УДК 004.4:005.8:005.334:001.891 DOI: 10.20998/2413-3000.2025.10.6

О. О. ЯСІНЕЦЬКИЙ, Т. Г. ФЕСЕНКО

УПРАВЛІННЯ РИЗИКАМИ ІТ ПРОЄКТІВ: АНАЛІТИЧНИЙ ОГЛЯД ДОСЛІДЖЕНЬ

Метою дослідження стало визначення публікаційного кола знань з управління ризиками ІТ проєктів та ідентифікація сучасних інструментів, методів, артефактів для ефективного управління ризиками. Окреслено базові принципи, процеси, методи та інструменти управління ризиками проєктів в міжнародних системах знань і стандартів («Guide to the Project Management Body of Knowledge», «ISO 31000:2018. Risk management – Guidelines», «The standard for risk management in portfolios, programs, and projects»). Наголошується, що використання структурованих підходів дозволяє мінімізувати невизначеність, підвищити гнучкість у прийнятті рішень і забезпечити ефективне досягнення цілей високотехнологічного проєкту. Проаналізовано дисертаційні роботи з управління ризиками проєктів у сфері інформаційних технологій (Information Technology, IT), захищені в Україні у 2021–2024 рр. Виявлено, що більшість теоретико-практичних результатів представлено в контексті галузі знань 12 – Інформаційні технології (спеціальності 122 – Комп'ютерні науки). Застосовано VosViewer Software для бібліометричного аналізу публікації, індексованих у науково-метричній базі Scopus. Створено бібліометричні карти ключових слів досліджень з управління ризиками ІТ проєктів та структуровано їх у дванадцять кластерів: методи управління ризиками та активами в ІТ проєктах; геоінформаційні системи, блокчейн та віртуальна реальність для сталого розвитку; інтелектуальні системи та автоматизація в управлінні інженерними проєктами; цифрова трансформація та управління змінами в інженерії; інформаційна безпека, великі дані та довіра в управлінні проєктами; управління ризиками в розробці програмних продуктів на основі інформаційного моделювання будівель (Building Information Modeling, BIM), Інтернету речей (Internet of Things, IoT) та хмарних технологій; цифрове будівництво: стратегії, безпека та співпраця; цифрові технології для управління безпекою в будівництві; аналітика для управління ризиками ІТ проєктами; управління проєктами e-Government; управління ризиками кібербезпеки; IT outsourcing: управління, стратегії та інтеграція. Представлена вибірка документів, найбільш дотичних для подальших науково-дослідних розвідок. Отримані результати можуть слугувати основою для подальших наукових досліджень у сфері управління безпекою та кібербезпекою ІТ-проєктів.

Ключові слова: бібліометричний аналіз, управління ризиками, інформаційні технології (ІТ), ІТ проєкт.

O. YASINETSKYI, T. FESENKO

IT PROJECT RISK MANAGEMENT: AN ANALYTICAL REVIEW OF RESEARCH

The purpose of the study was to determine the published body of knowledge on IT project risk management and identify modern tools, methods, artifacts for effective risk management. The basic principles, processes, methods, and tools of project risk management in international knowledge systems and standards ("Guide to the Project Management Body of Knowledge", "ISO 31000:2018. Risk management - Guidelines", 'The standard for risk management in portfolios, programs, and projects'). It is emphasized that the use of structured approaches allows minimizing uncertainty, increasing flexibility in decision-making and ensuring the effective achievement of high-tech project goals. The dissertations on risk management of projects in the field of information technology (IT), defended in Ukraine in 2021-2024, were analyzed. It was found that most of the theoretical and practical results are presented in the context of the field of knowledge 12 - Information Technology (specialty 122 - Computer Science). VosViewer Software was used for the bibliometric analysis of publications indexed in the Scopus scientific and metric database. Bibliometric maps of keywords of research on IT project risk management were created and structured into twelve clusters: methods of risk and asset management in IT projects; geographic information systems, blockchain and virtual reality for sustainable development; intelligent systems and automation in engineering project management; digital transformation and change management in engineering; information security, big data and trust in project management; risk management in the development of software products based on Building Information Modeling (BIM), Internet of Things (IoT) and cloud technologies; digital construction strategies, security, and collaboration; digital technologies for safety management in construction; analytics for IT project risk management; e-Government project management; cybersecurity risk management; IT outsourcing: management, strategies, and integration. A selection of documents most relevant for further research is presented. The results obtained can serve as a basis for further research in the field of security and cybersecurity management of IT projects.

Keywords: bibliometric analysis, risk management; information technology (IT); IT project.

Вступ. Ризик-менеджмент є критично важливою складовою управління високотехнологічними проєктами. ІТ проєкти характеризуються високим рівнем невизначеності, динамічними змінами вимог, технологічною складністю та значними фінансовими ризиками. Ефективне управління ризиками дозволяє мінімізувати потенційні загрози, оптимізувати використання ресурсів та забезпечити досягнення цілей ІТ-проєкту в межах визначених термінів і бюджету.

В системі знань Project Management Body of Knowledge (PMBOK) управління ризиками є однією з ключових областей знань, яка взаємопов'язана з управлінням графіком/термінами, вартістю, ресурсами, якістю проєкту. У PMBOK область знань «Project Risk Management» була представлена сімома процесами [1, 2]:

1) планування управління ризиками (Plan Risk Management);

2) ідентифікація ризиків (Identify Risks);

3) якісний аналіз ризиків (Perform Qualitative Risk Analysis);

4) кількісний аналіз ризиків (Perform Quantitative Risk Analysis);

5) планування реагування на ризики (Plan Risk Responses);

6) імплементація впливу на ризики (Implement Risk Responses);

7) моніторинг ризиків (Monitor Risks).

Ефективне виконання процесів управління ризиками передбачало 15 видів «інструментів та методів», зокрема: збір, аналіз даних; аудит; стратегії загроз, можливостей, можливого і загального реагування; розподіл ризиків; представлення даних; експертна оцінка; міжособистісні та командні навички;

наради; база даних ефективних рішень; прийняття рішень; інформаційна система управління проєктами.

Найбільшу кількість видів методів та інструментів потребує виконання процесу «Планування реагування на ризики» [1–3].

У новій редакції PMBOK [4] управління ризиками презентується на рівні принципу управління проєктами – «Оптимізувати реагування на ризики» («Optimize Risk Responses») та в контексті сфери виконання «Невизначеність» («Uncertainty Performance Domain»). Заходи реагування на ризики повинні бути [4, с. 53]: відповідними значущості ризику; економічно ефективними; реалістичними в контексті проєкту; погодженими відповідними стейкхолдерами; у власності відповідальної особи.

Сфера виконання «Невизначеність» охоплює різні аспекти і наслідки реалізації ризикованих подій. Розробка сценаріїв успішного подолання різних форм невизначеності буде передбачати застосування «власних пулів» інструментів. Так, варіантами реагування на загальну невизначеність можуть бути: збір додаткової інформації; підготовка до декількох варіантів кінцевих результатів (наприклад, основне рішення та рішення з врахуванням форс мажорної ситуації); компромісні альтернативні рішення; реагування на несподівані зміни – розвиток стійкості.

Дослідження і розв'язання неоднозначності реалізується шляхом застосування:

- прогресивної декомпозиції, як ітеративного процесу підвищення рівня деталізації плану управління проєктом за рахунок врахування більшого обсягу інформації та більш коректних оцінок;
- експериментів для виявлення причинно-наслідкових взаємозв'язків;
- прототипів для ідентифікації взаємозв'язків між різними змінними.

Зробити правильні прогнози та оцінки ймовірності потенційного кінцевого результату допоможуть інструменти «подолання зі складністю»: роз'єднання (відокремлення частин системи, зменшення кількості взаємопов'язаних змінних); симуляція компонентів системи; врахування багатогранності точок зору на систему; балансування між даними та ретроспективними показниками; ітерації; залучення стейкхолдерів; «запобіжні» заходи (наприклад, створеня резервних копій).

В середовищах, схильних до швидких та неочікуваних змін, які впливають на вартість і розклад проєкту, може виникати волатильність (volatility). Уникнути впливу волатильності на показники проєкту можливо за рахунок аналізу альтернатив та використання резерву вартості та(або) розкладу.

Для ефективного управління ризиками команді ІТ проєкту необхідно розглядати п'ять альтернативних стратегій:

1) уникнення (для загроз) або використання (для можливостей);

2) екскалація (якщо реакція на ризик перевищує повноваження менеджера);

3) прийняття або розподіл наслідків ризиків третій стороні;

4) пом'якшення (для загроз) або посилення (для можливостей);

5) прийняття ризику без планування жодних заходів.

Про ефективне управління ризиками будуть свідчити створені артефакти виконання проєкту, такі як: реєстр ризиків, план управління ризиками, ієрархічна структура ризиків, діаграма причин і наслідків, звіт про ризики, угоди та контракти та ін. (табл. 1).

Таблиця 1 – Відповідність артефактів управління ризиками використанню в сферах виконання проєкту

Артефакти управлі ння ризиками	Сфера «Виконання»					
	Стейкхолдери	Планування	Проєктна робота	Постачання	Вимірювання	Невизначеність
Артефакти журналів та реєстрів						
Журнал припущень		X	X	X		X
Беклог з урахуванням ризиків		X				X
Реєстр ризиків		X	X	X		X
Артефакт-план						
План управління ризиками		X	X			X
Артефакт діаграм ієрархії						
Ієрархічна структура ризиків			X			X
Артефакт інформації та візуальних даних						
Діаграма причин і наслідків			X	X		X
Артефакт звітності						
Звіт про ризики			X			X
Угоди та контракти						
З фіксованою вартістю	X	X	X	X	X	X
З відшкодуванням витрат	X	X	X	X	X	X
Контракт «Час та матеріали»	X	X	X	X	X	X
Невизначене постачання невизначеної кількості (Indefinite time indefinite quantity, IDIQ)	X	X	X	X	X	X
Інші угоди	X	X	X	X	X	X

Міжнародним стандартом «ISO 31000:2018. Risk management – Guidelines» [5] визначено принципи та рекомендації щодо комплексного підходу для виявлення, аналізу, оцінки, реагування, моніторингу та передачі інформації про ризики. До інструментів і методів пом'якшення загроз та посилення можливостей включено:

- всебічне розуміння (Comprehensive Understanding): сприяє спільному розумінню ризиків, їх природи та способів управління ними в усій організації;

- прийняття стратегічних рішень (Strategic Decision-Making): рекомендації допомагають включити управління ризиками в процеси управління, стратегії, планування, звітності, політику, цінності та культуру організації;

- операційна досконалість (Operational Excellence): впровадження ISO 31000 може привести до підвищення ефективності, оскільки допомагає організаціям вчасно розпізнавати потенційні загрози та можливості, розумно розподіляти ресурси та підвищувати довіру зацікавлених сторін;

- проактивний підхід (Proactive Approach): ISO 31000 надає організаціям можливість передбачати та вирішувати ризики безпосередньо, перетворюючи потенційні виклики на стратегічні переваги;

- довіра зацікавлених сторін (Stakeholder Confidence): структурований підхід до управління ризиками сигналізує зацікавленим сторонам – від інвесторів до клієнтів – про те, що організація надійно готова долати невизначеності, зміцнюючи довіру та надійність.

У стандарті [6] визначено компоненти управління ризиками для інтеграції на рівні управління портфелями, програмами та проєктами. Життєвий цикл управління ризиками (Risk Management Life Cycle, RMLC) окреслює послідовність логічних фаз/процесів [6, с. 28–29], які корелюються з сьома процесами області знань «Project Risk Management» [1, 2]. Для ефективного управління ризиками та виконання процесів RMLC необхідно дотримуватись принципів (Principles of Risk Management) [6]:

- досягнення досконалості в практиці управління ризиками;

- узгодження управління ризиками з організаційною стратегією та практикою управління;

- зосередження на найбільш вагомих і впливових ризиках;

- дотримання балансу між впливом на ризик та досягнутої цінності проєкту;

- сприяння культурі управління ризиками;

- подолання складності для досягнення успішних результатів проєкту завдяки управлінню ризиками;

- постійне удосконалення навичок з управління ризиками.

Отже, управління ризиками ІТ-проєктів є багатогранним процесом, що охоплює ідентифікацію, аналіз, планування та реагування на ризики з урахуванням сучасних стандартів і кращих практик. Використання структурованих підходів, таких як PMBOK, ISO 31000 та RMLC, дозволяє мінімізувати невизначеність, підвищити гнучкість у прийнятті рішень і забезпечити ефективне досягнення цілей проєкту. Водночас, зростання складності ІТ-проєктів потребує постійного вдосконалення методичного інструментарію для аналізу та реагування на ризики.

Мета і завдання дослідження. Метою дослідження є окреслення публікаційного кола знань з управління ризиками ІТ проєктів та ідентифікація сучасних інструментів, методів, артефактів для ефективного управління ризиками.

Для досягнення поставленої мети дослідження були сформульовані наступні завдання:

- здійснити пошук дисертаційних досліджень з управління ризиками ІТ проєктів, окреслити наявні науково-практичні результати та виявити дослідницькі прогалини;

- проаналізувати публікації за тематикою «управління ризиками ІТ проєктів», розміщені у науково-метричній базі Scopus, шляхом розробки бібліографічних карт із використанням VosViewer Software.

Аналіз дисертаційних досліджень з управління ІТ проєктами. Управління ризиками ІТ проєктів досліджується в контексті різних галузей знань: інформаційних технологій [7–9], управління та адміністрування [10, 11], економіки [12, 13].

У дисертації [7] авторкою розроблено комплекс моделей інтегрованого управління загрозами та можливостями в ІТ проєктах. Запропонована модель RIO-RIT-REO-RET-аналізу дозволяє на етапі ідентифікації ризиків аналізувати проєкт з точку зору: сильних або слабких сторін, сприятливих можливостей та загроз. Застосовуючи інтелектуальну модель вибору оптимальної стратегії управління ризиками (загрозами та можливостями) можна враховувати графи розвитку подій, синергію можливих загроз та можливостей.

У [8] ризик розглядається крізь призму випадків: «ІТ-інцидентів» та «ІТ-загроз». Автором запропоновано метод визначення стану захищеності об’єктів критичної інформаційної інфраструктури від ІТ ризиків, який передбачає виконання наступних дій: визначення загальних метрик ІТ-безпеки; обчислення індексу цифрової трансформації; розрахунок кількісних параметрів стану захищеності та аналізу результатів з розробкою рекомендацій для оптимізації захисту. Для визначення пріоритетів ІТ-інцидентів застосовується метод парних порівнянь (метод аналізу ієрархій), для оцінювання ІТ-загроз – методи багатокритеріального прийняття рішень TODIM (Interactive Multi-Criteria Decision Making,), STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege).

В [9] акцентується увага на інформаційних ризиках, які супроводжують процес цифрової трансформації бізнесу і призводять до втрати конфіденційності, цілісності та доступності інформації в компанії. Автором запропонована «концептуальна модель управління інформаційними ризиками в проєктах цифрової трансформації бізнесу», яка ґрунтується на організаційному підході: «оточення → організація → проєкт». Такий підхід дозволяє на етапі оптимізації бізнес-процесів дозволяє врахувати імовірність настання інформаційних ризиків та обирати той варіант оптимізаційного процесу, який буде найменш ризикованим та відповідати вимогам стейкхолдерів проєкту.

У дисертації [10] досліджувались теоретичні, методичні та практичні аспекти формування системи управління ризиками в ІТ-проєктах. Запропонована автором інтегрована система управління ризиками ІТ-

проєкту включає: визначення цілей проєкту, схильності до ризику, комунікацію рівня схильності до ризику в команді і узгодження його із зацікавленими сторонами, впровадження ризик-апетиту в загальні процеси управління проєктом, моніторинг ризик-апетиту в процесі виконання проєкту. Процес формування програми управління ризиками проєкту розглядається як цикл з шести етапів: ідентифікація ризиків; аналіз ризиків проєкту; планування зменшення впливу ризиків; моніторинг ризиків; закриття ризиків в реєстрі ризиків; бюджетування ризиків. Запропонований підхід дозволить проєктним менеджерам розробляти програми управління ризиками проєкту з врахуванням контексту та інтересів усіх стейкхолдерів.

В [11] розроблено комплекс рішень для організаційно-економічного забезпечення системи управління проєктними ризиками в ІТ-компаніях. Запропонований концептуальний підхід до формування системи управління проєктними ризиками передбачає синхронізацію усіх складових системи (елементів і процесів): мету; суб'єкти; об'єкти; засоби управлінського впливу; три основні функціональні підсистеми забезпечення (організаційну, економічну та поведінкову); етап діагностики та моніторингу. В рамках організаційного підходу до функціонування команди проєкту, яка використовує гнучкі методології (Scrum, Lean та Kanban), ідентифіковано основні проблеми, що виникають у процесі реалізації проєкту в ІТ-секторі, та запропоновано дії реагування на фактори впливу на ефективність.

Авторкою дисертації [12] представлена концепція ризик-орієнтованого управління системою економічної безпеки підприємства, яка поєднує підходи, принципи, методи та інструменти ризик-орієнтованого управління із методологічними засадами забезпечення економічної безпеки. Запропонований комплекс інструментів управління ризиками (класифікатор ризиків, матриця ризиків, вимоги до кваліфікації ризик менеджера, перелік ризиків і загроз економічної безпеки та ін.) враховує особливості практики українських ІТ компаній.

В дисертаційній роботі [13] досліджувались теоретико-методичні та прикладні засади розвитку управління ризиками в телекомунікаційних підприємствах у нових економічних реаліях (повномасштабного вторгнення російської федерації в Україну). Запропоновані методичні підходи до модернізації механізму розвитку управління ризиками ґрунтуються на структуруванні контрольно-дозвільної комплаєнс-функції та запроваджені проактивних методів управління. Розроблено кватровекторну модель розвитку управління ризиками на телекомунікаційних підприємствах та модель взаємозв'язку «стратегічні наміри – ризики» з врахуванням: ризиків, пов'язаних з воєнним та післявоєнним відновленням; ризиками реструктуризації, модернізації та розвитку; інвестиційними ризиками, комплаєнс-ризиками, ІТ-ризиками.

Бібліометричний аналіз досліджень з управління ризиками ІТ проєктів. В науково-метричній базі Scopus за результатом пошукового запиту «Information AND technology AND project AND risk AND management» виявлено 4 306 документів, опублікованих у 1963-2025 роках, більшість з яких презентовані за останні 10 років (2 160 документів, 2015–2025 рр.). В результаті бібліометричного аналізу за предметом дослідження виявлено, що дослідницькі завдання з управління ризиками ІТ проєктів виконувались в контексті 27 областей (галузей) знань: від інженерії та комп'ютерних наук до мистецтва та гуманітарних наук (див. рис. 1). На наступному етапі аналізувались публікації, які відносились до галузі інженерії (Engineering), комп'ютерних наук (Computer Science), бізнесу і менеджменту (Business, Management and Accounting) – 1 597 документі.

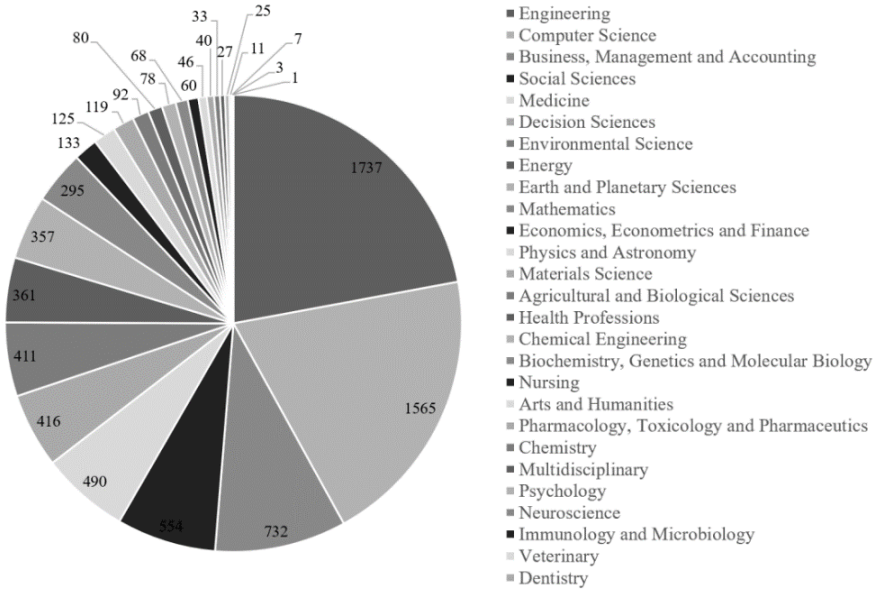


Рис. 1. Репрезентативність публікацій з управління ризиками ІТ проєктів, розміщених у науково-метричній базі Scopus, за предметними областями (галузями)

Для публікації результатів досліджень автори частіше обирали журнали:

- «ACM International Conference Proceeding Series» (37 документів);
- «Applied Mechanics and Materials Series» (32 документа);
- «Lecture Notes in Networks and Systems» (31 документ);
- «Ceur Workshop Proceedings» (30 документів);
- «Procedia Computer Science» (29 документів).

Водночас найбільш цитовані публікації розміщені у таких виданнях як:

- Australasian Journal of «Construction Economics and Building» (стаття [14] цитувалась 559 раз);
- IEEE Transactions on Software Engineering (стаття [15] цитувалась 557 раз);
- «Journal of Construction Engineering and Management» (стаття [16] цитувалась 546 раз);
- «Journal of Construction Engineering and Management» (стаття [17] цитувалась 406 раз);
- «IEEE Communications Surveys and Tutorials» (рецензія [18] цитувалась 395 раз).

Географія досліджень з управління ризиками ІТ проєктів охоплює авторів з 88 країн світу, зокрема: Сполучених Штатів Америки (322 документів), Китаю (208 документів), Великої Британії (126 документів), Австралії (64 документа), Канади (54 документа), України (25 документів). Найбільшу кількість публікацій мають дослідники, які працюють у таких установах, як:

- The Hong Kong Polytechnic University (Китай) – 12 документів;
- Georgia State University (Грузія) та Huazhong University of Science and Technology (Китай) – по 11 документів;
- Universiti Teknologi MARA (Малазія) та University of Tehran (Іран) – по 10 документів.

Важливим елементом бібліометричного аналізу є частота використання ключових слів. Встановлено, що у 1 597 досліджуваних документах міститься 160 ключових слів, такі як:

- «Project Management» (згадується у 654 документах);
- «Risk Management» (згадується у 539 документах);
- «Project Management» (згадується у 529 документах);
- «Information Technology» (згадується у 427 документах);
- «Risk Assessment» (згадується у 377 документах);
- «Information Management» (згадується у 310 документах).

Застосування веб-інструменту WordItOut дозволило згенерувати хмару ключових слів на тему «управління ризиками ІТ проєктів» (див. рис. 2). Діаграма частоти використання ключових слів представлена на рис. 3.

Рис. 2. Хмара ключових слів публікацій з управління ризиками ІТ проєктів, розміщених у науково-метричній базі Scopus, із використанням онлайн-інструменту WordItOut

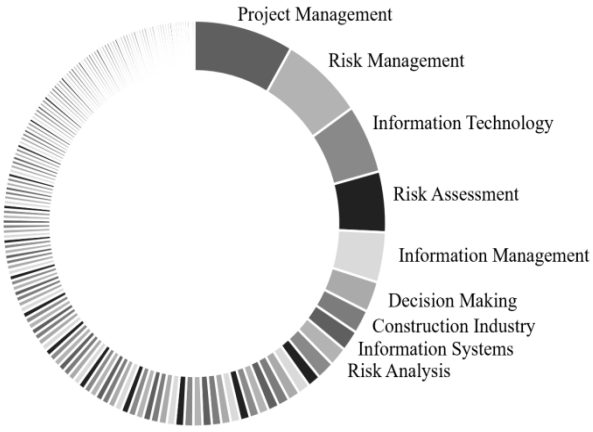


Рис. 3. Діаграма частоти згадування ключових слів у публікаціях з управління ризиками ІТ проєктів, розміщених у науково-метричній базі Scopus

Кластерний аналіз досліджень з управління ризиками ІТ проєктів здійснювався із використанням програми VOSviewer. На рис. 4 наведена бібліометрична карта для 123 ключових слів (які відповідали обмеженню «мінімальна кількість повторів – 5»), структурованих у 12 кластерів:

- кластер 1 (червоний колір) – 17 ключових слів (project risk management, risk control, risk evaluation, risk identification, risk mitigation, asset management knowledge management та ін.);
- кластер 2 (зелений колір) – 15 ключових слів (evaluation, project performance, blockchain, virtual reality, ontology, sustainable development та ін);
- кластер 3 (синій колір) – 14 ключових слів (artificial intelligence, machine learning, natural language processing, neural networks, data analysis, decision support system та ін.);
- кластер 4 (гірчичний колір) – 12 ключових слів (change management, digital technologies, digital transformation, industry 4.0, information system, supply chain management та ін.);
- кластер 5 (фіолетовий колір) – 11 ключових слів (cyber security, information security, security, privacy, trust, interoperability, big data та ін.);

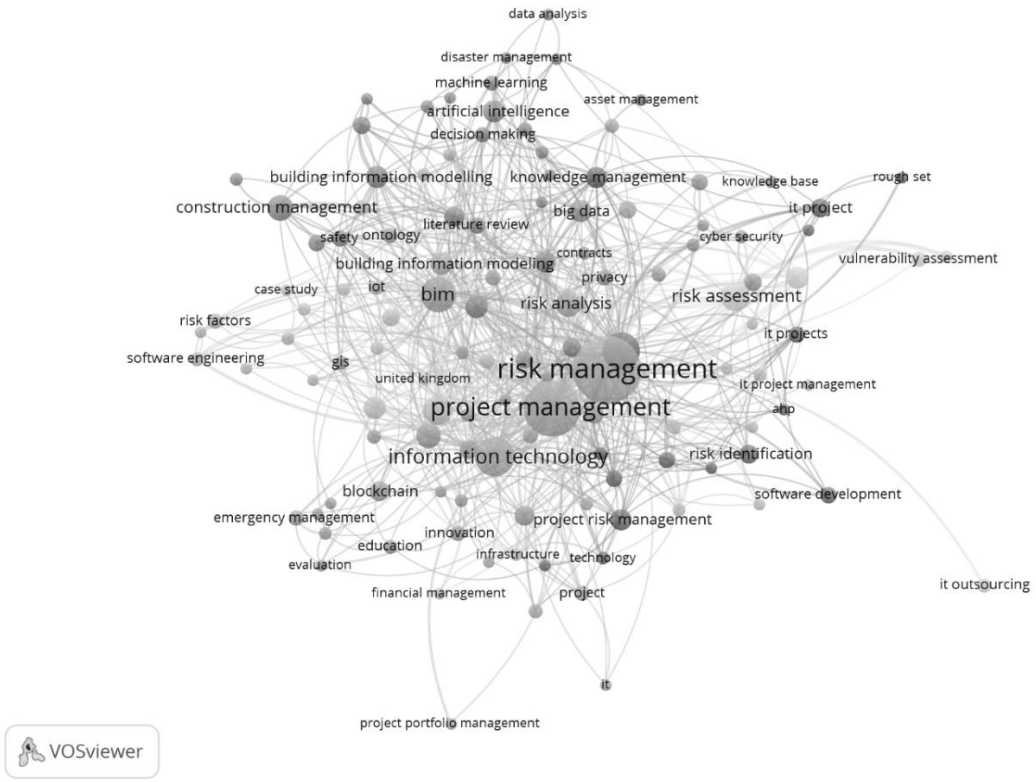


Рис. 4. Бібліометрична карта кластерів ключових слів (items) публікацій з управління ризиками IT проєктів, розміщених у науково-метричній базі Scopus

- кластер 6 (бірюзовий колір) – 11 ключових слів (cloud computing, internet of things, risk factors, risk management, project planning, scheduling та ін.);

- кластер 7 (помаранчевий колір) – 10 ключових слів (adoption, integration, stakeholders, strategy, bim, construction safety та ін.);

- кластер 8 (коричневий колір) – 10 ключових слів (decision making, information management, information systems, safety management, building information modelling та ін.);

- кластер 9 (рожевий колір) – 10 ключових слів (data mining, decision support systems, project portfolio management, risk analysis та ін.);

- кластер 10 (кораловий колір) – 8 ключових слів (critical success factors, e-government, implementation, it governance та ін.);

- кластер 11 (салатовий колір) – 4 ключових слова (cybersecurity, process safety lifecycle, risk assessment, vulnerability assessment);

- кластер 12 (блакитний колір) містить тільки одне ключове слово – «IT outsourcing».

Для 123 ключових слів програма VOSviewer встановила 671 взаємозв'язків. При цьому програма дозволяє «підсвічувати» взаємозв'язки для кожного слова (див. рис. 5). Примітно, що за останні два роки в дослідженнях з управління ризиками в IT проєктах використовувались ключові слова: artificial learning, machine learning, blockchain, digital transformation, internet of things, dig data, digital twin, natural language processing, automation (див. рис. 5).

Структуризація ключових слів за кластерами дозволила виявити, що значна кількість досліджень з управління ризиками IT проєктами (опублікованих у Scopus) стосується використання технологій інформаційного моделювання будівель (Building Information Modeling, BIM), геоінформаційних систем, (Geographic information system, GIS), інтелектуальних систем та автоматизації в будівництві (табл. 2):

- кластер 2. Геоінформаційні системи (ГІС), блокчейн та віртуальна реальність для сталого розвитку;

- кластер 3. Інтелектуальні системи та автоматизація в управлінні інженерними проєктами;

- кластер 4. Цифрова трансформація та управління змінами в інженерії;

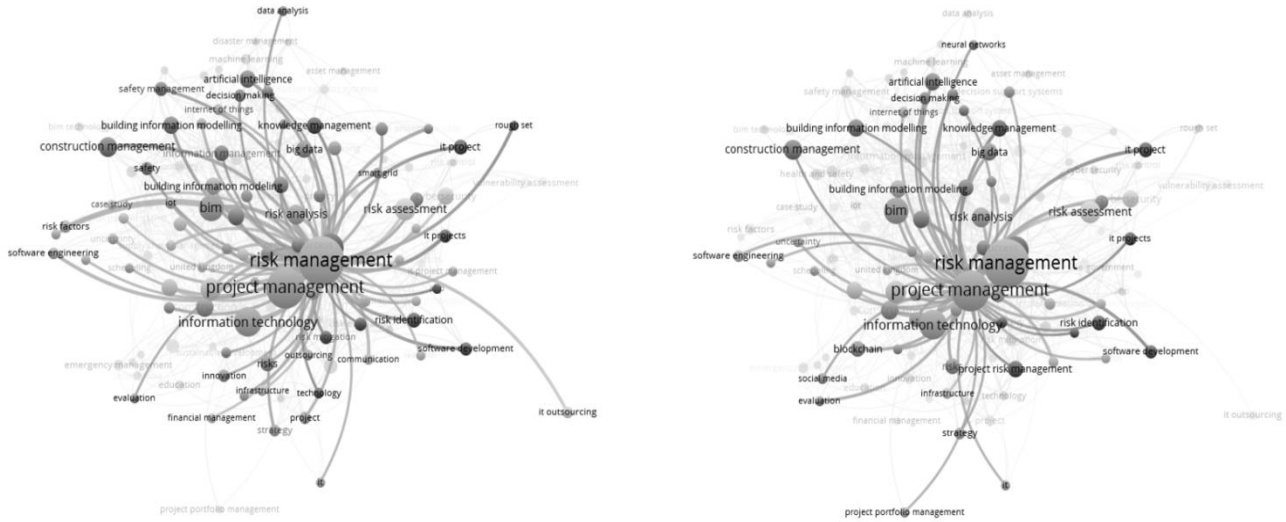
- кластер 5. Інформаційна безпека, великі дані та довіра в управлінні проєктами;

- кластер 6. Управління ризиками в розробці програмних продуктів на основі BIM, IoT та хмарних технологій;

- кластер 7. Цифрове будівництво: стратегії, безпека та співпраця;

- кластер 8. Цифрові технології для управління безпекою в будівництві.

Менш популярними предметами дослідження були питання електронного урядування (Кластер 10. Управління проєктами e-Government) та кібербезпеки (Кластер 11. Управління ризиками кібербезпеки).



а *б*

Рис. 5. Приклади бібліометричних карт для вибраних ключових слів (items) з «підсвіченням» взаємозв'язків: а – «Risk Management»; б – «Project Management»

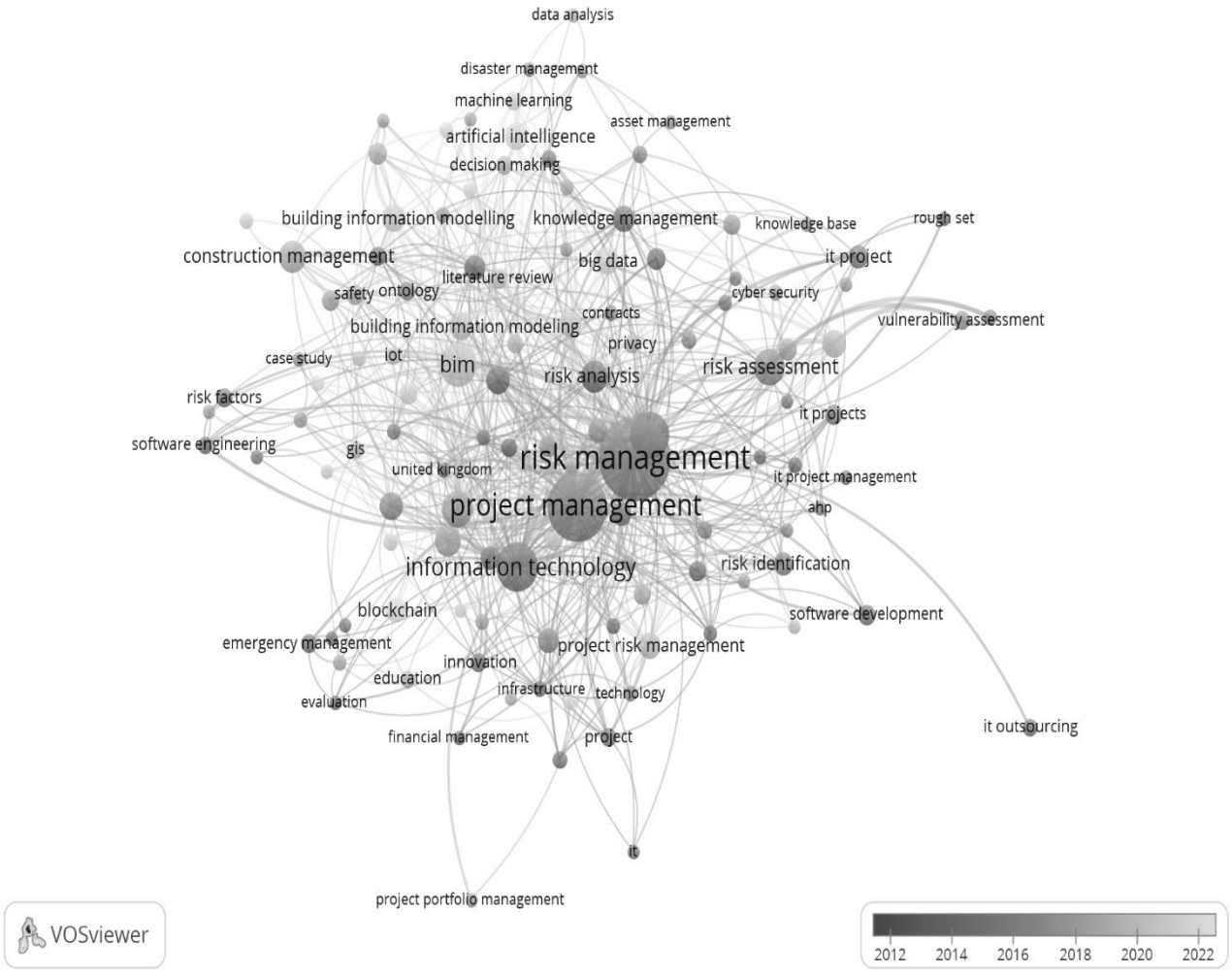


Рис. 6. Бібліометрична карта ключових слів (items) публікацій з управління ризиками ІТ проєктів, розміщених у науково-метричній базі Scopus

Таблиця 2 – Структуризація ключових слів (items) у дослідженнях з управління ризиками IT проєктів, розміщених у науково-метричній базі Scopus

Назва кластеру	Ключові слова (items)	Опис кластеру
Кластер 1. Методи управління ризиками та активами в IT проєктах	- **Project risk management; Risk;** Risk control; Risk evaluation; Risk identification; Risk mitigation; Asset management Knowledge management; - **AHP** (Analytic Hierarchy Process); **Fuzzy Logic; Rough Set;** - **IT project; IT projects; Software Development;** Technology; Complexity; COVID-19	Охоплює концепції, методи та інструменти для управління ризиками в IT проєктах. Також поєднує підходи до оцінки ризиків, прийняття рішень, управління активами та технологічні аспекти, що забезпечують ефективне управління невизначеністю та складністю високотехнологічних проєктів
Кластер 2. Геоінформаційні системи (ГІС), блокчейн та віртуальна реальність для сталого розвитку	- **Risks; Evaluation; Project performance;** - **Blockchain; GIS** (Geographic information system); **Virtual reality**; Social media; Innovation; Ontology; - **Sustainable development**; Emergency management; Construction; Education; Earth observation; Natural disasters	Включає технології та методи управління ризиками IT проєктів, що допомагають враховувати контекст, зокрема: кризового менеджменту, аналізу природних загроз, будівництва, освіти, сталого розвитку. Використання блокчейну, ГІС, віртуальної реальності та соціальних медіа допомагає мінімізувати ризики, підвищити ефективність проєктів та сприяти їх безпечному розвитку.
Кластер 3. Інтелектуальні системи та автоматизація в управлінні інженерними проєктами	- **Artificial Intelligence** (AI); **Machine Learning** (ML); Natural Language Processing (NLP); Neural Networks; - **Data analysis; Decision support system**; Automation; Disaster management; **Building Information Modeling** (BIM); Sensors; - Construction project management; Design; Literature review; Project success	Відображає застосування інноваційних технологій у сфері управління ризиками IT проєктів переважно у будівництві та інженерії, такі як: штучний інтелект (AI), автоматизацію, аналіз даних, BIM, сенсори та системи підтримки прийняття рішень (DSS). Ці технології використовуються для зменшення ризиків і підвищення ефективності проєктів.
Кластер 4. Цифрова трансформація та управління змінами в інженерії	- **Change management**; Digital technologies; Digital transformation; Industry 4.0; - **Information system**; Radio-Frequency Identification **(RFID)**; Supply chain management; Financial management - **Infrastructure**; Case study; Construction industry; United Kingdom	Охоплює ключові аспекти (технічні, фінансові, організаційні та операційні), які супроводжують ризики цифрової трансформації та впровадження Індустрії 4.0 в інженерії, у тому числі будівництві, логістиці
Кластер 5. Інформаційна безпека, великі дані та довіра в управлінні проєктами	- **Cyber security**; **Information security**; Security; Privacy; Trust; - **Interoperability**; Big Data; Construction project; Contracts; Knowledge base; Smart Grid	Об'єднує аспекти кібербезпеки, довіри, конфіденційності, великих даних і цифрової інфраструктури у контексті управління ризиками IT проєктів у будівництві та енергетиці (Smart Grid)
Кластер 6. Управління ризиками в розробці програмних продуктів на основі BIM, IoT та хмарних технологій	- **BIM; Cloud Computing; Internet of Things** (IoT); - **Risk factors**; Risk management; Project planning; Scheduling - Software engineering; **Software risk;** Uncertainty	Відображає взаємозв'язок між управлінням ризиками, плануванням, розробкою програмного забезпечення та специфікою застосування BIM-технологій, IoT і хмарних обчислень
Кластер 7. Цифрове будівництво: стратегії, безпека та співпраця	- **Adoption**; Integration; Stakeholders; Strategy; - **BIM; Collaboration; Construction Safety**; Digital Twin; Supply chain	Характеризує комплексний підхід впровадження BIM, що враховує взаємозв'язок цифрових технологій та організацією співпраці між різними учасниками, безпекою для досягнення стратегічних завдань та управління ризиками
Кластер 8. Цифрові технології для управління безпекою в будівництві	- **Decision making; Information management; Information systems; Safety management**; - BIM technology; Building information modelling; Construction management; Health and safety; Occupational health and safety; Safety	Відображає взаємозв'язок між управлінням IT ризиками та впровадженням цифрових технологій у будівництві. Успішне управління цими ризиками дозволяє підвищити ефективність будівельних процесів, покращити безпеку праці та мінімізувати можливі технічні та організаційні загрози.
Кластер 9. Аналітика для управління ризиками IT проєктів	Data mining; **Decision Support Systems**; Information technology; IT; Management; Outsourcing; Project; **Project Management; Project Portfolio Management; Risk Analysis**	Охоплює аспекти використання сучасних технологій аналізу даних, системи підтримки прийняття рішень для мінімізації ризиків, оптимізацію ресурсів та стратегічне управління портфелем IT проєктів
Кластер 10. Управління проєктами e-Government	**Communication; Critical success factors**; E-Government; Implementation; Information technologies; **IT Governance**; **IT project management**; Research	Характеризує ключові аспекти управління ризиками IT проєктів цифрового врядування (*e-Government*), ефективного управління комунікаціями та забезпечення відповідності стандартам управління (*IT Governance*)
Кластер 11. Управління ризиками кібербезпеки	**Cybersecurity**; Process safety lifecycle; **Risk assessment; Vulnerability assessment**	Основна увага приділяється ідентифікації потенційних кіберзагроз, оцінці ризиків, розробці стратегій реагування та забезпечення безперервної безпеки інформаційних систем
Кластер 12. IT Outsourcing: управління, стратегії та інтеграція	IT outsourcing	Передбачає передачу зовнішнім постачальникам IT функцій, таких як: стратегічне планування, управління ризиками, інтеграція зовнішніх рішень, ефективна взаємодія зі стейкхолдерами. Основна увага приділяється вибору підрядників, управлінню контрактами, контролю якості послуг, забезпеченню безпеки даних та оптимізації витрат.

Подальший пошук публікацій більш релевантних до наукових інтересів дослідника може базуватись на обмеженні пошуку за ключовими словами відповідного кластера(рів). Наприклад, задавши обмеження пошуку словами «Security of Data», «Safety Management», «Cybersecurity», «Cyber Security» із 1 597 документів було відібрано 210 публікацій, з яких знайдено дев'ять документів, найбільш дотичних до тематики управління безпекою та кібербезпекою в IT проєктах (див. табл. 3).

Таблиця 3 – Публікації з управління ризиками IT проєктів, розміщені у науково-метричній базі Scopus, які найбільш релевантні для Кластера 11. Управління ризиками кібербезпеки

Назва документу	Автор(ри)	Тип документа	Рік	Кількість цитат
Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects [19]	de Carvalho R. M., Del Prete C., Martin Y S., Araujo Rivero R. M., Önen M., Schiavo F. P., Rumín Á. C., Mouratidis H., Yelmo J. C., Koukovini M. N., Yelmo J. C.	Article	2020	14
Cyberspace and Cybersecurity [20]	Kostopoulos G.K.	Book Chapter	2012	8
Development of Metamodel for Information Security Risk Management [21]	Salem M., Othman S. H., Al-Dhaqm A., Ali A.	Book Chapter	2023	8
The role of data governance in cybersecurity for E-municipal services: Implications from the case of Turkey [22]	Çubuk E. B. S., Zeren H. E., Demirdöven B.	Book Chapter	2022	4
Simulation of information security risks of availability of project documents based on fuzzy logic [23]	Shushura O. M., Asieieva L. A., Nedashkivskiy O. L., Havrylko Y. V., Moroz Y. O., Smailova S. S., Sarsembayev M.	Article	2022	4
Security infrastructure technology for integrated utilization of big data: Applied to the living safety and medical fields [24]	Miyaji S., Mimoto T.	Book	2020	3
Understanding lean & safety projects: Analysis of case studies [25]	Crema M., Verbano C.	Article	2017	2
Challenges in cybersecurity and privacy – the European research landscape [26]	Bernabe J. B., Skarmeta A.	Book	2019	1
Cyber Security Control Systems for Operational Technology [27]	Sriram S.	Book Chapter	2024	0

Висновки. Управління ризиками є невід'ємною частиною реалізації високотехнологічних проєктів. Для ефективного управління ризиками застосовуються різноманітні інструменти та методи, такі як збір і аналіз даних, стратегічне прийняття рішень, симуляція, прогресивна деталізація та інші. Дотримання стандартів [3–5] сприяє системному підходу до управління ризиками та підвищенню довіри зацікавлених сторін. Разом з тим, складність IT-проєктів та швидкі зміни середовища потребують безперервного удосконалення методичного інструментарію для аналізу та реагування на ризики.

Аналіз існуючих дисертаційних досліджень показав, що управління ризиками IT проєктів розглядається в контексті різних галузей знань, зокрема інформаційних технологій (спеціальності 122 – Комп'ютерні науки), управління та адміністрування, економіки і були захищені у 2021–2024 рр. Виявлено певні дослідницькі прогалини: по-перше, недостатня увага приділялась використанню динамічних методів аналізу ризиків (у тому числі, інструментів штучного інтелекту, машинного навчання), по-друге, відсутній ґрунтовний аналіз ризиків кібербезпеки в умовах цифрової трансформації та роботи з хмарними технологіями.

Бібліометричний аналіз публікацій, розміщених у науково-метричній базі Scopus, із використанням програми VOSviewer дозволив розробити бібліометричні карти ключових слів та візуалізувати дослідниці акценти у формуванні знань з управління ризиками IT проєктів. Описано дванадцять кластерів ключових слів: 1 – Методи управління ризиками та активами в IT проєктах; 2 – Геоінформаційні системи, блокчейн та віртуальна реальність для сталого розвитку; 3 – Інтелектуальні системи та автоматизація в управлінні інженерними проєктами; 4 – Цифрова трансформація та управління змінами в інженерії; 5 – Інформаційна безпека, великі дані та довіра в управлінні проєктами; 6 – Управління ризиками в розробці програмних продуктів на основі BIM, IoT та хмарних технологій; 7 – Цифрове будівництво: стратегії, безпека та співпраця; 8 – Цифрові технології для управління безпекою в будівництві; 9 – Аналітика для управління ризиками IT проєктами; 10 – Управління проєктами e-Government; 11 – Управління ризиками кібербезпеки; 12 – IT outsourcing: управління, стратегії та інтеграція.

Кластерний аналіз дозволив виявити, що більшість публікацій (сім кластерів із дванадцяти) презентують результати використання BIM-технологій GIS-систем та автоматизації в будівництві і в меншій мірі представлені рішення для управління ризиками проєктів електронного урядування та кібербезпеки.

Перспективним напрямком для подальших досліджень вбачається аналіз поведінкових аспектів ризик-менеджменту, застосування AI та Big Data для прогнозування та моделювання ризиків, а також управління ризиками кібербезпеки.

Список літератури

1. *A Guide to the project management body of knowledge (PMBOK® Guide): Sixth Edition*. USA: Project Management Institute, 2017. 756 p.
2. Фесенко Т. Г. *Управління проектами: теорія та практика виконання проектних дій: навч. посібник*. Харків : ХНАМГ, 2012. – 181 с.
3. Фесенко Т. Г., Мохамед Абдулсалам Сієк Алі. Моделювання оцінки «Risk Management» в системі управління будівельними проектами. *Вісник Черкаського державного технологічного університету. Серія : Технічні науки*. 2018. № 2. С. 120–127. URL:: http://nbuv.gov.ua/UJRN/Vchdtu_2018_2_21.
4. *A Guide to the project management body of knowledge (PMBOK® Guide: Seven Edition) and The standard for project management*. USA: Project Management Institute, 2021. 370 p.
5. *ISO 31000:2018. Risk management. Guidelines*. Switzerland, 2018. 16 p.
6. *The standard for risk management in portfolios, programs, and projects*. USA: Project Management Institute, 2019. 175 p.
7. Грабіна К. В. *Моделі та методи інформаційної технології управління ризиками в ІТ-проєктах: дис. … д-ра філос. : 122 – Комп'ютерні науки*. Сум.ДУ. Суми, 2024. 185 с. URL:: https://essuir.sumdu.edu.ua/bitstream-download/123456789/97100/1/Hrabina_K_PhD_thesis.pdf. (дата звертання : 19 січня 2025).
8. Положенцев А. А. *Методи та засоби управління ІТ-інцидентами на об'єктах критичної інформаційної інфраструктури: дис. … д-ра філос. : 122 – Комп'ютерні науки*. НАУ. Київ, 2024. 180 с. URL: https://vchenarada.nau.edu.ua/wp-content/uploads/2024/07/disertatsiya-Polozhentsev.pdf. (дата звертання : 19 січня 2025).
9. Семко О. В. *Інформаційна технологія управління інформаційними ризиками в проєктах цифрової трансформації бізнесу: дис. … д-ра філос. : 122 – Комп'ютерні науки.* ЧДТУ. Черкаси, 2024. 210 с. URL: https://er.chdtu.edu.ua/handle/ChSTU/4792. (дата звертання : 19 січня 2025).
10. Макарчук І. В. *Управління ризиками ІТ-проєктів на підприємстві: дис. … д-ра філос. : 073 – Менеджмент*. ДТЕУ. Київ, 2023. 254 с. URL: https://knute.edu.ua/file/Mg==/adcd9a7a02ff2aff4977bfaab4ba86ba.pdf. (дата звертання : 19 січня 2025)
11. Іванов М. Є. *Організаційно-економічне забезпечення системи управління проектними ризиками в ІТ-компаніях: дис. … д-ра філос. : 073 – Менеджмент*. НДЦ індустр. пробл. розв. Харків, 2023. 217 с. URL: https://ndc-ipr.org/media/spec_council/abstracts/Ivanov_MYe_PhD_Thesis_3.pdf. (дата звертання : 19 січня 2025).
12. Герасименко О. М. *Ризик-орієнтоване управління в системі економічної безпеки підприємства: дис. … д-ра екон. наук. : 21.04.02 – економічна безпека суб'єктів господарської діяльності*. ЧНУ ім. Б. Хмельницького. ПВНЗ «КРОУ». Київ, 2021. 667 с. URL: ttps://library.krok.edu.ua/media/library/category/disertatsiji-avtoreferati-vidguki/gerasimenko_2021-disertatsija.pdf. (дата звертання : 19 січня 2025).
13. Захаржевська А. А. *Розвиток управління ризиками телекомунікаційних підприємств: автореф. … канд. екон. наук. : 08.00.04 – економіка та управління підприємствами*. Держ. ун-т телекомун. Київ, 2024. 24 с. URL: https://duikt.edu.ua/uploads/p_1537_93188893.pdf?file=p_1537_93188893.pdf. (дата звертання : 19 січня 2025).
14. Azhar S., Khalfan M., Maqsood T. Building information modelling (BIM): now and beyond. *Construction Economics and Building*. 2015. № 12(4). P. 15–28. doi.org/10.5130/AJCEB.v12i4.3032.
15. Putnam L. H. A General Empirical Solution to the Macro Software Sizing and Estimating Problem. *IEEE Transactions on Software Engineering*. 1978. № SE-4 (4). P. 345–361. doi.org\10.1109/TSE.1978.231521.
16. Zhang X. Critical success factors for public-private partnerships in infrastructure development. J*ournal of Construction Engineering and Management*. 2005. № 131 (1). P. 3–14. doi.org\10.1061/(ASCE)0733-9364(2005)131:1(3).
17. Carter G., Smith S. D. Safety hazard identification on construction projects. *Journal of Construction Engineering and Management.* 2005. № 32(2). P. 197–205. doi.org\10.1061/(ASCE)0733-9364(2006)132:2(197).
18. Khan R., Kumar P., Jayakody D. N. K., Liyanage M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys and Tutorials*. 2020. № 22 (1). P. 196–248, 8792139. doi.org\10.1109/COMST.2019.2933899.
19. de Carvalho R. M., Del Prete C., Martin Y S., Araujo Rivero R. M., Önen M., Schiavo F. P., Rumín Á. C., Mouratidis H., Yelmo J. C., Koukovini M. N., Yelmo J. C. Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects. *SN Computer Science*. 2020. № 1 (4). P. 217. doi.org\10.1007/s42979-020-00218-8.
20. Kostopoulos G. K. *Cyberspace and Cybersecurity*. 2012. 210 p.
21. Salem M., Othman S. H., Al-Dhaqm A., Ali A. Development of Metamodel for Information Security Risk Management. *Studies in Computational Intelligence*. 2023. № 1080. P. 243–253. doi.org\10.1007/978-3-031-21199-7_17.
22. Çubuk E. B. S., Zeren H. E., Demirdöven B. The role of data governance in cybersecurity for E-municipal services: Implications from the case of Turkey. *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*. 2022. P. 410–425. doi.org\10.4018/978-1-6684-5284-4.ch020.
23. Shushura O. M., Asieieva L. A., Nedashkivskiy O. L., Havrylko Y. V., Moroz Y. O., Smailova S. S., Sarsembayev M. Simulation of information security risks of availability of project documents based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska*. 2022. № 12 (3). P. 64–68. doi.org\10.35784/iapgos.3033.
24. Miyaji S., Mimoto T. Security infrastructure technology for integrated utilization of big data: Applied to the living safety and medical fields. *Singapore: Springer Nature*, 2022. 166 p.
25. Crema M., Verbano C. Understanding lean & safety projects: Analysis of case studies. *Journal of Technology Management and Innovation*. 2017. № 12 (4), P. 29–41. doi.org\10.4067/s0718-27242017000400004.
26. Bernabe J. B., Skarmeta A. *Challenges in cybersecurity and privacy – the European research landscape*. 328 p.
27. Sriram S. Security Control Systems for Operational Technology. *Industrial Control Systems*. 2024. P. 285–302. doi.org\ 10.1002/9781119829430.ch13.

References (transliterated)

1. A Guide to the project management body of knowledge (PMBOK® Guide): Sixth Edition. Project Management Institute, 2017 756 p.
2. Fesenko T. G. *Upravlinnya proektamy: teoriya ta praktyka vykonannya proektnykh diy: navch. posibnyk* [Project Management: Theory and Practice of Project Activities: A Manual]. Kharkiv, KHNAMG, 2012. 18 p.
3. Fesenko T. G., Mohamed Addulsalam Seek Ali. Modelyuvannya otsinky «Risk Management» v systemi upravlinnya budivel′nymy proektamy [Modeling of "Risk Management" assessment in the construction project management system]. *Visnyk Cherkas'koho derzhavnoho tekhnolohichnoho universytetu. Seriya : Tekhnichni nauky* [Bulletin of Cherkasy State Technological University. Series: Technical Sciences]. 2018, no. 2. pp. 120–127. Available at: http://nbuv.gov.ua/UJRN/Vchdtu_2018_2_21. (accessed 19.01.2025).
4. A Guide to the project management body of knowledge (PMBOK® Guide: Seven Edition) and The standard for project management. USA, Project Management Institute, 2021. 370 p.
5. ISO 31000:2018. Risk management – Guidelines. Switzerland, 2018. 16 p.
6. The standard for risk management in portfolios, programs, and projects. USA: Project Management Institute, 2019. 175 p.
7. Hrabina K. V. *Modeli ta metody informatsiynoyi tekhnolohiyi upravlinnya ryzykamy v IT-proyektakh* [Models and methods of information technology risk management in IT projects]: dissertation … Ph.D. : 122 – Computer Science / Sumy State University. Sumy, 2024. 185 p. Available at: https://essuir.sumdu.edu.ua/bitstream-download/123456789/97100/1/Hrabina_K_PhD_thesis.pdf. (accessed 19.01.2025).
8. Polozhentsev A. A. *Metody ta zasoby upravlinnya IT-intsydentamy na ob"yektakh krytychnoyi informatsiynoyi infrastruktury* [Methods and tools for managing IT incidents at critical information infrastructure facilities]: dissertation … Ph.D. : 122 – Computer

Science / NAU. Kyiv, 2024. 180 p. Available at: https://vchenarada.nau.edu.ua/wp-content/uploads/2024/07/disertatsiya-Polozhentsev.pdf. (accessed 19.01.2025).
9. Semko O. V. *Informatsiyna tekhnolohiya upravlinnya informatsiynymy ryzykamy v proyektakh tsyfrovoyi transformatsiyi biznesu* [Information technology for managing information risks in digital business transformation projects]: dissertation … Dr. Phil. : 122 – Computer Sciences / ChDTU. Cherkasy, 2024. 210 p. Available at: https://er.chdtu.edu.ua/handle/ChSTU/4792. (accessed 19.01.2025).
10. Makarchuk I. V. *Upravlinnya ryzykamy IT-proyektiv na pidpryyemstvi* [Risk management of IT projects at the enterprise]: diss. … Dr. Phil. : 073 – Management / DTEU. Kyiv, 2023. 254 p. Available at: https://knute.edu.ua/file/Mg==/adcd9a7a02ff2aff4977bfaab4ba86ba.pdf. (accessed 19.01.2025).
11. Ivanov M. Ye. *Orhanizatsiyno-ekonomichne zabezpechennya systemy upravlinnya proektnymy ryzykamy v IT-kompaniyakh* [Organizational and economic support of the project risk management system in IT companies]: diss. … Dr. Phil. : 073 – Management / NDC industrial problems development. Kharkiv, 2023. 217 p. Available at: https://ndc-ipr.org/media/spec_council/abstracts/Ivanov_MYe_PhD_Thesis_3.pdf. (accessed 19.01.2025).
12. Gerasimenko O. M. *Ryzyk-oriyentovane upravlinnya v systemi ekonomichnoyi bezpeky pidpryyemstva* [Risk-oriented management in the system of economic security of an enterprise]: dissertation … Dr. of Economics. Sciences: 21.04.02 – economic security of economic entities / B. Khmelnytskyi National University of Ukraine. – PVNIZ "KROU". Kyiv, 2021. 667 p. Available at: ttps://library.krok.edu.ua/media/library/category/disertatsiji-avtoreferati-vidguki/gerasimenko_2021-disertatsija.pdf. (accessed 19.01.2025).
13. Zakharzhevska A. A. *Rozvytok upravlinnya ryzykamy telekomunikatsiynykh pidpryyemstv* [Development of risk management of telecommunications enterprises]: author's abstract ... candidate of economic sciences: 08.00.04 – economics and enterprise management / State University of Telecommunications. Kyiv, 2024. 24 p. Available at : https://duikt.edu.ua/uploads/p_1537_93188893.pdf?file=p_1537_93188893.pdf. (accessed 19.01.2025).
14. Azhar S., Khalfan M., Maqsood T. Building information modelling (BIM): now and beyond. *Construction Economics and Building*. 2015, no. 12, issue 4, pp. 15–28. doi.org/10.5130/AJCEB.v12i4.3032.
15. Putnam L. H. A General Empirical Solution to the Macro Software Sizing and Estimating Problem. I*EEE Transactions on Software Engineering.* 1978, no. SE-4, issue 4, pp. 345–361. doi.org\10.1109/TSE.1978.231521.
16. Zhang X. Critical success factors for public-private partnerships in infrastructure development. *Journal of Construction Engineering and Management.* 2005, no. 131, issue l, pp. 3–14. doi.org\10.1061/(ASCE)0733-9364(2005)131:1(3).
17. Carter G., Smith S. D. Safety hazard identification on construction projects. *Journal of Construction Engineering and Management*. 2005, no. 32, issue 2, pp. 197–205. doi.org\10.1061/(ASCE)0733-9364(2006)132:2(197).
18. Khan R., Kumar P., Jayakody D. N. K., Liyanage M. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. *IEEE Communications Surveys and Tutorials.* 2020, no. 22, issue 1, pp. 196–248, 8792139. doi.org\10.1109/COMST.2019.2933899.
19. de Carvalho R. M., Del Prete C., Martin Y S., Araujo Rivero R. M., Önen M., Schiavo F. P., Rumín Á. C., Mouratidis H., Yelmo J. C., Koukovini M. N., Yelmo J. C. Protecting Citizens' Personal Data and Privacy: Joint Effort from GDPR EU Cluster Research Projects. *SN Computer Science.* 2020. no. 1, issue 4, pp. 217. doi.org\10.1007/s42979-020-00218-8.
20. Kostopoulos G. K. *Cyberspace and Cybersecurity*. 2012, 210 p.
21. Salem M., Othman S. H., Al-Dhaqm A., Ali A. Development of Metamodel for Information Security Risk Management. *Studies in Computational Intelligence.* 2023, no. 1080, pp. 243–253. doi.org\10.1007/978-3-031-21199-7_17.
22. Çubuk E. B. S., Zeren H. E., Demirdöven B. The role of data governance in cybersecurity for E-municipal services: Implications from the case of Turkey. *Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications*. 2022, pp. 410–425. doi.org\10.4018/978-1-6684-5284-4.ch020.
23. Shushura O. M., Asieieva L. A., Nedashkivskiy O. L., Havrylko Y. V., Moroz Y. O., Smailova S. S., Sarsembayev M. Simulation of information security risks of availability of project documents based on fuzzy logic. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Srodowiska.* 2022, no. 12, issue 3, pp. 64–68. doi.org\10.35784/iapgos.3033.
24. Miyaji S., Mimoto T. Security infrastructure technology for integrated utilization of big data: Applied to the living safety and medical fields. *Singapore: Springer Nature*, 2022, 166 p.
25. Crema M., Verbano C. Understanding lean & safety projects: Analysis of case studies. J*ournal of Technology Management and Innovation.* 2017. no. 12, issue 4, pp. 29–41. doi.org\10.4067/s0718-27242017000400004.
26. Bernabe J. B., Skarmeta A. Challenges in cybersecurity and privacy – the European research landscape. 328 p.
27. Sriram S. Security Control Systems for Operational Technology. *Industrial Control Systems*. 2024, pp. 285–302. doi.org\10.1002/9781119829430.ch13.

Надійшла (received) 19.01.2025

Відомості про авторів / About the Authors

Ясинецький Олег Олегович (Yasinetskyi Oleh) – здобувач третього рівня вищої освіти (доктор філософії) ОНП «Інформаційні системи та технології» (126 – Інформаційні системи та технології)», Харківський Національний університет радіоелектроніки; e-mail: oleh.yasinetskyi@nure.ua; ORCID: https://orcid.org/0009-0001-8771-4465.

Фесенко Тетяна Григорівна (Fesenko Tetiana) – доктор технічних наук, професор, Харківський Національний університет радіоелектроніки, професор кафедри електронних обчислювальних машин; e-mail: tetiana.fesenko@nure.ua. ORCID: https://orcid.org/0000-0001-9636-9598.