лише джерело їх виникнення, а й сферу прояву наслідків. Одна подія може мати комплексну природу: помилка моделі здатна виникнути через технічний дефект, неякісні дані або неправильну інтерпретацію результату персоналом, а наслідком стати виробничий брак, додаткові витрати чи нормативна невідповідність. Тому поділ на технічні, організаційні, кадрові, інформаційно-кібербезпекові, регуляторні та соціально-етичні ризики виконує не лише описову, а й управлінську функцію: дозволяє пов'язати кожну групу з відповідальними підрозділами та відповідними механізмами реагування – валідацією моделей, управлінням даними, навчанням персоналу, комплаєнсом і аудитом.

Вибір способу оцінювання ризику залежить від зрілості цифрової системи та доступності емпіричних даних. Для

стабільно експлуатованих процесів із накопиченою статистикою доцільні кількісні моделі, однак на ранніх етапах проєкту впровадження ШІ повна база відмов та інцидентів зазвичай відсутня. За таких умов надмірна математизація може створювати ілюзію точності, яка не відповідає якості вихідних даних. Тому в роботі обрано напівкількісний підхід: експертна ідентифікація поєднується з нормованою оцінкою ймовірності та впливу. Матриця «ймовірність-вплив» слугує інструментом первинної структуризації та пріоритизації, після якої критичні ризики можуть деталізуватися кількісними методами в міру накопичення даних.

Запропонований алгоритм складається з п'яти послідовних етапів: ідентифікації ризиків, експертного оцінювання, побудови ризик-профілю, визначення пріоритетів і планування заходів реагування. Його логіка відповідає загальним принципам ISO 31000:2018 і рекомендаціям ISO/IEC 23894:2023 щодо інтеграції ризик-менеджменту у процеси, пов'язані із ШІ, але адаптована до потреб СУЯ виробничого підприємства.

Таблиця 1

Алгоритм оцінювання ризиків інтеграції ШІ в СУЯ

Етап	Суть / ключові дії	Вихід (результат)
1. Ідентифікація ризиків	Аналіз внутрішнього та зовнішнього середовища; визначення технічних, організаційних, кадрових, інформаційно-кібербезпекових, регуляторних та соціально-етичних джерел ризику; формулювання потенційних ризикових подій.	Реєстр ризиків із зазначенням номера, опису ризикової події та сфери її виникнення.
2. Експертне оцінювання	Узгодження експертами нормованих оцінок ймовірності виникнення ризику (Р) та сили його впливу (І) в інтервалі від 0 до 1. Вплив оцінюється з урахуванням якості й безпеки продукції, безперервності процесів, витрат, строків, інформаційної безпеки та нормативної відповідності.	Значення Р та І для кожної ризикової події.
3. Побудова ризик-профілю	Розрахунок інтегрального ризик-індексу $R = P \times I$ та розміщення ризиків у матриці «ймовірність-вплив».	Матриця ризиків та інтегральні значення R.
4. Пріоритизація ризиків	Віднесення ризиків до встановлених рівнів: $R \geq 0,40$ – критичний; 0,24-0,39 – суттєвий; 0,11–0,23 – помірний; $R \leq 0,10$ – низький.	Перелік ризиків, ранжований за рівнем пріоритетності.
5. Планування реагування та контроль	Визначення превентивних і коригувальних заходів для пріоритетних ризиків; встановлення відповідальних осіб і механізмів контролю; повторне оцінювання ризику після реалізації заходів.	План управління ризиками та оцінка залишкового ризику.

Джерело : систематизовано автором

На першому етапі практичної апробації експерти уточнили перелік ризикових подій, після чого для кожної

позиції узгодили оцінки Р та І. Результати наведено в табл. 2.

Таблиця 2

Результати експертного оцінювання ризиків проєкту

№	Ризик	Р	І	Індекс $R = P \times I$	Рівень
1	Низька якість даних для навчання моделі ШІ	0,7	0,8	0,56	Критичний
2	Низька залученість та опір персоналу	0,9	0,4	0,36	Суттєвий
3	Перевищення бюджету	0,5	0,4	0,20	Помірний
4	Звільнення ключового співробітника	0,5	0,8	0,40	Критичний
5	Недооцінка складності інтеграції	0,7	0,4	0,28	Суттєвий
6	Зміна законодавства щодо даних та ШІ	0,3	0,4	0,12	Помірний
7	Кібератака, витік даних	0,3	0,8	0,24	Суттєвий
8	Невідповідність рішення очікуванням керівництва	0,5	0,8	0,40	Критичний
9	Апаратний збій серверів	0,3	0,8	0,24	Суттєвий
10	Затримки від постачальників	0,5	0,2	0,10	Низький
11	Помилки в калібруванні системи ШІ	0,5	0,8	0,40	Критичний
12	Недостатнє тестування	0,5	0,4	0,20	Помірний
13	Втрата фінансування	0,3	0,8	0,24	Суттєвий
14	Конфлікти між ІТ та виробництвом	0,7	0,2	0,14	Помірний
15	Необхідність донавчання моделі	0,9	0,2	0,18	Помірний
16	Бюрократичні затримки	0,7	0,2	0,14	Помірний
17	Відключення електропостачання	0,5	0,1	0,05	Низький
18	Несумісність обладнання	0,3	0,4	0,12	Помірний
19	Зміна пріоритетів керівництва	0,4	0,8	0,32	Суттєвий
20	Помилки у технічному завданні	0,5	0,8	0,40	Критичний
21	Низька продуктивність архітектури ШІ	0,3	0,4	0,12	Помірний
22	Хвороби ключових фахівців	0,4	0,2	0,08	Низький
23	Складність у формалізації критеріїв якості	0,7	0,4	0,28	Суттєвий
24	Проблеми з ліцензуванням ПЗ	0,3	0,2	0,06	Низький
25	Зростання конкуренції	0,2	0,4	0,08	Низький
26	Відключення інтернету та енергосистем	0,9	0,8	0,72	Критичний
27	Мобілізація ключових фахівців	0,8	0,8	0,64	Критичний
28	Пошкодження ІТ-інфраструктури	0,4	0,8	0,32	Суттєвий
29	Психологічне виснаження команди	0,9	0,4	0,36	Суттєвий

Джерело: складено автором за результатами експертного оцінювання

Експертне оцінювання охопило 29 ризикових подій (Таблиця 2). Найвищі індекси отримали відключення інтернету та енергосистем (0,72), мобілізація ключових фахівців (0,64) і низька якість даних для навчання моделі (0,56). До критичного рівня також віднесено звільнення ключового фахівця, невідповідність рішення очікуванням керівництва, помилки калібрування та технічного завдання. Узагальнений розподіл становив 7 критичних, 9 суттєвих, 8 помірних і 5 низьких ризиків та підтверджує, що для проєкту впровадження ШІ суттєвими є не лише алгоритмічні, а й кадрові, організаційні та інфраструктурні фактори.

Матриця «ймовірність-вплив» дає змогу візуально відобразити розподіл ідентифікованих ризиків та визначити зони їх найбільшої концентрації. Найвищі значення інтегрального ризик-індексу характерні переважно для подій із високим рівнем впливу, що свідчить про особливу значущість кадрових, інфраструктурних, інформаційних та управлінських факторів у процесі інтеграції ШІ в СУА.

Найбільш критичними є ризики, пов'язані з відключенням інтернету та енергосистем, мобілізацією та звільненням ключових фахівців, низькою якістю даних для навчання моделі ШІ, помилками калібрування і технічного завдання, а також

невідповідністю рішення очікуванням керівництва. Отриманий ризик-профіль підтверджує необхідність комплексного підходу до управління ризиками, який не

обмежується лише технічними характеристиками системи ІІІ.

Таблиця 3

Матриця «ймовірність-вплив» (номери ризиків)

Ймовірність Р	I = 0,1	I = 0,2	I = 0,4	I = 0,8
0,81–1,00	–	15	2, 29	26
0,61–0,80	–	14, 16	5, 23	1, 27
0,41–0,60	17	10	3, 12	4, 8, 11, 20
0,21–0,40	–	22, 24	6, 18, 21	7, 9, 13, 19, 28
0,00–0,20	–	–	25	–

Джерело: складено автором

На завершальному етапі оцінювання ризиків здійснено розроблення заходів реагування для подій, віднесених до критичного рівня. З огляду на те, що такі ризики можуть безпосередньо впливати на безперервність виробничих процесів, якість продукції, стабільність функціонування СУЯ та реалізацію проєкту інтеграції ІІІ, для кожного з них визначено комплекс превентивних і коригувальних дій. Превентивні заходи спрямовані на зниження ймовірності виникнення ризикової події, тоді як коригувальні – на мінімізацію її наслідків у разі реалізації. Узагальнені результати наведено в табл. 4.

Аналіз запропонованих заходів свідчить, що реагування на критичні ризики має охоплювати одночасно превентивну та коригувальну складові. Для ризиків, пов'язаних із якістю даних і функціонуванням моделей ІІІ, пріоритетними є аудит, очищення, валідація, повторне калібрування та можливість тимчасового переходу до ручного контролю. Кадрові ризики потребують крос-навчання, дублювання компетенцій і планування наступництва, тоді як інфраструктурні – резервування живлення, каналів зв'язку та інформаційних ресурсів. Управлінські ризики доцільно мінімізувати через

формалізацію вимог, погодження критеріїв приймання, колективне рев'ю технічного завдання та повторне тестування. Таким чином, запропоновані заходи спрямовані не лише на мінімізацію наслідків ризикових подій, а й на зниження ймовірності їх виникнення та підвищення стійкості системи управління якістю.

Практична цінність підходу полягає у прямому перетворенні результатів оцінювання на реєстр ризиків і план дій. Повторне оцінювання після реалізації заходів дає змогу фіксувати залишковий ризик та використовувати його у внутрішньому аудиті й циклі постійного вдосконалення СУЯ.

Висновки. У результаті дослідження обґрунтовано доцільність застосування ризик-орієнтованого підходу до інтеграції штучного інтелекту в систему управління якістю виробничого підприємства. Теоретичне узагальнення положень міжнародних стандартів і наукових досліджень дало змогу систематизувати ризики за технічними, організаційними, кадровими, інформаційно-кібербезпековими, регуляторними та соціально-етичними напрямками та визначити необхідність їх оцінювання протягом усього життєвого циклу ІІІ-рішення.

Таблиця 4

Заходи реагування на критичні ризики

№	Найменування ризику	Превентивні заходи	Коригувальні заходи
1	Низька якість даних для навчання моделі ІІІ	Аудит і очищення даних; стандартизація процедур їх збору; автоматизована валідація; регламентація введення та оновлення даних.	Повернення до перевіреного набору даних; повторне очищення даних; донавчання та повторна валідація моделі.
4	Звільнення ключового фахівця	Крос-навчання персоналу; документування критичних процесів; дублювання ключових компетенцій; формування кадрового резерву.	Тимчасовий перерозподіл функцій між членами команди; залучення резервного спеціаліста; коригування строків виконання робіт.
8	Невідповідність рішення очікуванням керівництва	Погодження критеріїв приймання результату; регулярні демонстрації проміжних результатів; ревію технічного завдання та залучення ключових стейкхолдерів.	Уточнення вимог і пріоритетів; внесення змін до технічного завдання; проведення повторного циклу тестування.
11	Помилки в калібруванні системи ІІІ	Лабораторне та пілотне калібрування; використання контрольних вибірок; тестування в умовах, наближених до виробничих; застосування принципу human-in-the-loop.	Тимчасове припинення автоматизованого прийняття рішень; перехід до ручного контролю; повторне калібрування та валідація моделі.
20	Помилки у технічному завданні	Колективне ревію технічного завдання; стандартизовані шаблони вимог; формалізація критеріїв якості; контроль і простежуваність змін.	Коригування технічного завдання; повторна оцінка впливу внесених змін; проведення регресійного тестування системи.
26	Відключення електроенергії та інтернету	Використання ДБЖ і генераторів для критичної інфраструктури; резервні канали зв'язку; резервування серверної інфраструктури; можливість локальної роботи критичних функцій.	Перехід на резервні джерела живлення та канали зв'язку; відновлення даних; перевірка їх цілісності та працездатності інформаційних систем після відновлення роботи.
27	Мобілізація ключових технічних фахівців	Крос-навчання; дублювання функціональних ролей; документування процесів; формування плану наступництва.	Передача функцій підготовленим резервним працівникам; перерозподіл завдань; перегляд строків реалізації проєкту та критичних залежностей.

Джерело: складено автором за результатами оцінювання ризиків

Запропоновано напівкількісний підхід до оцінювання ризиків, який поєднує експертне визначення ймовірності та впливу з формуванням інтегрального ризик-індексу та матриці «ймовірність-вплив», забезпечує можливість порівняння різнорідних ризикових подій за єдиною шкалою та визначення пріоритетності управлінського реагування за умов обмеженої статистичної інформації. Методичний підхід узгоджено з положеннями ISO 9001, ISO 13485, ISO 31000, ISO/IEC 23894 та ISO/IEC 42001 і адаптовано до особливостей системи управління якістю виробничого підприємства.

Практична апробація на ТОВ «КСЕНКО АВТОПРОДАКШН» охопила

29 ризикових подій. За результатами експертного оцінювання 7 ризиків віднесено до критичних, 9 – до суттєвих, 8 – до помірних і 5 – до низьких. Найвищі значення ризик-індексу отримали відключення інтернету та енергосистем, мобілізація ключових фахівців і низька якість даних для навчання моделі ІІІ. Отримані результати засвідчили, що критичний ризик-профіль інтеграції ІІІ формується не лише технологічними чинниками, а й кадровими, організаційними та інфраструктурними загрозами.

Для критичних ризиків сформовано комплекс превентивних і коригувальних заходів, що охоплює аудит і валідацію даних, калібрування моделей, резервування

інфраструктури та каналів зв'язку, крос-навчання персоналу, дублювання критичних компетенцій, формалізацію вимог і повторне тестування, що дає змогу трансформувати результати оцінювання ризиків у практичний план управлінських дій та надалі контролювати залишковий ризик у межах внутрішнього аудиту і постійного вдосконалення СУЯ.

Наукова новизна дослідження полягає в адаптації положень загального ризик-менеджменту та стандартів управління ІІІ до єдиної процедури оцінювання ризиків у системі управління якістю виробничого підприємства, яка поєднує специфічні для ІІІ, виробничі, кадрові та інфраструктурні загрози в межах спільної системи пріоритизації.

Практичне значення полягає у можливості використання запропонованого

підходу для формування реєстру ризиків, визначення пріоритетів реагування та контролю залишкового ризику без необхідності застосування складних статистичних моделей. Очікуваний соціально-економічний ефект пов'язаний зі зниженням імовірності виробничих збоїв, непродуктивних витрат, втрат якості та залежності від окремих критичних ресурсів.

Обмеженням дослідження є експертний характер оцінок та апробація підходу на одному підприємстві. Подальші дослідження доцільно спрямувати на перевірку запропонованої методики на ширшій вибірці виробничих підприємств, порівняння експертних оцінок із фактичними даними про інциденти та уточнення порогових значень ризику на основі накопиченої статистики.

Конфлікт інтересів. Автори заявляють, що дослідження проводилося за відсутності будь-яких комерційних або фінансових відносин, які могли б бути витлумачені як потенційний конфлікт інтересів.

Фінансування. Автори заявляють, що публікацію цієї статті профінансовано авторами самостійно.

Етична заява. Усі процедури, виконані в межах цього дослідження, відповідали інституційним та міжнародним етичним стандартам.

Заява щодо генеративного ІІІ. Генеративний штучний інтелект використовувався як допоміжний інструмент для структурного та мовного редагування рукопису. Остаточна перевірка фактичних тверджень, розрахунків, бібліографічних даних і формулювань здійснюється авторами, які несуть повну відповідальність за зміст статті.

Внесок авторів. Усі автори зробили однаковий внесок у розроблення концепції дослідження, написання тексту та затвердження остаточної версії рукопису.

Література:

1. International Organization for Standardization. (2015). ISO 9001:2015 Quality management systems – Requirements. <https://www.iso.org/standard/62085.html>
2. International Organization for Standardization. (2016). ISO 13485:2016 Medical devices – Quality management systems – Requirements for regulatory purposes. <https://www.iso.org/standard/59752.html>
3. International Organization for Standardization. (2018). ISO 31000:2018 Risk management – Guidelines. <https://www.iso.org/standard/65694.html>
4. International Organization for Standardization, & International Electrotechnical Commission. (2023a). ISO/IEC 23894:2023 Information technology—Artificial intelligence – Guidance on risk management. <https://www.iso.org/standard/77304.html>
5. International Organization for Standardization, & International Electrotechnical Commission. (2023b). ISO/IEC 42001:2023 Information technology – Artificial intelligence— Management system. <https://www.iso.org/standard/42001.html>
6. Ashmore, R., Calinescu, R., & Paterson, C. (2021). Assuring the machine learning lifecycle: Desiderata, methods, and challenges. *ACM Computing Surveys*, 54(5), Article 111, 1-39. <https://doi.org/10.1145/3453444>
7. Дашко, І. М., & Никончук, Г. В. (2025). Вплив штучного інтелекту на процеси прийняття управлінських рішень. *Економічний простір*, 204, 82-88. <https://doi.org/10.30838/EP.204.82-88>
8. Escobar, C. A., McGovern, M. E., & Morales-Menendez, R. (2021). Quality 4.0: A review of big data challenges in manufacturing. *Journal of Intelligent*

Manufacturing, 32, 2319-2334.
<https://doi.org/10.1007/s10845-021-01765-4>

9.Ковальчук, І., & Орлова-Курилова, О. (2025). Цифрова трансформація управління якістю на підприємстві засобами штучного інтелекту. *Вчені записки Університету «КРОК»*, 3(79), 294–300.
<https://doi.org/10.31732/2663-2209-2025-79-294-300>

10.Кривда, О. В., & Кашпуренко, Т. О. (2023). Ризики впровадження штучного інтелекту на підприємствах. У *Бізнес, інновації, менеджмент: проблеми та перспективи: збірник тез доповідей IV Міжнародної науково-практичної конференції*. КІП ім. Ігоря Сікорського, Видавництво «Політехніка».

11.Крискун, І., & Орлова-Курилова, О. (2025). Керування ризиками в управлінні ІТ-проєктами з використанням інструментів штучного інтелекту. *Вчені записки Університету «КРОК»*, 2(78), 315–325. <https://doi.org/10.31732/2663-2209-2025-78-315-325>

12.КСЕНКО Авто Продакшн. (n.d.). *Офіційний сайт*. <https://ksenkoautoproduction.com/>

13.Morley, J., Floridi, L., Kinsey, L., & Elhalal, A. (2020). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices. *Science and*

Engineering Ethics, 26, 2141-2168.
<https://doi.org/10.1007/s11948-019-00165-5>

14.Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33-44). Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372873>

15.Скіцько, О., Складанний, П., Ширшов, Р., Гуменюк, М., & Ворохоб, М. (2023). Загрози та ризики використання штучного інтелекту. *Кібербезпека: освіта, наука, техніка*, 2(22), 6–18.
<https://doi.org/10.28925/2663-4023.2023.22.618>

16.Tercan, H., & Meisen, T. (2022). Machine learning and deep learning based predictive quality in manufacturing: A systematic review. *Journal of Intelligent Manufacturing*, 33, 1879-1905.
<https://doi.org/10.1007/s10845-022-01963-8>

17.Трикуліч, П. П. (2025). Ризики впровадження штучного інтелекту у підприємницьку діяльність. *Економіка та суспільство*, 71.
<https://doi.org/10.32782/2524-0072/2025-71-159>