DOI: https://doi.org/10.32782/2521-666X/2026-93-10
УДК 004.89:005.334:005.311

Шевчук І.Б.
доктор економічних наук, професор,
Львівський національний університет імені Івана Франка
ORCID: https://orcid.org/0000-0003-4386-3730
Васьків О.М.
старший викладач,
Львівський національний університет імені Івана Франка
ORCID: https://orcid.org/0000-0001-8312-2828

Shevchuk Iryna, Vaskiv Oksana
Ivan Franko National University of Lviv

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В УПРАВЛІННІ БІЗНЕС-РИЗИКАМИ

INTELLIGENT DECISION SUPPORT SYSTEMS IN BUSINESS RISK MANAGEMENT

У статті обґрунтовано доцільність застосування інтелектуальних систем підтримки прийняття рішень як інтегрованого інструменту управління бізнес-ризиками в умовах цифрової трансформації. Показано, що традиційні підходи до ризик-менеджменту потребують доповнення сучасними аналітичними та цифровими інструментами, здатними забезпечити оперативність і роботу з великими обсягами даних. ІСППР поєднують вимірювання соціально-економічних процесів, кількісне оцінювання ризиків і формування управлінських рішень в єдину систему. Доведено, що якість управління економічними ризиками безпосередньо залежить від використання релевантних індикаторів, економетричних моделей і методів прогнозування. Особливу увагу приділено взаємозв'язку бізнес- та ІТ-ризиків, які в умовах цифровізації набувають інтегрованого характеру та мають враховуватися в межах проєктного й стратегічного управління. Поєднання аналітичних інструментів і цифрових платформ формує основу більш системного та обґрунтованого ризик-менеджменту.

Ключові слова: *бізнес-ризики, ІТ-ризик, інтелектуальні системи підтримки прийняття рішень, CRAMM, COBIT for Risk, FRAP, OCTAVE, AI-based Risk Management, Predictive Risk Analytics, GRC-платформи, Digital Risk Protection, прогнозування ризиків, моделювання ризиків.*

The article substantiates the feasibility of using intelligent decision support systems (IDS) as an integrated tool for managing business risks in the context of digital transformation of the economy. It is shown that traditional approaches to risk management, while maintaining methodological value, need to be supplemented with analytical and digital components that ensure efficiency, adaptability and the ability to work with large arrays of structured and unstructured data. IDS act as a connecting link between measuring socio-economic processes, quantitative risk assessment and the formation of sound management decisions. It is proven that the effectiveness of economic risk management largely depends on the quality of tools for measuring and assessing socio-economic indicators, in particular the use of indicators, indices, econometric models, methods of multivariate analysis and predictive analytics. The integration of these tools into the ISPR structure allows to increase the accuracy of risk identification, assess their probability and potential consequences, as well as to form alternative response scenarios. Special attention is paid to the interrelationship of business and IT risks, which is of particular importance in the context of digitalization of business processes. It has been established that IT risks are increasingly acting as a functional component of the overall system of economic risks of the enterprise, which necessitates their integrated consideration within project management and strategic management. The use of intelligent decision-making support systems in the project environment contributes to increasing the transparency of management procedures, harmonizing the risk-oriented approach with project objectives and optimizing resource allocation. Thus, the combination of modern tools for measuring socio-economic processes, analytical assessment methods and intelligent digital platforms forms a new model of business risk management, focused on proactivity, systematicity and validity of management decisions. Promising areas of further research include the development of integrated models for assessing business and IT risks based on machine learning, the formation of industry indicators of digital resilience of enterprises, as well as the testing of intelligent DSS in the practice of managing investment and innovation projects.

Keywords: *business risks, IT risk, intelligent decision support systems, CRAMM, COBIT for Risk, FRAP, OCTAVE, AI-based Risk Management, Predictive Risk Analytics, GRC platforms, Digital Risk Protection, risk forecasting, risk modeling.*

Постановка проблеми. Сучасний етап розвитку світової економіки характеризується зростанням рівня невизначеності, турбулентності ринкового середовища та ускладненням структури бізнес-ризиків, що суттєво підвищує вимоги до якості управлінських рішень. Глобалізація, цифровізація бізнес-процесів, поширення платформних моделей, використання великих даних і штучного інтелекту зумовлюють появу нових типів фінансових, операційних, кібернетичних та стратегічних ризиків, які важко ідентифікувати та оцінити за допомогою традиційних інструментів ризик-менеджменту. У цих умовах зростає роль інтелектуальних систем підтримки прийняття рішень (ІСППР), здатних інтегрувати аналітичні моделі, цифрові дані та експертні знання для своєчасного виявлення ризиків, оцінювання їх імовірності та потенційних наслідків, а також обґрунтування альтернатив управлінського реагування.

В Україні проблема управління бізнес-ризиками загострюється внаслідок воєнних викликів, макроекономічної нестабільності, порушення логістичних ланцюгів і зростання кіберзагроз, що суттєво ускладнює процеси стратегічного та оперативного управління підприємствами. Водночас практичне впровадження інтелектуальних систем підтримки прийняття рішень стримується фрагментарністю інформаційного забезпечення, обмеженістю формалізованих даних і недостатньою адаптацією наявних цифрових рішень до специфіки українського бізнес-середовища. Це зумовлює актуальність наукового осмислення можливостей і обмежень використання інтелектуальних систем підтримки прийняття рішень в управлінні бізнес-ризиками та формування методологічних підходів до їх застосування з метою підвищення стійкості й адаптивності суб'єктів господарювання в умовах високої невизначеності.

Аналіз останніх досліджень і публікацій. Проблематика управління ризиками в умовах цифровізації економіки та трансформації бізнес-процесів широко представлена у вітчизняних наукових дослідженнях. У працях В. В. Македона та О. О. Ковніра [18, с. 76–82] розкрито вплив цифрових технологій на процеси управління інвестиційними проєктами та обґрунтовано необхідність використання аналітичних і інформаційних інструментів для зниження проєктних ризиків. Питання формування інноваційних підходів до ризик-менеджменту в публічному секторі, зокрема в контексті захисту прав споживачів, висвітлено у дослідженні О. Л. Бобось [8, с. 349–354], де акцент зроблено на зростанні ролі цифрових інструментів у системі управління ризиками. Значну увагу проблемам управління ризиками в цифровій економіці, зокрема у сфері фінансової безпеки та трансформаційних змін, приділено в роботі О. М. Десятнюка та О. В. Птащенка [12, с. 238–247].

Окремі аспекти використання цифрових платформ як інструментів підвищення ефективності стратегічного планування та управління ризиками досліджено М. А. Петренком [19], а також у працях В. І. Зюзюна та Д. О. Ляшенка [17, с. 137–143], де запропоновано концептуальну модель управління ризиками в проєктах створення онлайн-платформ. Особливості ризик-менеджменту в ІТ-галузі та в умовах цифровізації економічних систем проаналізовано в дослідженні М. І. Пешка та О. Г. Мельника [20, с. 193–198]. Питання управління ризиками інвестиційних проєктів і цифрової трансформації також розглядаються у працях В. Чернеги та М. Клименка [23, с. 119–123], Р. Зварича, Ю. Дудника, В. Гомотюка та С. Боднара [16, с. 38–53], а також у дослідженні В. П. Далика та С. В. Ткача [11, с. 281–288], де узагальнено міжнародний досвід використання інформаційних технологій для мінімізації бізнес-ризиків. Теоретичні засади, підходи та методи управління ризиками на рівні підприємств систематизовано у роботі Н. Ю. Захарової [15, с. 203–209].

Водночас, попри наявність значного наукового доробку, у зазначених дослідженнях переважає зосередження на окремих аспектах цифровізації, галузевих особливостях або класичних підходах до ризик-менеджменту. Питання формування та використання інтелектуальних систем підтримки прийняття рішень як інтегрованого інструменту управління бізнес-ризиками, що поєднує аналітику даних, прогнозування та елементи штучного інтелекту, залишаються недостатньо систематизованими. Це зумовлює потребу у подальших дослідженнях, спрямованих на узагальнення сучасних цифрових і інтелектуальних підходів до підтримки управлінських рішень у сфері управління бізнес-ризиками.

Мета статті – теоретичне обґрунтування та прикладний аналіз можливостей використання інтелектуальних систем підтримки прийняття рішень у процесі управління бізнес-ризиками для підвищення обґрунтованості управлінських рішень, зниження рівня невизначеності та мінімізації негативних наслідків ризикових подій у діяльності суб'єктів господарювання.

Виклад основного матеріалу. У сьогоднішній час впевнено можна стверджувати, що ми живемо у столітті, де технології формують майбутнє. Кожен, хто залучений у сфері бізнесу в реальному часі, знає, наскільки важливими стали технології для бізнесу. На початкових етапах бізнес у повній мірі залежав від робочої сили, проте з розвитком технологій бізнес прагне розвиватися разом з ними. Незалежно від напрямку бізнесу, технології важливі для його

ефективності та успіху. Оскільки, технології мають невід'ємне значення у бізнесі, то до бізнес-ризиків відносять і ІТ-ризики.

Розглядаючи підприємницькі ризики, можна стверджувати, що немає єдиного погляду на ризики і на їх співвідношення (чи тотожність) з бізнес-ризиками [9, с. 40-48]. Якщо розглядати ризик зі сторони бізнесу, то це – ризик можливості неадекватного прибутку або навіть збитків, пов'язаних з невизначеністю такою як конкуренція, зміна смаку та попиту клієнтів, вартість введення, зміна урядової політики тощо. Діловий ризик виникає внаслідок конкуренції, кон'юнктури ринку, асортименту товарів тощо. Двома основними факторами, що призводять до бізнес-ризику, є:

1. Внутрішній ризик – ризик, який виникає внаслідок подій, які відбуваються в організації. Ці ризики є контрольованими. Вони виникають через такі фактори, як страйки, зупинки роботи профспілки, аварії на заводі, недбалість працівників, збій машин, технологічна застарілість, пошкодження товару, спалах пожежі тощо;

2. Зовнішній ризик – ризик, що виникає внаслідок зовнішніх подій для фірми, і тому він не піддається контролю. Він може виникнути через коливання цін, зміни смаку клієнтів, урядових норм, обставини непереборної сили тощо [10; 14, с. 80–87].

У класичній структурі бізнес-ризиків виділяють фінансові, стратегічні, операційні, ринкові, правові та репутаційні ризики [2]. Будь-який із цих ризиків має ІТ-вимір, що дозволяє говорити про ІТ-ризики як механізм реалізації бізнес-ризиків. Тобто ІТ-ризик – це загроза для бізнес-даних, критичних систем та бізнес-процесів. Він пов'язаний із такими аспектами як: використання, володіння, функціонування, залучення ІТ в організації. ІТ-ризики можуть завдати шкоду цінності бізнесу, вони часто виникають через некоректне управління процесами та подіями [6]. У стратегічному ризику ІТ-ризик «вбудований» як невідповідність ІТ-архітектури стратегії бізнесу, у фінансовому – збої платіжних систем, втрати через кібератаки, в операційному – відмова ІТ-систем, помилки даних, downtime, ринковому – витік клієнтських даних, цифрова репутація, правовому – порушення вимог захисту даних, комплаєнс-ризики.

Таким чином, у структурі бізнес-ризиків ІТ-ризики є функціональною складовою, що відображає цифрову природу сучасних бізнес-процесів. Стратегічні, фінансові, операційні та репутаційні ризики реалізуються через інформаційні системи, цифрові платформи та інфраструктуру обробки даних, що зумовлює трансформацію класичної структури бізнес-ризиків у ризик-орієнтовану модель із виокремленням ІТ-компоненти. У цьому контексті ІТ-ризики виступають інструментом конкретизації та кількісного вимірювання бізнес-ризиків, забезпечуючи їх інтеграцію в інтелектуальні СППР. Такий підхід дозволяє поєднати технічні показники функціонування ІТ-систем із соціально-економічними наслідками для бізнесу та підвищити обґрунтованість управлінських рішень в умовах цифрової трансформації.

Дослідження ІТ-ризиків дає можливість поділу їх на три категорії (рис. 1), а саме *першу*, яка викликана діями персоналу, тобто, забезпечення його в суворій відповідності з виконуваними співробітником функціями і контроль використання ресурсів; *другу*, куди відносяться збої або відмови устаткування; *третю*, які пов'язані з використанням нелегального програмного забезпечення.

Як уже зазначалось, ІТ-ризики є джерелом бізнес-ризиків і охоплюють цілий ряд важливих для бізнесу напрямків, як-от: доступність, продуктивність, безпека та відповідальність (рис. 2).

Будь-яка зміна в інформаційній інфраструктурі робить прямий або непрямий вплив на всі сторони діяльності підприємства і, власне, ця обставина зна-

Рис. 1. Категорії ІТ-ризиків

Джерело: розроблено авторами

чно ускладнює аналіз ефективності впровадження ІТ, оскільки дуже складно виділити вплив інформаційних технологій на функціонування компанії, як окрему змінну і досить важко охопити всі напрямки впливу використовуваних ІТ.

Стратегія управління ризиком – це мистецтво управління діяльністю підприємством у невизначеній господарській ситуації, що ґрунтується на прогнозуванні ризику і прийомах його зниження.

Щодо системи управління ризиками, то вона складається з двох підсистем: об'єкта управління і суб'єкта управління (рис. 3). *Об'єкт управління* – це безпосередньо ризик, ризиковані вкладення капіталу й економічні відносини між суб'єктами в процесі підприємницької діяльності. *Суб'єктом управління* є спеціальна група людей, що здійснює цілеспрямоване функціонування об'єкта управління, використовуючи різні прийоми і способи управлінського впливу [22].

Для успішного володіння ризиковими ситуаціями бізнесу слід дотримуватись основних принципів управління ризиками. По-перше, не можна ризикувати більше, ніж дозволяє власний капітал. По-друге, не можна ризикувати великим заради малого. По-третє, необхідно завчасно оцінювати можливі наслідки ризику [22].

В умовах цифрової економіки та зростання ролі інформаційних технологій ці принципи потребують доповнення з урахуванням специфіки ІТ-ризиків. Зокрема, доцільним є дотримання принципу превентивності, що передбачає проактивний моніторинг цифрового середовища та раннє виявлення загроз; принципу безперервності управління ризиками, який полягає у постійному контролі функціонування інформаційних систем і захисту даних; принципу інтегрованості, що забезпечує узгодженість управління ІТ-ризиками із загальною стратегією розвитку підприємства; принципу адаптивності, який передбачає гнучке реагування на технологічні зміни та нові кіберзагрози; а також принципу ризик-орієнтованої цифрової безпеки, спрямованого на пріоритетний захист критичних бізнес-процесів та інформаційних активів.

Одними з найпоширеніших у світі методик управління ІТ-ризиками є CRAMM, COBIT for Risk, FRAP, OCTAVE, які поряд з певними перевагами мають і свої обмеження [5; 21]. Методика CRAMM (CCTA Risk Analysis and Management Method) базується на стандартах управління інформаційної безпеки та описує підхід до якісної оцінки ризиків, яка проводиться на основі аналізу цінності ІТ-активу для бізнесу, вразливостей, погроз і ймовірності їх

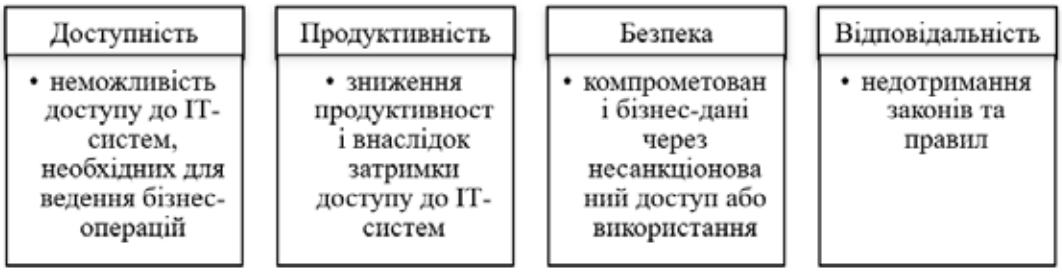

Рис. 2. ІТ-ризики, які застосовуються для бізнесу

Джерело: розроблено авторами на основі [6]

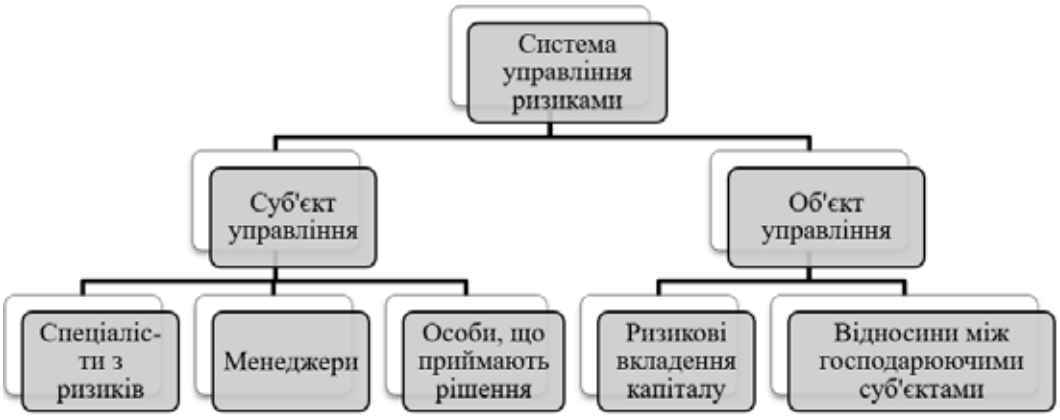

Рис. 3. Підсистеми управління ризиками

Джерело: розроблено авторами на основі [22]

реалізації. Процес управління ризиками за методикою CRAMM складається із наступних п'яти етапів: ініціювання, ідентифікація та оцінка IT-активів, оцінка загроз і вразливостей, обчислення ризику, управління ризиком (рис. 4).

Що стосується методики COBIT, при реалізації функції і процесу управління IT-ризиками в організації, то вона включає компоненти, які мають значний вплив на ризики та процес управління ними: принципи, політика та процедури організації; процеси; організаційна структура; інформація; корпоративна культура, етика і правила поведінки; люди, їх досвід і компетенції; IT-сервіси, IT-інфраструктура і додатки [21].

Методика FRAP (Facilitated Risk Analysis Process) описує підхід до якісної оцінки ризиків. Її метою є виявлення, оцінка та документування складу ризиків інформаційної безпеки для заздалегідь певній галузі дослідження.

Для проведення аналізу та оцінки ризиків інформаційної безпеки формується проєктна команда, а результати мозкових штурмів, що проводяться під час сесій ідентифікації та оцінювання ризиків, узагальнено та представлено на рис. 5.

Методика OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) описує підхід до якісної оцінки ризиків. Актуальною версією методології є OCTAVE Allegro. Дана методологія призначена для формалізації і оптимізації процесу оцінки ризиків інформаційної безпеки в організації та забезпечення можливості отримання необхідних організації результатів з мінімальними витратами часу і ресурсів. Відповідно до OCTAVE All процес управління IT-ризиками складається з таких чотирьох основних етапів як визначення пріоритетів, профілювання IT-активів, ідентифікація загроз та ідентифікація і розробка ризиків (рис. 6).

Зважаючи на зростання рівня невизначеності зовнішнього середовища, ускладнення бізнес-процесів та цифрову трансформацію управління, особливої актуальності набуває критичний аналіз традиційних методик управління ризиками з позицій їх придатності до використання в інтелектуальних системах підтримки прийняття рішень. Класичні підходи до ідентифікації та оцінювання ризиків, такі як CRAMM, COBIT, FRAP та OCTAVE, залишаються важливою методологічною основою ризик-менеджменту, проте їх ефективність у сучасних умовах

Рис. 4. Етапи управління ризиками за методологією CRAMM

Джерело: складено авторами на основі [5; 21]

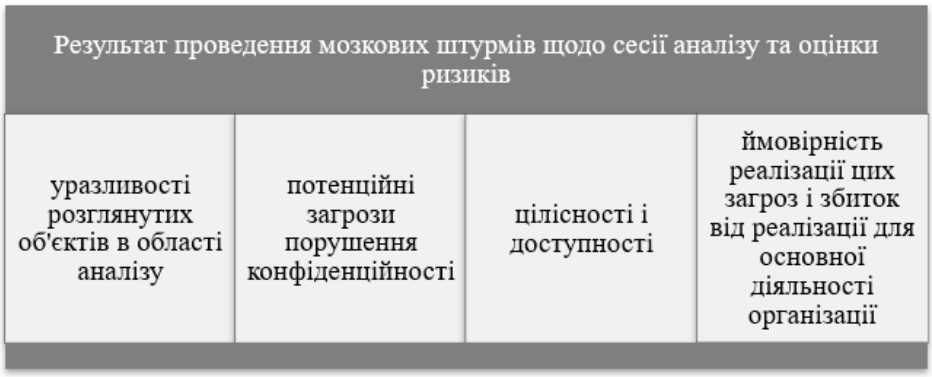

Рис. 5. Результат проведення мозкових штурмів щодо сесії аналізу та оцінки ризиків

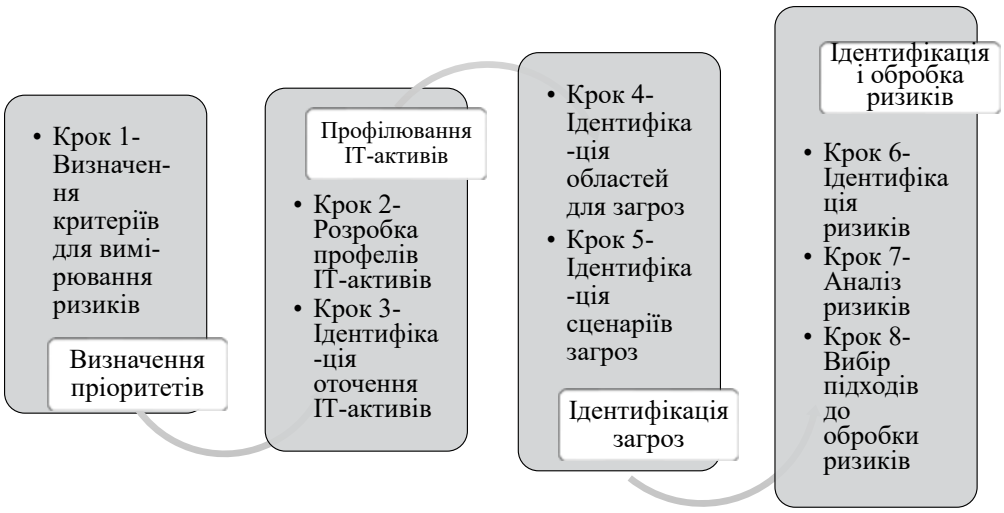

Рис. 6. Процес управління ризиками методологією OCTAVE Allegro

Джерело: розроблено авторами

значною мірою визначається можливістю автоматизації, інтеграції з цифровими платформами, аналітичними інструментами та технологіями штучного інтелекту. У цьому контексті доцільним є порівняння зазначених методик з урахуванням їхніх переваг і обмежень, а також потенціалу інтеграції з інтелектуальними СППР, що дозволяє оцінити їх спроможність забезпечувати обґрунтовані управлінські рішення в умовах динамічних бізнес-ризиків (табл. 1).

Класичні методики управління ризиками формують методологічне підґрунтя для побудови інтелектуальних СППР, однак їх ефективність у сучасному цифровому середовищі суттєво зростає лише за умови інтеграції з інструментами аналітики даних, ШІ та автоматизованого сценарного моделювання.

Як бачимо, традиційні методики управління ризиками мають низку обмежень, зумовлених їх переважно статичним характером, орієнтацією на ретроспективні дані та високим рівнем експертної суб'єктивності. У більшості випадків такі підходи передбачають періодичне, а не безперервне оцінювання ризиків, що знижує їхню здатність своєчасно реагувати на швидкі зміни зовнішнього та внутрішнього середовища. Крім того, класичні методики обмежено працюють з великими обсягами неструктурованих даних і недостатньо враховують складні нелінійні взаємозв'язки між ризиковими чинниками, що є характерним для сучасних цифрових бізнес-моделей. Значні часові та ресурсні витрати на збір і обробку інформації, а також труднощі інтеграції з корпоративними ІС додатково знижують їх ефективність в умовах високої невизначеності. Саме ці обмеження зумовлюють зростання інтересу до інтелектуалізованих підходів управління ризиками, заснованих на використанні ШІ, машинного навчання та прогнозної аналітики, як-от: AI-based Risk Management, Predictive Risk Analytics, GRC-платформи з елементами машинного навчання та Digital Risk Protection (табл. 2).

AI-based Risk Management орієнтований на автоматизовану ідентифікацію, оцінювання та моніторинг ризиків у режимі реального часу, що дає змогу не лише фіксувати наявні загрози, а й формувати адаптивні сценарії реагування з урахуванням змін зо-

Таблиця 1

Порівняння класичних методик управління бізнес-ризиками з урахуванням їх придатності до використання в ІСППР

Методика	Переваги	Недоліки	Потенціал інтеграції з ІСППР	Роль ШІ та аналітики
CRAMM	– Зрозумілий формалізований опис методології, що мінімізує можливість виникнення помилок при реалізації процесів аналізу та управління ризиками; – наявність засобів автоматизації аналізу ризиків забезпечує мінімізацію трудовитрат і часу, який є виділений на виконання заходів з аналізу та управління ризиками.	– Висока складність і трудомісткість збору вихідних даних; – великі витрати ресурсів та часу на реалізацію процесів аналізу та управління IT-ризиками.	Високий – може бути основою знаннєвих баз і rule-based DSS.	Автоматизація збору даних, використання експертних систем для оцінки ризиків
COBIT	– Зв'язок із загальною бібліотекою COBIT; – багаторазово апробований метод; – наявність зрозумілого формалізованого опису методології.	– Залученість великої кількості зацікавлених осіб; – відсутність можливості оцінки ризиків в грошах.	Середній – високий – інтегрується з GRC та BI-системами.	Аналітика KPI, сценарне моделювання, підтримка стратегічних рішень.
FRAP	– Простота і прозорість процесу; – мінімальні трудовитрати на виконання аналізу і оцінки ризиків; – залучення невеликої кількості учасників забезпечує мінімізацію витрат на комунікації всередині проектної команди і узгодження результатів з усіма зацікавленими особами.	– Відсутність жорстко регламентованого процесу управління ризиками та докладних допоміжних матеріалів, таких як каталоги загроз, вразливостей і т.д.; – відсутність можливості глибокої декомпозиції, докладної і точної оцінки ризиків.	Низький–середній – використовується як вхідний етап для DSS.	Підтримка групових рішень, експертні опитування, fuzzy-логіка
OCTAVE	– Ітеративний підхід забезпечує поступове збільшення глибини аналізу ризиків; – невисокі трудовитрати на виконання аналізу і оцінки ризиків.	– Відсутність докладних допоміжних матеріалів; – відсутність можливості оцінки ризиків в грошах.	Середній – добре поєднується з аналітичними модулями DSS.	Машинне навчання для виявлення патернів ризиків, сценарний аналіз.

Джерело: складено авторами

внішнього середовища [1]. Predictive Risk Analytics доповнює цей підхід за рахунок використання економетричних, статистичних і машинних моделей для прогнозування ймовірності настання ризикових подій та оцінювання їх потенційних наслідків, що істотно підвищує проактивність управлінських рішень [4]. Водночас GRC-платформи з елементами машинного навчання забезпечують комплексну інтеграцію управління ризиками, відповідністю та корпоративним контролем, створюючи єдине інформаційно-аналітичне середовище для прийняття рішень на різних рівнях управління [3; 13]. Окреме місце посідають платформи Digital Risk Protection (DRP), які спеціалізуються на виявленні цифрових, репутаційних та кіберризиків шляхом аналізу великих масивів відкритих і напівструктурованих даних, зокрема в онлайн-середовищі [7]. Сукупно ці підходи формують нове покоління інтелектуальних систем підтримки прийняття рішень в управлінні бізнес-ризиками, здатних знизити рівень невизначеності, підвищити точність оцінок і забезпечити більш стійкий розвиток суб'єктів господарювання в умовах цифрової економіки.

Інтелектуальні СППР в управлінні бізнес-ризиками тісно пов'язані з інструментами вимірювання та оцінювання соціально-економічних процесів, оскільки саме результати кількісного аналізу формують інформаційну основу управлінських рішень. Вимірювання соціально-економічних показників, використання індикаторів, індексів і результатів цифрових опитувань дозволяє ідентифікувати потенційні джерела ризиків, тоді як застосування економетричних, статистичних і багатовимірних методів забезпечує їх кількісне оцінювання та прогнозування. Зокрема, для аналізу макро- та мезоекономічних ризиків можуть використовуватися індекси економічної невизначеності (Economic Policy Uncertainty Index), індекси ділової активності (PMI),

Таблиця 2

Порівняння інтелектуалізованих підходів управління бізнес-ризиками

Методика	Переваги	Недоліки	Потенціал інтеграції з ІСППР	Роль ШІ та аналітики
AI-based Risk Management	– Автоматизоване виявлення та оцінювання ризиків у реальному часі; – адаптивність і самонавчання моделей; – висока точність прогнозів.	– Залежність від якості даних; – складність інтерпретації результатів.	Високий – є ядром сучасних інтелектуальних СППР.	Ключова: машинне навчання, нейронні мережі, обробка великих даних.
Predictive Risk Analytics	– Прогнозування ризиків і раннє виявлення загроз; – підтримка проактивного управління.	– Чутливість до структурних зламів; – потреба в регулярному оновленні моделей.	Високий – інтегрується з DSS та BI-системами.	ШІ використовується для прогнозування, аналітика – для інтерпретації результатів.
GRC-платформи з ML	– Комплексне управління ризиками, відповідністю та контролем; – автоматизація процесів управління ризиками.	– Висока вартість впровадження; – складність налаштування.	Високий – повнофункціональні платформи ІСППР для великих організацій.	ML використовується для оцінювання ризиків, аналітика – для підтримки управлінських рішень.
Digital Risk Protection (DRP)	– Моніторинг цифрових та репутаційних ризиків у реальному часі; – аналіз відкритих джерел і цифрового середовища.	– Вузька спеціалізація на цифрових ризиках; – потреба інтеграції з іншими системами.	Середній–високий – як спеціалізований модуль ІСППР.	ШІ застосовується для моніторингу, NLP та аналізу поведінкових даних.

Джерело: складено авторами

індекси споживчих очікувань, а також показники фінансової стійкості та ліквідності підприємств. Для вимірювання інституційних і цифрових ризиків доцільним є використання індексів цифрової готовності, індексу розвитку електронного урядування, показників кіберстійкості та результатів цифрових опитувань менеджерів і експертів.

Кількісне оцінювання та прогнозування ризиків у межах інтелектуальних СППР може здійснюватися із застосуванням економетричних моделей регресійного аналізу, моделей часових рядів (ARIMA, SARIMA), панельних моделей для виявлення детермінант ризиків на рівні галузей або регіонів, а також логіт- і пробіт-моделей для оцінювання ймовірності настання ризикових подій. Для аналізу складних і багатовимірних соціально-економічних процесів використовуються факторний аналіз, кластеризація, методи головних компонент, що дозволяє виокремити типові профілі ризиків і сегменти бізнес-середовища. Прогнозна складова ІСППР може бути посилена за рахунок застосування методів машинного навчання (дерева рішень, random forest, нейронні мережі), які забезпечують адаптивне моделювання ризиків з урахуванням динаміки соціально-економічних показників і поведінкових факторів.

Інтелектуальні системи інтегрують ці інструменти в єдине аналітичне середовище, трансформуючи результати вимірювань соціально-економічних процесів у сценарії управлінських рішень, спрямованих на мінімізацію ризиків і підвищення стійкості бізнесу в умовах високої невизначеності.

Висновки. У сучасних умовах цифрової трансформації управління бізнес-ризиками не може обмежуватися використанням окремих методик чи програмних продуктів. Практика свідчить, що навіть найефективніші інструменти аналізу не забезпечують належного результату без системного поєднання вимірювання соціально-економічних процесів, аналітичного оцінювання та інтеграції цих результатів у процес прийняття управлінських рішень. У цьому контексті інтелектуальні системи підтримки прийняття рішень виступають не лише технологічним рішенням, а й методологічною платформою, що об'єднує економічні ризики, ІТ-компоненту та інструменти кількісного аналізу в межах проєктного й стратегічного управління. Вирішальним стає не стільки сам факт цифровізації, скільки здатність організації перетворювати дані на обґрунтовані управлінські дії та забезпечувати узгодженість між аналітикою, ризик-менеджментом і цілями розвитку бізнесу.

Подальші дослідження доцільно спрямувати на розроблення адаптивних моделей інтеграції ІСППР у систему управління економічними та ІТ-ризиками, удосконалення індикаторів цифрової стійкості підприємств, а також емпіричну апробацію інтелектуальних підходів у практиці реалізації інвестиційних і цифрових проєктів.

Список літератури:

1. AI in Risk Management: Framework and Use Cases. URL: https://visuresolutions.com/alm-guide/ai-in-risk-management/
2. Business Risk. URL: https://businessjargons.com/businessrisk.html?fbclid=IwAR0BhV81y0fe0V0JlEekCXgq0XjJK5ekWrycGn96R-zT-azxE7S82PeQVXY.
3. GRC й кібербезпека. URL: https://www.sap.com/ukraine/products/ financial-management/grc.html
4. Predictive Analytics for Risk Management: Uses, Types & Benefits. URL: https://predikdata.com/predictive-analytics-for-risk-management/
5. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. URL: https://www.mdpi.com/2079-9292/12/17/3629
6. The Board and IT Risk. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technology-risk-in-fs.pdf
7. What is Digital Risk Protection (DRP)? URL: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-digital-risk-protection-drp/
8. Бобось О. Л. Інноваційні стратегії управління ризиками для забезпечення захисту прав споживачів у сучасному публічному секторі України. *Право та державне управління.* 2023. № 4. С. 349–354.
9. Воронко Р. М. Оцінка та контроль бізнес-ризиків суб'єктів господарювання споживчої кооперації України. *Вісник НУ «Львівська політехніка». Серія: Менеджмент та підприємництво в Україні : етапи становлення і проблеми розвитку.* 2017. № 862. С. 40–48.
10. Гожий О., Кобилінський І., Лугінець Д. Підхід до оцінювання ризиків у задачах планування. *Вісник НУ «Львівська політехніка». Комп'ютерні науки та інформаційні технології.* 2014. № 800. С. 98–105. URL: http://ena.lp.edu.ua:8080/bitstream/ntb/25926/1/16-98-105.pdf
11. Далик В. П., Ткач С. В. Використання інформаційних технологій для мінімізації ризиків в управлінні бізнесом у світлі міжнародного досвіду. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична.* 2024. Вип. 42. С. 281–288.
12. Десятнюк О.М., Птащенко О.В. Управління ризиками в цифровій економіці: фінансова безпека та трансформаційні зміни. *Європейський науковий журнал економічних та фінансових інновацій.* 2024. № 2 (14). С. 238–247. DOI: https://doi.org/10.32750/2024-0223
13. Дорожня карта впровадження рішення GRC. URL: https://continuumgrc.com/uk/a-roadmap-for-adopting-a-grc-solution/
14. Єсєєва І. В. Москаленко В. О. Основні види ризиків та їх вплив на конкурентоспроможність молокопереробних підприємств. *Економіка і організація управління.* 2014. № 3 (19)-4 (20). С. 80–87.
15. Захарова, Н. Ю. Управління ризиками на підприємстві: сутність, підходи та методи. *Бізнес Інформ.* 2023. № 1. С. 203–209. URL: http://eprints.mdpu.org.ua/id/eprint/12796/1/businessinform-2023-1_0-pages-203_209.pdf
16. Зварич Р., Дудник Ю., Гомотюк В., Боднар С. Ризик-менеджмент цифрової трансформації в умовах пандемії. *Вісник економіки.* 2022. № 1. С. 38–53.
17. Зюзюн В. І., Ляшенко Д. О. Концептуальна модель управління ризиками в проєкті створення онлайн-платформи високовартісних товарів. *Комп'ютерні науки та інформаційні технології.* 2025. № 1. С. 137–143.
18. Македон В.В., Ковнір О.О. Цифрова трансформація процесу управління інвестиційними проектами підприємства. *Держава та регіони. Серія: Економіка та підприємництво.* 2024. № 3 (133). С. 76–82.
19. Петренко М. А. Цифрові платформи як інструмент підвищення ефективності стратегічного планування в агросекторі. *Актуальні питання економічних наук.* 2015. № 11. DOI: https://doi.org/10.5281/zenodo.15567891
20. Пешко М. І., Мельник О. Г. Управління ризиками в ІТ-галузі в умовах цифровізації економічних систем. *Проблеми економіки*. 2025. № 1 (63). С. 193–198.
21. Сидоркін П., Горліченко С., Некоз В., Шилан, М. Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 for Risk. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 47 (2). С. 41–47. DOI: 10.33099/2311-7249/2023-47-2-41-47
22. Сучасні підходи до оцінки ризиків інформаційних технологій. Управління ризиками ІТ. *Active Audit Agency.* 2010. URL: https://ppt-online.org/172211
23. Чернега В., Клименко М. Сучасні підходи до ризик-менеджменту інвестиційних проєктів. *Молодий вчений.* 2022. Vol. 11 (111). С. 119–123. DOI: https://doi.org/10.32839/2304-5809/2022-11-111-25

References:

1. AI in Risk Management: Framework and Use Cases. Available at: https://visuresolutions.com/alm-guide/ai-in-risk-management/
2. Business Risk. Available at: https://businessjargons.com/businessrisk.html? fbclid=IwAR0BhV81y0fe0V0JlEekCXgq0XjJK5ekWrycGn96R-zT-azxE7S82PeQVXY. .
3. GRC y kiberbezpeka [GRC and cybersecurity]. Available at: https://www.sap.com/ukraine/products/ financial-management/grc.html
4. Predictive Analytics for Risk Management: Uses, Types & Benefits. Available at: https://predikdata.com/predictive-analytics-for-risk-management/
5. Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. Available at: https://www.mdpi.com/2079-9292/12/17/3629

6. The Board and IT Risk. Available at: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-ccg-information-technology-risk-in-fs.pdf

7. What is Digital Risk Protection (DRP)? Available at: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-digital-risk-protection-drp/

8. Bobos O. L. (2023) Innovatsiini stratehii upravlinnia ryzykamy dlia zabezpechennia zakhystu prav spozhyvachiv u suchasnomu publichnomu sektori Ukrainy [Innovative risk management strategies to ensure consumer protection in the modern public sector of Ukraine]. *Pravo ta derzhavne upravlinnia – Law and public administration*, vol 4, pp. 349–354.

9. Voronko R. M. (2017). Otsinka ta kontrol biznes-ryzykiv subiektiv hospodariuvannia spozhyvchoi kooperatsii Ukrainy [Assessment and control of business risks of consumer cooperative entities in Ukraine]. *Visnyk NU "Lvivska politekhnika". Seriia: Menedzhment ta pidpryiemnytstvo v Ukraini : etapy stanovlennia i problemy rozvytku – Bulletin of the National University "Lviv Polytechnic". Series: Management and Entrepreneurship in Ukraine: Stages of Formation and Problems of Development*, vol. 862, pp. 40–48.

10. Gozhy O., Kobylinsky I., Luhinets D. (2014). Pidkhid do otsiniuvannia ryzykiv u zadachakh planuvannia [Approach to risk assessment in planning tasks]. *Visnyk NU "Lvivska politekhnika". Kompiuterni nauky ta informatsiini tekhnolohii – Bulletin of Lviv Polytechnic National University. Computer Science and Information Technologies*, vol. 800, pp. 98–105. Available at: http://ena.lp.edu.ua:8080/ bitstream/ntb/25926/1/16-98-105.pdf .

11. Dalyk V.P., Tkach S.V. (2024). Vykorystannia informatsiinykh tekhnolohii dlia minimizatsii ryzykiv v upravlinni biznesom u svitli mizhnarodnoho dosvidu [Using information technology to minimize risks in business management in the light of international experience]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna. Seriia yurydychna – Scientific notes of the Lviv University of Business and Law. Economic series. Legal series*, vol. 42, pp. 281–288.

12. Desyatnyuk O.M., Ptashchenko O.V. (2024). Upravlinnia ryzykamy v tsyfrovii ekonomitsi: finansova bezpeka ta transformatsiini zminy [Risk Management in the Digital Economy: Financial Security and Transformational Change]. *Yevropeiskyi naukovyi zhurnal ekonomichnykh ta finansovykh innovatsii – European Scientific Journal of Economic and Financial Innovation*, vol. 2 (14), pp. 238–247. DOI: https://doi.org/10.32750/2024-0223

13. Dorozhnia karta vprovadzhennia rishennia GRC [GRC solution implementation roadmap]. Available at: https://continuumgrc.com/uk/a-roadmap-for-adopting-a-grc-solution/

14. Yeseeva I. V. Moskalenko V. O. (2014). Osnovni vydy ryzykiv ta yikh vplyv na konkurentospromozhnist molokopererobnykh pidpryiemstv [Main types of risks and their impact on the competitiveness of dairy processing enterprises]. *Ekonomika i orhanizatsiia upravlinnia – Economics and management organization*, vol. 3 (19)-4 (20), pp. 80–87.

15. Zakharova N. Yu. (2023). Upravlinnia ryzykamy na pidpryiemstvi: sutnist, pidkhody ta metody [Enterprise risk management: essence, approaches and methods]. *Biznes Inform – Business Inform*, vol. 1, pp. 203–209. Available at: http://eprints.mdpu.org.ua/id/eprint/12796/1/businessinform-2023-1_0-pages-203_209.pdf

16. Zvarych R., Dudnik Y., Homotyuk V., Bodnar S. (2022). Ryzyk-menedzhment tsyfrovoi transformatsii v umovakh pandemii [Risk management of digital transformation in a pandemic]. *Visnyk ekonomiky – Economic Bulletin*, vol. 1, pp. 38–53.

17. Zyuzyun V. I., Lyashenko D. O. (2025). Kontseptualna model upravlinnia ryzykamy v proiekti stvorennia onlain-platformy vysokovartisnykh tovariv [Conceptual model of risk management in the project of creating an online platform for high-value goods]. *Kompiuterni nauky ta informatsiini tekhnolohii – Computer Science and Information Technology*, vol. 1, pp. 137–143.

18. Makedon V.V., Kovnir O.O. (2024). Tsyfrova transformatsiia protsesu upravlinnia investytsiinymy proektamy pidpryiemstva [Digital transformation of the enterprise's investment project management process]. *Derzhava ta rehiony. Seriia: Ekonomika ta pidpryiemnytstvo – State and Regions. Series: Economy and Entrepreneurship*, vol. 3 (133), pp. 76–82.

19. Petrenko M. A. (2015). Tsyfrovi platformy yak instrument pidvyshchennia efektyvnosti stratehichnoho planuvannia v ahrosektori [Digital platforms as a tool for increasing the efficiency of strategic planning in the agricultural sector]. *Aktualni pytannia ekonomichnykh nauk – Current issues in economic sciences*, vol. 11. DOI: https://doi.org/10.5281/zenodo.15567891

20. Peshko M. I., Melnyk O. G. (2025). Upravlinnia ryzykamy v IT-haluzi v umovakh tsyfrovizatsii ekonomichnykh system [Risk management in the IT industry in the context of digitalization of economic systems]. *Problemy ekonomiky – Economic problems*, vol. 1 (63), pp. 193–198.

21. Sidorkin P., Gorlichenko S., Nekoz V., Shilan M. (2023). Metody upravlinnia ryzykamy informatsiinoi bezpeky CRAMM ta COBIT 5 for Risk [Information security risk management methods CRAMM and COBIT 5 for Risk]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern information technologies in the field of security and defense*, vol. 47 (2), pp. 41–47. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-41-47

22. Suchasni pidkhody do otsinky ryzykiv informatsiinykh tekhnolohii. Upravlinnia ryzykamy IT [Modern approaches to information technology risk assessment. IT risk management]. Available at: https://ppt-online.org/172211

23. Chernega V., Klymenko M. (2022). Suchasni pidkhody do ryzyk-menedzhmentu investytsiinykh proiektiv [Modern approaches to risk management of investment projects]. *Molodyi vchenyi – Young scientist*, vol. 11 (111), pp. 119–123. DOI: https://doi.org/10.32839/2304-5809/2022-11-111-25

Дата надходження статті: 27.01.2026
Дата прийняття статті: 16.02.2026
Дата публікації статті: 25.02.2026