МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет ім. В. Н. Каразіна

Факультет: **ІПП Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **122 Комп'ютерні науки**
Освітня програма: **Комп'ютерні науки та інформаційні технології в бізнесі**

Група: АК-41Б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

«ДОСЛІДЖЕННЯ РИЗИКІВ У ПРОЄКТАХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ» ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

здобувача вищої освіти Булгакової Олесі Артемівни

Робота допущена до захисту в ЕК

протокол кафедри ІТММ № 13 від 31.05. 2025 р.

Завідувач кафедри ІТММ

к.п.н.

_____ Н. І. Стяглик

Науковий керівник:

к.ф.-м.н, доц.

_____ Чеканова Н. М.

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут «Каразінський банківський інститут»
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 122 Комп'ютерні науки
Освітня програма Комп'ютерні науки та інформаційні технології в бізнесі

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали, прізвище
«__08__» лютого 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Булгакової Олесі Артемівни
(прізвище, ім'я, по батькові студента)

1. Тема роботи «Дослідження ризиків у проєктах з використанням штучного інтелекту»

керівник роботи к.ф.-м.н, доц. Н. М. Чеканова
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом по університету від "08" лютого 2025 року № 4601-5/335

2. Строк подання студентом роботи 10 травня 2025 року

3. Перелік питань, які потрібно розробити

У розділі 1: розглянути поняття та класифікацію ризиків, дослідити методи ідентифікації та оцінки ризиків.
У розділі 2: проаналізувати проєкти із впровадження штучного інтелекту, оцінити ризики у проєктах з використанням штучного інтелекту, розробити план управління ризиками у проєктах зі штучним інтелектом.
У розділі 3: дослідити проблеми використання штучного інтелекту у IT-проєктах, визначити перспективи використання штучного інтелекту у IT-проєктах.

4. План роботи

№ з/п	Назва етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

5. Дата видачі завдання 25 січня 2024 року

Студент _____ ___О. А. Булгакова__
Підпис ініціали, прізвище

Керівник роботи _____ _Н. М. Чеканова__
Підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ МАГІСТЕРСЬКУ РОБОТУ
«ДОСЛІДЖЕННЯ РИЗИКІВ У ПРОЄКТАХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ»
Булгакової Олесі Артемівни

Кваліфікаційна магістерська робота містить: 70 сторінок, 6 таблиць, 4 рисунки, список літератури з 63 найменувань.

Об'єктом дослідження є управління ризиками у проєктах.

Предмет дослідження – теоретичні та практичні аспекти управління ризиками у проєктах з використання штучного інтелекту.

Мета кваліфікаційної бакалаврської роботи полягає у аналізі проєктів із впровадженням штучного інтелекту, розробці плану управління ризиками у проєктах зі штучним інтелектом, визначенні проблематики використання штучного інтелекту у проєктах; визначенні перспектив використання штучного інтелекту у проєктах.

Завданнями кваліфікаційної магістерської роботи є:

- у першому розділі розглянути поняття та класифікацію ризиків у проєктах з використанням штучного інтелекту, дослідити методи ідентифікації та оцінки ризиків проєктів з використанням штучного інтелекту;
- у другому розділі проаналізувати проєкти із впровадження штучного інтелекту, оцінити ризики у проєктах з використанням штучного інтелекту, розробити план управління ризиками у проєктах зі штучним інтелектом;
- у третьому розділі дослідити проблеми використання штучного інтелекту у ІТ-проєктах, визначити перспективи використання штучного інтелекту у ІТ-проєктах.

Актуальність дослідження. Застосування штучного інтелекту в проєктах зумовлює нові ризики, що потребують глибокого аналізу та управління.

За результатами дослідження визначено ключові ризики ШІ-проєктів, розроблено ефективні підходи до їх ідентифікації, оцінювання та подальшого усунення.

Практична новизна: запропоновано інноваційну модель, управління ризиками, орієнтовану спеціально на особливості впровадження штучного інтелекту у проєктах.

Одержані результати можуть використовуватися компаніями різних галузей для безпечного й ефективного впровадження технологій штучного інтелекту.

КЛЮЧОВІ СЛОВА: ШТУЧНИЙ ІНТЕЛЕКТ, УПРАВЛІННЯ РИЗИКАМИ, ІДЕНТИФІКАЦІЯ РИЗИКІВ, ОЦІНКА РИЗИКІВ, ІННОВАЦІЙНІ ПРОЄКТИ, ПРОЄКТНИЙ МЕНЕДЖМЕНТ.

ABSTRACT
AT QUALIFICATION MAGISTER WORK

The qualifying master's thesis contains: 70 pages, 6 tables, 4 figures, a list of 63 references.

The object of research is risk management in projects.

The subject of research is theoretical and practical aspects of risk management in projects using artificial intelligence.

The purpose of the bachelor's thesis is to analyze projects with the introduction of artificial intelligence, develop a risk management plan for projects with artificial intelligence, identify problems of using artificial intelligence in projects; determine the prospects for using artificial intelligence in projects.

The tasks of the qualifying master's thesis are:

- In the first section, consider the concept and classification of risks in projects using artificial intelligence, explore methods for identifying and assessing risks in projects using artificial intelligence;

- in the second section, analyze artificial intelligence projects, assess risks in projects using artificial intelligence, and develop a risk management plan for artificial intelligence projects;

- in the third section, examine the problems of using artificial intelligence in IT projects and determine the prospects for using artificial intelligence in IT projects.

Relevance of the study. The use of artificial intelligence in projects creates new risks that require in-depth analysis and management.

The study identified the key risks of AI projects and developed effective approaches to their identification, assessment, and subsequent elimination.

Practical novelty: an innovative risk management model focused specifically on the peculiarities of implementing artificial intelligence in projects is proposed.

The results can be used by companies in various industries for the safe and effective implementation of artificial intelligence technologies.

KEYWORDS: ARTIFICIAL INTELLIGENCE, RISK MANAGEMENT, RISK IDENTIFICATION, RISK ASSESSMENT, INNOVATIVE PROJECTS, PROJECT MANAGEMENT.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. В умовах стрімкої цифровізації світової економіки, ризики, пов’язані з впровадженням та експлуатацією інноваційних технологій, зокрема штучного інтелекту, набули нової ваги та складності. Українські підприємства, орієнтовані на адаптацію до вимог сучасного конкурентного середовища, змушені працювати в умовах невизначеності, що посилюється як воєнним станом, так і нестабільністю зовнішніх ринків. У цьому контексті ефективне управління ризиками стало не просто бажаним інструментом, а критично необхідною складовою стратегічного управління. Особливо це стосується тих секторів, де цифрові рішення, зокрема на основі ШІ, впроваджуються у виробничі, логістичні та управлінські процеси, що створює як нові можливості, так і нові загрози.

Виклики, пов’язані з адаптацією штучного інтелекту до реалій українського бізнесу, потребують переосмислення традиційних підходів до оцінки та ідентифікації ризиків. Україна наразі знаходиться у фазі трансформації національної економіки з опорою на інновації та ІТ-рішення. Проте відсутність сталих регламентів з кібербезпеки, обмежений доступ до сучасних методик ризик-менеджменту та недостатній рівень цифрової грамотності управлінців створюють потенційно небезпечні сценарії. Відтак, дослідження, спрямовані на осмислення методів управління ризиками у сфері застосування ШІ, є не лише актуальними в глобальному вимірі, а й особливо релевантними у вітчизняному контексті як інструмент зменшення невизначеності та підвищення стабільності функціонування бізнесу.

Теоретичні засади економічного ризику ґрунтовно висвітлені у працях таких українських науковців, як М. В. Боровик, В. В. Вітлінський, І. Ю. Івченко, Н. І. Машина та Ю. О. Швець. Автори детально аналізують природу ризику, класифікаційні підходи та методи його кількісного й якісного аналізу, що закладає міцну основу для подальших досліджень. У роботах Т. А. Васильєвої, Я. М. Кривича та В. А. Підсолонка особливу увагу приділено

прикладним аспектам ризик-менеджменту на підприємствах. Останні публікації, зокрема статті О. О. Олійника та К. Е. Шурди, акцентують увагу на потребі в ідентифікації новітніх ризиків, що виникають у результаті технологічного розвитку, зокрема у сфері цифрової трансформації бізнесу.

Міжнародний дискурс проблематики значною мірою зосереджений на ризиках, пов'язаних зі штучним інтелектом, його алгоритмічною прозорістю, етикою застосування та потенційними кіберзагрозами. У працях S. Bhatia, R. Kreutzer, T. Cheatham, а також у звітах McKinsey Global Institute та World Economic Forum, порушуються питання балансу між ефективністю ШІ-рішень і загрозами, які вони генерують. Сучасні дослідження створюють підґрунтя для формування інтегрованих моделей ризик-менеджменту, релевантних для українських підприємств, що впроваджують інноваційні цифрові технології.

Мета дослідження полягає у аналізі проєктів із впровадженням штучного інтелекту, розробці плану управління ризиками у проєктах зі штучним інтелектом, визначенні проблематики використання штучного інтелекту у проєктах; визначенні перспектив використання штучного інтелекту у проєктах.

Для досягнення поставленої мети дослідження необхідно виконати наступні **завдання**:

- дослідити поняття та класифікацію ризиків;
- розглянути методи ідентифікації та оцінки ризиків;
- проаналізувати проєкти із впровадження штучного інтелекту;
- оцінити ризики у проєктах з використанням штучного інтелекту;
- розробити план управління ризиками у проєктах зі штучним інтелектом;
- розглянути проблеми використання штучного інтелекту у проєктах;
- визначити перспективи використання штучного інтелекту у проєктах.

Об'єктом дослідження є управління ризиками у проєктах.

Предметом дослідження є теоретичні та практичні аспекти управління ризиками у проєктах з використання штучного інтелекту.

Методи дослідження. У процесі дослідження було застосовано комплекс методів, зокрема аналіз наукової та прикладної літератури, порівняльний аналіз підходів до оцінювання ризиків впровадження ШІ, метод експертних оцінок для визначення потенційних загроз, а також елементи системного підходу для формування цілісного бачення проблематики.

Інформаційна база дослідження. Інформаційну основу роботи склали публікації у фахових журналах, звіти міжнародних аналітичних центрів (OECD, McKinsey, World Economic Forum), аналітичні доповіді з тематики ризиків штучного інтелекту, нормативно-правові документи, а також сучасні кейси з практики впровадження ШІ у проєктну діяльність різних галузей.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДИЧНІ ОСНОВИ РИЗИКІВ У ПРОЄКТАХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

1.1. Поняття та класифікація ризиків

Ризик є невід'ємною складовою будь-якої сфери суспільного життя. Його поняття бере свій початок у сфері азартних ігор, де виникла необхідність оцінювати загрози, з якими стикаються учасники. Сам термін походить від латинського «risicare», що означає «приймати рішення». Існують й інші тлумачення: від грецького «ridsikon, ridsa» – скеля; італійського «risiko» – небезпека, загроза; французького «risqoe» – ризик, загроза.

Ризик – це багатогранне явище, що має значний вплив не лише на економіку, а й на всі аспекти людської діяльності. Попри його важливість, у законодавстві немає єдиного підходу до його визначення. Наприклад, в українській правовій системі немає загальноприйнятого визначення терміна «ризик». Лише у статті 1 Закону України «Про об'єкти підвищеної небезпеки» № 2245-III від 18 січня 2001 року сформульовано поняття ризику: це ступінь імовірності настання певної негативної події в конкретний момент часу або за певних умов на території об’єкта підвищеної небезпеки та/або за його межами. Водночас у згаданому законі поняття ризику розглядається виключно в контексті діяльності суб’єктів господарювання, що володіють або використовують такі об’єкти [12].

Аналіз сучасної економічної літератури свідчить про відсутність єдиного підходу до трактування поняття «ризик». Більшість дослідників схиляються до того, що ризик слід розглядати як імовірність негативного результату певної діяльності.

Так, І. Івченко визначає ризик як «ймовірність втрат або недоотримання доходу порівняно з прогнозованим варіантом» [5].

На думку В. Г. Пасічника та О. В. Акіліної, суть ризику полягає в тому,

що кожне підприємство у процесі економічної та фінансової діяльності перебуває під загрозою втрати прибутку чи платоспроможності через непередбачувані зміни внутрішнього середовища [10].

«Економічний енциклопедичний словник» під редакцією С. В. Мочерного визначає ризик як «невизначеність і можливість настання подій із негативними наслідками (втрати, недоотримання прибутку тощо), спричиненими певними діями або рішеннями» [7].

А. Г. Загородній та Г. Л. Вознюк тлумачать ризик як «реалізовану можливість виникнення непередбачених втрат очікуваного прибутку, майна, коштів унаслідок випадкових змін умов економічної діяльності чи несприятливих обставин» [4].

С. В. Мочерний також розглядає ризик як «невід'ємний елемент процесу прийняття рішень в умовах невизначеності» [7].

Ю. В. Сенейко вважає, що ризик – це можливість виникнення ситуації, яка може призвести до відхилення від поставленої мети (спричинити втрати або недоотримання прибутку) або ж залишитися без змін [13].

Дослідники В. А. Підсолонко, А. Ф. Процай, Т. Л. Миронова та В. О. Василенко визначають ризик як явище, що проявляється у співвідношенні вигод і втрат на тлі невизначеності. Вони наголошують на складній взаємодії між поточним станом суб'єкта господарювання та можливостями його трансформації у майбутньому. Ризик виникає внаслідок впливу внутрішніх і зовнішніх чинників, випадкових та закономірних процесів, а також причинно-наслідкових зв'язків [11].

Як економічна категорія, ризик характеризується можливістю настання певної події, що може призвести як до втрат, так і до нульового або позитивного результату.

Однак трактування поняття «ризик» у науковій літературі значно відрізняється. Деякі дослідники акцентують увагу виключно на потенційних втратах або прибутках, тоді як інші пов'язують його з умовами прийняття рішень. Наприклад, О. І. Ястремський зазначає, що ризик існує лише тоді, коли

рішення ухвалюється в умовах невизначеності, а його результат має значення для того, хто це рішення приймає [17].

Г. В. Осовська визначає ризик як ситуаційну характеристику діяльності економічного суб'єкта, що виникає в умовах невизначеності [9].

Науковці Н. І. Машина та В. В. Вітлінський розглядають ризик у межах економічної системи. Машина трактує його як об'єктивно-суб'єктивну категорію, що пов'язана з подоланням невизначеності, випадковості та конфліктних ситуацій. На її думку, ризик відображає ступінь досягнення запланованого результату [6].

В. В. Вітлінський пропонує інше визначення, підкреслюючи, що ризик є економічною категорією, яка демонструє сприйняття невизначеності та конфліктів з боку учасників економічних процесів. Він безпосередньо пов'язаний із цілепокладанням, управлінням, прийняттям рішень та оцінкою можливих загроз і невикористаних шансів [3].

Аналізуючи різні підходи до визначення ризику, можна дійти висновку, що в науковій літературі існує безліч його трактувань. Більшість авторів формулюють власне визначення цього поняття (В. В. Вітлінський, Н. І. Машина, С. В. Мочерний тощо), тоді як лише незначна частина дослідників поділяє їх погляди. Одна група науковців (І. Івченко, В. Пасічник, О. Акіліна) концентрується лише на негативних наслідках ризику, тоді як інші (Ю. Сенейко, В. Підсолонко, А. Процай, Т. Миронова, В. Василенко) вбачають у ньому також позитивні аспекти.

У ринкових умовах ризик зазвичай асоціюється з економічними результатами, які можуть бути як сприятливими (тоді ризик є можливістю), так і негативними (ризик як загроза). Тому ризикова ситуація виникає лише за наявності щонайменше двох альтернативних сценаріїв, що передбачають різні наслідки. З цієї точки зору ризик можна визначити як ймовірність:

- настання негативних наслідків у результаті певних дій;
- будь-яких відхилень від запланованих показників;
- появи як позитивних, так і небажаних результатів.

Одним із поширених наслідків реалізації ризику є прийняття помилкових рішень, що спричиняє збитки. Вони можуть мати різний характер [2]:

1. Матеріальні збитки – виникають у вигляді незапланованих витрат на ремонт обладнання, закупівлю сировини, оплату енергоресурсів тощо.

2. Трудові втрати – вимірюються втраченим робочим часом через непередбачувані обставини.

3. Фінансові втрати – обчислюються у вигляді прямих грошових втрат, додаткових податкових зобов’язань або недоотриманого прибутку.

4. Часові витрати – виражаються у вигляді затримок (від кількох годин до місяців) у досягненні запланованого результату.

5. Специфічні втрати – включають моральні (втрата ділової репутації), соціальні (втрата довіри споживачів) тощо.

Об’єктом ризику зазвичай виступає матеріальна складова (особа чи майно) або майновий інтерес (нематеріальна характеристика, наприклад, прибуток).

Водночас ризик не обмежується лише його наслідками чи ймовірністю певної події – він також розкривається через чинники, що його спричиняють. Джерелом ризику є подія, ймовірність настання якої можна оцінити, однак точний час і місце її реалізації залишаються невизначеними. Це зумовлено особливостями ринкових процесів, впливом зовнішнього середовища та внутрішніх факторів, зокрема особистими характеристиками тих, хто ухвалює рішення.

Залежно від природи походження, ризик має три основні аспекти:

1. Об’єктивний – ризик є невід’ємною частиною реальних процесів і явищ, незалежно від того, чи усвідомлює його суб’єкт.

2. Суб’єктивний – ризик залежить від індивідуального сприйняття, що формується на основі моральних, психологічних та ідеологічних факторів.

3. Об’єктивно-суб’єктивний – ризик визначається як сукупність об’єктивних умов і суб’єктивних підходів до його оцінки.

Серед ключових джерел ризику виділяють [1]:

1. Невизначеність природних процесів та явищ – стихійні лиха (землетруси, урагани, град тощо), які негативно впливають на результати господарської діяльності.

2. Випадковість подій – обумовлена ймовірнісним характером соціально-економічних і технологічних процесів, що унеможливлює точне прогнозування результатів.

3. Конфліктність інтересів і тенденцій – наприклад, конкуренція на ринку.

4. Інформаційні обмеження – недостатність або низька якість доступної інформації.

5. Неможливість повного пізнання об’єктів, процесів і явищ.

6. Різноманітність соціально-психологічних підходів і оцінок – різні погляди на ухвалення рішень.

Отже, ризик як явище має складну структуру, яка включає три ключові елементи (рис. 1.1):

1. Джерело ризику – події чи групи подій, що становлять потенційну загрозу втрат або створюють можливість отримання додаткових вигод.

2. Об’єкт ризику – той, на кого або на що впливає джерело ризику.

3. Наслідки ризику – результати як негативного, так і позитивного впливу ризику.

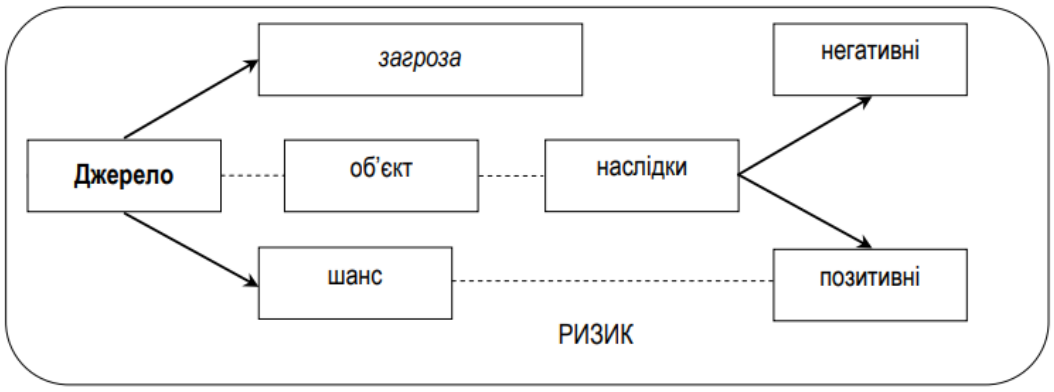

Рис. 1.1. Структура ризику [2]

Ризик можна проаналізувати зі структурної точки зору, розглянувши наступні ключові фактори [14]:

- потенційна загроза (небезпека);
- вплив ризику;
- вразливість (чутливість до ризику);
- ступінь взаємодії між ризиками.

Потенційна загроза – це можливість виникнення збитку або іншого прояву ризику, зумовленого характеристиками об'єкта, конкретним ризиковим сценарієм і типом збитку. Потенційна загроза є фундаментальним аспектом ризику, оскільки без небезпеки ризик не може існувати.

Вплив ризику описує ситуацію, яка створює потенціал для збитків або інших ризикових наслідків. З технічної точки зору, це стосується одиниць спостереження. Одиниці спостереження можуть варіюватися залежно від контексту: наприклад, у дослідженнях смертності це може бути кількість людей; в оцінці ризиків стихійних лих це може означати розмір ураженої території.

Вразливість вимірює потенційну серйозність шкоди, яка може бути завдана об'єкту, що аналізується. Вона являє собою як кількісну оцінку ризику, так і розуміння того, як різні фактори впливають на рівень ризику.

Взаємодія з іншими ризиками передбачає розгляд набору або портфеля ризиків. У цьому контексті взаємозв'язки між ризиками розглядаються в широкому сенсі, не обмежуючись лише тим, чи є вони статистично пов'язаними чи ні.

Штучний інтелект (ШІ) є трансформаційною силою, що пропонує величезний потенціал, але водночас несе в собі складні ризики [29]. З одного боку, штучний інтелект покращує бізнес-операції, оптимізує процес прийняття рішень і підвищує якість обслуговування клієнтів, а його внесок у світову економіку, за прогнозами, досягне 13 трильйонів доларів США щорічно до 2030 року. З іншого боку, швидке розгортання ШІ викликає занепокоєння щодо етичних наслідків, вразливостей у сфері безпеки та

непередбачуваних наслідків, які організації повинні ретельно враховувати [27].

Ризики, пов'язані зі штучним інтелектом, можна умовно поділити на кілька категорій. Технічні ризики виникають через алгоритмічні упередження, системні помилки та непередбачуваність моделей машинного навчання. Операційні ризики виникають внаслідок інтеграції ШІ в бізнес-процеси, що потенційно може призвести до фінансових втрат, репутаційних збитків або невідповідності нормативним вимогам. Етичні та соціальні ризики складаються з таких проблем, як дискримінація, порушення конфіденційності та дезінформація, тоді як ризики безпеки пов'язані з такими загрозами, як ворожі атаки або кібервторгнення, керовані штучним інтелектом.

Можливі ризики ШІ можна згрупувати в п'ять основних категорій, кожна з яких має кілька підкатегорій. Групи охоплюють різноманітні проблеми та перешкоди, пов'язані з розвитком і застосуванням ШІ. Розглянемо п'ять основних категорій потенційних ризиків ШІ разом з їх підкатегоріями:

1. Етичні та соціальні ризики. Однією з основних загроз, пов’язаних із застосуванням штучного інтелекту, є проблема упередженості та дискримінації. Алгоритми ШІ, навчаючись на даних, можуть відтворювати існуючі соціальні нерівності, що призводить до несправедливого ставлення у сферах зайнятості, фінансових послуг та правосуддя [45]. Штучний інтелект залежить від великих масивів персональних даних, що створює значні ризики для конфіденційності та інформаційної безпеки. Несанкціонований доступ, зловживання або неналежне управління цими даними можуть призвести до серйозних наслідків для громадян і компаній [46].

Соціальною загрозою є зміни на ринку праці, викликані широким впровадженням ШІ. Автоматизація багатьох процесів може спричинити масове витіснення працівників із низки професій, що, у свою чергу, посилить соціально-економічну нерівність та призведе до необхідності перекваліфікації значної кількості людей [23]. Окрему проблему становить питання відповідальності та підзвітності: якщо автономна система приймає рішення,

що призводять до помилок або шкоди, визначення відповідальних осіб ускладнюється через відсутність прозорості та можливості інтерпретації складних алгоритмів [34].

2. Безпекові ризики. Загрозу становить можливість зловмисного використання штучного інтелекту, оскільки він може бути застосований для створення кібератак, генерації дезінформації або навіть для управління автономними бойовими системами [24]. Водночас нестабільність та непередбачуваність алгоритмів призводять до небажаних наслідків, наприклад, помилкові рішення або збої у критично важливих системах [38]. Адверсарні атаки на ШІ цілеспрямовано змінюють вхідні дані, що спричиняє небезпечні помилки у розпізнаванні образів, прогнозуванні та прийнятті рішень.

Якщо ШІ має можливість ухвалювати самостійні рішення без людського втручання, існує ризик, що його дії можуть виходити за межі початково закладених параметрів, що потенційно спричинить непередбачувані наслідки [40]. Відсутність людського контролю над ключовими аспектами функціонування ШІ може призвести до етичних дилем і підвищених ризиків при використанні таких технологій у критично важливих сферах, як транспорт, охорона здоров’я чи військова справа [53].

3. Економічні ризики. Впровадження штучного інтелекту змінює структуру економіки, і одним із основних ризиків є скорочення робочих місць. Автоматизація процесів може призвести до того, що значна частина працівників у традиційних галузях залишиться без роботи, що посилить соціальну напруженість і збільшити рівень безробіття [32]. Водночас концентрація контролю над технологіями ШІ у руках кількох великих компаній може призвести до монополізації ринку, що ускладнить доступ малих і середніх підприємств до передових інновацій та створить нерівні умови для конкуренції [56].

У випадку, якщо основні галузі економіки покладатимуться на ШІ без належних резервних механізмів, технічні збої або вразливості можуть

призвести до серйозних економічних наслідків. Втрата контролю над критично важливими ШІ-системами або їх раптова недоступність можуть спричинити збитки для компаній та державних структур [22]. Для забезпечення стабільного функціонування економіки необхідно впроваджувати стратегії диверсифікації, які дозволять зменшити залежність від ШІ та знизити потенційні ризики.

4. Правові та регуляторні ризики. Правові аспекти застосування штучного інтелекту залишаються недостатньо врегульованими, зокрема у сфері інтелектуальної власності. Виникає питання, кому належать права на результати, створені за допомогою ШІ: розробникам алгоритмів, користувачам чи самій системі [25]. Відсутність чітких правових норм може спричинити конфлікти щодо авторських прав та патентного законодавства.

У багатьох випадках чинне законодавство не враховує специфіку роботи алгоритмічних систем, що створює прогалини у визначенні відповідальних сторін у випадку заподіяння шкоди [62]. Використання великих обсягів персональних даних для навчання моделей ШІ потребує дотримання вимог щодо конфіденційності, таких як Загальний регламент захисту даних (GDPR). Забезпечення дотримання норм приватності є критично важливим для захисту прав громадян та запобігання зловживанням. Для ефективного регулювання технологій необхідно розробляти прозорі й зрозумілі нормативно-правові рамки, що сприятимуть етичному та безпечному використанню штучного інтелекту [63].

5. Ризики взаємодії людини та ШІ. Широке використання штучного інтелекту може призвести до зміни характеру взаємодії між людьми та технологіями. Надмірна залежність від автоматизованих систем може знизити рівень самостійності людських рішень та спричинити етичні дилеми, особливо якщо ШІ впливає на важливі аспекти життя: медичне діагностування чи фінансове планування [51].

Додатково, постійна взаємодія з ШІ може змінити соціальну поведінку людей, зменшуючи кількість міжособистісних комунікацій та змінюючи

традиційні соціальні норми [39]. Існує також ризик підсилення соціальних упереджень, оскільки алгоритми можуть відтворювати наявні стереотипи, що може призвести до несправедливих рішень у критично важливих сферах.

Таким чином, для безпечного та ефективного використання штучного інтелекту необхідно розробити комплексні регуляторні механізми, що передбачатимуть прозорість алгоритмів, етичні стандарти та відповідальність у прийнятті рішень. Без активного контролю та запровадження нормативних заходів потенційні ризики впливатимуть на економічну стабільність, соціальну рівність та безпеку суспільства.

Підприємствам варто розуміти фактори, що впливають на виникнення ризиків у проєктах із залученням ШІ. До таких факторів часто належать ті, які формують організацію роботи підприємства, його навички та досвід у використанні ШІ. Надалі розглянуто перелік факторів впливу, що пов’язують використання ШІ у проєктах та, як приклад, ризик кіберзахисту [21]:

1. Позиція в ланцюгу постачання та схильність до інновацій. Організації, які є лідерами у впровадженні штучного інтелекту (як постачальники технологій, так і як споживачі з передовими можливостями), можуть стикатися з підвищеними ризиками через використання новітніх технологій, що можуть містити невиявлені вразливості. Більш консервативні користувачі, які застосовують зріліші AI-рішення, зазвичай зазнають менших ризиків, оскільки про їх вразливості та ефективні заходи контролю вже накопичено більше знань.

2. Характер бізнесу. Галузь, у якій функціонує компанія, безпосередньо впливає на рівень її кіберризиків. Наприклад, підприємства, що забезпечують критичну національну інфраструктуру, можуть зазнавати підвищених загроз з боку зловмисників, які мають високий потенціал завдання шкоди або шукають значну цінність. Організації частіше підлягають жорсткому регулюванню у сфері кібербезпеки. Масштаб бізнесу також впливає на його можливості щодо впровадження заходів мінімізації AI-ризиків, тоді як рівень взаємозалежності з іншими компаніями визначає масштаб поширення можливих наслідків

компрометації.

3. Географічний контекст. Регіон, у якому компанія здійснює свою діяльність, суттєво впливає на її кібербезпеку та рівень залишкового ризику. Кіберзахищеність країни може визначати ступінь регулювання, якому підпорядковується організація. Також це може впливати на доступ до кваліфікованих фахівців, хоча для великих транснаціональних компаній ця проблема є менш критичною. Доступність надійної державної кіберінфраструктури, а також механізмів обміну даними про загрози та розвідки також відіграє важливу роль.

4. Рівень автономності AI: Чим більше штучний інтелект діє автономно, без людського контролю, тим вищі ризики для компанії. Значно менші ризики спостерігаються у випадках, коли рівень автономності низький або існує ефективний людський нагляд, що обмежує поширення потенційних загроз.

5. Контекст загроз: Рівень ризику значною мірою залежить від характеристик зловмисників, з якими стикається організація. Чим більш підготовленими, ресурсно забезпеченими та мотивованими є атакувальні суб’єкти, тим вищі загрози для потенційних жертв.

Підприємствам необхідно оцінювати, як саме ці ризики впливають на їх діяльність. Оцінка дає змогу на наступних етапах ідентифікувати можливі загрози та їх наслідки, а також розробити відповідні заходи реагування.

З огляду на міждисциплінарний характер ризиків, пов'язаних зі штучним інтелектом, традиційних підходів до управління ризиками може бути недостатньо. Організації повинні прийняти активну міжфункціональну стратегію, яка передбачає лідерство на всіх рівнях – від керівників до технічних спеціалістів з IT, безпеки та комплаєнсу. Ефективні системи управління, ретельна оцінка ризиків і постійний моніторинг програм штучного інтелекту мають вирішальне значення для забезпечення балансу між інноваціями та відповідальністю.

1.2. Методи ідентифікації та оцінки ризиків

Компанії, які надають пріоритет виявленню та запобіганню потенційним ризикам, зазвичай демонструють більш стабільну роботу та вищу прибутковість порівняно з тими, хто не звертає уваги на ці питання. Розуміння першопричин ризиків, передбачення їх потенційного впливу та розпізнавання їх походження є важливими кроками у прийнятті обґрунтованих та ефективних управлінських рішень. Управління ризиками - це не просто епізодичне занепокоєння керівництва компанії, а постійний процес, невід'ємний від щоденної діяльності бізнесу. Оцінка рівнів ризиків та розробка стратегій для їх зниження є ключовим аспектом управління, поряд з іншими функціями, такими як управління фінансами, людськими ресурсами та контролем якості.

Ідентифікація ризиків вимагає глибокого розуміння їх джерел, подій, причин і потенційних наслідків. Джерело ризику – це об'єкт або фактор, що має внутрішній потенціал спричинити ризик, як самостійно, так і в поєднанні з іншими факторами. Джерела ризику можуть бути як фізичними, так і нематеріальними.

Подія – це зміна або явище, що відбувається за певних обставин. Подія може проявлятися по-різному і бути спричинена різними факторами.

Наслідки – це результати цих подій, які впливають на здатність організації досягати своїх цілей. Подія може призвести до кількох наслідків, які можуть як позитивно, так і негативно вплинути на досягнення цілей, і їх можна виміряти як якісно, так і кількісно.

Щоб ефективно ідентифікувати ризики, необхідно розуміти бізнес-середовище, в якому вони діють. Розуміння бізнес-середовища надає можливість описати ризики, пов'язані з діяльністю компанії. Застосування комплексного підходу допомагає виявити весь спектр ризиків, присутніх у діяльності організації. Одним з ефективних методів управління цим є класифікація ризиків, яка впорядковує ризики на основі причинно-

наслідкових зв'язків, що лежать в основі процесу ідентифікації.

Ризики можна розпізнати, проаналізувавши основні причини потенційних подій та їх наслідки. Інший підхід полягає у дослідженні наслідків або збоїв, що спостерігалися раніше, і відстеженні їх до джерела, що дозволяє передбачити потенційні майбутні ризики (рис. 1.2).

Рис. 1.2. Напрями ідентифікації ризиків [14]

Під час ідентифікації ризиків дуже важливо враховувати кожен елемент, що бере участь у цьому процесі (рис. 1.3).

Рис. 1.3. Головні складові ідентифікації ризиків [14]

Ідентифікація ризиків допомагає визначити обсяг зусиль з управління ризиками шляхом встановлення контексту ризику, що включає оцінку як внутрішніх, так і зовнішніх факторів, а також визначення обсягу та критеріїв

ризику. Однак, перш ніж зануритися в ці деталі, важливо зрозуміти основні елементи ідентифікації (табл. 1.1).

Таблиця 1.1

Характеристика елементів ідентифікації ризиків [15]

Опис елемента	Ключові характеристики
Подія ризику	Зміна або поява певного явища або сукупності обставин
Причини ризику	Джерело, відповідальне за створення ситуації ризику
Фактори ризику	Умови, за яких причини ризику проявляються і призводять до виникнення ситуації ризику
Ризикова ситуація	Подія, спричинена причинами та факторами ризику, яка може призвести до негативних або позитивних наслідків
Тип ризику	Походження ризикової ситуації, що визначає, яка зацікавлена сторона ініціює ризик
Метод виявлення	Підхід, який використовується для виявлення ситуації ризику
Наслідки	Наслідки, які виникають у разі настання ризикової ситуації
Ймовірність	Кількісна оцінка ймовірності того, що подія відбудеться, представлена у вигляді числа від 0 (неможливо) до 1 (точно)
Вірогідність	Шанс того, що подія відбудеться
Тяжкість	Міра впливу події на організацію та/або її зацікавлені сторони
Вразливість	Невід'ємна характеристика активу, яка робить його чутливим до впливу джерел ризику, що потенційно може призвести до наслідків

По суті, ідентифікація ризиків є основоположним кроком у загальному процесі управління ризиками. Якщо конкретний ризик не ідентифіковано, будь-які зусилля з його пом'якшення або не будуть здійснені, або матимуть значно меншу ефективність.

У цьому контексті важливо підкреслити важливість вибору методів ідентифікації ризиків, які є науково обґрунтованими та економічно доцільними. Сучасний діловий світ пропонує широкий спектр методів, інструментів і прийомів, призначених для виявлення найбільш значущих ризиків у будь-якій організації. Серед них особливою популярністю на практиці користуються наступні методи: мозковий штурм, опитування зацікавлених сторін, метод Дельфі, діаграми спорідненості, SWOT-аналіз, структурована техніка «Що, якщо» (SWIFT), аналіз сценаріїв, контрольні списки, попередній аналіз небезпек, дослідження небезпек та експлуатаційної придатності (HAZOP), аналіз небезпек та критичних контрольних точок

(HACCP), причинно-наслідковий аналіз та інші [8; 16].

Зі зростанням ролі штучного інтелекту в Індустрії 6.0 постає низка викликів, що матимуть вплив на різні сфери економіки та суспільства. Серед ключових ризиків виділяються питання безпеки даних, дискримінації, зміни ринку праці, юридичних та етичних аспектів, а також проблеми надійності та підзвітності технологій.

Одним із найсерйозніших ризиків є загроза безпеці даних та конфіденційності. ШІ оперує величезними масивами інформації, що створює можливості для кіберзлочинців здійснювати атаки, зламувати системи та викрадати персональні дані [46]. Алгоритмічна складність ШІ ускладнює виявлення та усунення вразливостей, що підсилює загрозу зловживань та несанкціонованого доступу до інформації.

Наступною проблемою є упередженість алгоритмів та дискримінація. Оскільки моделі ШІ навчаються на історичних даних, наявність у них системних упереджень може призводити до несправедливих рішень, зокрема у сфері працевлаштування, кредитування чи правосуддя. Проблема становить ризик для соціальної справедливості та рівності можливостей, що вимагає ретельного аналізу вхідних даних та розробки механізмів зниження алгоритмічної дискримінації [18].

ШІ спричиняє трансформації ринку праці, що може призвести до масового витіснення робочої сили з традиційних секторів економіки [20]. Автоматизація процесів підвищує продуктивність, проте водночас загрожує скороченням робочих місць та соціально-економічними дисбалансами. Відтак, важливо інвестувати у перекваліфікацію працівників, що забезпечить їм можливості адаптації до нових професійних вимог.

Використання ШІ створює юридичні та етичні виклики, зокрема щодо відповідальності за ухвалені алгоритмами рішення. У сферах, де ШІ використовується для оцінки ризиків чи прийняття правових рішень, існує загроза порушення прав людини, а також потенційна непрозорість процесів. Вирішення перелічених питань вимагає впровадження чітких нормативних

актів, що регламентуватимуть застосування ШІ та забезпечуватимуть дотримання етичних стандартів.

Останнім, але не менш важливим ризиком є відсутність надійності та прозорості алгоритмів. Оскільки багато моделей ШІ працюють за принципом «чорної скриньки», тобто без можливості чітко пояснити логіку їх рішень, це ускладнює процес встановлення відповідальності за можливі помилки [37]. Недостатня підзвітність та складність у визначенні джерела помилок можуть призводити до серйозних наслідків, особливо в критично важливих галузях. Для подолання цього виклику необхідно впроваджувати алгоритми з високим рівнем пояснюваності та розробляти чіткі механізми відповідальності.

Отже, широке впровадження ШІ в Індустрії 6.0 супроводжується значними ризиками, що стосуються безпеки, етики, соціально-економічних змін та юридичної відповідальності. Для мінімізації загроз необхідно розробляти прозорі та підзвітні системи ШІ, вдосконалювати нормативно-правову базу та забезпечувати умови для безперервного навчання й адаптації працівників до нових технологічних умов.

У табл. 1.2 розглянемо ідентифіковані ризики використання ШІ у проєктах, методи та способи їх ідентифікації та напрямки оцінки/впровадження запобіжних заходів щодо їх мінімізації.

Таблиця 1.2

Ідентифікація ризиків використання ШІ у сучасних проєктах

Ризик	Методи ідентифікації	Ключові напрямки оцінки/запобігання ризику
Ризики безпеки даних та конфіденційності	Проведення регулярних аудитів безпеки	1. Визначення критичних інформаційних активів. 2. Класифікація потенційних загроз 3. Розробка стратегії захисту та мінімізації вразливостей 4. Впровадження систем контролю безпеки 5. Моніторинг та актуалізація заходів безпеки
Ризики упередженості та дискримінації	Проведення оцінки упередженості штучного інтелекту	1. Аналіз джерел навчальних даних. 2. Виявлення потенційних упереджень у вихідних даних. 3. Оцінка рівня упередженості в алгоритмах ШІ. 4. Коригування параметрів системи для зменшення викривлень.

Продовження табл. 1.2

Ризик	Методи ідентифікації	Ключові напрямки оцінки/запобігання ризику
Ризики упередженості та дискримінації	Проведення оцінки упередженості штучного інтелекту	5. Постійний моніторинг справедливості та точності рішень ШІ.
Ризики втрати робочих місць	Аналіз та прогнозування змін на ринку праці	1. Визначення професій, найбільш схильних до автоматизації. 2. Оцінка рівня кваліфікації працівників. 3. Визначення потенційних нових робочих місць. 4. Розробка освітніх і тренінгових програм. 5. Моніторинг ефективності заходів з перепідготовки кадрів.
Юридичні та етичні ризики	Регулярний юридичний та етичний аналіз	1. Дослідження правових та етичних аспектів використання ШІ. 2. Виявлення можливих порушень прав на конфіденційність або дискримінації. 3. Розробка політик та рекомендацій для мінімізації ризиків. 4. Регулярний перегляд та оновлення політик відповідності.
Ризики надійності та відповідальності	Контроль ефективності та відповідальності систем ШІ	1. Постійний моніторинг продуктивності системи для виявлення помилок. 2. Впровадження процедур для виявлення та усунення недоліків. 3. Визначення відповідальних осіб за нагляд та виправлення помилок. 4. Розробка процедур документування роботи системи. 5. Регулярний перегляд та коригування процесів оцінки ефективності та відповідальності.

Отже, оцінка та кількісне вимірювання ризиків ШІ є важливим завданням, особливо для великих компаній, оскільки фінансове оцінювання ризиків може суттєво впливати на прийняття управлінських рішень. Окрім потенційних втрат у вартості бренду, падіння біржової капіталізації та штрафних санкцій, репутаційні ризики можуть бути оцінені через опитування експертів, анкетування співробітників або інші методи аналізу.

Існує кілька варіантів стратегій управління ризиками ШІ. По-перше, удосконалення нормативно-правової бази. Наприклад, у сфері автономного транспорту активно адаптуються законодавчі акти для регулювання впровадження цієї технології, паралельно з розвитком галузевих стандартів.

По-друге, необхідним є оновлення супутніх регулювань, зокрема у сфері страхування. Для автономних транспортних засобів це може означати введення обов'язкового страхування, що відповідатиме специфіці цієї технології.

По-третє, багато компаній, незалежно від вимог законодавства, впроваджують посилені етичні стандарти у своїй діяльності та постачальницьких ланцюгах.

Наприклад, обвал будівлі Rana Plaza у Бангладеш у 2013 році викликав суспільний резонанс, що змусило міжнародні компанії змінювати підходи до відповідальності за умови праці у країнах постачальників. Подібні питання виникали щодо використання дитячої праці у видобутку кобальту для електронної промисловості (Apple, Samsung).

Деякі компанії також використовують питання конфіденційності даних як конкурентну перевагу. Наприклад, пошукова система DuckDuckGo позиціонує себе як альтернативу Google, при цьому наголошує на політиці відмови від збору персональних даних користувачів. Дії компанії демонструють, що управління ризиками ШІ не лише зменшує загрози, але й може стати фактором стратегічної диференціації на ринку.

З поширенням штучного інтелекту в різних галузях економіки він стає важливим інструментом для оцінки та ідентифікації ризиків. Величезні обсяги даних і автономне ухвалення рішень забезпечують значні переваги, але водночас створюють нові загрози. Важливість управління ризиками ШІ зростає, адже організації прагнуть максимізувати його користь, та при цьому мінімізувати потенційні негативні наслідки.

Ефективна стратегія управління ризиками має включати розуміння специфіки ШІ, створення адаптованої до конкретних галузей методології ідентифікації ризиків, а також залучення всіх зацікавлених сторін для забезпечення комплексного підходу. Серед ключових загроз – кібератаки, порушення конфіденційності, упередженість алгоритмів і етичні дилеми, що включають питання справедливості, прозорості та відповідальності. Для

забезпечення дієвості процесу ідентифікації ризиків необхідно його постійне оновлення відповідно до динаміки розвитку ШІ та змін у сфері загроз.

Необхідним наразі для проєктів є ефективне комунікування виявлених ризиків і стратегій їх оцінки між усіма учасниками процесу. В умовах Industry 6.0 формування культури усвідомлення ризиків сприяє довірі, співпраці та відповідальному застосуванню ШІ. У підсумку, завдяки впровадженню надійних стратегій оцінки та управління ризиками організації можуть отримати максимальну користь від ШІ, одночасно мінімізувати його загрози.

Висновок до розділу 1

Ризик є важливою складовою будь-якої діяльності, йому притаманна складна структура, яка включає джерела, об’єкти та наслідки, як негативні, так і позитивні. Визначення ризику варіюються в науковій літературі, зокрема через різні підходи до трактування його наслідків і впливу на прийняття рішень. Ризик завжди супроводжує прийняття будь-яких рішень, особливо в умовах невизначеності, що робить його важливим фактором для планування і управління. Оскільки ризики можуть мати далекосяжні наслідки, необхідно приділяти належну увагу їх оцінці та управлінню на всіх етапах діяльності.

Серед основних джерел ризику виділяються природні процеси, соціально-економічні фактори та інформаційні обмеження. Оцінка ризику повинна враховувати потенційну загрозу, вразливість об’єкта та взаємодію з іншими ризиками для розробки ефективних стратегій управління. Важливо також враховувати змінність зовнішнього середовища, яке може впливати на рівень ризику і змінювати його характеристики. Це вимагає гнучких підходів до управління ризиками, що дозволяють оперативно адаптувати стратегії в умовах непередбачуваних ситуацій.

Ідентифікація та оцінка ризиків є ключовими елементами ефективного управління ризиками, оскільки дозволяють виявити можливі загрози та мінімізувати їх вплив на організацію. Найбільше значення мають методи, які

дозволяють врахувати як внутрішні, так і зовнішні фактори, а також розробка стратегій для зниження ризиків на основі систематичного аналізу. Прогнозування ризиків на основі історичних даних і сценаріїв розвитку є важливим інструментом для забезпечення стабільності та безпеки в діяльності організацій.

У сучасних умовах застосування штучного інтелекту в Індустрії 6.0 виникають нові ризики, пов'язані з безпекою даних, упередженістю алгоритмів, змінами на ринку праці та юридичними питаннями, що вимагає розробки спеціальних заходів для їх мінімізації. Важливим аспектом є регулярний моніторинг і адаптація до змінюваних умов. Крім того, виникає необхідність у створенні міждисциплінарних команд для ефективної оцінки та управління новими типами ризиків, пов'язаними з технологічними інноваціями.

РОЗДІЛ 2
ПРАКТИЧНЕ ДОСЛІДЖЕННЯ РИЗИКІВ У ПРОЄКТАХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

2.1. Аналіз проєктів із впровадження штучного інтелекту

У контексті Індустрії 4.0 високотехнологічні ініціативи, спрямовані на оцифрування бізнес-процесів, посідають центральне місце [44]. Як зазначають J. Q. Cao та S. H. Zhang [28], багато традиційних методологій виконання проектів поступово замінюються новими підходами, пристосованими до сучасних технологічних імперативів. Високотехнологічні підходи враховують інтеграцію ШІ, попит на гнучкість, зменшення формальностей, особливо в комунікації та документації, інформаційну асиметрію між постачальниками та клієнтами, а також підвищену вразливість до внутрішніх і зовнішніх організаційних збоїв.

S. Spałek [54] підтверджує попередні висновки та визначають кілька нових тенденцій у сучасному управлінні проектами. Серед них – інтеграція штучного інтелекту та віртуальної реальності (VR) для підвищення ефективності роботи команди, розширення міжнародних проектних ініціатив, поширення цифрових інструментів для управління проектами, зростаючий акцент на немонетарних стратегіях мотивації, пріоритетність сталого розвитку та корпоративної соціальної відповідальності. Набирає популярності методологія Agile, зростає актуальність масштабних, складних «мегапроектів».

Враховуючи технологічні та організаційні складнощі, притаманні ініціативам Індустрії 4.0, розгортання гнучких методологій впровадження стає необхідністю. Динамічний і часто непередбачуваний характер проектів вимагає адаптивної системи управління. Від керівників проектів все частіше вимагається інтегрувати гібридний підхід, поєднуючи усталені рутини з передовими цифровими компетенціями, особливо тими, що пов'язані зі

штучним інтелектом.

Проекти, що працюють в рамках парадигми Індустрії 4.0, часто виконуються в умовах невизначеності або навіть глибокої невизначеності [60], в дуже нестабільному середовищі. Зовнішні та внутрішні фактори зумовлюють необхідність прийняття гнучких та адаптивних стратегій управління проектами, посилених завдяки застосуванню інструментів на основі штучного інтелекту.

При аналізі проектів зі штучного інтелекту значна увага приділяється інтеграції інтелектуальних систем у практику управління проектами. Інститут управління проектами (Project Management Institute, PMI) визначає управління проектами як структуровану сукупність принципів, методів і методологій, спрямованих на ефективне планування, виконання, контроль і оцінку результатів для забезпечення успіху проекту [49]. У цьому контексті застосування штучного інтелекту має трансформаційний потенціал, особливо в оптимізації та автоматизації проектних процесів у різних галузях.

Проекти штучного інтелекту за своєю суттю спираються на міждисциплінарні підходи, оскільки використовують методології з інформатики, математики, статистики, когнітивної психології та нейронаук [52]. Основи підтримують моделювання, розробку і розгортання систем штучного інтелекту, здатних до інтелектуальної поведінки в складних організаційних структурах.

Прийняття принципів управління проектами на основі даних (Data-driven project management, DdPM) є ключовим для виконання проектів на основі ШІ. DdPM наголошує на використанні великих обсягів релевантних даних для підвищення надійності рішень. Класичні інструменти управління проектами, такі як метод оцінки та аналізу програм (PERT), методи критичного шляху, управління зробленою вартістю (EVM), процес аналітичної ієрархії (AHP) і Lean Six Sigma, забезпечують кількісну основу для планування і розподілу ресурсів у проектах ШІ [59]. Однак ШІ розширює їх, з урахуванням обробки даних у реальному часі та предиктивної аналітики, що

створює пропозицію динамічного середовища для підтримки прийняття рішень.

Еволюцію платформ штучного інтелекту в управлінні проектами можна розглядати як просунуту фазу DdPM, коли можливості штучного інтелекту інтегруються в хмарні середовища для вирішення подвійної проблеми – високої складності впровадження та підвищених очікувань користувачів. Прикладом еволюції є поява ботів для управління проектами (Project Management Bots, PMB), інтелектуальних програмних агентів. На відміну від роботизованої автоматизації процесів (RPA), PMB працюють переважно через діалогові інтерфейси – текстові або голосові – у вигляді чат-ботів або цифрових асистентів, які полегшують координацію завдань, оновлення статусів та комунікацію із зацікавленими сторонами [46].

Попри стрімкий розвиток, сучасні інструменти штучного інтелекту слугують скоріше допоміжними механізмами, ніж повноцінною заміною людей, які керують проектами. Їх корисність полягає в чітко визначених, повторюваних завданнях і сферах, де розпізнавання образів або інтерпретація великих масивів даних є критично важливими. Отже, розвиток ШІ в управлінні проектами триває двома основними шляхами: вдосконалення специфічних для конкретної галузі функціональних можливостей і покращення інтерфейсів між людиною і ШІ, як, наприклад, у системах на кшталт Google Duplex.

Зрештою, аналіз проектів ШІ підкреслює подвійний імператив: використовувати алгоритмічну ефективність і можливості навчання, при цьому робити надійний інтерфейс для людського нагляду і стратегічного керівництва.

Проблеми, з якими стикаються при розробці проектів зі штучного інтелекту, часто виникають через обмежене розуміння нових технологій або невизначеності, пов'язані з алгоритмічною продуктивністю, якістю даних або системною інтеграцією. Прогалини в знаннях потребують структурованих дослідницьких методологій для інформування про розробку та впровадження.

З огляду на тісний взаємозв'язок між ШІ та практичним застосуванням у різних галузях, вирішення таких питань повинно мати відчутні, застосовні результати для фахівців-практиків і зацікавлених сторін у галузі ШІ.

Однією з ефективних методологій якісного дослідження, яка може бути застосована в контексті ШІ, є метод кейс-стаді. Кейс-стаді забезпечує поглиблене емпіричне дослідження застосування AI в реальних проєктах, що дає змогу вивчити поведінку системи, динаміку впровадження та продуктивність у конкретних умовах. У контексті аналізу проектів ШІ він дозволяє всебічно вивчити розгортання інтелектуальних систем у різних сферах, таких як виробництво, освіта, сільське господарство і логістика, пропонуючи розуміння факторів успіху, обмежень і найкращих практик [30].

Надалі розглянуто два питання, що стосуються використання ШІ у проєктах:

1. Міра, якою технології ШІ впроваджуються протягом життєвого циклу проєкту, орієнтованих на ШІ, у промисловому середовищі.

2. Очікувані етапи розвитку інтеграції штучного інтелекту в процеси управління проєктами.

У табл. 2.1 наведено структуру проаналізованих проєктів Індустрії 4.0 на основі штучного інтелекту з використанням методу тематичних досліджень. Усі розглянуті проєкти були частиною ширших ініціатив цифрової трансформації, що характеризуються інтеграцією передових технологій, керованих даними. Згідно з M. Kotarba [41], цифрова трансформація передбачає систематичну адаптацію бізнес-моделей у відповідь на швидкі технологічні зміни, які, своєю чергою, впливають на організаційні процеси та очікування користувачів.

Дослідження по проєктах проводилось у період 2024-2025 рр, охоплювало всі етапи проєкту: підготовку, впровадження та експлуатацію. Проєкти використовували методології Agile та Waterfall, залежно від складності системи та вимог домену. Кожна проектна команда складалася з міжфункціональної групи, до якої входили фахівці зі штучного інтелекту,

інженери з обробки даних, кінцеві користувачі та стратегічні стейкхолдери. Інструменти штучного інтелекту були впроваджені для підвищення операційної ефективності, автоматизації робочих процесів і підтримки прийняття рішень.

Таблиця 2.1

Результати аналізу проєктів із впровадженням ШІ

	Проект A	Проект B	Проект C	Проект D
Опис проекту	Модернізація ERP-системи - перехід на хмарне сховище	MIS, що підтримує управління багатоярусним складом	Впровадження системи автоматизації роботи на великій фермі	Впровадження платформи електронного навчання
Кількість членів проектної групи	25	50	20	40
Діапазон проекту	Модулі ERP-системи: фінансово-бухгалтерський облік, логістика, управління виробництвом	Системні модулі: Системи управління складом, RFID	IT-система, що аналізує параметри ґрунту за допомогою датчиків. Інформація на базі Microsoft Azure передається до хабу, який аналізує дані з усієї території ферми	Впровадження платформи електронного навчання, що дозволяє створювати та розповсюджувати тренінги в розподіленій архітектурі
Методологія завершення проекту	Waterfall (водоспад)	Waterfall (водоспад)	Agile	Agile
Спектр використання ШІ в управлінні проектами	1. Переклад 2. Розпізнавання тексту - Введення рахунків-фактур в облікову систему 3. Виконавчі елементи - роботизована автоматизація процесів у сфері введення даних до системи	1. Переклад 2. Розпізнавання тексту - Введення рахунків-фактур в систему обліку 3. Виконавчі елементи - роботизована автоматизація процесів в області введення даних в систему 4. (Мульти)агентна система - чат-бот	1. Переклад 2. Розпізнавання тексту - введення рахунків-фактур в облікову систему 3. Сенсорні елементи - виявлення аномалій у фізико-хімічних параметрах ґрунту	1. Переклад 2. (Мульти)агентна система - чат-бот

Аналіз показав, що інструменти мовного перекладу є найбільш часто використовуваним додатком ШІ, який допомагає передусім у багатомовному спілкуванні, документуванні та навчанні користувачів. Інструмент значно покращив співпрацю між географічно розподіленими командами.

Другим за популярністю інструментом було оптичне розпізнавання символів (OCR). OCR уможливило автоматизоване оцифрування і класифікацію проектних документів, таких як рахунки-фактури і звіти, для передачі у внутрішні системи, такі як ERP і DMS, для впорядкованого потоку даних.

Роботизована автоматизація процесів (RPA) використовувалася для виконання повторюваних адміністративних завдань, таких як відстеження відхилень від бюджету та генерування сповіщень про перевитрати. Автоматизація була ключовою для зменшення ручної праці та підвищення точності.

Чат-боти, що функціонують як мультиагентні системи, були розгорнуті в сценаріях служби підтримки, відповідаючи на запити користувачів після розгортання. Боти використовували обробку природної мови (NLP) і динамічні бази знань для надання негайних, релевантних відповідей, підвищуючи задоволеність користувачів і дотримання SLA.

Інструменти штучного інтелекту, керовані Інтернетом речей, були розгорнуті в сільськогосподарському проекті, де сенсорні мережі збирали дані про навколишнє середовище (наприклад, pH ґрунту, вологість). Дані передавалися на хмарні платформи для виявлення аномалій у режимі реального часу, що сприяло точному землеробству.

По суті, всі досліджені функціональні можливості ШІ сприяли автоматизації та розширенню процесів управління проектами, тим самим зменшуючи транзакційні накладні витрати і покращуючи підтримку прийняття рішень. Отже, практичний аналіз підтверджує теоретичні здобутки, що сьогодні існує зростаюче значення штучного інтелекту, оскільки виникає потреба підвищення продуктивності та гнучкості проєктів у цифрових

екосистемах.

Штучний інтелект різною мірою використовується протягом усього життєвого циклу проектів, орієнтованих на штучний інтелект. Щоб проаналізувати використання ШІ в таких проєктах, було розроблено узагальнену модель життєвого циклу проєкту зі штучним інтелектом. Модель ґрунтується на методологіях, запозичених зі специфічних для ШІ фреймворків і стандартів управління проєктами, таких як CRISP-DM (Cross Industry Standard Process for Data Mining), TDSP (Team Data Science Process) від Microsoft і сучасних конвеєрів машинного навчання на основі Agile, а також усталених проєктних фреймворків, таких як PMI PMBOK, PRINCE2, і практик MLOps, що інтегрують сервісні принципи ITIL.

Синтезований життєвий цикл ШІ-проекту складається з трьох етапів, на яких систематично оцінювалася роль та інтеграція технологій ШІ.

1. Етап перший – підготовка та фаза техніко-економічного обґрунтування. Початковий етап складається з двох фаз:

- формулювання проблеми та техніко-економічний аналіз - передбачає побудову проблемної області ШІ, попередній аналіз даних, визначення бізнес-проблеми, яку потрібно вирішити за допомогою ШІ, оцінку доступності та якості даних, аналіз готовності інфраструктури (хмарної/локальної), формування мультидисциплінарної команди проекту ШІ, оцінку ризиків (у тому числі, питання упередженості та справедливості), а також оцінку витрат і вигод від ініціативи з впровадження ШІ.

- вибір інструментарію та постачальника - включає в себе складання шорт-листа платформ штучного інтелекту (наприклад, TensorFlow, PyTorch, AWS SageMaker), підготовку запиту на пропозицію (RFP), порівняльну оцінку рішень постачальників на основі критеріїв продуктивності, інтерпретованості, відповідності вимогам (наприклад, готовності до GDPR), а також формування партнерських відносин або ліцензійних угод.

2. Етап другий – розробка та розгортання моделі. Основний етап впровадження містить п’ять ітеративних і взаємопов’язаних фаз:

- початок проекту та налаштування середовища - включає зустрічі з визначення обсягу проекту, налаштування хмарних середовищ, систем контролю версій, конвеєрів даних та початкову конфігурацію середовищ машинного навчання.

- інженерія даних і попередня обробка – включає в себе поглиблене очищення даних, розробку функцій, обробку незбалансованих наборів даних і підготовку навчальних даних; часто включає в себе співпрацю зі зберігачами даних і експертами в предметній області.

- етап моделювання - охоплює вибір алгоритмів (наприклад, дерева рішень, ШНМ, трансформатори), навчання та оцінювання моделей з використанням методів перехресної перевірки та налаштування гіперпараметрів. На цьому етапі проводиться аудит інтерпретованості та справедливості.

- етап валідації та тестування - включає інтеграційне тестування в рамках більшої системи, синтетичне та реальне тестування моделі, перевірку стійкості в умовах конкуренції, документування результатів роботи моделі та огляд зацікавлених сторін.

- розгортання та моніторинг (Go-Live) - охоплює розгортання моделі у виробничому середовищі з використанням конвеєрів CI/CD, навчання користувачів системам зі штучним інтелектом, готовність до висновків у реальному часі, а також підтримку після розгортання для виявлення дрейфу та погіршення продуктивності.

3. Етап третій – операції після розгортання. Заключний етап складається з двох підетапів:

- операційний аналіз і безперервне навчання – складається з оглядів після розгортання, аналізу першопричин збоїв, визначення нових потреб у даних та оцінки етичних і соціальних наслідків розгорнутої моделі.

- постійна підтримка моделі та управління постачальниками – включає вибір або підтвердження постачальників підтримки MLOps, формулювання угоди SLA, оцінку стратегій перепідготовки кадрів та визначення шляхів

ескалації у разі збоїв у роботі моделі або порушення законодавства.

У табл. 2.2 окреслено сферу використання інструментів штучного інтелекту на описаних вище етапах життєвого циклу. Наприклад, моделі перекладу (наприклад, інструменти NLP на основі трансформаторів) використовувалися для вирішення завдань документації; модулі розпізнавання тексту та розпізнавання допомагали під час оцифрування застарілих документів; інструменти RPA (роботизована автоматизація процесів) сприяли створенню звітів зі штучного інтелекту; а інтегровані петлі зворотного зв'язку з датчиками були впроваджені під час тестування моделей і моніторингу розгортання в реальному часі.

Таблиця 2.2

Діапазон використанні ШІ в управлінні проєктами протягом усього життєвого циклу

<table>
<tr><td colspan="2">Етап 1</td><td colspan="5">Етап 2</td><td colspan="2">Етап 3</td></tr>
<tr><td>Фаза 1</td><td>Фаза 2</td><td>Фаза 3</td><td>Фаза 4</td><td>Фаза 5</td><td>Фаза 6</td><td>Фаза 7</td><td>Фаза 8</td><td>Фаза 9</td></tr>
<tr><td rowspan="6">Переклад</td><td rowspan="6">Переклад</td><td>Переклад</td><td>Переклад</td><td>Переклад</td><td>Переклад</td><td>Переклад</td><td>Переклад</td><td>Переклад</td></tr>
<tr><td>Розпізнавання тексту</td><td>Розпізнавання тексту</td><td>Розпізнавання тексту</td><td>Агентська система – Чатбот</td><td>Агентська система – Чатбот</td><td>Агентська система – Чатбот</td><td>Агентська система – Чатбот</td></tr>
<tr><td rowspan="4">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td><td rowspan="4">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td><td rowspan="4">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td><td>Розпізнавання тексту</td><td>Розпізнавання тексту</td><td rowspan="4">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td><td rowspan="4">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td></tr>
<tr><td rowspan="3">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td><td rowspan="3">Виконавчі елементи - Роботизована автоматизація технологічних процесів</td></tr>
<tr><td>Сенсорний елемент</td></tr>
</table>

Тим не менш, аналіз показує, що інструменти для проєктів ШІ, як

правило, стосуються окремих сегментів життєвого циклу, а не пропонують наскрізну підтримку. Часткова інтеграція обмежує ефективність і масштабованість управління проектами ШІ.

У даний час інструменти ШІ підтримують управління проектами ШІ в основному в сферах автоматизації завдань, допоміжних функцій і базового виявлення аномалій. Інструменти ще не розвинулися настільки, щоб надавати комплексну підтримку впродовж усього життєвого циклу ШІ-проекту.

Існує явна невідповідність між очікуваннями керівників проектів і поточним функціоналом проектних інформаційних систем зі штучним інтелектом. Виділені шість етапів розвитку - від автоматизації до повної автономії - відображають більш широку траєкторію зрілості ШІ в різних галузях.

Щоб подолати розрив між можливостями та очікуваннями, необхідно зробити акцент на майбутньому розвитку:

1. Поглиблену інтеграцію інструментів ШІ в життєві цикли проектів ШІ, особливо на етапах, що вимагають прийняття рішень, таких як моделювання і розгортання.

2. Прозорість поведінки інструментів ШІ, у тому числі зрозумілі інтерфейси ШІ (XAI), дотримання етичних норм і рамки юридичної відповідальності [43].

3. Створення централізованих наборів даних проєктів ШІ - такі репозиторії дозволять проводити бенчмаркінг, передачу доменів і навчання автономних агентів для прийняття рішень на рівні проєкту.

4. Синергетична інтеграція між інструментами проєктів ШІ та додатками Індустрії 4.0, завдяки чому компоненти ШІ в різних системах (наприклад, прогнозоване технічне обслуговування та оптимізація ланцюжка поставок) можуть взаємодіяти, використовуючи спільні протоколи ШІ.

Сучасну ситуацію щодо управління проектами ШІ можна порівняти з автономними автомобілями на ранніх стадіях – функціональними, але обмеженими, подібно до адаптивного круїз-контролю або систем допомоги

при утриманні в смузі руху. Повністю автономні системи управління проектами ШІ, подібні до безпілотних автомобілів, все ще перебувають на стадії розробки, що вимагає міждисциплінарної співпраці та ретельної перевірки для того, щоб стати життєздатними.

2.2. Оцінка ризиків у проєктах з використанням штучного інтелекту

Інтеграція штучного інтелекту в управління проектами значно трансформувала сферу стартапів та сучасних ІТ-проєктів, адже виникла пропозиція можливостей автоматизації, оптимізації та прийняття рішень на основі даних. Однак разом з прогресом з'являється складний набір ризиків, які необхідно систематично виявляти, оцінювати та пом'якшувати. Оцінка ризиків у проєктах зі штучним інтелектом – це не лише технічна вправа, а й багатовимірний процес, що охоплює етичні, соціальні, правові та організаційні аспекти. Здатність ШІ впливати на прийняття відповідальних рішень підкреслює важливість розробки надійних методологій, які забезпечують безпечне, справедливе та підзвітне впровадження.

В основі оцінки ризиків, пов'язаних зі штучним інтелектом, лежить визнання того, що системи штучного інтелекту працюють в умовах невизначеності та складності. Проєкти з використанням ШІ часто включають моделі машинного навчання, навчені на історичних даних, які можуть бути неповними, упередженими або нерепрезентативними, що може призвести до помилкових результатів, особливо в динамічних контекстах, де середовище змінюється з часом. Оцінка ризиків повинна враховувати надійність і адаптивність систем ШІ в реальних умовах. На відміну від детермінованих систем, ШІ демонструє імовірнісну поведінку, що ускладнює традиційні моделі ризику, які спираються на лінійний причинно-наслідковий зв'язок.

Центральним фактором ризику є якість даних. Моделі ШІ настільки хороші, наскільки хороші дані, на яких вони навчаються. Низька якість даних, що характеризується шумом, відсутністю значень або системними зсувами,

може серйозно вплинути на продуктивність моделі. Використання персональних або конфіденційних даних створює значні проблеми з їх конфіденційністю. Нормативно-правові акти, такі як Загальний регламент про захист даних (GDPR) та Каліфорнійський закон про конфіденційність споживачів (CCPA), накладають суворі вимоги до збору, зберігання та використання даних. Порушення можуть призвести до юридичних санкцій і шкоди репутації, що вимагає суворого управління даними в рамках оцінки ризиків проектів зі штучного інтелекту.

Ще однією серйозною проблемою є алгоритмічна упередженість, коли системи ШІ ненавмисно посилюють соціальні упередження, присутні в навчальних даних, що особливо проблематично в таких секторах, як фінанси, охорона здоров'я, рекрутинг і кримінальне правосуддя, де упереджені результати можуть непропорційно впливати на вразливі групи населення. Тому алгоритмічний аудит і показники справедливості повинні бути невід'ємною частиною будь-якої стратегії оцінки ризиків ШІ. Однак кількісне визначення справедливості за своєю суттю є складним завданням, оскільки воно часто пов'язане з балансуванням між такими суперечливими цілями, як точність і рівність.

Водночас непрозорість багатьох моделей ШІ - особливо систем глибокого навчання – створює проблему для прозорості та підзвітності. Так званий «чорний ящик» нейронних мереж ускладнює пояснення того, як приймаються рішення, що суперечить правовим та етичним вимогам до пояснюваності. Для вирішення цієї проблеми з'явилися фреймворки поясненого штучного інтелекту (Explainable AI, XAI), які надають інтерпретовані результати без значного зниження продуктивності моделі. Попри багатообіцяючу перспективу, методи XAI все ще розвиваються і поки що не можуть гарантувати повну прозорість у всіх сферах.

З точки зору надійності системи, системи штучного інтелекту чутливі до ворожих атак і погіршення продуктивності з часом через дрейф даних або застарілість моделі. Ворожі вхідні дані - спеціально створені збурення, які

обманюють моделі ШІ, - можуть підірвати безпеку і довіру до систем ШІ. Моделі, навчені за певних умов, можуть давати збої при розгортанні в нових умовах, що підкреслює необхідність постійного моніторингу та оновлення. Включення автоматизованих циклів зворотного зв'язку та надійних механізмів перевірки на етапах розробки та після розгортання є важливим для зменшення таких ризиків.

Етичні міркування виходять за рамки алгоритмічної справедливості і стосуються питань автономії, людської гідності та підзвітності. Системи ШІ, які приймають автономні рішення, ставлять питання про делегування моральної відповідальності. Наприклад, якщо система ШІ, що використовується в охороні здоров'я, ставить помилковий діагноз, незрозуміло, хто несе за це відповідальність - розробники, дослідники даних чи кінцеві користувачі. Створення чітких структур управління та систем підзвітності має вирішальне значення для вирішення цих дилем і зміцнення суспільної довіри.

Методології управління проектами, такі як PRINCE2 і PMBOK, почали включати компоненти оцінки ризиків ШІ в свої структури. Однак ці традиційні методології повинні розвиватися далі, щоб врахувати унікальні характеристики ШІ, такі як динамічне навчання, недетермінованість і етична невизначеність. Еволюція передбачає не лише технічні корективи, а й культурні зміни в організаціях з акцентом на міждисциплінарну співпрацю та етичну рефлексію.

Комплексна оцінка ризиків ШІ повинна включати поєднання якісних і кількісних методів. Якісні методи включають інтерв'ю із зацікавленими сторонами, дослідження Дельфі та аналіз сценаріїв, які дають змогу отримати контекстуальне розуміння. Кількісні підходи, такі як імовірнісна оцінка ризиків (IOP), аналіз чутливості та статистичне тестування, дають змогу отримати вимірювані показники ймовірності та впливу ризиків. Методи можуть бути синтезовані в матриці ризиків, які відображають потенційні загрози з урахуванням їх ймовірності та серйозності, що полегшує визначення

пріоритетів і планування заходів із пом'якшення наслідків.

У табл. 2.3 наведено матрицю ризиків, адаптовану до проєктних середовищ на основі ШІ, що поєднує технічні, етичні та організаційні аспекти.

Таблиця 2.3

Матриця ризиків проектів із використанням ШІ

Вимір ризику	Конкретний ризик	Рівень впливу	Рівень ймовірності	Стратегія пом’якшення
Якість даних	Неповні або упереджені навчальні дані	Високий	Середній	Аудит даних, перебалансування наборів даних
Конфіденційність і безпека	Порушення персональних даних	Висока	Висока	Шифрування, ШІ, що зберігає конфіденційність, дотримання нормативних вимог
Алгоритмічна упередженість	Дискримінаційні результати	Висока	Середня	Метрики справедливості, алгоритми корекції упередженості
Надійність системи	Дрейф моделі або ворожі атаки	Середня	Висока	Моніторинг у режимі реального часу, протоколи перенавчання
Етичні та правові	Відсутність прозорості або підзвітності	Висока	Середня	Зрозумілий ШІ, чіткі правові рамки
Вплив на людину	Опір впровадженню, втрата довіри	Середній	Середня	Управління змінами, залучення зацікавлених сторін

На додаток до статичної оцінки, ризики проєктів ШІ необхідно динамічно переглядати протягом усього життєвого циклу проєкту. Оскільки моделі з часом навчаються і адаптуються, їх профілі ризиків також змінюються. Тому дуже важливими є динамічні методи оцінки ризиків, що включають зворотний зв'язок від розгорнутих систем і кінцевих користувачів. Безперервна оцінка ризиків не лише забезпечує стійкість, але й сприяє ранньому виявленню нових загроз.

Ще одним значним ризиком є дефіцит кваліфікованих фахівців, які можуть подолати розрив між розробкою ШІ та застосуванням у конкретних

галузях. Дефіцит талантів збільшує ймовірність помилок при впровадженні та невідповідних рішень. Інвестиції в навчання, міждисциплінарну співпрацю та передачу знань мають вирішальне значення для формування людського капіталу, необхідного для ефективного впровадження ШІ.

Проекти ШІ часто страждають від завищених очікувань через хайп і надмірне просування. Нереалістичні терміни і результати можуть призвести до провалу проекту або неправильного сприйняття зацікавленими сторонами. Тому оцінка ризиків повинна включати оцінку реалістичності та управління очікуваннями, гарантуючи, що цілі проекту є досяжними з технічної та етичної точки зору.

Масштабованість рішень ШІ створює додаткові ризики, пов'язані з операційною інтеграцією. Моделі, які добре працюють в пілотних умовах, можуть не мати ефективного масштабування через відмінності в якості даних, системній інфраструктурі або організаційній культурі. Моделювання перед розгортанням і ретельне пілотне тестування в різних умовах може допомогти виявити ці приховані ризики перед повномасштабним впровадженням.

Зростаюча кількість літератури також підкреслює важливість узгодження управління ризиками ШІ з Цілями сталого розвитку (ЦСР) Організації Об'єднаних Націй, особливо в забезпеченні інклюзивного і справедливого технологічного розвитку. Оцінка ризиків повинна враховувати соціальні та екологічні наслідки застосування ШІ, особливо в таких секторах, як сільське господарство, освіта та охорона здоров'я, де ця технологія може мати широкі соціальні наслідки.

Розгортання ШІ в критично важливих об'єктах інфраструктури, таких як енергосистеми, транспортні мережі та фінансові системи, вимагає підвищених стандартів безпеки. Несправності або кібератаки на ці системи можуть мати каскадні наслідки, що робить системний ризик критично важливою сферою уваги. Для оцінки цих ризиків на макрорівні рекомендується використовувати моделювання на основі сценаріїв і стрес-тестування.

Оскільки системи штучного інтелекту все більше взаємодіють з іншими

інтелектуальними системами в Інтернеті речей (IoT) і кіберфізичних середовищах, складність взаємозалежностей ризиків зростає. Тому при оцінці ризиків необхідно застосовувати системний підхід, визнаючи, що вихід з ладу одного компонента може поширитися по мережі з експоненціальними наслідками.

Отже, оцінка ризиків у проектах з використанням ШІ - це міждисциплінарний і динамічний процес, який повинен враховувати технічні, етичні, правові та людські фактори. Багатогранна природа ШІ вимагає комплексних стратегій управління ризиками, заснованих на емпіричних даних і етичних принципах. Розробляючи надійні механізми оцінювання та розвиваючи культуру безперервного оцінювання та підзвітності, організації можуть використати трансформаційний потенціал ШІ, мінімізуючи пов'язані з ним ризики.

2.3. Розробка плану управління ризиками у проектах зі штучним інтелектом

Розробка комплексного плану управління ризиками для проектів зі штучного інтелекту є важливим заходом, який вирішує унікальні проблеми, пов'язані з розгортанням передових технологій. Подібні плани повинні передбачати системний підхід до виявлення, оцінки, пом'якшення та моніторингу ризиків протягом усього життєвого циклу проекту зі штучного інтелекту. Даний процес є особливо важливим з огляду на невизначеність і складність, притаманні системам ШІ, які вимагають як технічної кмітливості, так і стратегічного передбачення.

Першим кроком у розробці ефективного плану управління ризиками є чітке визначення обсягу та цілей проекту. Перший крок передбачає розуміння передбачуваного застосування системи ШІ, операційного контексту, в якому вона буде розгорнута, і потенційної взаємодії з різними зацікавленими сторонами. Чітке формулювання цілей проєкту слугує фундаментом, на якому

будуються всі подальші дії, пов'язані з ризиками, гарантуючи, що план залишається узгодженим як з технічними, так і з бізнес-пріоритетами.

За цим має слідувати ретельний процес ідентифікації ризиків, в ході якого всі потенційні джерела ризиків систематично каталогізуються. У проектах ШІ ризики можуть виникати через технічні фактори, такі як варіабельність продуктивності моделі та проблеми з якістю даних, а також через етичні, правові та організаційні аспекти. Виявлення цих ризиків на ранній стадії дає змогу керівникам проєктів застосовувати проактивний, а не реактивний підхід до їх зменшення.

План управління ризиками повинен включати надійну методологію оцінки ризиків, яка кількісно визначає як ймовірність виникнення, так і потенційний вплив кожного ідентифікованого ризику. Подвійна система оцінки дозволяє керівникам проектів визначати пріоритетність ризиків на основі їх серйозності та ймовірності. Система може бути додатково збагачена за рахунок використання історичних даних, експертних висновків і прогнозної аналітики, що в сукупності підвищує точність оцінок ризиків.

Одна з ефективних стратегій класифікації ризиків у проєктах ШІ передбачає їх групування за окремими категоріями, у тому числі технічні, етичні, юридичні та операційні ризики. Наприклад, технічні ризики можуть охоплювати такі проблеми, як упередженість алгоритмів або збій системи, тоді як етичні ризики можуть стосуватися питань прозорості та підзвітності. Правові ризики часто пов'язані з дотриманням законодавства про захист даних, а операційні ризики можуть виникати через неадекватну інфраструктуру або обмеженість ресурсів.

Для ілюстрації категоризації та стратегій пом'якшення ризиків розглянемо табл. 2.4, в якій узагальнено ключові аспекти ризиків у проектах ШІ, а також потенційний вплив і відповідні заходи щодо пом'якшення:

У наведеній табл. 2.4 подано стислий огляд основних категорій ризиків, з якими зазвичай стикаються проєкти зі штучного інтелекту, а також запропоновано цільові стратегії для зменшення кожного з них.

Багатовимірний підхід гарантує, що план управління ризиками буде комплексним і адаптованим до різних сценаріїв проекту.

Таблиця 2.4

Основні аспекти ризиків у проектах із використанням ШІ

Категорія ризику	Потенційний вплив	Стратегія пом’якшення
Технічні	Дрейф моделі, погіршення продуктивності, ворожі атаки	Надійне тестування, безперервний моніторинг і регулярне оновлення моделі
Якість даних та конфіденційність	Неточні результати, порушення даних	Перевірка даних, шифрування та методи збереження конфіденційності
Етика	Алгоритмічна упередженість, відсутність прозорості	Аудит справедливості, зрозумілі фреймворки ШІ, комітети з етичного нагляду
Правові та регуляторні	Невідповідність, юридична відповідальність	Аудит відповідності, дотримання стандартів, юридичні огляд
Операційна	Проблеми інтеграції, обмеженість ресурсів	Детальне планування, залучення зацікавлених сторін та планування на випадок надзвичайних ситуацій

Наступним важливим етапом в управлінні ризиками, окрім ідентифікації та категоризації, є розробка конкретних стратегій пом'якшення ризиків, адаптованих до кожної категорії ризиків. Стратегії повинні бути як превентивними, так і коригуючими за своєю природою. Превентивні заходи можуть включати прийняття суворих протоколів забезпечення якості та інтеграцію етичних принципів у процес розробки, тоді як коригувальні дії можуть включати заздалегідь визначені плани реагування на системні збої або витоки даних.

Бажано інтегрувати в план управління поєднання якісних і кількісних інструментів оцінки ризиків. Якісні інструменти, такі як інтерв'ю з експертами та панелі Дельфі, надають детальне розуміння потенційних ризиків, тоді як кількісні методи, такі як статистичне моделювання та аналіз чутливості, пропонують вимірювані метрики ризику. Змішаний підхід сприяє більш точному і дієвому розумінню ризиків.

Ключовим елементом плану управління ризиками є визначення чітких ролей та обов'язків, що гарантує, що кожен член проектної команди розуміє

свою роль в управлінні та зменшенні ризиків. Наприклад, аналітики даних можуть відповідати за забезпечення надійності моделі, а юридичні радники - за дотримання нормативних вимог. Міжфункціональна команда з управління ризиками, до складу якої входять технічні експерти, фахівці з етики та юристи, має важливе значення для цілісного нагляду за ризиками.

Комунікація та прозорість є життєво важливими компонентами успішної реалізації плану управління ризиками. Регулярне звітування, як внутрішнє, так і перед зовнішніми зацікавленими сторонами, допомагає підтримувати обізнаність про ризики, що виникають, та ефективність стратегій їх зниження. Прозорі канали комунікації також сприяють зміцненню довіри між зацікавленими сторонами та полегшують спільне вирішення проблем у разі виникнення непередбачуваних викликів.

Управління ризиками в проектах ШІ - це не одноразова вправа, а скоріше динамічний та ітеративний процес. Постійний моніторинг і періодична переоцінка ризиків необхідні для адаптації до мінливих параметрів проекту і технологічного прогресу. Циклічний процес гарантує, що стратегії пом'якшення наслідків залишатимуться ефективними протягом тривалого часу, навіть якщо з'являться нові ризики або зміняться вже існуючі.

План також повинен включати стратегії на випадок непередбачених обставин, які стосуються найгірших сценаріїв. Стратегії можуть передбачати виділення резервних ресурсів, заздалегідь визначені протоколи дій у надзвичайних ситуаціях або навіть тимчасове призупинення певних видів діяльності за проектом до моменту зниження ризиків. Заходи готовності можуть значно зменшити вплив непередбачуваних подій на проект в цілому.

Паралельно організації повинні інвестувати в розвиток внутрішнього потенціалу для управління ризиками. Навчальні програми, семінари та сертифікаційні курси з методології оцінки ризиків можуть підвищити кваліфікацію проектної команди, тим самим підвищуючи ефективність плану управління ризиками. Розвиток цих компетенцій є довгостроковою інвестицією, яка сприяє загальній стійкості організації.

Використання нових технологій для підтримки управління ризиками є ще одним перспективним напрямком. Наприклад, передові методи аналітики та машинного навчання можна застосовувати для прогнозування потенційних ризиків на основі історичних даних проекту. Можливості прогнозування уможливлюють більш проактивний підхід, коли ризики передбачаються і вирішуються до того, як вони переростають у критичні проблеми.

Залучення зацікавлених сторін є важливим аспектом розробки надійного плану управління ризиками. Залучення клієнтів, кінцевих користувачів і регуляторних органів на ранній стадії процесу планування може забезпечити цінний зворотний зв'язок і гарантувати, що стратегії управління ризиками відповідають більш широким очікуванням і стандартам. Спільний підхід не тільки підвищує довіру до плану, але й сприяє формуванню спільного почуття відповідальності за зниження ризиків.

Дотримання правових і регуляторних норм має бути вплетено в структуру плану управління ризиками. Проекти ШІ підпадають під вплив змінної регуляторної ситуації, і недотримання вимог може призвести до значних юридичних і фінансових наслідків. Постійний моніторинг регуляторних змін і періодичні аудити необхідні для того, щоб забезпечити відповідність проекту чинним законодавчим вимогам.

Етичні міркування глибоко вбудовані в процес управління ризиками для проектів ШІ. Забезпечення того, щоб системи ШІ працювали без упереджень, зберігали прозорість і поважали автономію користувачів, має важливе значення для підтримки суспільної довіри. Тому план управління ризиками повинен включати чіткі етичні настанови та механізми незалежної етичної експертизи, які слугують додатковим захистом від ненавмисної шкоди.

Отже, розробка плану управління ризиками для проектів зі штучного інтелекту вимагає структурованого, міждисциплінарного та проактивного підходу. Виявляючи ризики на ранніх стадіях, використовуючи надійні методи оцінки та інтегруючи комплексні стратегії пом'якшення, організації можуть орієнтуватися в складнощах розгортання ШІ, убезпечуючи себе від

потенційних збоїв. Динамічний ітеративний процес не тільки підвищує технічну надійність систем ШІ, але й гарантує, що етичні, правові та операційні стандарти будуть неухильно дотримуватися протягом усього життєвого циклу проекту.

Висновок до розділу 2

Проекти, що включають штучний інтелект, демонструють значний потенціал для оптимізації управлінських процесів, зокрема через автоматизацію та використання даних в реальному часі. Інструменти ШІ, такі як мовний переклад, оптичне розпізнавання символів та роботизована автоматизація, активно впроваджуються для покращення ефективності та зменшення адміністративного навантаження. Використання таких технологій сприяє підвищенню точності та зниженню залежності від людського фактору в рутинних операціях. Однак, основною проблемою залишаються питання інтеграції цих інструментів в організаційні процеси та необхідність адаптації до специфіки кожного проекту.

Процес оцінки ризиків у проєктах зі штучним інтелектом вимагає комплексного підходу, що охоплює як технічні, так і етичні, соціальні та правові аспекти. Визначальними факторами є якість даних, алгоритмічна упередженість та прозорість моделей, що суттєво впливають на точність та справедливість результатів. Потрібно постійно адаптувати методології управління ризиками до специфіки ШІ, з урахуванням змін та потенційних етичних проблем. Тому важливими є міждисциплінарні підходи, постійний моніторинг і взаємодія з усіма зацікавленими сторонами для зниження ризиків у таких проєктах.

Розробка плану управління ризиками для проектів зі штучним інтелектом передбачає системний підхід, який охоплює ідентифікацію, оцінку та пом'якшення ризиків через уведення чітких стратегій для кожної категорії. Використання комплексних методів оцінки ризиків, таких як статистичне

моделювання і аналітика, дозволяє приймати обґрунтовані рішення, які враховують потенційний вплив і ймовірність кожного ризику. Залучення зацікавлених сторін і інтеграція етичних та правових аспектів у процес забезпечує довіру до проекту і гарантує його відповідність нормативним вимогам.

РОЗДІЛ 3
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ПРОЄКТІВ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ

3.1. Проблеми використання штучного інтелекту у проєктах

Використання штучного інтелекту у проектах є складним, багаторівневим процесом, який передбачає взаємодію між різними технологічними, організаційними та управлінськими підсистемами. Для системного аналізу взаємозв'язків між основними компонентами впровадження ШІ доцільним є застосування структури, запропонованої на рис. 3.1 [61; 48; 33], яка демонструє кореляції між процесом розробки (PD), областями застосування ШІ, власне системами штучного інтелекту та інформаційно-технологічною інфраструктурою (ITI). У центрі аналізу перебуває так звана «сходи знань» (knowledge staircase), яка структурує інформаційні потоки в умовах знання-інтенсивної діяльності, дозволяючи окреслити вузлові точки проблемності на кожному етапі реалізації проектів із застосуванням ШІ.

Важливою відправною точкою є те, що процеси, пов'язані з розробкою продуктів або впровадженням проєктів, потребують ретельної деталізації інформаційної моделі – від рівня метамоделей до конкретних процесних компонентів. Наявні наукові метамоделі не забезпечують достатнього рівня деталізації для адаптації до задач із використанням ШІ. Розрив між абстрактною моделлю та практикою вимагає удосконалення формалізованих описів, зокрема для мультидисциплінарних команд, де можливі різночитання термінології та різні підходи до моделювання [31].

У лівій частині схеми подано зв'язки між метамоделями, референтними процесами підприємства та конкретними проектними процедурами. Деталізація на рівні процесних компонентів дає змогу виявити, яка саме інформація, знання й дані є критично важливими для реалізації ШІ-рішень.

Однак у реальній практиці підприємства часто не мають методичних засобів для формалізації цих процесів.

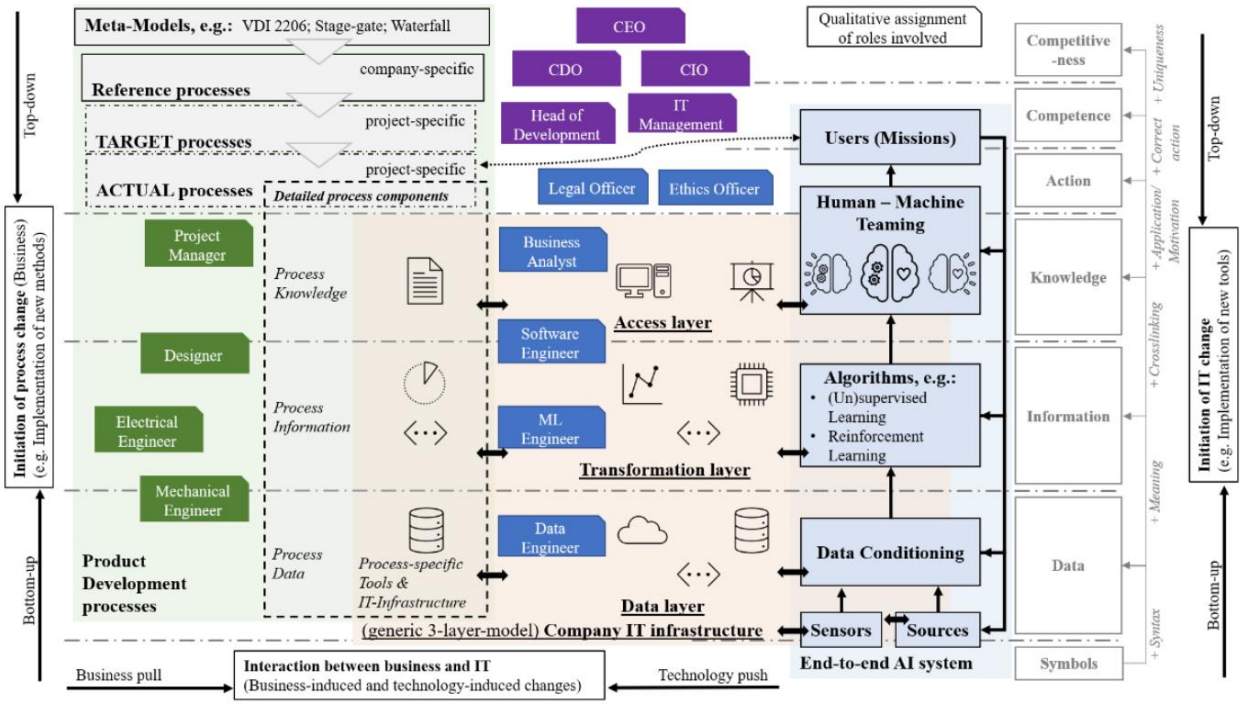

Рис. 3.1. Систематичне відображення кореляцій між розглянутими доменами [47]

Іншою фундаментальною проблемою є відсутність уніфікованих підходів до збору, структурування та опису даних у межах розробницьких процесів. Потреба в чіткому визначенні даних і знань, які повинні бути наявними для реалізації ШІ-рішень, залишається відкритою.

Як зазначають K. Gericke і L. Blessing [36], існуючі проектні моделі рідко здатні ініціювати інновації, зокрема ті, що виникають внаслідок «технологічного поштовху» (technology push). Моделі містять переважно опис «що потрібно робити», залишаючи поза увагою механізми реалізації, а також не враховують специфіку міждисциплінарної взаємодії, яка є характерною для ШІ-проектів.

Ще однією значущою проблемою є відсутність стандартизованих механізмів для збору й опису даних, які мають бути використані в контексті розробки ШІ. Через недостатній рівень деталізації метамоделі не забезпечують

надійної основи для побудови ефективних алгоритмів (роцесні компоненти на рис. 3.1). У роботах M. Wilmsen [61] і K. Gericke [35] акцентується увага на розриві між академічними дослідженнями й промисловою практикою, що проявляється у слабкому трансфері знань та ускладненій комунікації між учасниками проектів. Для досягнення результативного впровадження ШІ потрібно мати чітко описані етапи діяльності, стандартизовані дані й прозорі інтерфейси взаємодії.

Складність зростає при необхідності інтеграції ШІ із загальною IT-інфраструктурою підприємства. Центральна частина рис. 3.1 ілюструє модель ITI на трьох рівнях, яка є базисом для реалізації ШІ-систем. Відсутність узгодження між специфічними інструментами процесу та загальною ITI компанії часто призводить до технічних бар'єрів. Проблема ускладнюється тим, що в реальному середовищі більшість підприємств не володіють достатньою кількістю IT- або ШІ-експертів, що підтверджується результатами дослідження Bitkom [55]: 62% компаній зазначають нестачу фахівців і даних, а 48% – відсутність технічної експертизи. У 22% організацій немає визначених кейсів застосування ШІ.

На правому боці рис. 3.1 представлена структура end-to-end ШІ-системи [33], яка охоплює не лише технологічну складову, а й рівні репрезентації знань, необхідні для людсько-машинної взаємодії. Саме ця особливість відкриває нові горизонти для інтеграції ШІ в проектне управління, однак одночасно ускладнює процес, оскільки вимагає наявності зрілих управлінських функцій, здатних координувати крос-функціональні команди. Відсутність чітко визначених ролей, а також проблеми з комунікацією між дисциплінами створюють передумови для невірного тлумачення даних і зниження ефективності ШІ-рішень [26].

Окрему проблему становить розрив між «top-down» та «bottom-up» підходами. Ініціативи, що запускаються керівництвом (наприклад, впровадження нових IT-інструментів), часто не узгоджуються з практичними потребами користувачів процесів, а потенціал, виявлений на операційному

рівні, залишається нереалізованим. Як зазначає A. Aranda-Muñoz [19], до процесу ідентифікації можливостей застосування ШІ мають бути залучені й працівники без ґрунтовної ІТ-освіти. Вони можуть виступати джерелом цінних інсайтів завдяки володінню предметною областю. Проте без відповідних методів інтеграції таких знань існує ризик формування «втрачених ланок» між рівнями управління.

Ще однією важливою проблемою є відсутність уніфікованих підходів до управління життєвим циклом проєктів, у яких використовується машинне навчання. Як показує дослідження S. Rädler і E. Rigger [50], 63% компаній обирають алгоритми ШІ виключно на основі експертних знань, тоді як лише 13% посилаються на методологію, і лише 3% – на заздалегідь визначений інструментарій, що свідчить про відсутність усталених практик і стандартів у цій сфері. За наявності такого стану речей стає майже неможливим достовірно оцінити економічну ефективність інвестицій у ШІ [57].

Серед організаційних бар’єрів використання ШІ у проєктній діяльності варто виділити:

- недостатню деталізацію процесних моделей, яка унеможливлює точну ідентифікацію потенціалу для ШІ;
- брак уніфікованих методик опису даних у межах розробницьких завдань;
- недостатнє врахування трансдисциплінарного характеру проектної діяльності;
- відсутність стандартів для життєвого циклу моделей машинного навчання.

Сучасні інструменти управління, які мали б підтримувати реалізацію ШІ в проектах, мають суттєві обмеження. Наприклад, St. Gallen Management Model [58] чи AI Deployment Canvas [42] пропонують корисні підходи, але не надають достатнього рівня деталізації для компаній з низькою ІТ-зрілістю. Існує також метод ідентифікації кейсів застосування ШІ, але він не враховує специфіку міждисциплінарної інтеграції або обмеженість ресурсів у малих

підприємствах. Таким чином, потреба у гнучких, багаторівневих і адаптивних методичних підходах до управління проектами із застосуванням ШІ залишається вкрай актуальною.

3.2. Перспективи використання штучного інтелекту у проєктах

Штучний інтелект став трансформаційною силою в різних галузях, змінивши спосіб концептуалізації, виконання та управління проектами. Його інтеграція в робочі процеси проектів – це не просто технологічний прогрес, а зміна парадигми, яка обіцяє підвищити ефективність, точність та інноваційність. Перспективи використання штучного інтелекту в проєктах охоплюють широкий спектр сфер – від автоматизації рутинних завдань до предиктивної аналітики та сприяння творчому розв'язанню проблем. Оскільки організації все більше визнають потенціал штучного інтелекту, його впровадження стає не просто можливістю, а необхідністю для збереження конкурентоспроможності в глобальному світі, що швидко змінюється.

Однією з найважливіших переваг штучного інтелекту в управлінні проектами є його здатність впорядковувати процеси та оптимізувати розподіл ресурсів. Традиційне управління проектами часто покладається на ручний контроль, який може бути схильний до людських помилок і неефективності. Натомість інструменти на основі штучного інтелекту здатні аналізувати величезні масиви даних у режимі реального часу, виявляючи закономірності та тенденції, які інакше могли б залишитися непоміченими. Наприклад, алгоритми машинного навчання можуть передбачити потенційні вузькі місця в термінах проекту, аналізуючи історичні дані та поточні показники прогресу.

Прогностична здатність дозволяє менеджерам проєктів проактивно вирішувати проблеми до того, як вони загострюються, забезпечуючи безперебійне виконання та зменшуючи затримки. ШІ може допомогти в розподілі ресурсів, оскільки оцінюватиме навички членів команди, їх доступність і робоче навантаження, таким чином розподіляючи завдання

таким чином, щоб максимізувати продуктивність і мінімізувати вигорання.

Окрім підвищення операційної ефективності, ШІ також має величезний потенціал для покращення процесу прийняття рішень завдяки розширеній аналітиці. У складних проектах рішення часто доводиться приймати в умовах невизначеності, коли неповна або неоднозначна інформація може призвести до неоптимальних результатів. Системи штучного інтелекту можуть пом'якшити цю проблему, синтезуючи дані з різних джерел і надаючи дієві висновки. Наприклад, алгоритми обробки природної мови (NLP) можуть аналізувати неструктуровані дані, такі як протоколи зустрічей, електронні листи та звіти, щоб виокремити важливу інформацію. Можливість дозволяє керівникам проєктів приймати обґрунтовані рішення на основі всебічного розуміння стану проєкту та його ризиків. Симуляції та моделювання сценаріїв на основі штучного інтелекту дозволяють командам досліджувати різні результати та стратегії, що дає їм змогу обрати найефективніший шлях розвитку.

Ще однією переконливою перспективою застосування ШІ в проектах є його роль у стимулюванні інновацій та креативності. Попри те, що ШІ часто асоціюється з автоматизацією та ефективністю, він також здатен посилити людську винахідливість. Наприклад, генеративні моделі ШІ можуть допомогти дизайнерам, інженерам і розробникам, генеруючи нові ідеї, прототипи та рішення. Генеративні моделі аналізують існуючі проекти або кодові бази і пропонувати поліпшення або абсолютно нові підходи, прискорюючи етап розробки проектів. Штучний інтелект може сприяти співпраці, руйнуючи ізоляцію між відділами. Завдяки централізованим платформам для обміну ідеями та відгуками, інструменти штучного інтелекту можуть забезпечити інтеграцію різних точок зору в життєвий цикл проекту, що призведе до більш надійних та інноваційних результатів.

Попри численні переваги, інтеграція штучного інтелекту в проекти не позбавлена проблем. Однією з головних проблем є етичні наслідки використання систем штучного інтелекту, особливо в чутливих середовищах

або в ситуаціях з високими ставками. Такі питання, як упередженість в алгоритмічному прийнятті рішень, конфіденційність даних і підзвітність, повинні бути ретельно розглянуті, щоб забезпечити відповідальне використання ШІ. Організації повинні встановити чіткі керівні принципи та системи управління для нагляду за впровадженням ШІ, забезпечуючи прозорість і справедливість. Існує проблема підвищення кваліфікації робочої сили для ефективного використання технологій штучного інтелекту. Працівників потрібно навчити не лише використовувати інструменти штучного інтелекту, а й інтерпретувати їх результати та розуміти їх обмеження.

Масштабованість рішень зі штучним інтелектом створює як можливості, так і виклики. З одного боку, системи штучного інтелекту можна масштабувати для роботи з проектами різного розміру та складності, що робить їх пристосованими до різноманітних організаційних потреб. Наприклад, невеликі стартапи можуть використовувати платформи для управління проектами на основі штучного інтелекту, щоб конкурувати з великими підприємствами, оптимізуючи свої обмежені ресурси.

З іншого боку, масштабування ШІ вимагає значних інвестицій в інфраструктуру, управління даними та кібербезпеку. Організації повинні порівнювати витрати з потенційними вигодами, оскільки мають гарантувати, що їх ініціативи в галузі ШІ відповідають стратегічним цілям. Динамічна природа технології ШІ вимагає постійних оновлень і вдосконалень для підтримки її ефективності, що додає ще один рівень складності до її впровадження.

Майбутнє ШІ в проектах, ймовірно, буде визначатися досягненнями в таких нових технологіях, як квантові обчислення, периферійний ШІ і федеративне навчання. Квантові обчислення, наприклад, можуть революціонізувати проблеми оптимізації, вирішувати їх експоненціально швидше, ніж класичні комп'ютери, що дозволить досягти безпрецедентного рівня точності в плануванні проєктів. Граничний ШІ, який передбачає обробку

даних локально на пристроях, а не на централізованих серверах, може покращити прийняття рішень в режимі реального часу у віддалених або обмежених ресурсами середовищах. Федеративне навчання – метод, який дозволяє навчати моделі ШІ на децентралізованих пристроях, зберігаючи при цьому конфіденційність даних – вирішить деякі етичні проблеми, пов'язані зі штучним інтелектом.

Щоб повністю реалізувати перспективи ШІ в проектах, організації повинні прийняти цілісний підхід, який об'єднує технології, людей і процеси, що передбачає не лише інвестиції в передові інструменти, а й розвиток культури експериментів і безперервного навчання. Керівники повинні заохочувати свої команди сприймати штучний інтелект як партнера для співпраці, а не як заміну людського досвіду. Таким чином вони зможуть використати весь потенціал штучного інтелекту для стимулювання інновацій, підвищення ефективності та досягнення найкращих результатів у проєктах. Зрештою, успішна інтеграція ШІ в проекти залежатиме від збалансованого поєднання технологічної досконалості, етичної відповідальності та людської винахідливості.

Отже, перспективи використання штучного інтелекту в проектах є широкими і багатогранними, пропонуючи трансформаційні можливості в різних галузях. Від оптимізації розподілу ресурсів і вдосконалення процесу прийняття рішень до стимулювання творчості та вирішення етичних проблем - штучний інтелект має потенціал, щоб переосмислити способи управління проектами та їх виконання. Однак реалізація цих переваг вимагає стратегічного і вдумливого підходу, який збалансовує технологічні інновації з людськими цінностями. Організації, які успішно інтегрують штучний інтелект у свої проєктні робочі процеси, матимуть всі шанси процвітати у більш конкурентному та динамічному світі.

Висновок до розділу 3

Основні проблеми впровадження штучного інтелекту у проєктах зумовлені відсутністю стандартів для детального опису процесів, збору даних та інтеграції з інформаційно-технологічною інфраструктурою. Розрив між теоретичними моделями і реальними потребами підприємств ускладнює адаптацію ШІ до конкретних завдань. Також значною перешкодою є недостатній рівень співпраці між різними дисциплінами, що веде до неефективного використання можливостей технологій. Вирішення цих проблем потребує впровадження гнучких та адаптивних підходів до управління проєктами з використанням штучного інтелекту.

Штучний інтелект має великий потенціал для трансформації управління проектами, зокрема через оптимізацію розподілу ресурсів, покращення процесу прийняття рішень та стимулювання інновацій. Його здатність до прогностичного аналізу і реального часу дає можливість проактивно вирішувати проблеми, зменшуючи затримки і підвищуючи ефективність. Водночас, для успішної інтеграції ШІ в проекти важливо враховувати етичні питання, забезпечення конфіденційності та відповідальності. Майбутнє використання ШІ в управлінні проектами залежатиме від розвитку нових технологій, таких як квантові обчислення і федеративне навчання, що відкривають нові можливості для вдосконалення процесів.

ВИСНОВКИ

За результатами досягнення поставленої мети дослідження можемо зробити наступні висновки:

1. Ризик є невід'ємною частиною будь-якої діяльності та має складну структуру, що включає джерела, об'єкти та можливі наслідки, як негативні, так і позитивні. У наукових колах існує різноманіття підходів до визначення ризику, що пояснюється відмінностями в трактуванні його наслідків та впливу на процес прийняття рішень. До основних джерел ризику належать природні явища, соціально-економічні фактори та обмеження в обміні інформацією. Оцінка ризику повинна враховувати не лише потенційну загрозу, але й вразливість об'єкта та взаємодію з іншими ризиками, що є необхідними умовами для розробки ефективних стратегій управління.

2. Ідентифікація та оцінка ризиків є критично важливими етапами у процесі управління ризиками, адже вони дають можливість своєчасно виявити загрози і мінімізувати їх вплив на організацію. Найбільшу цінність мають методи, що дозволяють враховувати як внутрішні, так і зовнішні чинники, а також розробка стратегій зниження ризиків на основі глибокого системного аналізу. В умовах розвитку Індустрії 6.0, що включає використання штучного інтелекту, з'являються нові ризики, пов'язані з безпекою даних, упередженістю алгоритмів, змінами на ринку праці та правовими проблемами, що потребують розробки спеціалізованих заходів для їх нейтралізації. Важливою складовою є постійний моніторинг і здатність адаптуватися до динамічних умов.

3. Проєкти, що включають застосування штучного інтелекту, відкривають великі можливості для підвищення ефективності управлінських процесів, зокрема завдяки автоматизації операцій і обробці даних в реальному часі. ШІ-технології, такі як машинний переклад, оптичне розпізнавання символів і роботизовані системи, активно впроваджуються для покращення операційних результатів і зменшення навантаження на адміністративний

персонал. Вони дозволяють підвищити точність і знизити вплив людського фактору в рутинних задачах. Однак важливим викликом залишається інтеграція цих інструментів у бізнес-процеси, що потребує адаптації до специфічних вимог кожного проєкту.

4. Оцінка ризиків у проектах зі штучним інтелектом повинна ґрунтуватися на комплексному підході, який охоплює технічні, етичні, соціальні та правові аспекти. Ключовими факторами є якість даних, можливі алгоритмічні упередження та прозорість моделей, що безпосередньо впливають на точність і об’єктивність результатів. Для ефективного управління ризиками необхідно постійно адаптувати стратегії, з урахуванням специфіки технологій ШІ і динамічних змін в середовищі. Важливим аспектом є застосування міждисциплінарних підходів, постійний моніторинг процесів і активна взаємодія з усіма зацікавленими сторонами для зниження ризиків.

5. Розробка стратегії управління ризиками для проєктів зі штучним інтелектом має включати системний підхід, що передбачає не лише ідентифікацію й оцінку ризиків, а й створення чітких стратегій для їх пом'якшення. Використання методів, таких як статистичне моделювання та аналітика даних, дозволяє обґрунтовано оцінювати ймовірність ризиків і їх можливий вплив. Залучення ключових учасників процесу, а також інтеграція етичних і правових аспектів, підвищують довіру до проєкту та забезпечують його відповідність законодавчим вимогам.

6. Інтеграція штучного інтелекту у проєкти стикається з кількома важливими викликами, зокрема через відсутність чітких стандартів для опису процесів, збору даних та їх взаємодії з існуючою інформаційною інфраструктурою. Існуючий розрив між теоретичними розробками та реальними потребами підприємств ускладнює ефективне застосування ШІ для вирішення специфічних завдань. Недостатній рівень міждисциплінарної співпраці також гальмує максимальне використання потенціалу технологій. Подолання цих перешкод вимагає гнучкішого підходу до управління проектами, що включає штучний інтелект, а також адаптивних стратегій для

вирішення конкретних проблем.

7. Штучний інтелект здатний значно змінити підходи до управління проектами, зокрема в аспектах оптимізації ресурсів, покращення прийняття рішень та стимулювання інноваційних процесів. Його здатність до прогностичного аналізу та роботи в режимі реального часу дозволяє проактивно вирішувати виникаючі проблеми, знижуючи затримки та підвищуючи ефективність. Проте для успішного впровадження ШІ у проєкти важливо ретельно враховувати етичні питання та забезпечення конфіденційності і прозорості. Дальші досягнення у розвитку таких технологій, як квантові обчислення та федеративне навчання, можуть ще більше підвищити ефективність застосування ШІ в управлінні проектами.

ПЕРЕЛІК ПОСИЛАНЬ

1. Боровик М. В. Ризик-менеджмент: конспект лекцій. Харків: ХНУМГ ім. О. М. Бекетова, 2018. 67 с.

2. Васильєва Т. А., Кривич Я. М. Економічний ризик: методи оцінки та управління: навч. посіб. Суми: ДВНЗ «УАБС НБУ», 2015. 208 с.

3. Вітлінський В. В. Ризикологія в економіці та підприємництві: монографія. Київ: КНЕУ, 2004. 480 с.

4. Загородній А. Г., Вознюк Г. Л. Фінансово-економічний словник. Київ: Знання, 2007. 1072 с.

5. Івченко І. Ю. Моделювання економічних ризиків і ризикових ситуацій. Навчальний посібник. Київ: Центр учбової літератури, 2007. 344 с.

6. Машина Н. І. Економічний ризик і методи його вимірювання: навч. посіб. Київ: ЦУЛ, 2003. 188 с.

7. Мочерний С. В. Економічна енциклопедія: У трьох томах. Том 3. Київ: Видавничий Центр «Академія», 2002. 952 с.

8. Олійник О. О. Ідентифікація ризиків як складова процесу управління ризиками в бізнесі. *Вісник НУВГП*. 2022. № 2 (98). Сс. 192-199.

9. Осовська Г. В. Менеджмент організацій: навч. посіб. Київ: Кондор, 2005. 854 с.

10. Пасічник В. Г., Акіліна О. В. Планування діяльності підприємства. Навчальний посібник. Київ: Центр навчальної літератури, 2005. 256 с.

11. Підсолонко В. А., Процай А. Ф., Миронова Т. Л., Василенко В. О. Підприємництво: навч. посіб. Київ: КНЛ, 2003. 616 с.

12. Про об’єкти підвищеної небезпеки: Закон України від 18.01.2001 р. № 2245-III. URL: https://zakon.rada.gov.ua/laws/show/2245-14#Text (дата звернення: 10.02.2025).

13. Сенейко Ю. Сучасні підходи до трактування категорії «ризик». *Регіональна економіка*. 2006. №1. С.206-211.

14. Цопа В. Ідентифікація і класифікація ризиків. Київ: Тех Медіа

Груп, 2023. URL: https://qualityexpert.com.ua/articles/657215-identyfikatsiya-i-klasyfikatsiya-ryzykiv (дата звернення: 11.02.2025).

15. Швець Ю. О. Ризики в діяльності промислових підприємств: види, методи оцінки та заходи подолання ризику. *Науковий вісник УНУ*. 2018. № 17 (2). С. 131-135.

16. Шурда К. Е. Методи якісного та кількісного аналізу ризиків. *Економіка*. 2020. № 4. С. 64-72.

17. Ястремський О. І. Основи теорії економічного ризику: навчальний посібник для студентів екон. спец. вищ. навч. закладів. Київ: «АртЕк», 1997. 248 с.

18. Aattouri I., Mouncif H., Rida M. Modeling of an AI based enterprise callbot with natural language processing and machine learning algorithms. *IAES International Journal of Artificial Intelligence*. 2023. № 12(2). С. 943

19. Aranda-Muñoz Á., Florin U., Yamamoto Y., Eriksson Y., Sandström K. Co-Designing with AI in Sight. *Proceedings of the 17th International Design Conference. Online, 23–26 May 2022*. Cambridge : Cambridge University Press, University of Cambridge, 2022. P. 101–110.

20. Araujo T., Helberger N., Kruikemeier S., De Vreese C. H. In AI we trust? *Perceptions about automated decision-making by artificial intelligence. AI & society*. 2020. № 35. С. 611-623.

21. Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards. AI Govemance Alliance In collaboration with the Global Cyber Security Capacity Centre, University of Oxford. 2025. URL: https://reports.weforum.org/docs/WEF_Artificial_Intelligence_and_Cybersecurity_Balancing_Risks_and_Rewards_2025.pdf (дата звернення: 12.02.2025).

22. Barth T. J., Arnold E. AIand administrative discretion: Implications for public administration. *The American Review of Public Administration*. 1999. № 29(4). P. 332-351.

23. Bhatia S., Singh A. K. Developments in AIa global perspective. *Delhi Business Review*. 2019. № 20 (1). P. 1-15.

24. Bicchierai I., Schiavone E., Brancati F. Modelling and Assessing the Risk of Cascading Effects with ResilBlockly. *In 2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. 2022. P. 261-266.

25. Bisoyi A. Ownership, liability, patentability, and creativity issues in artificial intelligence. *Information Security Journal: A Global Perspective*. 2022. № 31(4). P. 377-386.

26. Briard T., Jean C., Aoussat A., Véron P., Le Cardinal J., Wartzack S. Data-driven design challenges in the early stages of the product development process. *Proceedings of the 23rd International Conference on Engineering Design. Gothenburg, Sweden, 16–20 August 2021*. P. 851–860.

27. Bughin J., Seong J., Manyika J., Chui M. Notes from the AI frontier: Modeling the impact of AI on the world economy. McKinsey Global Institute. 2018. URL: https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy (дата звернення: 12.02.2025).

28. Cao J.Q., Zhang S.H. ITIL Incident Management Process Reengineering in Industry 4.0 Environments. *Proceedings of the 2nd International Conference on Advances in Mechanical Engineering and Industrial Informatics (AMEII 2016*). 2016. № 73. P. 1011–1016.

29. Cheatham B., Javanmardian K., Samandari H. Confronting the risks of artificial intelligence. McKinsey Quarterly. 2019. URL: https://surl.lu/jhvmuq (дата звернення: 12.02.2025).

30. Czakon W. (ed.) Podstawy metodologii badań w naukach. Warszawa, 2011. 263 p.

31. Eisenbart B., Gericke K., Blessing L. A framework for comparing design modelling approaches across disciplines. *Proceedings of the 18th International Conference on Engineering Design*. Lyngby/Copenhagen, Denmark, 15–19 August 2011. P. 344–355.

32. Ernst E., Merola R., Samaan D. Economics of artificial intelligence: Implications for the future of work. *IZA Journal of Labor Policy*. 2019. № 9(1).

33. Gadepally V., Goodwin J., Kepner J., Reuther A., Reynolds H., Samsi S., Su J., Martinez D. AI Enabling Technologies: A Survey. *arXiv preprint*. 2019. URL: arXiv:1905.03592 (дата звернення: 07.04.2025).

34. Geis J. R., Brady A. P., Wu C. C., Spencer J., Ranschaert E., Jaremko J. L., Kohli M. Ethics of AIin radiology: summary of the joint European and North American multisociety statement. *Canadian Association of Radiologists Journal*, 2019. № 70(4). P. 329-334.

35. Gericke K., Adolphy S., Qureshi A.J., Blessing L., Stark R. Opening up Design Methodology. *The Future of Transdisciplinary Design: Proceedings of the Workshop on «The Future of Transdisciplinary Design»*. Cham : Springer, 2021. P. 3–14.

36. Gericke K., Blessing L. An analysis of design process models across disciplines. *Proceedings of the 12th International Design Conference. Dubrovnik, Croatia, 21–24 May 2012*. P. 171–180.

37. Haluza D., Jungwirth D. AIand Ten Societal Megatrends: An Exploratory Study Using GPT-3. *Systems*. 2023. № 11(3). С. 120.

38. Hamon R., Junklewitz H., Sanchez I. Robustness and explainability of artificial intelligence. Publications Office of the European Union, 2020. 207 p.

39. Jarrahi M. H., Askay D., Eshraghi A., Smith P. AIand knowledge management: A partnership between human and AI. *Business Horizons*. 2023. № 66(1). P. 87-99.

40. Javaid M., Haleem A., Singh R. P., Suman R. AI applications for industry 4.0: A literaturebased study. *Journal of Industrial Integration and Management*. 2022. № 7(1). P. 83-111.

41. Kotarba M. Digital transformation of business models. *Foundations of Managemen*t. 2018. № 10. DOI: 10.2478/fman-2018-0011 (дата звернення: 05.04.2025).

42. Kreutzer R.T., Sirrenberg M. Künstliche Intelligenz verstehen. Wiesbaden : Springer Fachmedien Wiesbaden, 2019. 316 с.

43. Larsson S., Heintz F. Transparency in Artificial Intelligence. *Internet*

Policy Review. 2020. № 9 (2). P. 1–16. DOI: 10.14763/2020.2.1469.

44. Lee J. Industry 4.0 in Big Data environment. *German Harting Magazine*. 2013. № 26. P. 8–10.

45. Loza de Siles E. AIBias and Discrimination: Will We Pull the Arc of the Moral Universe Towards Justice?. *J. Int'l & Comp. L*. 2021. № 8. P. 513.

46. Mazurek G., Małagocka K. Perception of privacy and data protection in the context of the development of artificial intelligence. *Journal of Management Analytics*. 2019. № 6(4). P. 344-364.

47. Müller B., Roth D., Kreimeyer M. Barriers to the use of artificial intelligence in the product development – a survey of dimensions involved. *Proceedings of the International Conference on Engineering Design (ICED23)*. 2023. P. 757–766.

48. North K., Maier R. Wissen 4.0 – Wissensmanagement im digitalen Wandel. *HMD Praxis der Wirtschaftsinformatik*. 2018. №55 (4). P. 665–681.

49. Project Management Institute. A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Fourth edition. Newtown Square, 2008. 459 p.

50. Rädler S., Rigger E. A Survey on the Challenges Hindering the Application of Data Science, Digital Twins and Design Automation in Engineering Practice. *Proceedings of the 17th International Design Conference. Online, 23–26 May 2022*. Cambridge : Cambridge University Press, University of Cambridge, 2022. P. 1699–1708.

51. Rodríguez-Espíndola O., Chowdhury S., Dey P. K., Albores P., Emrouznejad A. Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*. 2022. 178.

52. Rowley J. The wisdom hierarchy: Representations of the DIKW hierarchy. *Journal of Information Science*. 2007. №33 (2). P. 163–180.

53. Sharma S., Islam N., Singh G., Dhir A. Why Do Retail Customers Adopt AI(AI) Based Autonomous Decision-Making Systems?. IEEE Transactions

on Engineering Management, 2022.

54. Spałek S. Zarządzanie projektami w erze przemysłu 4.0. *Ekonomika i Organizacja Przedsiębiorstwa*. 2017. № 9. P. 106–112.

55. Streim A., Uhl M. KI gilt in der deutschen Wirtschaft als Zukunftstechnologie – wird aber selten genutzt. Berlin, Germany, 2022. URL: https://www.bitkom.org/Presse/Presseinformation/KuenstlicheIntelligenz-2022 (дата звернення: 07.04.2025).

56. Truby J. Governing AIto benefit the UN sustainable development goals. *Sustainable Development*. 2020. № 28(4). P. 946-959.

57. Ulrich M., Bachlechner D. Wirtschaftliche Bewertung von KI in der Praxis – Status Quo, methodische Ansätze und Handlungsempfehlungen. *HMD Praxis der Wirtschaftsinformatik*. 2020. №57 (1). P. 46–59.

58. van Giffen B., Borth D., Brenner W. Management von Künstlicher Intelligenz in Unternehmen. *HMD Praxis der Wirtschaftsinformatik*. 2020. №57 (1). P. 4–20.

59. Vanhoucke M. Project Management with Dynamic Scheduling: Baseline Scheduling. Risk Analysis and Project Control. 2nd ed. Berlin : Springer, 2012. 310 p.

60. Walker W.E., Marchau V.A.W.J., Swanson D. Addressing deep uncertainty using adaptive policies: Introduction to section 2. *Technological Forecasting & Social Change*. 2010. № 77. P.. 917–923.

61. Wilmsen M., Gericke K., Jäckle M., Albers A. Method for the identification of requirements for designing reference processes. *Proceedings of the 16th International Design Conference. Cavtat, Croatia, 26–29 October 2020*. P. 1175–1184.

62. Završnik A. In Defence of Ethics and the Law in AI Governance: The Case of Computer Vision. In Artificial Intelligence, Social Harms and Human Rights. : Springer International Publishing, 2023. P. 101-139.

63. Zhu L., Xu X., Lu Q., Governatori G., Whittle J. AI and ethics—Operationalizing responsible AI. *Humanity Driven AI: Productivity, Well-being,*

*Sustainability and Partners*hip. 2023. P. 15-33.