УДК 330.3
DOI: 10.31732/2663-2209-2025-78-315-325

КЕРУВАННЯ РИЗИКАМИ В УПРАВЛІННІ ІТ-ПРОЄКТАМИ З ВИКОРИСТАННЯМ ІНСТРУМЕНТІВ ШТУЧНОГО ІТЕЛЕКТУ

Іван Крискун[1], Ольга Орлова-Курилова[2]

[1]Аспірант, кафедра управлінських технологій ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна, e-mail: kryskunim@krok.edu.ua, ORCID: https://orcid.org/0009-0003-9608-3604

[2]Д-р екон. наук доцент, професор кафедри інформаційного менеджменту, математики та статистики, ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна, e-mail: orlovakov@krok.edu.ua, ORCID: https://orcid.org/0000-0001-8382-8070

RISK MANAGEMENT IN IT PROJECTS USING ARTIFICIAL INTELLIGENCE TOOLS

Ivan Kryskun[1], Olga Orlova-Kurilova[2]

[1]Postgraduate student, department of management technologies, "KROK" University, Kyiv, Ukraine, e-mail: kryskunim@krok.edu.ua, ORCID: https://orcid.org/0009-0003-9608-3604

[2]PhD(Economics), Associate Professor, Professor of the Department of Information Management, Mathematics and Statistics, "KROK" University, Kyiv, Ukraine, e-mail: orlovakov@krok.edu.ua, ORCID: https://orcid.org/0000-0001-8382-8070

Анотація. *У статті досліджено особливості управління ризиками в ІТ-проєктах з використанням інструментів штучного інтелекту (ШІ). Проаналізовано останні дослідження українських та закордонних науковців які демонструють зростаючий інтерес до використання ШІ в управлінні проєктами. Зокрема, поєднання машинного, глибокого та підкріплювального навчання у Scrum підвищує точність прогнозування ризиків у гнучких проєктах, а також вказують на значну роль ШІ при діджиталізації підприємств. Визначено ключові етапи управління ризиками, на яких застосування ШІ є доцільним для підвищення точності оцінювання загроз, оперативного виявлення потенційних небезпек та вибору ефективних стратегій їх мінімізації. Особливу увагу приділено використанню алгоритмів машинного навчання, глибокого навчання та генеративного ШІ для проактивної ідентифікації ризиків, прогнозування їх наслідків та розробки рекомендацій щодо реагування. У статті наводяться практичні приклади використання ШІ в управлінні ризиками ІТ-проєктів, зокрема у методологіях Waterfall та Agile. Запропоновано застосування ШІ на етапах ідентифікації, якісної та кількісної оцінки ризиків, планування заходів реагування, моніторингу й контролю. Наведено приклади використання градієнтного бустингу, нейронних мереж і великих мовних моделей для автоматичного формування реєстрів ризиків, прогнозування ймовірності їх матеріалізації та розрахунку оптимальних резервів часу і бюджету. Розглянуто перспективи впровадження інструментів ШІ як складової сучасних підходів до управління проєктами, а також акцентовано на необхідності забезпечення прозорості алгоритмів і розвитку компетенцій персоналу для ефективної взаємодії з цими інструментами. Зроблено висновок, що інтеграція ШІ у процеси управління ризиками дає змогу перейти від реактивної до прогностично-адаптивної моделі керування проєктами, знижуючи витрати й підвищуючи ймовірність досягнення цілей у ІТ-індустрії.*

Ключові слова: *управління ризиками, ІТ-проєкти, штучний інтелект, машинне навчання, Agile, Waterfall, прогнозування ризиків.*

Формули: *0; рис.: 1; табл.: 1, бібл.: 26*

Abstract. *The article explores the specifics of risk management in IT projects through the use of artificial intelligence (AI) tools. It analyses recent studies by Ukrainian and international scholars that show a growing interest in applying AI to project management. In particular, combining machine-, deep- and reinforcement-learning techniques within Scrum has been found to improve the accuracy of risk forecasting in agile projects and to highlight AI's significant role in enterprise digitalization.*

Key risk-management stages where AI is most beneficial—enhancing threat-assessment accuracy, rapidly detecting potential hazards, and selecting effective mitigation strategies—are identified. Special attention is paid to the use of machine-learning, deep-learning and generative-AI algorithms for proactive risk identification, prediction of consequences, and development of response recommendations. The paper presents practical examples of AI-driven risk management in IT projects under both Waterfall and Agile methodologies.

AI adoption is proposed for the stages of risk identification, qualitative and quantitative assessment, response planning, monitoring and control. Illustrative cases show gradient boosting, neural networks and large language models automatically generating risk registers, forecasting the likelihood of risk materialisation, and calculating optimal time and budget reserves.

The prospects of integrating AI tools as an integral part of modern project-management approaches are considered, with emphasis on ensuring algorithmic transparency and developing staff competencies for effective collaboration with these tools. The study concludes that embedding AI into risk-management processes enables a shift from a reactive to a predictive-adaptive project-control model, reducing costs and increasing the probability of achieving objectives in the IT industry.

Keywords: *risk management, IT projects, artificial intelligence, machine learning, Agile, Waterfall, risk prediction.*

Formulas*: 0; fig.: 1; tabl.: 1; bibl.:26*

Вступ. Сучасні ІТ-проєкти характеризуються високою динамічністю та невизначеністю, що зумовлює виникнення численних ризиків, здатних негативно впливати на фінансові показники підприємств. Традиційні методи аналізу ризиків в ІТ-проєктах з ростом складності проєкту вимагають багато зусиль та можуть давати значні похибки. Застосування штучного інтелекту (ШІ) дозволить автоматизувати аналіз ризиків, прогнозувати можливі загрози та мінімізувати негативні наслідки.

Аналіз останніх досліджень та публікацій. Останні дослідження свідчать про зростаючий інтерес до використання штучного інтелекту при управлінні проєктами. Зокрема Бачинський (2024) у своєму дослідженні розглядає еволюцію використання ШІ в управлінні проєктами та аналізує приклади впровадження ШІ-інструментів в ІТ-секторі. Автор підкреслює невід'ємність ШІ як компонента сучасного управління проєктами, підкреслює здатність ШІ автоматизувати процеси, підвищувати продуктивність команди та покращувати якість управлінських рішень. Розглянуто конкретні вигоди і виклики застосування ШІ: з одного боку, технології (розумні планувальники, чат-боти, системи аналітики) - дають змогу ефективніше будувати ієрархічні структури робіт (WBS) та робити прогнозну аналітику; з іншого – існують проблеми інтеграції інструментів у традиційні методології та існує необхідність навчання персоналу працювати з ними. У висновках автор зазначає, що попри певні недоліки, тренд на впровадження ШІ в управління проєктами (особливо в ІТ-галузі) є невідворотним, рекомендує зосередити майбутні дослідження на вдосконаленні стратегій впровадження ШІ та адаптації організаційної структури під ці зміни.

Українські дослідники активно розглядають питання управління ризиками в ІТ-галузі, зокрема з допомогою методів експертної оцінки Данченко, Семко та Гайдаєнко (2022) у своїй науковій праці розглядають методи експертної оцінки для аналізу ризиків в ІТ-проєктах. Обґрунтовують можливість застосування методу «Дельфі», як одного з методів колективної експертної оцінки інформаційних ризиків в ІТ-проєктах, проаналізовані його переваги та недоліки.

Рябчиков (2024) у своїй роботі досліджує інтеграцію технологій ШІ в процеси управління ризиками в рамках гнучкої методології «Скрам». Автор аналізує різні моделі ШІ, включаючи машинне навчання, глибоке навчання (Deep learning) та навчання з підкріпленням, підкреслюючи їх потенціал для вдосконалення управління ризиками в «Скрам-проєктах». Висновки дослідження свідчать, що впровадження ШІ дозволяє проєктним командам ефективніше та точніше виявляти, оцінювати ризики. Це особливо важливо для проєктів, які використовують гнучкі методології, оскільки вони часто стикаються зі змінами в розкладі та вимогах. Завдяки ШІ команди можуть прогнозувати потенційні проблеми та розробляти стратегії їх пом'якшення, що сприяє підвищенню успішності проєктів.

Sanjay (2024) у своєму дослідженні використовує історичні данні проєктів для покращення процесів ідентифікації та управління ризиками за допомогою передбачуваної аналітики та машинного навчання. Результати дослідження показали, що модель Gradient Boosting Machine (GBM) досягла високих показників: точність 85%, точність передбачення 82%, повнота - 85% та F1-міра 80%. Ці результати перевершують

попередні моделі та свідчать про потенціал використання передбачуваної аналітики та машинного навчання для покращення управління ризиками в проєктах.

Ложачевська О.М., Орлова-Курилова О.В. та ін. (2021) у своєму дослідженні з моделювання адаптивного управління інноваційними підприємствами в умовах трансформації логістичних та маркетингових стратегій взаємодії держави та бізнесу, діджиталізації та сталого розвитку, підкреслюють на важливості діджиталізації та сталого розвитку при взаємодії держави та бізнесу.

Використання ШІ для моделювання адаптивного управління інноваційними підприємствами пришвидшить процес діджиталізації.

Постановка завдання. Метою цього дослідження є визначення етапів управління ризиками в ІТ-проєктах де доцільно використовувати інструменти ШІ. Підвищення точності оцінювання ризиків, оперативного виявлення загроз та вибору ефективних стратегій їх мінімізації. З огляду на значні обсяги даних, які генеруються під час реалізації ІТ-проєктів, існує необхідність автоматизації процесів аналізу та управління ризиками. Інструменти ШІ, що базуються на методах машинного навчання, глибокого навчання та генеративного ШІ, пропонують нові можливості для проактивної ідентифікації ризиків, прогнозування наслідків та формування рекомендацій для прийняття рішень.

Результати дослідження. Управління ризиками є важливою складовою ІТ-проєктів. Доцільно почати наше дослідження з питання, яке потребує окремого розгляду, а саме: Що ж таке ризик? На підставі декількох джерел ми з'ясували, що ризиком є невизначена подія або умова, яка, у разі настання, має позитивний або негативний вплив на одну або декілька цілей проєкту, відповідно до визначення в PMI (2021). Згідно з визначенням в ДСТУ ISO 73:2013: «ризиком є невизначеність щодо досягнення цілей». Врахування та пом'якшення таких невизначенностей на ранніх етапах може значно знизити кількість проблем під час реалізації проєкту та мінімізувати збитки. Назарова, Парасій-Вергуненко та Остапець (2021) класифікують ризики за різними категоріями. За сферою виникнення: політичні; економічні; операційні; юридичні. За рівнем впливу та наслідками: катастрофічні; критичні; високі; середні; низькі. За рівнем управління: стратегічні; тактичні.

Ризики з якими зазвичай зустрічається менеджер проєкту при реалізації програмного застосунку представлені в Таблиці 1.

Таблиця 1

Ризики пов'язані з управлінням ІТ-проєктами

Назва ризику	Опис ризику
Розширення обсягу робіт (Scope Creep)	Збільшення обсягу проєкту понад початковий план через додавання нових функцій або вимог стейкголдерів, що призводить до затримок та перевищення бюджету.
Затримка графіку виконання	Затримки у термінах виконання проєкту часто викликані неадекватним плануванням, непередбаченими технічними проблемами або невірною оцінкою тривалості завдань.
Перевитрати бюджету	Перевищення виділеного бюджету проєкту через недооцінку, зміну вимог проєкту або зовнішній вплив, що впливає на прогнози вартості.
Технологічні ризики	Ризики, пов'язані з впровадженням нових або неперевірених технологій, включаючи проблеми інтеграції, проблеми з продуктивністю або швидке старіння, які можуть перешкоджати успіху проєкту.
Ресурсні ризики	Ризики, що виникають через відсутність або неадекватність кваліфікованого персоналу, що може призвести до затримок, зниження продуктивності та погіршення результатів проєкту.

Джерело: систематизовано авторами на основі (Flyvbjerg, 2009; Kerzner, 2017; Gupta, 2023; PMI, 2021; SAP LeanIX, 2025)

Варто зазначити, що перелічені категорії не є взаємовиключними: в реальних проєктах один ризик може впливати одразу на кілька сфер. Наприклад, технологічний ризик (невдале впровадження нової технології) може спричинити фінансові втрати (перевищення бюджету на усунення проблем) та операційні збої (затримка графіку). Тому, необхідно відзначити окремо, що комплексне управління ризиками має враховувати всю різноманітність ризиків та їх вплив і взаємозв'язки.

Підхід до виявлення й обробки ризиків, значною мірою залежить від обраної методології управління проєктом. Класичні послідовні моделі (Waterfall) передбачають ретельне планування ризиків на початку проєкту. У традиційному каскадному підході команди на початку намагаються зібрати вичерпний список можливих ризикових подій, оцінити ймовірність їх виникнення та вплив (Vishal Rewari, 2024), а також розробити плани реагування на кожен суттєвий ризик. Стандарт PMI PMBOK визначає структурований процес управління ризиками, що включає планування управління ризиками, ідентифікацію ризиків, якісну та кількісну їх оцінку, планування реагування та подальший моніторинг і контроль ризиків протягом виконання проєкту (PMI, 2021). У Waterfall-проєктах на початку створюється реєстр ризиків (Risk Register) – документ, де перелічено всі виявлені ризики, їхні характеристики та стратегії протидії. Цей документ регулярно переглядається на стадіях контрольних точок (phase gate reviews), щоб перед переходом до наступної фази переконатися, що існуючі ризики під контролем і не з'явилися нові. Перевагою каскадного підходу є те, що завдяки інтенсивному аналізу на початку можна передбачити багато проблем і закласти резерви часу чи бюджету. Waterfall добре працює в умовах, коли цілі та вимоги проєкту чітко визначені й мало змінюються (Vishal Rewari, 2024). Прикладом є проєкти в аерокосмічній чи оборонній галузі, коли витрачаються роки на планування і аналіз ризиків перед побудовою систем, оскільки ціна помилки надзвичайно висока. Натомість у динамічних сферах на кшталт розробки програмного забезпечення, каскадна модель має недоліки. Спостерігається часта зміна вимог під час розробки програмного забезпечення, відкриваються нові обставини, і попередній план ризиків може стати неактуальним. Якщо під час реалізації Waterfall-проєкту виникає непередбачений ризик, вносити зміни складно і коштовно, що знижує гнучкість команди.

На противагу цьому, гнучкі методології (Agile) приділяють увагу безперервному управлінню ризиками на всіх етапах. Agile-підхід (в його різних реалізаціях – Scrum, Kanban, XP тощо) передбачає ітеративний розвиток продукту короткими циклами (спринтами), після кожного з яких проводиться оцінка отриманих результатів і коригування планів. У контексті ризиків це означає, що команда постійно шукає та обговорює нові загрози. Ризики в Agile не оформлюються окремим документом на початку, натомість їхнє виявлення та усунення інтегровано в регулярні командні активності. Зокрема, в Scrum під час кожного щоденного Стендап-мітингу (scrum daily standup) команда відстежує прогрес і перешкоди. Будь-які перешкоди можуть сигналізувати про настання ризикової події чи появу нового ризику. Планування спринту дозволяє переглянути потенційні ризики перед початком кожної ітерації, а ретроспективи наприкінці спринтів дають змогу проаналізувати, які ризики матеріалізувалися і як покращити процес, щоб уникнути їх у майбутньому (Magdalena Firlit, 2020).

У практиці реалізації Agile-проєктів існує хибна думка, ніби "гнучкі команди не потребують управління ризиками". Однак це міф: ризики притаманні будь-якому

проєкту, незалежно від підходу (Magdalena Firlit, 2020).

Фактично Scrum-команди керують ризиками, просто роблять це інакше ніж у Waterfall – менш формально, але більш постійно. Як зауважує автор Firlit (2020), при неправильному поєднанні традиційного управління ризиками з гнучкими практиками можна втратити адаптивність і прозорість, що призведе до гірших результатів. Натомість правильно організований Scrum забезпечує постійне відстеження та ескалацію ризиків внутрішньо командою, без потреби в окремому "менеджері з ризиків". Наприклад, виявлені під час спринту ризики можуть оформлюватися у вигляді задач в беклозі (як Spikes – задачі на дослідження для зменшення технічної невизначеності, або як окремі пункти плану з пом'якшення ризику). Пріоритети беклогу можуть коригуватися, якщо певний ризик стає серйозним – команда присвятить наступний спринт вирішенню проблеми або обходу ризикового аспекту. Така гнучкість дозволяє суттєво знизити сукупний ризик проєкту.

З огляду на складність сучасних IT-проєктів та велику кількість даних, які вони генерують, дедалі більшої привабливості набувають інструменти ШІ для автоматизації й удосконалення управління ризиками.

ШІ, у відповідності до визначення Баранова (2023) - це певна сукупність методів, способів, засобів та технологій, насамперед, комп'ютерних, що імітує (моделює) когнітивні функції, які мають критерії, характеристики та показники еквівалентні критеріям, характеристикам та показникам відповідних когнітивних функцій людини.

В контексті даного дослідження під ШІ пропонуємо розглядати набір інструментів на базі генеративного ШІ, глибокого та машинного навчання.

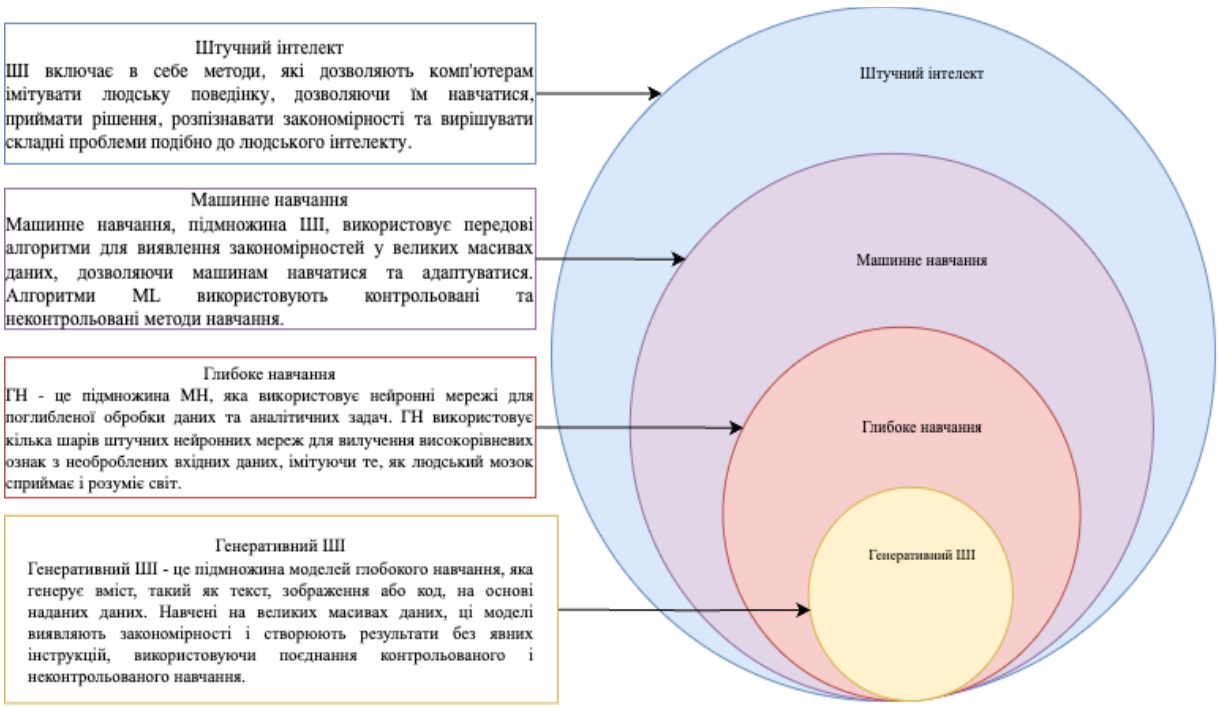

Рис. 1. Що таке штучний інтелект?

Джерело: розроблено авторами на основі праці Sussmann (2024)

Відповідно до обраної теми, представляє науковий та практичний інтерес розгляд застосування ШІ для керування ризиками. Сучасні рішення на базі ШІ здатні аналізувати інформацію з попередніх проєктів (накопичені історичні

дані про тривалість завдань, дефекти, зміни вимог, бюджети тощо) та аналізуючи дані поточного ходу робіт (стан виконання завдань, комунікації команди, метрики якості) для того, щоб заздалегідь попередити про потенційні ризики. Наукові дослідження підтверджують перспективність такого підходу. Наприклад Bauskar, Madhavaram та Galla (2024) запропонували модель машинного навчання для проактивного оцінювання ризиків проєкту на основі даних про час виконання завдань, використання ресурсів і результати минулих проєктів.

Застосування градієнтного бустингу (Gradient Boosting Machine) дозволило досягти 85% точності у прогнозуванні ризикових ситуацій (зважаючи на метрики precision/recall) – цей результат перевершив попередні моделі у дослідженні Bauskar, Madhavaram та Galla (2024).

Bauskar, Madhavaram та Galla (2024) відмічають також, що використання ШІ для оцінки ризиків дало і практичний ефект: за рахунок точніших прогнозів команда змогла ефективніше розподілити ресурси (коефіцієнт використання ресурсів зріс до 85% проти 70% при традиційних підходах) та знизити загальні витрати проєкту на 10% (порівняно з 5% економії при звичайному плануванні).

Отримані дані свідчать, що ШІ може не лише завчасно виявляти проблеми, а й пропонувати оптимальні рішення, які підвищують успішність проєктів.

Розглянемо застосування ШІ для ідентифікації ризиків. Одним з перших етапів управління ризиками є їх виявлення, вважаємо що ШІ здатен значно розширити можливості менеджера проєкту. Завдяки методам аналізу текстів та даних (NLP, data mining) ШІ може автоматично переглядати документацію проєкту, вимоги, технічні завдання, історію комунікацій (електронні листи, чати) у пошуках сигналів потенційних ризиків. Наприклад, ШІ-моделі можуть аналізувати формулювання вимог і виявляти двозначності, пропуски, що вказують на ризик непорозуміння між замовником і розробниками. Подібні інструменти здатні складати попередній список ризиків (draft Risk Register) з описами – такі можливості, зокрема, декларуються в “AI Risk Register” від компанії Raidlog, яка обіцяє ідентифікувати до 75% ризиків проєкту автоматично на основі проєктних даних. На наш погляд, подібні маркетингові заяви потребують критичної оцінки та спостереження, але тренд є очевидним: розумні алгоритми можуть швидко обробляти інформацію, недоступну для людини вручну, і висувати гіпотези про ризики.

Можна навести інший приклад, це використання генеративних моделей на кшталт ChatGPT для брейнштормінгу ризиків. Даючи великій мовній моделі опис проєкту і запит про можливі проблеми, менеджер може отримати перелік ризик-факторів, про які він міг не задуматися, з відповідними поясненнями. Як зазначається у дослідженні Центру проєктних інновацій, генеративні моделі ШІ (напр. ChatGPT, Google Gemini) виконують глибокий аналіз даних і генерують прогнози, що раніше були недосяжні для багатьох команд Center for Project Innovation (2024). ШІ може швидко переглянути величезні масиви історичних даних та вказати на фактори ризику до того, як вони стануть проблемою, що дозволить команді діяти проактивно, а не реактивно Center for Project Innovation (2024). Такий підхід підвищує шанси на успіх проєкту і знижує стрес для команди, оскільки небезпеки виявляються не в останній момент, а передбачаються заздалегідь

Розглянемо як використовується ШІ для оцінки та аналізу ризиків. Після ідентифікації ризику постає завдання оцінити його і визначити пріоритети. Класичні методи (експертна оцінка, аналіз матриці ймовірність-вплив) є суб’єктивними і залежать від досвіду менеджерів, що може призводити до похибок (Antić, 2023). ШІ натомість здатен проводити об’єктивний аналіз на основі опрацьованих даних. Зокрема, алгоритми машинного навчання можуть прогнозувати ймовірність настання певного ризику та

очікуваний розмір збитків, опираючись на статистику схожих випадків у минулому. Це дозволяє ранжувати ризики за їхнім потенційним впливом з більшою точністю. Сучасні інструменти проєктного менеджменту вже вбудовують такі можливості. Наприклад, платформа Wrike (2025) реалізувала функцію AI Project Risk Prediction, що дозволяє моніторити хід проєкту та автоматично надавати йому рівень ризику – низький, середній чи високий. Ця система машинного навчання аналізує десятки факторів: складність проєктної структури (кількість завдань, підзадач, залежностей); статистику виконання (кількість прострочених та завершених задач); завантаженість команди (скільки проєктів веде відповідальний менеджер, скільки задач на одного виконавця); активність у задачах. На основі цих даних модель на базі ШІ виводить зведений показник, який є індикатором загрози зриву дедлайнів. Цей алгоритм замінив собою колишню спрощену систему індикаторів (Project Health), яка базувалась лише на відхиленні від графіку. В результаті менеджер отримує більш комплексну оцінку ризику, враховуючи приховані тенденції (наприклад, якщо відповідальному керівнику притаманно хронічне не вкладання у терміни минулих проєктів, модель врахує цей "людський" фактор) (Wrike, 2025). Подібні рішення дозволяють виявити проблемний проєкт чи напрямок ще до того, як ситуація стане критичною. Виникає можливість вжити необхідних заходів, а саме: перерозподілити ресурси; спростити вимоги; переглянути план.

Доцільно також відмітити, що ШІ може допомогти і з якісною оцінкою ризиків, надаючи аналітичну підтримку. Наприклад, деякі системи використовують метод обробки природньої мови для аналізу описів ризиків у реєстрі, а також автоматичного присвоєння категорій або рейтингу пріоритетності. У характеристиках інструменту RAW@AI (Risk Awareness Wizard) від Risk-Academy декларується, що на основі опису ризику, наданого користувачем, є можливість визначити його тип, розбити складні ризики на компоненти та запропонувати дії з пом'якшення наслідків (RISK-ACADEMY Blog, 2024). Вказані можливості інструменту ще проходять апробацію, але вони відкривають шлях до напівавтоматичного заповнення ризикових матриць та прискорення аналізу. Інструмент може моделювати різні сценарії розвитку подій (наприклад, методи симуляції Монте-Карло знову набувають актуальності в комбінації з машинним навчанням, що краще оцінює розподіл ймовірностей на основі даних). Таким чином, прогнозована аналітика (Predictive Analytics) на базі ШІ дедалі стає частиною інструментарію керівника проєктів, що дозволяючи приймати рішення на підставі фактів та алгоритмів, а не лише інтуїції. На думку експертів, алгоритми ШІ для оцінки ризиків можуть помітно підвищити точність, швидкість ухвалення рішень у проєктах (Atlassian, 2025).

Представляє певний науковий та практичний інтерес перспективи використання ШІ для реагування на ризики та прийняття рішень. Після оцінки ризику необхідно обрати стратегію реагування: уникнення; пом'якшення; передачі чи прийняття ризику. ШІ може стати помічником на цьому етапі. По-перше, ШІ-інструменти здатні генерувати рекомендації на основі баз знань та попереднього досвіду. Наприклад, якщо виявлено ризик перевищення термінів через недооцінювання складності задачі, система може порадити розбити її на менші підзадачі або залучити додаткового розробника, спираючись на те, що такі дії допомогли в минулому у схожих проєктах. Деякі сучасні платформи керування проєктами інтегрують віртуальних помічників (чатботів) на базі ШІ, які можуть відповісти менеджеру на запитання типу: "Що я можу зробити, щоб знизити ризик X?" – використовуючи архівовані в них бібліотеки передових практик. По-друге, ШІ підтримує оптимізацію планів під наявні ризики. Існують рішення, що

автоматично коригують розклад проєкту при виникненні відхилень. Наприклад, якщо модель передбачає високий ризик зриву певного етапу, інструмент ШІ може перерахувати графік з урахуванням буферів часу чи запропонувати змінити послідовність задач, аби мінімізувати вплив проблеми.

У дослідженні виконаному Sanjay, Chandrakanth та Eswar (2024), алгоритм на основі машинного навчання фактично виконував роль системи підтримки прийняття рішень – він показував, які аспекти проєкту (час, ресурси) потрібно скоригувати, щоб досягти кращих результатів. Таким чином, ШІ не тільки сигналізує про проблему, але й допомагає знайти ефективний план дій.

Окремий напрям виокремлюється стосовно використання ШІ у вузьких доменах ризиків, наприклад, в кібербезпеці, що теж стосується ІТ-проєктів (особливо розробки ПЗ). ШІ в управлінні безпековими ризиками вже зарекомендував себе в деяких напрямках практичного застосування: сучасні системи кібербезпеки масово впроваджують машинне навчання для виявлення аномалій у трафіку; поведінкова біометрія користувачів; аналізу вразливостей. Наприклад, платформа Darktrace використовує ШІ для виявлення кібер загроз у режимі реального часу, навчаючись нормальній поведінці мережі і повідомляючи про відхилення, що можуть свідчити про атаку (Filipsson, 2025). Інша система – Balbix – застосовує ансамбль моделей ШІ для пріоритезації ризиків у кіберпросторі: вона аналізує дані про вразливості (CVE), неправильні налаштування, застаріле ПЗ та бізнес-контекст активів, щоб визначити, які з знайдених проблем становлять найбільшу загрозу для організації Babix (2025). Balbix навіть залучає великі мовні моделі (LLM) для прогнозування тактики зловмисників та визначення скільки часу залишилося до можливого використання знайденої вразливості.

Такі рішення дозволяють командам безпеки ІТ-проєктів зосередитися на найбільш критичних ризиках. Фактично ШІ виконує роль аналітика, який безперервно переглядає гори технічних даних і надає висновки: “Ось ці 5 вразливостей з 500 потребують негайного виправлення, бо становлять 90% сумарного ризику”. Для проєктного менеджера це означає можливість вчасно спрямувати зусилля команди на усунення саме тих недоліків, що можуть зірвати проєкт або призвести до інцидентів.

ШІ-інструменти для реагування на ризики охоплюють ще наступні завдання: автоматизація рутинних дій (наприклад, створення резервних копій, встановлення оновлень безпеки за розкладом); розрахунок резервів (деякі системи на основі статистики можуть порадити, який резерв бюджету чи часу закласти під конкретний ризик з потрібним рівнем надійності).

Розглянемо процеси моніторингу ризиків та навчання на основі ШІ. На етапі контролю ризиків ШІ надає можливості використання інструментів. Завдяки безперервному моніторингу проєктних метрик і зовнішніх даних, ШІ-системи можуть сигналізувати про появу нових ризиків або про зміну статусу існуючих. Наприклад, якщо команда використовує DevOps-підхід, то засоби моніторингу продуктивності та логів (APM) на базі машинного навчання здатні виявити деградацію роботи сервісу після розгортання нової версії – це свідчить про технічний ризик (помилки в коді) і дозволяє оперативно виконати повернення до стабільної версії, що дозволяє запобігти серйозному збою. Для управління проєктом корисним є те, що ШІ може агрегувати інформацію з різних джерел і надавати її у зручному вигляді: дашборди з ризик-індикаторами в реальному часі; автоматичні звіти для стейкголдерів з акцентом на топ-5 ризиків та статусі дій щодо них. Інтеграція зображувальної аналітики (наприклад, трендові графіки ризиків) і прогнозів на майбутні спринти дозволяє командам проактивно керувати ризиками. Необхідно відмітити, що ШІ може самонавчатися на основі даних проєкту. Якщо певний тип ризику

регулярно не спрацьовує (не реалізується), модель з часом знижує його пріоритет, і навпаки, часто пропущені ризики приведуть до корекції вагових коефіцієнтів алгоритму, аби наступного разу схожі сигнали не були проігноровані. Таким чином, системи управління ризиками на основі ШІ стають розумнішими з кожним проєктом, накопичуючи експертизу. За певних умов ШІ може навіть підтримувати розповсюдження кращих практик між проєктами: великі корпорації, що ведуть десятки ІТ-проєктів, можуть використовувати єдину ШІ-платформу, яка вчиться на всіх проєктах і підказує менеджерам нових команд, на що варто звернути увагу. Наприклад, якщо в компанії стартап впровадив нову бібліотеку і це спричинило серйозні проблеми, система ризик-менеджменту з ШІ може рекомендувати іншим проєктам бути обережними з тією ж технологією або принаймні включити її як окремий пункт реєстру ризиків.

Необхідно наголосити на певних обмеженнях та викликах, які виникають при застосуванні ШІ. По-перше, алгоритми машинного навчання або моделі ШІ залежать від якості й повноти даних. Якщо історичні дані проєктів містять помилки, упередження або не охоплюють нетипові випадки, моделі будуть робити хибні висновки. Є ризик надмірної впевненості у прогнозах ШІ, це означає що команда може проігнорувати інтуїцію та досвід, покладаючись на "розумну" систему, яка, не застрахована від помилок. По-друге, ШІ погано передбачає "чорних лебедів" – тобто абсолютно нові, небачені раніше ризики. Як відзначають аналітики, ШІ-моделі добре ідентифікують ті ризики, що вже траплялися у минулому, але можуть бути недостатньо ефективними у прогнозуванні принципово нових загроз (Center for Project Innovation, 2024). Якщо проєкт використовує інноваційний підхід або працює у новій сфері, статистика минулого буде не ефективною. У таких ситуаціях все одно потрібне експертне мислення та перспективне мислення від команди. По-третє, впровадження ШІ-інструментів потребує ресурсів і компетенцій. Необхідно налаштувати модель під специфіку організації, навчити персонал правильно інтерпретувати результати. Важливим також є аспект довіри – не всі менеджери готові довірити критично важливі рішення "чорному ящику" ШІ. Використання Agile (як і ШІ) само по собі не гарантує успіху, але допомагає швидше виявляти проблеми. Водночас, якщо команда ігноруватиме сигнали від ШІ, проєкт може зазнати невдачі раніше. Ця думка перегукується з принципом: технологія є інструментом, а не панацеєю. ШІ, на нашу думку, повинен доповнювати професіоналізм команди, а не заміняти його. Це підтверджується тим, що провідні компанії впроваджують ШІ-рішення поступово, паралельно направляють свої зусилля та ресурси на удосконалення процесів управління ризиками та навчання персоналу.

Висновки. Управління ризиками в ІТ-проєктах – багатогранне завдання, від правильного виконання якого залежить успіх або провал проєкту. Кожен ІТ-проєкт потребує індивідуального підходу до їх ідентифікації та мінімізації. Традиційні методології управління проєктами (Waterfall, каскадні моделі) пропонують структурований, але мало гнучкий механізм роботи з ризиками, який ефективний у стабільних умовах, проте може давати збої при швидких змінах. Натомість гнучкі методи (Agile, Scrum) вбудовують управління ризиками у щоденну роботу команди, що, значно підвищує ймовірність успіху проєкту. Кожна з методологій має свої сильні та слабкі сторони в контексті ризик-менеджменту, і на практиці часто використовується комбінація підходів, аби і передбачити більше ризиків наперед, і залишитися готовими до несподіванок.

Застосування ШІ поступово змінює парадигму керування ризиками в ІТ-проєктах. Сучасні ШІ-інструменти здатні не тільки автоматизувати рутинні аспекти (моніторинг метрик, ведення реєстру

ризиків, звітування), але й виявляти приховані тенденції та робити прогнози з точністю, недосяжною для людини. ШІ допомагає перейти від реактивної моделі (“гасіння пожеж”) до проактивної – коли потенційні проблеми прогнозуються і вирішуються ще до того, як вони вплинули на проєкт. Практичні приклади показують значний позитивний результат: від підвищення ефективності використання ресурсів і скорочення витрат до покращення показників дотримання термінів та якості. Особливо відчутний ефект ШІ має у великих портфелях проєктів і в галузях з великими даними (наприклад, кібер безпека), де людина фізично не встигне проаналізувати весь обсяг інформації. Водночас, впровадження ШІ у ризик-менеджмент висуває нові вимоги. Необхідно забезпечити якісні дані для навчання моделей, підтримувати прозорість алгоритмів (щоб пояснювати команді, чому саме той чи інший ризик визнано критичним), та не забувати про експертну оцінку. ШІ, як правило, вказує «що станеться», але рішення «що з цим робити» все ще повинно ухвалюватися людиною, враховуючи ширший контекст, етичні та стратегічні міркування. Наукові дослідження в цій галузі наразі перебувають на підйомі. Це свідчить про те, що спільнота розробників і дослідників визнає важливість проблеми та бачить перспективи в новітніх технологіях. Існує десятки комерційних продуктів і відкритих рішень, які допомагають менеджерам проєктів керувати ризиками за допомогою ШІ. Платформа на зразок Raidlog, яка забезпечує ідентифікацію більшість ризиків проєкту автоматично на основі проєктних даних. Спеціалізовані, як то Darktrace для виявлення кібер загроз. Ця розгалуженість інструментів підтверджує, що універсального рішення не існує – кожна організація обирає інструмент під свої потреби (одні зосереджені на фінансовій проблематиці, інші – на технічних загрозах чи відповідності стандартам).

ШІ значно підвищує ефективність управління ризиками в ІТ-проєктах, надаючи змогу глибшого аналізу і швидшого реагування. Він не скасовує базових принципів ризик-менеджменту, а підсилює їх. Нами відмічається що, як і раніше, потрібно ідентифікувати ризики, оцінювати їх та приймати рішення, але з ШІ ці кроки стають більш обґрунтованими і оперативними. Організації, що впроваджують ШІ для керування ризиками, отримують конкурентну перевагу у вигляді більш передбачуваних та успішних проєктів. Водночас, слід пам’ятати, що людський фактор залишається визначальним. ШІ є інструментом в руках компетентної команди. Найкращих результатів досягають ті проєкти, де поєднуються досвід і творчість людей із потужністю ШІ-аналізу. З огляду на стрімкий розвиток технологій, можна очікувати, що в недалекому майбутньому системи ШІ стануть невід’ємною частиною стандартних засобів управління проєктами, так само як сьогодні стали звичними інструменти для спільної роботи чи автоматизації розробки. Використання ШІ для управління ризиками вже зараз демонструє високу ефективність, а в перспективі – здатне трансформувати підходи до реалізації складних ІТ-проєктів, роблячи їх більш надійними та керованими в умовах невизначеності.

Література:

1. БАРАНОВ, О. А. (2023), Визначення терміну «штучний інтелект», ORCID. https://orcid.org/0000-0003-3233-6687

2.Бачинський, О. І. (2024). Використання штучного інтелекту як інструменту управління проєктами. URL: https://economyandsociety.in.ua/index.php/journal/article/download/3734/3656/ (дата звернення 09.03.2025)

3.Данченко, О. Б., & Семко, О. В. (2022). Метод експертної оцінки інформаційних ризиків в ІТ-проєктах. URL: https://er.chdtu.edu.ua/bitstream/ChSTU/4631/1/%D0%9E%D0%B4%D0%B5%D1%81%D0%B0%2022-23.pdf (дата звернення 09.03.2025)

4. Ложачевська О. М., Орлова-Курилова О. В., Макаренко Н. О., Рубежанська В. О. Моделювання адаптивного управління інноваційними підприємствами в умовах трансформації логістичних та маркетингових стратегій взаємодії держави та бізнесу, діджиталізації та сталого розвитку. Економіка та держава. 2021. № 11. С. 9–13. DOI: 10.32702/2306-6806.2021.11.9 URL:

http://www.economy.in.ua/?n=11&y=2021 (дата звернення 09.03.2025)
5. Макарчук, І. В. (2023). Управління ризиками IT-проєктів на підприємстві [Дисертація доктора філософії, Державний торговельно-економічний університет]. URL: https://knute.edu.ua/file/Mg%3D%3D/adcd9a7a02ff2aff4977bfaab4ba86ba.pdf (дата звернення 09.03.2025)
6. Назарова, К., Парасій-Вергуненко І., Остапець А. (2023). Класифікація ризиків компаній IT-індустрії. URL: https://journals.knute.edu.ua/scientia-fructuosa/article/view/1892/1757 (дата звернення 09.03.2025)
7. Рябчиков, О. М. (2024). Використання штучного інтелекту при управлінні ризиками в проєктах за методологією СКРАМ. URL: https://journals.dut.edu.ua/index.php/emb/article/view/2935 (дата звернення 09.03.2025)
8. Atlassian (2025), How to utilize AI for project management. URL: https://www.atlassian.com/work-management/project-management/ai-project-management#:~:text=Risk%20management (дата звернення 08.03.2025)
9. Babix (2025), A Smarter AI for Cyber Risk Management, URL: https://www.balbix.com/product/ai/#:~:text=Balbix%20AI%20enables%20security%20teams,the%20areas%20of%20greatest%20risk (дата звернення 09.03.2025)
10. Center for Project Innovation (2024), Embracing AI for Project Risk Management, URL: https://project.info/embracing-ai-for-project-risk-management/
11. Center for Project Innovation (2024), URL: https://project.info/embracing-ai-for-project-risk-management/
12. Flyvbjerg, B. (2009). Survival of the unfittest: Why the worst projects often fail. International Journal of Project Management, 27(4), 431–443. URL: https://www.researchgate.net/publication/46511516_Survival_of_the_Unfittest_Why_the_Worst_Infrastructure_Gets_Built_-_And_What_We_Can_Do_About_It
13. Filipsson, F. (2025), Top 10 AI tools for risk assessment and management, URL: https://redresscompliance.com/top-10-ai-tools-for-risk-assessment-and-management/#:~:text=,commerce%20risk%20management%2C%20fraud%20prevention (дата звернення 09.03.2025)
14. Raynus, J. (2025). Integrating AI with Project Management. URL: https://amsconsulting.com/articles/integrating-ai-with-project-management/ (дата звернення 16.02.2025)
15. Antić, K. (2023), URL: Implementing artificial intelligence tools for risk management in software projects. DOI: 10.5937/tehnika2306735A
16. Kerzner, H. (2017). *Project Management: A Systems Approach to Planning, Scheduling, and Controlling* (12th ed.). Hoboken, NJ: Wiley.
17. Magdalena Firlit (2020), Managing Risk with Scrum. URL: https://www.scrum.org/resources/blog/managing-risk-scrum#:~:text=Myth (дата звернення 16.02.2025)
18. Gupta, M. (2023). 6 Effective Ways to Mitigate Resource Risks in Project Management. URL: https://www.projecttimes.com/articles/6-effective-ways-to-mitigate-resource-risks-in-project-management/ (дата звернення 16.02.2025)
19. Sussmann, M. (2024), “What are the differences between artificial intelligence, machine learning, deep learning and generative AI?”, URL: https://www.sumologic.com/blog/machine-learning-deep-learning/ (дата звернення 08.03.2025)
20. Project Management Institute. (2021). A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition. Newtown Square, PA: Project Management Institute.
21. Raidlog, The world’s first AI powered Risk Register. URL: https://raidlog.com/ai/ (дата звернення 08.03.2025)
22. RISK-ACADEMY Blog (2024), Controversial thoughts about modern day risk management in non-financial companies, training and consulting services. URL: https://riskacademy.blog/risk-management-ai/#:~:text=Risk%20Assessment%20,suggest%20mitigations%2C%20write%20risk (дата звернення 08.03.2025)
23. Sanjay Ramdas Bauskar, Chandrakanth Rao Madhavaram, Eswar Prasad Galla (2024), Predictive Analytics for Project Risk Management Using Machine Learning. URL: https://www.scirp.org/journal/paperinformation?paperid=137197#:~:text=current%20work%20proposes%20a%20new,demonstrate%20that%20the%20Gradient%20Boosting (дата звернення 08.03.2025)
24. SAP LeanIX (2025). Technology Risk Management. URL: https://www.leanix.net/en/wiki/trm/technology-risk-management (дата звернення 16.02.2025)
25. Vishal Rewari (2024), Agile vs Waterfall: Risk Management Compared. URL: https://optiblack.com/insights/agile-vs-waterfall-risk-management-compared#:~:text=match%20at%20L146%20In%20Waterfall%2C,Teams%20aim%20to (дата звернення 08.03.2025)
26. Wrike, AI Project Risk Prediction. URL: https://help.wrike.com/hc/en-us/articles/360055046934-AI-Project-Risk-Prediction#:~:text=AI%20Project%20Risk%20Prediction%C2%A0monitors%20your,based%20reports (дата звернення 08.03.2025)