

<https://doi.org/10.31891/2307-5740-2025-348-6-61>

УДК 338.47:005.591.6:004.8

ВОЛІКОВ Володимир

Інститут монокристалів Національної академії наук України

<https://orcid.org/0000-0002-4107-6277>e-mail: valdemar12@meta.ua

ПАНЧЕНКО Ігор

Valera Logistics Inc.

<https://orcid.org/0009-0006-3449-9614>e-mail: cruze5823@gmail.com

МЕТОДИЧНИЙ ПІДХІД ДО ОЦІНКИ ІННОВАЦІЙНИХ РИЗИКІВ ІНТЕГРАЦІЇ СИСТЕМ ШІ (ADAS/CMS) У ДІЯЛЬНІСТЬ ТРАНСПОРТНИХ ПІДПРИЄМСТВ

У статті обґрунтовано методичний підхід до оцінки інноваційних ризиків, що виникають при інтеграції систем штучного інтелекту (ADAS/CMS) у діяльність вітчизняних транспортних підприємств, який складається з чотирьох етапів: 1) підготовка та встановлення контексту; 2) ідентифікація та класифікація ризиків; 3) оцінка та аналіз ризиків; 4) пом'якшення, моніторинг та вдосконалення стратегії. Здійснено систематизацію та типізацію ключових ризиків інтеграції систем ШІ за шістьма категоріями, що охоплюють такі аспекти: технологічні, операційні, кібербезпекові, юридичні та страхові, етичні та соціальні, фінансові. Валідацію підходу здійснено через сценарне моделювання SCRAM та експертний метод. Встановлено, що найбільшу загрозу становлять кібербезпекові, фінансові, а також юридичні та страхові ризики, тоді як етичні та соціальні ризики мають помірний, але динамічний характер і потребують постійного моніторингу. Розроблені стратегії мінімізації ризиків включають технічні, організаційні, нормативні та соціальні заходи, які забезпечують зниження рівня загроз до керованих значень. Запропонований методичний підхід є універсальним і може бути адаптований до різних типів вітчизняних транспортних підприємств, з різним рівнем автоматизації та стадіями впровадження систем штучного інтелекту.

Ключові слова: інноваційні ризики, управління ризиками, штучний інтелект, ADAS, CMS, транспортні підприємства, сценарний підхід, цифровізація.

VOLIKOV Volodymyr

Institute for Single Crystals of National Academy of Sciences of Ukraine

PANCHENKO Ihor

Valera Logistics Inc.

METHODOLOGICAL APPROACH TO THE ASSESSMENT OF INNOVATION RISKS IN THE INTEGRATION OF AI SYSTEMS (ADAS/CMS) INTO THE OPERATIONS OF TRANSPORT ENTERPRISES

The article substantiates a methodological approach to assessing innovation risks arising from the integration of Artificial Intelligence systems (ADAS/CMS) into the operations of domestic transport enterprises. The approach consists of four stages: 1) preparation and context establishment; 2) risk identification and classification; 3) risk assessment and analysis; 4) mitigation, monitoring, and strategy refinement. The study provides a systematization and categorization of key AI integration risks into six categories: technological (technical aspects of AI functioning, including component, algorithm, and integration reliability); operational (risks arising from AI-human interaction and enterprise processes); cybersecurity (threats of external interference affecting data integrity, control, and AI system confidentiality); legal and insurance (regulatory compliance, liability, and financial protection mechanisms); ethical and social (moral, societal, and psychological aspects, including bias and AI perception); and financial (economic aspects of AI implementation and operation). The dynamic risk assessment matrix is built as a 5x5 grid, taking into account the specifics of enterprises, such as: operational resilience, interaction with infrastructure and stakeholders. The approach was validated using SCRAM scenario modeling and expert methods. It was established that cybersecurity, financial, legal, and insurance risks pose the greatest threat, while ethical and social risks are moderate yet dynamic, requiring continuous monitoring. The developed risk mitigation strategies include technical, organizational, regulatory, and social measures that ensure the reduction of threat levels to manageable values. The proposed methodological approach is universal and can be adapted to various types of domestic transport enterprises with different levels of automation and stages of AI system implementation.

Keywords: innovative risks, risk management, artificial intelligence, ADAS, CMS, transport enterprises, scenario approach, digitalization.

Стаття надійшла до редакції / Received 01.11.2025

Прийнята до друку / Accepted 02.12.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Стрімкий розвиток цифрових технологій обумовлює інтеграцію інтелектуальних систем у діяльність автотранспортних підприємств. Застосування штучного інтелекту (ШІ) у складі автоматизованих систем допомоги водію ADAS (англ. Advanced Driver Assistance Systems) сприяє підвищенню безпеки дорожнього руху, ефективності експлуатації транспортних засобів, оптимізації логістичних процесів та покращенню екологічної ситуації в Україні. Важливим елементом цифрових технологій допомоги водію є системи моніторингу за допомогою камер – CMS (англ. Camera Monitoring System). Застосування таких технологій

дозволяє користувачам спостерігати за подіями навколо транспортного засобу на моніторі і зберігати записи на різних матеріальних носіях, що можуть бути електронними доказами в суді [1]. Водночас інтеграція систем ШІ у діяльність вітчизняних транспортних підприємств супроводжується багатоаспектними інноваційними ризиками, які охоплюють технологічну, операційну, кібербезпекову, юридичну, етичну та фінансову сфери.

Особливої актуальності проблема ідентифікації та оцінки інноваційних ризиків набуває в умовах високого рівня цифровізації транспортної галузі, забезпеченні кібербезпеки, нормативної невизначеності та правової відповідальності, розширення зобов'язань страхових компаній, виникненні нових етичних аспектів та обмеженості ресурсів.

У цьому контексті виникає необхідність розроблення методичного підходу до оцінки ризиків інтеграції систем ШІ (ADAS/CMS) у діяльність вітчизняних транспортних підприємств, який поєднує міжнародні стандарти управління ризиками, сценарне моделювання та експертне оцінювання.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Широкомасштабне впровадження систем ШІ на транспорті нерозривно пов'язано з процесом загальної цифровізації і допомагає мінімізувати кількість помилок водія завдяки здатності аналізувати величезні обсяги даних у реальному часі. Людський чинник (втома, емоції, неувважність тощо) є ключовим у виникненні аварійних ситуацій. Д. Кульова та ін. виокремили найбільш критичні порушення та провели оцінювання ризиків як передумови виникнення дорожньо-транспортної пригоди (ДТП) з вини водія [2].

Аналіз наукової літератури та міжнародних звітів у транспортній сфері свідчить про активну розробку регуляторних рамок та методологічних підходів до управління ризиками, пов'язаними з широкомасштабним впровадженням ШІ та ADAS/CMS на транспорті. Ori Igwe [3] досліджує правові проблеми, що виникають через стрімке впровадження технологій ШІ на глобальному рівні. Babatunde O. та ін. [4] діляться міжнародним правовим досвідом стосовно підходів до регулювання ШІ урядами США, Канади, Австралії та інших країн світу для зменшення потенційної шкоди від його використання та визначають інфраструктурні й регуляторні бар'єри для систем ланцюгів поставок на основі ШІ. Принципи та практичні рекомендації щодо впровадження ШІ на транспорті наведено в матеріалах Міжнародного транспортного форуму (2025) і підкреслено важливість управління ризиками, що передбачає: оцінку, пом'якшення та безпечне застосування ШІ до, під час і після впровадження. Інтеграція систем ШІ має базуватися на економічній доцільності, соціальній обґрунтованості та технологічній ефективності [5]. В. Самсонкін та ін. аналізують вплив кризових ситуацій на діяльність транспортних підприємств та шляхи підвищення їх стійкості [6]. В роботі [7] визначено основні чинники ризику інтеграції ШІ на морському транспорті це: сумісність існуючої інфраструктури, якість вихідних даних та регуляторні питання. Тарашевський М. наводить систематизовану класифікацію ризиків діяльності транспортних підприємств [8]. Zaidan E. та Ibrahim I.A. акцентують увагу на регуляторних проблемах в суспільстві, пов'язаних з впровадженням ШІ, досліджуючи ці аспекти в контексті глобального управління [9].

В ЄС для врегулювання використання ШІ та управління ризиками, пов'язаними з ними, було прийнято Акт про ШІ (англ. AI Act – Artificial Intelligence Act) [10], який класифікує системи за чотирма рівнями ризику: неприйнятний, високий, обмежений, мінімальний [11]. Всесвітня дорожня асоціація (англ. PIARC – Permanent International Association of Road Congresses) у звіті за 2023 р. наводить процес управління ризиками та пропонує застосовувати стандартизовані підходи до їх оцінки згідно міжнародних стандартів [12]. Організація економічного співробітництва та розвитку (англ. OECD – Organisation for Economic Co-operation and Development) у своєму звіті представляє структуру управління ризиками ШІ та систематичний спосіб управління ризиками «надійного ШІ» [13].

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Попри наявність значного світового досвіду впровадження інтелектуальних систем в транспортному секторі, існуючі рішення, пов'язані з інтеграцією систем ШІ (ADAS/CMS), не є універсальними та потребують адаптації цих моделей управління ризиками до специфічних умов України.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою статті є розробка та обґрунтування методичного підходу до кількісної та якісної оцінки інноваційних ризиків, виникаючих при інтеграції інтелектуальних систем ШІ (ADAS/CMS) в роботу вітчизняних транспортних підприємств та формування ефективних стратегій мінімізації цих ризиків.

Досягнення поставленої мети передбачає наступні завдання: систематизацію ризиків за ключовими категоріями, визначення рівнів їх критичності та формування практично орієнтованих стратегій управління ризиками в умовах цифрової трансформації транспортного сектору.

Обґрунтування методичного підходу базується на системі методів, що дозволяють комплексно дослідити ризики інтеграції штучного інтелекту. Контент-аналіз та порівняльний метод застосовано для класифікації ризиків. Шляхом індуктивного узагальнення кейсів та дедуктивної адаптації стандартів ISO сформовано теоретико-прикладний базис дослідження. Метод синтезу застосовано для інтеграції розрізнених

показників у цілісну модель, де ранжування загроз реалізовано через матричний аналіз. Валідацію результатів здійснено за допомогою сценарного підходу SCRAM та експертного методу.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

На Міжнародному транспортному форумі визначено основні напрями застосування ІІІ в транспортному секторі, які згруповано за п'ятьма метакатегоріями: 1) управління клієнтами; 2) експлуатація транспортних засобів; 3) стійкість транспорту; 4) управління мережею; 5) управління інфраструктурою. Для оцінки рівня можливостей ІІІ у порівнянні з людською продуктивністю було застосовано індикатори зі шкалою від 1 до 5 (де 1 – нижчий рівень, 5 – вищий рівень) та отримано наступний результат: мова – 3, соціальна взаємодія – 2, розв'язання проблем – 2, креативність – 3, метапізнання та критичне мислення – 2, знання, навчання та пам'ять – 3, зір – 3, маніпуляції – 2, роботизований інтелект – 2 [5, с. 34-35].

Інтеграція ІІІ приносить багато переваг при експлуатації інтелектуальних систем: економічне зростання; покращення продуктивності; підвищення комфорту, ефективності та безпеки; сталий розвиток; зростання результативності у сферах охорони здоров'я та освіти тощо. Проте створюються певні ризики для міжнародної спільноти, пов'язані з технологічною безпекою та правовим регулювання цього процесу, а саме: втрата робочих місць; соціальна нестабільність у сферах охорони здоров'я та розваг і фінансовому секторі; використання ІІІ як зброї; втрачання підзвітності та прозорості процесів; «алгоритмічне упередження», порушення конфіденційних даних та кіберзагроза; залежність людини від технологій; дезінформація та маніпуляція; вплив на критичну інфраструктуру через віруси та ін. З огляду на це критично важливим є створення структури світового рівня для міжнародного інституційного управління ІІІ з урахуванням ризиків його інтеграції в інтелектуальні системи, що передбачає розробку спільних стандартів та створення універсальних інструментів для запобігання руйнівних наслідків. Ефективне управління інтелектуальними системами необхідно здійснювати на основі застосування принципів, які зміцнюватимуть довіру до ІІІ, а саме: «людський нагляд, розуміння та етичні міркування» [9, с. 2].

Система ІІІ – «... це машинна система, яка для явних чи неявних цілей робить висновок на основі отриманих вхідних даних, як генерувати результати, такі як прогнози, контент, рекомендації або рішення, які можуть впливати на фізичне або віртуальне середовище. Різні системи ІІІ відрізняються рівнем автономності та адаптивності після розгортання» [5, с. 4]. «Надійний ІІІ» це системи, що працюють відповідно до основних принципів ІІІ ОЕСД: «принесення користі людям та планеті», «цінності та справедливості», «орієнтації на людину», «прозорості та пояснювання людині результату ІІІ», «надійності, безпеки та захисту», «підзвітності». При цьому життєвий цикл системи ІІІ включає такі фази: планування, проектування, збір даних, створення моделі, верифікація, валідація, розгортання та моніторинг, кожна з яких вимагає використання специфічних підходів до оцінки ризиків [13, с. 17-20]. Типологія ризиків, яку застосовує PIARC [12; 14], базується на міжнародних стандартах (ISO 31000, ISO 28000, ISO 27000), адаптована до специфіки транспортного сектору та вміщує загальні рамки ризик-менеджменту з наступними елементами: дорожня інфраструктура, транспортні системи, логістика, інтелектуальні транспортні системи, автоматизовані транспортні засоби, вантажні перевезення (в т.ч. небезпечні вантажі) та загрози, кібератаки, тероризм, вандалізм і пандемії. О. Горецький визначає групи чинників ризику ДТП на автомобільному транспорті що впливають на: 1) «рівень ризику»; 2) «ймовірність потрапляння в аварію»; 3) «важкість аварії»; 4) «важкість посттравматичних ускладнень» [6, с. 181]. Тарашевський М. наводить основні принципи управління ризиками транспортних підприємств це: «... системності, інтегрованості, гнучкості, динамічності, інформаційного забезпечення, безперервності, ефективності» [8, с. 155].

Jonas Schuett зазначає, що «систему управління ризиками необхідно створити, впровадити, задокументувати та підтримувати» і пропонує наступні визначення: «система управління ризиками вважається: **«створеною»**, якщо політики, процедури та інструкції з управління ризиками створені та затверджені відповідальними особами, що приймають рішення... **«впровадженою»**, якщо вона впроваджена на практиці (тобто відповідні працівники розуміють, чого від них очікують, і діють відповідно) ... **«задокументованою»**, якщо система описана систематично та впорядковано у формі письмових політик, процедур та інструкцій та може бути продемонстрована на запит національного компетентного органу... **«підтримуваною»**, якщо її регулярно переглядають та, за необхідності, оновлюють». Визначення та аналіз ризиків має обмежуватись «відомими та передбачуваними ризиками» при цьому «Ризик – це поєднання ймовірності виникнення шкоди та тяжкості цієї шкоди», тоді як «шкода означає будь-який негативний вплив на здоров'я, безпеку та основні права ... «ймовірність виникнення шкоди» є «функцією впливу небезпеки, виникнення небезпечної події, [та] можливостей уникнути або обмежити шкоду ... Ризик вважається «відомим», якщо шкода сталася в минулому або неодмінно виникне в майбутньому ... Ризик є «передбачуваним», якщо він ще не стався, але вже може бути ідентифікований» [10, с. 8-9]. Тарашевський М. зазначає, що в міжнародних стандартах при визначенні сутності ризиків використовуються такі категорії, як: «... ймовірність, потенційна подія, що може бути джерелом ризику у вигляді загрози, небезпеки, можливості, та наслідки впливу на цілі, кінцеві результати діяльності» [8, с. 36].

В основу структурованого процесу управління ризиками, наведеного в звіті PIARC [12, с. 16], закладено ітеративний підхід до ідентифікації, оцінки та зменшення впливу ризиків в транспортних системах.

Циклічна модель передбачає постійне вдосконалення, засноване на зворотному зв'язку від ключових кроків, а інтеграція таких елементів як комунікація, консультації, моніторинг та перегляд забезпечують адаптивність системи до загроз, пов'язаних з кримінальними діями або тероризмом. Блок-схема вміщує три основні компоненти: 1) встановлення контенту (розуміння зовнішнього середовища та внутрішніх факторів); 2) оцінка ризику (ідентифікація, аналіз, оцінка); 3) обробка ризику (уникнення, пом'якшення, передача або прийняття).

Аналіз досвіду Нігерії у порівнянні з США демонструє уповільнену інтеграцію і низьку ефективність використання інтелектуальних систем в країнах, які розвиваються та успішність в розвинених країнах, що доводить необхідність оцінки інфраструктури, нормативної бази та готовності персоналу ще до початку інтеграції ШІ. Ступінь ризиків та ефективність роботи ШІ залежить від розвиненості «екосистеми», яка вміщує: дані, цифрову та транспортну інфраструктуру, стандарти, кіберзахист, людські ресурси тощо. Babatunde O. та ін. доводять, що визначальним для успішності використання інтелектуальних систем є «зрілість екосистеми», в якій першорядним є навички та людський капітал, що забезпечується наявністю та доступністю певних фахівців. Ключові бар'єри, які уповільнюють інтеграцію ШІ наступні: 1) інфраструктурні: технологічна інфраструктура; транспортна та логістична інфраструктура; доступність даних та цифровізація; 2) регуляторні: правові та політичні рамки для ШІ; торговельні та митні правила; стандарти та відповідність [4, с. 158-163].

Для забезпечення громадської безпеки та дотримання законодавства застосовуються інструменти на базі ШІ, прикладом яких є «сценарний підхід до оцінки регуляторних ризиків та ризиків справедливості в системах спостереження за допомогою штучного інтелекту» (англ. SCRAM – Scenario-based Compliance and Risk Assessment Model). Ця модель використовує наступні критерії відповідності: законність, обмеження цілей, мінімізацію даних, точність даних та термін зберігання, тоді як метрики упередженості включають статистичну різницю паритету та коефіцієнт дисперсного впливу. Для обробки системного налаштування SCRAM застосовує дерево рішень з чотирьох етапів: 1) рівень відповідності; 2) рівень продуктивності; 3) шар зміщення; 4) рівень політики [15, с. 9-10].

Інтеграція ШІ у діяльність вітчизняних транспортних підприємств сприятиме підвищенню їхньої безпеки, ефективності та стійкості. Однак такі технології є високоризикованими, оскільки пов'язані з невизначеністю алгоритмів, залежністю від якісних даних, кіберзагрозами та нормативно-правовими прогалинами, що потребує системного управління ризиками. При цьому «оцінка переваг використання технології штучного інтелекту та її придатності для використання повинна проводитися разом з оцінкою її впливу та потенційних ризиків» [5, с. 5]. Якщо за оцінкою ризику, пов'язані із застосуванням певної технології, об'єктивно переважають потенційну її користь, виправданим кроком є застосування запобіжного заходу у вигляді призупинення або жорсткого лімітування її експлуатації [3, с. 3]. Як зазначено в матеріалах Міжнародного транспортного форуму «іноді не використовувати ШІ – це правильний вибір» [5, с. 3].

Адаптований до українських умов запропонований методичний підхід до оцінки інноваційних ризиків інтеграції систем ШІ (ADAS/CMS) у діяльність транспортних підприємств враховує ISO 26262, ISO 31000, ISO 28000, етапи RIAM (Risk Identification, Assessment, Mitigation), рекомендації PIARC та Міжнародного транспортного форуму, а також сучасні підходи сценарно-рамкової оцінки ризиків SCRAM. Побудовано методичний підхід як послідовність чотирьох взаємопов'язаних етапів: 1) підготовка та встановлення контексту; 2) ідентифікація та класифікація ризиків; 3) оцінка та аналіз ризиків; 4) пом'якшення, моніторинг та вдосконалення стратегії. На основі аналізу, ключові ризики інтеграції ШІ (ADAS/CMS) у транспортному секторі класифіковано за категоріями (табл. 1).

Таблиця 1

Категорії ризиків інтеграції ШІ в транспортному секторі

Код ризику	Категорії ризику	Опис	Оцінка	Заходи пом'якшення
R1	Технологічні	Збої алгоритмів, деградація сенсорів CMS	Висока ймовірність у складних умовах; вплив: ДТП.	Сенсорна ф'южн (англ. sensor fusion), тестування за ISO 26262, резервні модулі.
R2	Операційні	Зміна процесів, взаємодія людини-ШІ (неуважність).	Середня; вплив: зниження продуктивності.	Програми навчання, людино-машинний інтерфейс, моніторинг поведінки.
R3	Кібербезпекові	Несанкціонований доступ до даних та порушення їх цілісності.	Зростаюча; вплив: масові інциденти.	Шифрування, ISO 27001, регулярні оновлення.
R4	Юридичні та страхові	Невизначеність відповідальності, регуляторні зміни.	Низька, але критична; вплив: штрафи.	Контракти, моніторинг стандартів, страхування.
R5	Етичні та соціальні	Упередження в ШІ (англ. Bias in AI), опір автоматизації.	Середня; вплив: соціальні конфлікти.	Етичний аудит, громадські консультації, інклюзивні дані.
R6	Фінансові	Високі витрати на інтеграцію, невизначений ROI.	Висока; вплив: втрати.	Аналіз ROI, диверсифікація, моделювання сценаріїв.

Складено авторами за [2; 5; 6; 8; 9; 12; 13; 15]

Для проведення комплексного аналізу інноваційні ризики, пов'язані з інтеграцією ШІ (табл. 1) у діяльність вітчизняних транспортних підприємств, класифіковано на шість основних категорій: R1 (критичні для безпеки та мають високий вплив) – ризики, пов'язані з технічними аспектами функціонування ШІ, зокрема, ненадійність компонентів, алгоритмів та інтеграції; R2 (мають середній вплив, але можуть накопичуватись) – ризики, що виникають в процесі взаємодії ШІ з людиною та процесами на підприємстві; R3 (критичні для безпеки та мають високий вплив) – ризики, пов'язані з зовнішнім втручанням, що загрожують цілісності даних, контролю та конфіденційності систем ШІ; R4 (вплив критичний на етапі інтеграції ШІ) – ризики, пов'язані з регуляторними нормами, відповідальністю та фінансовими механізмами захисту (страхування); R5 (вплив середній але є загроза відмови від інновацій) – ризики, стосуються моральних, суспільних та психологічних аспектів використання ШІ, включаючи упередження та сприйняття технологій ШІ; R6 (вплив високий, впливає на прибутковість) – ризики, пов'язані з економічними аспектами впровадження та експлуатації ШІ.

Побудовану матрицю для методичного підходу оцінки інноваційних ризиків інтеграції систем ШІ (ADAS/CMS) наведено в таблиці 2.

Таблиця 2

Матриця оцінки ризиків «ризик-ймовірність-вплив»

Ймовірність, бал	Вплив, бал				
	1 - незначний	2 - легкий	3 - суттєвий	4 - критичний	5 - катастрофічний
5 - дуже висока	Помірний	Помірний	Високий	Дуже високий	Критичний
4 - висока	Низький	Помірний	Високий	Дуже високий	Критичний
3 - середня	Низький	Помірний	Помірний	Високий	Дуже високий
2 - низька	Дуже низький	Низький	Помірний	Високий	Дуже високий
1 - дуже низька	Дуже низький	Дуже низький	Низький	Помірний	Високий

Складено авторами за [2; 5; 6; 8; 9; 12; 13; 15]

Динамічну матрицю (табл. 2) побудовано як сітку 5x5, що враховує особливості підприємств, такі як: операційна стійкість, взаємодія з інфраструктурою та стейкхолдерами (водії, регулятори, постачальники). Оцінка ймовірності настання ризику за вертикальною віссю здійснюється за шкалою градації: дуже низька (до 5 % – 1 бал), низька (5–15 % – 2 бали), середня (16–35 % – 3 бали), висока (36–60 % – 4 бали) та дуже висока (понад 60 % – 5 балів). Горизонтальна вісь (вплив) оцінює рівень наслідку від ризику: незначний – мінімальний вплив без втрат (1 бал); легкий – локальні збої, незначні витрати (2 бали); суттєвий – потребує втручання менеджменту (3 бали); критичний – відчутні економічні чи операційні збитки (4 бали); катастрофічний – загроза безпеці існування, великі втрати, іміджеві ризики (5 балів).

Для валідації моделі, у контексті українських реалій, було залучено 12 експертів з досвідом в галузі понад 5 років, а саме: менеджери транспортних підприємств – 3; інженери з експлуатації та обслуговування інтелектуальних транспортних систем – 3; IT-фахівці – 3; представники страхових компаній – 3. Експерти оцінювали шість категорій ризиків (R1; R2; R3; R4; R5; R6) за 5-ти бальною шкалою Лайкерта (табл. 3).

Таблиця 3

Середні експертні оцінки ймовірності та наслідків

Код ризику	Ймовірність (P)	Наслідки (C)	Інтегральний ризик $R = P \times C$	Рівень
R1	3,2	4,5	14,4	Високий
R2	4,2	3,4	14,3	Високий
R3	3,3	4,7	15,5	Дуже високий
R4	4,6	4,1	18,9	Критичний
R5	2,9	3,8	11,0	Помірний
R6	4,5	3,9	17,6	Дуже високий

Складено авторами.

Узагальнені результати опитування експертів стосовно актуальності категорій ризиків та ефективності стратегій з відкритими запитаннями для коментарів наведено в таблиці 4.

Таблиця 4

Актуальність ризиків та ефективність стратегій

Код ризику	Актуальність (середня оцінка / SD)	Ефективність стратегій (середня оцінка / SD)	Ключові коментарі експертів
1	2	3	4
R1	4,5 / 0,4	4,1 / 0,5	Висока актуальність через кліматичні умови, сфокусуватись на резервних системах.
R2	4,2 / 0,3	4,3 / 0,4	Потреба в локалізованому навчанні; ефективність застосування людино-машинного інтерфейсу висока, але потребує значних інвестицій.
R3	4,7 / 0,2	3,9 / 0,4	Актуальність найвища через зростання кібератак; стратегії кібербезпеки ефективні, але бар'єром для малих підприємств є висока вартість.

1	2	3	4
R4	3,9 / 0,5	4,1 / 0,5	Невизначеність нормативної бази в Україні; пропонується партнерство з державними органами.
R5	3,8 / 0,4	3,9 / 0,6	Найнижча актуальність, проте важливі для репутації.
R6	4,3 / 0,3	4,3 / 0,4	Висока через економічну та політичну нестабільність; залучати міжнародні гранти.
Загальна середня	4,2 / 0,4	4,1 / 0,5	Модель релевантна, але потребує адаптації під локальні бюджети.

Складено авторами.

Інтерпретацію значень стандартного відхилення (SD) здійснено за наступною шкалою: низький рівень розкиду думок – $0 \leq SD \leq 0,5$; середній – $0,5 < SD \leq 1,0$; високий – $SD > 1,0$. Отримані низькі значення стандартного відхилення свідчать про високий ступінь консенсусу в оцінках експертів та підтверджують статистичну достовірність результатів дослідження.

На основі проведеного аналізу та оцінювання ризиків щодо інтеграції систем III (ADAS/CMS) у діяльність гіпотетичного транспортного підприємства для їх мінімізації розроблено відповідні заходи (табл. 5).

Таблиця 5

Матриця оцінки ризиків та стратегії їх мінімізації

Код ризику	Рівень ризику	Заходи з мінімізації ризиків
R1	Високий	<i>Запобіжні заходи:</i> 1) багаторівнева сенсорна надмірність; 2) валідація моделей III; 3) периферійна обробка (англ. Edge processing); 4) впровадження відмовостійких архітектур. <i>Коригувальні заходи:</i> 1) оновлення прошивки (мікропрограми) та моделей машинного навчання; 2) регламентне калібрування сенсорних систем; 3) моніторинг помилок людино-машинного інтерфейсу та усунення некоректних попереджень. <i>Стимульовані заходи:</i> 1) обмеження функціональності ADAS у складних погодних умовах; 2) застосування системи моніторингу технічних ризиків в режимі реального часу; 3) застосування захищених каналів передачі даних.
R2	Високий	<i>Запобіжні заходи:</i> 1) стандартизація операційних процедур; 2) навчання персоналу за комплексною системою; 3) проєктування людино-машинного інтерфейсу з акцентом на зниження когнітивного навантаження водія; 4) підтримка актуальності інфраструктурної інформації. <i>Коригувальні заходи:</i> 1) моніторинг експлуатаційних інцидентів з автоматичним формуванням звітів; 2) калібрування ADAS за даними експлуатації; 3) моніторинг когнітивної відповідності водіїв людино-машинного інтерфейсу. <i>Стимульовані заходи:</i> 1) диференціація роботи ADAS залежно від зовнішніх умов; 2) регламентація самостійності III в антропоцентричних процесах; 3) тривале верифікація рішень: водій – III – диспетчер.
R3	Дуже високий	<i>Запобіжні заходи (пріоритет — негайне впровадження):</i> 1) архітектурна ізоляція критичних систем керування від сервісних інтерфейсів; 2) наскрізне шифрування телематики з динамічною ротацією ключів; 3) Реалізація архітектури нульової довіри (англ. ZTA - Zero-Trust Architecture) у транспортній інфраструктурі; 4) Апаратна верифікація OTA-оновлень (англ. OTA - Over-the-Air) на базі TPM (англ. Trusted Platform Module); 5) реал-тайм детекція аномалій у сенсорних мережах та III-алгоритмах; 6) регламентація доступу контрагентів на засадах JIT-парадигми (англ. JIT - just-in-time). <i>Коригувальні заходи:</i> 1) резервування архітектурних компонентів керування та зв'язку; 2) диференційована деградація архітектури керування в умовах деструктивних кібервпливів; 3) сегментація серверної інфраструктури та механізми інкрементного відновлення даних. <i>Стимульовані заходи:</i> 1) Інтеграція транспортного «центра операцій безпеки» для верифікації телеметрії критичних систем керування; 2) валідація резистентності алгоритмів III методами імітації атак; 3) страхування кіберзагроз у системах із III.
R4	Критичний	<i>Запобіжні заходи.</i> Юридичні: 1) регламентація деліктної відповідальності суб'єктів експлуатації та виробництва; 2) сертифікація ADAS/CMS відповідно до міжнародних стандартів; 3) регламентація життєвого циклу систем: експлуатація, оновлення, тестування; 4) Гармонізація процесів обробки даних із вимогами GDPR (General Data Protection Regulation) та національного законодавства. Страхові: 1) адаптація страхових контрактів до умов функціонування інфраструктури III; 2) конвергенція кіберстрахування та страхування технологічних ризиків; 3) уніфікація протоколів збору доказової бази для страхових інцидентів; 4) інтеграція моніторингу технічного стану ADAS/CMS у страхові регламенти. <i>Компенсаційні заходи:</i> 1) впровадження протоколів резервної верифікації рішень III; 2) Реалізація дубльованих каналів ресстрації інцидентів (ADAS-log та телеметрія); 3) Реалізація принципу Legal-by-design у процесах системного оновлення. <i>Стимульовані заходи:</i> 1) періодичний юридичний аудит із застосуванням комплаєнс-стрес-тестування; 2) навчання персоналу щодо правового супроводу III та протоколювання інцидентів; 3) інтеграція страхового комплаєнс-моніторингу в систему ризик-менеджменту.
R5	Помірний	<i>Запобіжні заходи:</i> 1) Етична регламентація ADAS/CMS згідно з настановами ЄС (High-Level Expert Group AI) та OECD; 2) впровадження механізмів пояснюваного штучного інтелекту; 3) алгоритмічний аудит на предмет когнітивних упереджень та аномалій даних; 4) проєктування етичних людино-машинних інтерфейсів для нівелювання надмірної технотехнологічності; 5) застосування прозорої політики обробки персональних даних. <i>Компенсаційні заходи:</i> 1) навчання персоналу щодо меж автономності та цифрових компетенцій; 2) розроблення протоколів деградації управління при системних збоях III; 3) стратегічна комунікація щодо імплементації, лімітації та валідності технологій; 4) запровадження інституту незалежної експертизи операційних експесів.

		<i>Стимувальні заходи:</i> 1) моніторинг суспільної ресепції та управління репутаційними ризиками; 2) проведення комплексної соціальної оцінки технологічного впливу; 3) адаптивна корекція стратегій на основі емпіричних даних та фідбеку; 4) впровадження систем реляційної взаємодії для фіксації зауважень щодо ADAS/CMS.
R6	Дуже високий	<i>Запобіжні заходи:</i> 1) формування бюджетного резерву на непередбачувані видатки (10–20% від капітальних інвестицій); 2) оптимізація операційних видатків через механізми сервісних угод з постачальниками; 3) комплексне страхування конвергентних ризиків із включенням систем ADAS/CMS; 4) сценарне фінансове моделювання інвестиційних та операційних видатків при впровадженні систем; 5) формування резервів на покриття комплаєнс-ризиків та деліктних витрат. <i>Компенсаційні заходи:</i> 1) оптимізація капітальних інвестицій через диверсифікацію постачальників та інструменти лізингу; 2) оптимізація життєвого циклу програмного забезпечення та мікропрограм для мінімізації операційних витрат на підтримку; 3) впровадження системи індикаторів результативності імплементації ADAS/CMS. <i>Стимувальні заходи:</i> 1) періодичний фінансовий аудит та верифікація видатків; 2) оптимізація фінансової стійкості методами прогностичного моделювання та оцінки ризиків; 3) диверсифікація фінансових інструментів та комплексне страхування критичних активів.

Складено авторами за [2; 4; 5; 6; 7; 8; 12; 13; 15; 16; 17; 18; 19]

Проведена оцінка ризиків інтеграції ШІ (ADAS/CMS) на гіпотетичному вітчизняному транспортному підприємстві у 2025 році виявила: критичний рівень юридичних та страхових ризиків; високі технологічні, операційні, кібербезпекові та фінансові загрози; помірні етичні та соціальні ризики. Запропоновані стратегії мінімізації ризиків (табл. 5) включають технічні, організаційні, нормативні та соціальні заходи, які забезпечують зниження рівня загроз до керованих значень. Такий комплексний підхід підвищує безпеку, ефективність та стійкість підприємств при інтеграції систем ШІ у транспортному секторі.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

1. У статті обґрунтовано методичний підхід до оцінки інноваційних ризиків інтеграції систем штучного інтелекту (ADAS/CMS) у діяльність вітчизняних підприємств в умовах цифрової трансформації та зростання вимог до безпеки і стійкості транспортних систем. Запропонований комплексний підхід базується на поєднанні процесного, сценарного та експертного методів аналізу, що дозволяє системно ідентифікувати, оцінювати та ранжувати ризики з урахуванням специфіки транспортної галузі в Україні та високого рівня невизначеності.

2. Запропонований методичний підхід передбачає системну ідентифікацію та класифікацію ризиків за ключовими категоріями: технологічні, операційні, кібербезпекові, юридичні та страхові, етичні та соціальні, фінансові. Використання інструментарію міжнародних стандартів ризик-менеджменту у поєднанні зі сценарним аналізом забезпечує цілісну оцінку ймовірності та наслідків ризиків на різних етапах інтеграції штучного інтелекту.

3. Практична доцільність запропонованого підходу була підтверджена за результатами експертної валідації. Ключовою перевагою підходу є можливість виявлення критичних та дуже високих ризиків на ранніх стадіях інтеграції ШІ, що є підставою для обґрунтування управлінських рішень та формування адаптивних стратегій їх мінімізації. Встановлено, що найбільшу загрозу становлять кібербезпекові, фінансові, а також юридичні та страхові ризики, тоді як етичні та соціальні ризики мають помірний, але динамічний характер і потребують постійного моніторингу.

4. Запропонований методичний підхід є універсальним і може бути адаптований до різних типів вітчизняних транспортних підприємств, з різним рівнем автоматизації та стадіями впровадження систем штучного інтелекту.

5. Перспективи подальших наукових розвідок полягають в емпіричній перевірці запропонованого методичного підходу в реальних умовах функціонування вітчизняних транспортних підприємств та доповнення системи оцінки ризиків ШІ показниками, що характеризують ефективність діяльності та сталий розвиток, що сприятиме зниженню негативних наслідків інноваційних ризиків.

Література

1. Воліков В.В., Панченко І.В. Економічна доцільність впровадження оптичних систем спостереження в автомобілях: між інноваційною необхідністю та економічною надмірністю. Бізнес Інформ. 2025. № 10. С. 325 – 333. DOI: <https://doi.org/10.32983/2222-4459-2025-10-325-333>
2. Кульова Д. О. Безпека дорожнього руху в Україні : оцінювання ризиків і перспективи цифровізації / Д. О. Кульова, С. О. Магопєць, О. М. Лівіцький // Центральнотукаїнський науковий вісник. Технічні науки. – 2025. – Вип. 11(42), ч. II. – С. 278–285. – DOI: [https://doi.org/10.32515/2664-262X.2025.11\(42\).2.278-285](https://doi.org/10.32515/2664-262X.2025.11(42).2.278-285)
3. Ori Igwe, Artificial Intelligence: A Twenty First Century International Regulatory Challenge // *Athens Journal of Law* 2024, 10: 1-27. – DOI: <https://doi.org/10.30958/ajl.X-Y-Z>

- 4 Oyeyemi, Babatunde & John, Awodola & Awodola, Mosopeoluwa. (2025). Infrastructure and Regulatory Barriers to AI Supply Chain Systems in Nigeria vs. the U.S.. *Engineering Science & Technology Journal*. 6. 155-172. DOI: <https://doi.org/10.51594/estj.v6i4.1912>
- 5 AI for Transport Authorities: Principles and Practical Guidance. Paris: International Transport Forum, 2024. 80 p. URL: <https://www.itf-oecd.org/sites/default/files/docs/ai-transport-authorities.pdf>
- 6 Інжиніринг криз та ризиків транспортних послуг: кол. моногр. / В.М. Самсонкін, І.В. Ніколаєнко, Ю.В. Булгакова та ін.; за ред. В.М. Самсонкіна та І.В. Ніколаєнко. — Київ : Талком, 2021. — 312 с.
- 7 Durlík I, Miller T, Kostecka E, Tuński T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. *Applied Sciences*. 2024; 14(18):8420. <https://doi.org/10.3390/app14188420>
- 8 Тарашевський М. М. Організаційно-економічний механізм управління ризиками транспортних підприємств : дис. ... канд. екон. наук : 08.00.04 / Тарашевський Максим Михайлович. — Київ, 2021. — 298 с. URL: files.duit.edu.ua
- 9 Zaidan, E., Ibrahim, I.A. AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanit Soc Sci Commun* 11, 1121 (2024). <https://doi.org/10.1057/s41599-024-03560-x>
- 10 Регламент (ЄС) 2024/1689 Європейського Парламенту та Ради від 13 червня 2024 року про встановлення гармонізованих правил щодо штучного інтелекту та внесення змін до певних законодавчих актів Союзу (Акт про штучний інтелект). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.
- 11 Schuett, Jonas. (2023). Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*. 15. 1-19. DOI: <https://doi.org/10.1017/err.2023.1>
- 12 Road infrastructure and transport security: a PIARC technical report. Paris: PIARC, 2023. 216 p. URL: <https://ndu.kr.ua/files/51/-24/5/Road-Infrastructure-and-Transportation-Security-A-PIARC-Technical-Report.pdf>
- 13 Advancing accountability in AI. Governing and managing risks throughout the lifecycle for trustworthy AI. Paris: OECD Publishing, February 2023 No. 349. 72 p. ISBN 978-92-64-75411-4. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/02/advancing-accountability-in-ai_753bf8c8/2448f04b-en.pdf
- 14 Piarc World Road Association. Annual Report 2019–2020. — Paris: PIARC, 2020. — URL: <https://www.piarc.org/ressources/documents/Annual-Reports-Activity/a5f606d-34466-ANNUAL-REPORT-2019-2020-PIARC-World-Road-Association.pdf>.
- 15 Kesgin K, Kosunalp S, Beloiev I. SCRAM: A Scenario-Based Framework for Evaluating Regulatory and Fairness Risks in AI Surveillance Systems. *Applied Sciences*. 2025; 15(16):9038. <https://doi.org/10.3390/app15169038>
- 16 Understanding AI Risks in Transportation : White Paper / U.S. Department of Transportation. Washington, D.C., 2024. Sept. 26 p. URL: https://www.transportation.gov/sites/dot.gov/files/2024-09/HASS_COE_AI_Assurance_Whitepaper_AI_Risk_Sep2024.pdf
- 17 Tobiloba, Abiona. (2025). CYBERSECURITY CHALLENGES IN AI- ENABLED AUTONOMOUS TRANSPORTATION NETWORKS. *ResearchGate*. 2025. Sept. 14 p. URL: https://www.researchgate.net/publication/395539804_CYBERSECURITY_CHALLENGES_IN_AI-ENABLED_AUTONOMOUS_TRANSPORTATION_NETWORKS
- 18 Cyber Security in Road Transport 2025 : Report / Federal Office for Information Security (BSI). Bonn, 2025. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/Cybersecurity_road_transport.pdf

References

1. Volikov V. V., Panchenko I. V. The Economic Feasibility of Implementing Optical Surveillance Systems in Vehicles: Between Innovative Necessity and Economic Excess. *Business Inform*. 2025. № 10. С. 325 – 333. DOI: <https://doi.org/10.32983/2222-4459-2025-10-325-333>
2. Kulova, D. O., Mahopets, S. O., & Livitskiy, O. M. (2025). Bezpeka dorozhnoho rukhu v Ukraini: otsiniuvannya ryzykiv i perspektyvy tsyfrovizatsii [Road safety in Ukraine: risk assessment and perspectives of digitalization]. *Tsentralkoukrainskyi naukovy visnyk. Tekhnichni nauky* [Central Ukrainian Scientific Bulletin. Technical Sciences], 11(42), part II, 278–285. [https://doi.org/10.32515/2664-262X.2025.11\(42\).2.278-285](https://doi.org/10.32515/2664-262X.2025.11(42).2.278-285)
3. Ori Igwe, Artificial Intelligence: A Twenty First Century International Regulatory Challenge // *Athens Journal of Law* 2024, 10: 1-27. – DOI: <https://doi.org/10.30958/ajl.X-Y-Z>
4. AI for Transport Authorities: Principles and Practical Guidance. Paris: International Transport Forum, 2024. 80 p. URL: <https://www.itf-oecd.org/sites/default/files/docs/ai-transport-authorities.pdf>.
5. Samsonkin, V. M., Nikolaienko, I. V., Bulhakova, Yu. V. et al. (2021). Inzhynirynh kryz ta ryzykiv transportnykh posluh [Engineering of crises and risks of transport services: collective monograph]. In V. M. Samsonkin & I. V. Nikolaienko (Eds.). Kyiv: Talkom..
6. Durlík I, Miller T, Kostecka E, Tuński T. Artificial Intelligence in Maritime Transportation: A Comprehensive Review of Safety and Risk Management Applications. *Applied Sciences*. 2024; 14(18):8420. <https://doi.org/10.3390/app14188420> (<https://www.mdpi.com/2076-3417/14/18/8420>)
7. Tarashevskiy, M. M. (2021). Orhanizatsiino-ekonomichnyi mekhanizm upravlinnia ryzykamy transportnykh pidpriemstv [Organizational and economic mechanism of risk management of transport enterprises] (Doctoral dissertation, Kyiv). Retrieved from files.duit.edu.ua
8. Oyeyemi, Babatunde & John, Awodola & Awodola, Mosopeoluwa. (2025). Infrastructure and Regulatory Barriers to AI Supply Chain Systems in Nigeria vs. the U.S.. *Engineering Science & Technology Journal*. 6. 155-172. DOI: <https://doi.org/10.51594/estj.v6i4.1912>

-
9. Zaidan, E., Ibrahim, I.A. AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanit Soc Sci Commun* 11, 1121 (2024). <https://doi.org/10.1057/s41599-024-03560-x>
 10. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts (Artificial Intelligence Act). *Official Journal of the European Union*, L series. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
 11. Schuett, Jonas. (2023). Risk Management in the Artificial Intelligence Act. *European Journal of Risk Regulation*. 15. 1-19. DOI: 10.1017/err.2023.1.
 12. Road infrastructure and transport security: a PIARC technical report. Paris: PIARC, 2023. 216 p. URL: <https://ndu.kr.ua/files/51/-24/5/Road-Infrastructure-and-Transportation-Security-A-PIARC-Technical-Report.pdf>
 13. Advancing accountability in AI. Governing and managing risks throughout the lifecycle for trustworthy AI. Paris: OECD Publishing, February 2023 No. 349. 72 p. ISBN 978-92-64-75411-4. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/02/advancing-accountability-in-ai_753bf8c8/2448f04b-en.pdf
 14. Piarc World Road Association. Annual Report 2019–2020. — Paris: PIARC, 2020. — URL: <https://www.piarc.org/ressources/documents/Annual-Reports-Activity/a5f606d-34466-ANNUAL-REPORT-2019-2020-PIARC-World-Road-Association.pdf>
 15. Kesgin K, Kosunalp S, Beloev I. SCRAM: A Scenario-Based Framework for Evaluating Regulatory and Fairness Risks in AI Surveillance Systems. *Applied Sciences*. 2025; 15(16):9038. <https://doi.org/10.3390/app15169038>
 16. Understanding AI Risks in Transportation : White Paper / U.S. Department of Transportation. Washington, D.C., 2024. Sept. 26 p. URL: https://www.transportation.gov/sites/dot.gov/files/2024-09/HASS_COE_AI_Assurance_Whitepaper_AI_Risk_Sep2024.pdf
 17. Tobiloba, Abiona. (2025). CYBERSECURITY CHALLENGES IN AI- ENABLED AUTONOMOUS TRANSPORTATION NETWORKS. *ResearchGate*. 2025. Sept. 14 p. URL: https://www.researchgate.net/publication/395539804_CYBERSECURITY_CHALLENGES_IN_AI-ENABLED_AUTONOMOUS_TRANSPORTATION_NETWORKS
 18. Cyber Security in Road Transport 2025 : Report / Federal Office for Information Security (BSI). Bonn, 2025. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/Cybersecurity_road_transport.pdf