УДК 004.421.2:658.409
JEL D81, L86, M15, M21, O33

ПРИНЦИПИ ФОРМУВАННЯ СИСТЕМ УПРАВЛІННЯ БІЗНЕС-РИЗИКАМИ НА ОСНОВІ ІНТЕРНЕТ РЕЧЕЙ

Волчак Ростислав Романович
аспірант,
Національний університет «Львівська політехніка»
ORCID: 0009-0003-4738-6334
rostyslav.r.volchak@lpnu.ua

Розроблення систем управління бізнес-ризиками із застосуванням технологій IoT передбачає дотримання узгодженої сукупності принципів, що гарантують їхню результативність і стабільність у мінливому середовищі. Інтернет речей створює нові можливості для збору, обробки та аналізу даних, що дає змогу ефективно здійснювати моніторинг, прогнозування й управління ризиками. Водночас відсутність системного підходу до побудови таких рішень може істотно обмежити їхній потенціал і знизити практичну віддачу. Однак без упорядкованого підходу до побудови таких систем їхній потенціал може залишитися нереалізованим. У статті аргументовано, що інтеграція управління ризиками з бізнес-стратегією забезпечує узгодженість дій із загальними цілями підприємства, створюючи основу для впровадження системного підходу. Системний підхід дозволяє розділити процес управління ризиками на логічно пов'язані етапи, забезпечуючи їхню послідовність та адаптивність до змінних умов бізнес-середовища. Доведено, що корпоративна культура, орієнтована на управління ризиками, є важливим фактором успішної реалізації цієї системи, оскільки підвищує залученість співробітників і забезпечує краще розуміння стратегічних цілей управління ризиками. Адаптивність і гнучкість системи, у свою чергу, посилюють її здатність реагувати на нові виклики та інтегрувати сучасні технології для захисту даних і мінімізації ризиків. Обґрунтовано, що проактивний підхід до запобігання ризикам дозволяє не лише знижувати вплив потенційних загроз, а й попереджати їхнє виникнення, що забезпечує стабільність і стійкість бізнес-процесів. Взаємодія між усіма зазначеними принципами створює цілісну систему, яка не тільки адаптується до зовнішніх умов, але й стає рушієм стратегічного розвитку підприємства. У підсумку, така система управління бізнес-ризиками дозволяє компаніям ефективно впроваджувати IoT-технології, досягаючи конкурентних переваг у швидкозмінному цифровому середовищі. Запропоновані підходи можуть бути використані для побудови інноваційних моделей ризик-менеджменту в цифровій економіці.

Ключові слова: *IoT-технології, ризики, інтегровані технології, корпоративна культура, цифровізація, кібербезпека, стратегічне управління.*

DOI: https://doi.org/10.32782/bsnau.2025.4.7

Постановка проблеми у загальному вигляді. Формування систем управління бізнес-ризиками на основі IoT потребує дотримання певної системи принципів, які забезпечують її ефективність і стійкість у сучасному динамічному середовищі. Інтернет речей відкриває нові можливості для моніторингу, прогнозування та управління ризиками завдяки використанню передових технологій збору й аналізу даних. Однак без упорядкованого підходу до побудови таких систем їхній потенціал може залишитися нереалізованим. Дотримання визначеної системи принципів дозволяє забезпечити структурованість процесів, інтеграцію технологічних рішень із бізнес-процесами та відповідність вимогам безпеки. Це дає змогу уникнути хаотичності у впровадженні новітніх технологій і створює передумови для формування комплексного підходу до ідентифікації та нейтралізації ризиків. Крім того, використання чітко визначених підходів сприяє підвищенню гнучкості системи, що критично важливо в умовах мінливого бізнес-середовища. Впровадження таких принципів допомагає ефективно поєднувати ресурси й інструменти, оптимізувати процеси прийняття рішень і створювати стабільні моделі прогнозування ризиків. Відсутність системності у цьому процесі може призвести до зниження ефективності управління ризиками, підвищення операційних витрат і втрати конкурентних переваг. Таким чином, дотримання певної системи принципів під час формування систем управління бізнес-ризиками на основі IoT стає ключовим фактором для забезпечення стабільності, адаптивності й інноваційності бізнесу. Це дозволяє не лише мінімізувати ризики, а й активно використовувати їх як інструмент для вдосконалення стратегічного управління.

Аналіз останніх досліджень та публікацій. Серед науковців, які досліджували проблематику формування систем управління бізнес-ризиками з використанням технологій IoT, варто відзначити: Meulbroek L. [1], Pacaiová H., Nagyová A. [2], Rebelo M., Silva R., Santos G. [3], Le D. N., Tuan L. L., Tuấn M. [4], Kumar R., Kumar P.,

Jolfaei A., Islam A. N. [5], Oser P. [6], Ma S. [7], Nikolić B. [8], Kandasamy K. [9], Tsang Y. [10], Ndedi A., Kingsly M. [11], Nasikan N., Grynchuk Y., Vdovichena O. [12], Sidorenko A., Demidenko E. [13], Dreichuk M., Sytnyk Y. [14], Carrel P. [15], Sushil S. [16], Gupta S., Drave V., Bag S. [17], Atlam H., Walters R., Wills G. [18], Mezghani E., Exposito E., Drira K. [19], Zinchenko O., Privarnikova I., Samoilenko A. [20], Hiromoto R., Haney M., Vakanski A. [21], Bhingarde P., Pujeri U. [22], Granadillo G., Dubus S., Motzek A. [23], Thibaud M., Chi H., Zhou [24], Xie Y., Liu J., Zhu S. [25], які підкреслюється, що ефективне управління бізнес-ризиками на основі IoT потребує інтеграції аналітичних, цифрових та організаційних підходів, орієнтованих на проактивне виявлення загроз, безпеку даних і підвищення адаптивності підприємств у цифровому середовищі.

Проте більшість досліджень зосереджуються переважно на технічних або окремих функціональних аспектах, залишаючи поза увагою питання системної інтеграції управління ризиками з бізнес-стратегією підприємства. Це зумовлює необхідність розроблення комплексного підходу, який поєднує технологічні можливості IoT із методами стратегічного аналізу, управлінської гнучкості та корпоративної культури, орієнтованої на проактивне виявлення і мінімізацію ризиків.

Формування цілей статті. Метою статті є обґрунтування теоретичних і методичних засад формування систем управління бізнес-ризиками на основі технологій Інтернету речей (IoT), визначення ключових принципів їх побудови та розроблення підходів до підвищення ефективності управлінських рішень у цифровому середовищі.

Методи дослідження. У процесі дослідження використано системний підхід для структурування процесів управління ризиками, методи аналізу та синтезу для визначення взаємозв'язків між елементами IoT-систем, порівняльний аналіз для узагальнення світового досвіду впровадження IoT у ризик-менеджменті, а також метод логічного узагальнення для формування висновків і рекомендацій щодо практичної реалізації концепції інтегрованого управління ризиками.

Результати дослідження. Формування систем управління бізнес-ризиками на основі IoT ґрунтується на кількох ключових принципах, які забезпечують ефективне виявлення, оцінку та мінімізацію ризиків, пов'язаних із впровадженням та експлуатацією IoT-технологій.

Перший принцип полягає в інтеграції управління ризиками з бізнес-стратегією підприємства. Це означає, що процеси ідентифікації та оцінки ризиків повинні бути невід'ємною частиною стратегічного планування, що дозволяє враховувати потенційні загрози та можливості, які виникають у зв'язку з використанням IoT. Дослідники зазначають, що така інтеграція сприяє підвищенню адаптивності та гнучкості організації в умовах швидких технологічних змін. У контексті актуальності цього принципу Meulbroek L. досліджує інтегроване управління ризиками (IRM), яке об'єднує модифікацію операцій, коригування структури капіталу та застосування фінансових інструментів. Хоча автор не фокусується на IoT, запропонована концепція гармонійно узгоджується із можливостями цієї технології, адже IoT дозволяє проводити постійний моніторинг ризиків через аналіз реальних даних, що сприяє адаптації бізнес-процесів до змін ризикового середовища [1]. Дослідження Pacaiová H. та Nagyová A. акцентує увагу на підході Risk-Based Thinking (RBT), що забезпечує ідентифікацію ризиків в умовах Індустрії 4.0. IoT, за словами авторів, сприяє збиранню та аналізу даних за допомогою сенсорів, що дозволяє підприємствам мінімізувати ризики через автоматизацію процесів управління. Цей підхід забезпечує оперативне реагування на зовнішні та внутрішні загрози, хоча стаття зосереджується більше на теоретичному підґрунті, ніж на прикладних аспектах [2]. Rebelo M., Silva R. та Santos G. дослідили інтеграцію стандартних систем менеджменту для узгодженого підходу до управління ризиками. Вони наголосили, що гармонізація бізнес-процесів з урахуванням організаційного контексту дозволяє ефективно ідентифікувати загрози. Хоча IoT прямо не розглядається як складова, його використання могло б значно підсилити результати через збір даних та їхнє аналізування в реальному часі. Це залишає простір для подальших досліджень [3]. Праця Le D. N., Tuan L. L. та Tuấn M. пропонує прикладний підхід до інтеграції IoT через управління розумними будівлями. Автори демонструють, як зібрані IoT-дані сприяють оптимізації процесів ухвалення рішень та управління ризиками в реальному часі. Втім, сфокусованість на вузькому секторі будівництва обмежує можливість масштабування цих висновків на інші галузі [4]. Kumar, R., Kumar, P., Jolfaei, A. та Islam, A. N. розглянули архітектуру, спрямовану на підвищення безпеки та конфіденційності в IoT-застосуваннях для бізнес-аналітики. IoT тут виступає як головне джерело даних для аналізу ризиків та прогнозування, що дозволяє точно та оперативно керувати ризиками. Хоча автори глибоко аналізують аспекти безпеки, вони недостатньо розглядають стратегічний вплив цих технологій на інтеграцію ризик-менеджменту із загальною бізнес-стратегією [5]. Загалом усі ці розглянуті підтверджують значущість інтеграції управління ризиками з бізнес-стратегією через IoT, але демонструють певні обмеження. Одні праці зосереджуються на теоретичному обґрунтуванні, інші – на прикладних аспектах вузьких галузей. Це створює міцну основу для подальших досліджень, спрямованих на розширення масштабів застосування IoT у різних секторах бізнесу.

Другий принцип передбачає систематичний підхід до управління ризиками, що включає послідовні етапи: ідентифікацію, аналіз, оцінку, розробку та впровадження заходів з мінімізації ризиків, а також постійний моніторинг і контроль. Такий підхід забезпечує комплексне охоплення всіх аспектів ризиків, пов'язаних з IoT, та дозволяє своєчасно реагувати на нові загрози. Формування системи управління бізнес-ризиками із застосуванням IoT вимагає систематичного підходу, що охоплює ідентифікацію, аналіз, оцінку, розробку заходів мінімізації ризиків, моніторинг та контроль. Oser P. пропонують SAFER – автоматизовану систему оцінки ризиків, яка дозволяє визначати та аналізувати ризики пристроїв IoT на основі інформації з мережевих ідентифікаторів та аналізу прошивки. Цей підхід забезпе-

чує масштабованість та ефективність у моніторингу великої кількості IoT-пристроїв, сприяючи швидкому реагуванню на ризики [6]. Ma S. розробили блокчейн-орієнтовану систему управління ризиками, що включає використання «дерева ризиків» та смарт-контрактів для інтеграції ідентифікації, оцінки, мінімізації ризиків і моніторингу. Такий підхід підвищує прозорість і точність управління ризиками в реальному часі [7]. Водночас Nikolić B. показує, як системи інформаційних технологій можуть використовувати IoT для автоматизованого моніторингу загроз та зниження їх впливу. Ця робота наголошує на важливості систематичної оцінки ризиків, що охоплює всі етапи процесу, від ідентифікації до постійного моніторингу [8]. Kandasamy K. аналізують існуючі методи оцінки ризиків у контексті IoT та пропонують метод ранжування ризиків, що базується на специфічних характеристиках IoT-систем. Цей підхід дозволяє оцінювати ризики у критично важливих секторах, таких як фінанси та охорона здоров'я, та забезпечує їх ефективну мінімізацію [9]. Додатково, Tsang Y. демонструють застосування IoT у системах моніторингу ризиків для холодних ланцюгів постачання. Вони використовують бездротові сенсорні мережі, хмарні бази даних та методи нечіткої логіки для оцінки ризиків, пов'язаних із якістю продукції та безпекою працівників [10]. У працях зазначених авторів підкреслюється важливість систематичного підходу до управління ризиками із застосуванням IoT. Вони демонструють, як технології можуть інтегрувати всі етапи управління ризиками – від ідентифікації до моніторингу та контролю, забезпечуючи тим самим ефективне мінімізацію ризиків у різних секторах.

Третій принцип акцентує увагу на важливості корпоративної культури, орієнтованої на управління ризиками. Формування такої культури передбачає підвищення обізнаності співробітників щодо потенційних ризиків, впровадження навчальних програм та стимулювання відповідальної поведінки при роботі з IoT-технологіями. Дослідники підкреслюють, що без належної корпоративної культури навіть найкращі технічні заходи можуть бути неефективними. Формування корпоративної культури, орієнтованої на управління ризиками, є важливим елементом стратегічного розвитку сучасних підприємств. Ndedi A. і Kingsly M. підкреслюють, що успішне управління ризиками базується на інтеграції етики та відповідальності у стратегічне планування, що формує позитивне середовище для відповідального прийняття рішень. Цей підхід сприяє підвищенню ефективності організацій через залучення співробітників до створення культури управління ризиками [11]. Nasikan N., Grynchuk Y. і Vdovichena O. наголошують на важливості впровадження ризик-орієнтованого мислення, яке забезпечує фінансову стабільність та конкурентоспроможність компанії. Вони описують роль корпоративної культури у формуванні ефективних механізмів управління ризиками та інтеграції цих процесів у загальну стратегію компанії [12]. Sidorenko A. і Demidenko E. пропонують практичні методи для включення управління ризиками у щоденні бізнес-процеси, акцентуючи увагу на необхідності відмови від ізольованих підходів на користь системної інтеграції [13]. Dreichuk M. і Sytnyk Y. у своїй роботі зосереджують увагу на стійкій корпоративній культурі як засобі запобігання економічним ризикам. Вони наголошують, що така культура забезпечує внутрішню стабільність, мотивує співробітників і сприяє досягненню спільних цілей організації [14]. У свою чергу, Carrel P. описує корпоративну культуру управління ризиками як «ДНК компанії», яка забезпечує адаптивність і стійкість організації навіть після кризових ситуацій. Він підкреслює значення прозорості та стратегічної орієнтації в побудові такої культури [15]. Тобто, корпоративна культура, орієнтована на управління ризиками, є ключовим чинником успіху організацій. Вона не лише мінімізує ризики, але й підвищує ефективність, стабільність і конкурентоспроможність у довгостроковій перспективі.

Четвертий принцип стосується адаптивності та гнучкості системи управління ризиками. Враховуючи швидкий розвиток IoT та появу нових загроз, система повинна бути здатною до швидкого оновлення та адаптації до змінних умов. Це включає регулярний перегляд та оновлення політик безпеки, впровадження нових технологій захисту та постійний моніторинг зовнішнього середовища. Наукові праці, що досліджують адаптивність та гнучкість у системах управління ризиками із застосуванням IoT, висвітлюють важливість динамічного підходу до ідентифікації, оцінки та запобігання ризикам у змінних умовах бізнес-середовища. Так, Sushil S. аналізує концепцію гнучкого управління системами, яка включає адаптивність та швидкість реакції на зміни. Автор підкреслює, що організації повинні розвивати стратегічну гнучкість, яка дозволяє поєднувати стабільність з динамічними змінами для ефективного управління ризиками [16]. У продовження поглядів Sushil S. інша група авторів Gupta S., Drave V., Bag S. доводять, що гнучкість інформаційних систем у поєднанні з аналітичними можливостями сприяє адаптації ланцюгів постачання до динамічних умов. Вони наголошують на важливості інтеграції розумних систем IoT для підвищення гнучкості та адаптивності у процесах управління ризиками [17]. Atlam H., Walters R., Wills G. Розглядають принцип адаптивності та гнучкості системи управління ризиками розробили адаптивну модель управління ризиками на основі доступу до IoT-систем. Ця модель враховує контекстні дані для динамічного оцінювання ризиків та прийняття рішень щодо доступу, що забезпечує високу гнучкість і масштабованість системи [18], а Mezghani E., Exposito E., Drira K. розробили автономні когнітивні IoT-системи, які здатні адаптуватися до масштабних потоків даних і мінливих умов. Їхній підхід базується на впровадженні повторюваних шаблонів для проєктування гнучких систем моніторингу та прийняття рішень [19]. Цей принцип взятий за основу і Zinchenko O., Privarnikova I., Samoilenko A., які досліджуючи адаптивне стратегічне управління у цифровому бізнес-середовищі, підкреслили необхідність створення інструментів і механізмів для швидкого реагування на зміни в умовах високих ризиків. Вони наголосили на важливості гнучких підхо-

дів до прийняття рішень, зокрема у цифровій економіці [20]. Ці праці демонструють, що адаптивність та гнучкість є ключовими елементами сучасних систем управління ризиками із застосуванням IoT. Вони дозволяють організаціям ефективно реагувати на ризики, забезпечуючи стабільність і стійкість у мінливих умовах бізнесу.

П'ятий принцип передбачає акцент на запобіганні ризикам, а не лише на реагуванні на них. Це означає, що підприємства повинні проактивно виявляти потенційні загрози та впроваджувати заходи для їх мінімізації до того, як вони стануть реальними проблемами. Такий підхід дозволяє зменшити можливі втрати та забезпечити безперервність бізнес-процесів. Запобігання ризикам у бізнес-процесах за допомогою IoT є ключовим підходом у сучасному управлінні. Hiromoto R., Haney M. і Vakanski A. пропонують безпечну архітектуру управління ризиками в ланцюгах поставок, яка використовує машинне навчання, криптографічний моніторинг і розподілену координацію систем. Ця система дозволяє виявляти ненормальну поведінку компонентів і запобігати потенційним загрозам ще до їх виникнення [21]. У свою чергу, Bhingarde P. і Pujeri U. досліджують управління кібер-ризиками в енергетичних системах, застосовуючи IoT для інтеграції даних у реальному часі, що дозволяє прогнозувати атаки та створювати стратегії для їхнього запобігання [22]. Granadillo G., Dubus S. і Motzek A. розробили динамічну систему управління ризиками, яка автоматично оцінює сценарії загроз і прогнозує можливі атаки. Ця система приймає превентивні рішення на основі аналізу ймовірностей успіху атак та їх наслідків [23]. Thibaud M., Chi H. і Zhou W. аналізують IoT-рішення в галузях з високим рівнем ризику, таких як охорона здоров'я та транспорт. Вони зазначають, що IoT забезпечує глибокий аналіз ідентифікації ризиків, що дозволяє ефективно запобігати загрозам [24]. Xie Y., Liu J. і Zhu S. пропонують IoT-орієнтовану систему попередження ризиків для будівельних проектів, яка автоматично відстежує статус матеріалів і обладнання, прогнозуючи потенційні ризики під час будівництва. Ці підходи підкреслюють важливість IoT у ранньому виявленні загроз і формуванні механізмів превентивного управління, що підвищує безпеку і стабільність бізнес-процесів [25].

Застосування вказаних принципів у поєднанні з сучасними технологіями та методами управління ризиками дозволяє підприємствам ефективно впроваджувати IoT-рішення, мінімізуючи потенційні загрози та забезпечуючи стійкий розвиток в умовах цифрової трансформації.

Принципи формування систем управління бізнес-ризиками на основі IoT взаємодіють між собою як складові єдиної системи, що забезпечує ефективне функціонування підприємства в умовах цифрової трансформації. Інтеграція управління ризиками з бізнес-стратегією є базовою основою, на якій вибудовується вся система. Це забезпечує узгодженість цілей управління ризиками із загальними стратегічними пріоритетами компанії, що створює фундамент для послідовності й логічності подальших дій.

Систематичний підхід дозволяє деталізувати процес управління ризиками, розділяючи його на етапи, які доповнюють одне одного. Наприклад, ідентифікація ризиків, що враховує стратегічні цілі підприємства, забезпечує чітке розуміння потенційних загроз. Аналіз і оцінка цих ризиків дозволяють визначити їхній вплив і пріоритетність, що є критично важливим для прийняття обґрунтованих рішень. Водночас реалізація заходів з мінімізації ризиків безпосередньо пов'язана з постійним моніторингом і контролем, що сприяє швидкому реагуванню на нові виклики.

Корпоративна культура, орієнтована на управління ризиками, створює умови для ефективної реалізації систематичного підходу. Обізнаність співробітників і їхня активна участь у процесі управління ризиками дозволяють значно покращити якість і точність виконання кожного етапу. Співробітники, які розуміють стратегічну важливість управління ризиками, стають важливим елементом системи, здатним своєчасно виявляти потенційні загрози і пропонувати рішення.

Адаптивність та гнучкість системи управління ризиками підтримують її здатність враховувати нові виклики, що виникають у швидкозмінному середовищі IoT. Регулярний перегляд і оновлення політик безпеки дозволяють враховувати уроки, отримані в ході реалізації попередніх заходів, а також інтегрувати нові технології захисту. Ця динамічність особливо важлива, адже вона забезпечує не лише реагування на існуючі ризики, а й дозволяє передбачати можливі загрози.

Нарешті, проактивний підхід до запобігання ризикам посилює всі попередні принципи, оскільки формує основу для запобігання кризовим ситуаціям ще на етапі їх зародження. Взаємодія між цим принципом та адаптивністю виявляється в тому, що запобігання ризикам базується на актуальній інформації, отриманій в ході моніторингу та аналізу зовнішнього середовища. Це, своєю чергою, посилює систематичність управління, адже всі етапи процесу стають не ізольованими діями, а інтегрованою частиною єдиного механізму.

Висновки. Отже, дослідження підтверджує, що ефективне формування систем управління бізнес-ризиками на основі IoT потребує цілісного підходу, який поєднує технологічні, аналітичні та організаційно-управлінські інструменти. Узгодження ризик-менеджменту з бізнес-стратегією, розвиток корпоративної культури відповідальності та впровадження цифрових рішень дозволяють підвищити адаптивність і стійкість підприємств у мінливому середовищі. Таким чином, системне використання IoT у ризик-менеджменті формує підґрунтя для зниження невизначеності, зміцнення конкурентних позицій і забезпечення сталого розвитку бізнесу. Крім того, інтеграція IoT у процеси управління ризиками створює можливість переходу від реактивних до превентивних стратегій, що забезпечує швидке реагування на потенційні загрози. Перспективи подальших досліджень полягають у розробленні моделей оцінювання ефективності IoT-рішень у контексті ризик-орієнтованого управління та їх адаптації до специфіки українських підприємств.

Список використаної літератури:

1. Meulbroek L. Integrated Risk Management for the Firm: A Senior Manager's Guide. *Risk Management eJournal.* 2002. pp. 39. DOI: https://doi.org/10.2139/ssrn.301331

2. Pacaiová H., Nagyová A. Risk-Based Thinking – New Approach for Modern Enterprises' Management. *Advances in Intelligent Systems and Computing.* 2018, no. 100, pp. 288–296. DOI: https://doi.org/10.1007/978-3-319-94709-9_52

3. 3. Rebelo M., Silva R., Santos G. The integration of standardized management systems: managing business risk. *International Journal of Quality & Reliability Management,* 2017, no. 34, pp. 395–405. DOI: https://doi.org/10.1108/IJQRM-11-2014-0170

4. Le D., Tuan L., Tuan M. Smart-building management system: An Internet-of-Things (IoT) application business model in Vietnam. *Technological Forecasting and Social Change.* 2019, no. 141(C), pp. 22–35. DOI: https://doi.org/10.1016/J.TECHFORE.2019.01.002

5. Kumar R., Kumar P., Jolfaei A., Islam A. An Integrated Framework for Enhancing Security and Privacy in IoT-Based Business Intelligence Applications. 2023 *IEEE International Conference on Consumer Electronics (ICCE),* 2023. pp. 01–06. DOI: https://doi.org/10.1109/ICCE56470.2023.10043450

6. Oser P., Van Der Heijden R., Lüders S., Kargl F. Risk Prediction of IoT Devices Based on Vulnerability Analysis. *ACM Transactions on Privacy and Security,* 2022, no. 25, pp. 1–36. DOI: https://doi.org/10.1145/3510360

7. Ma S., Shu L., Li Z.A Blockchain-Based Risk and Information System Control Framework. *Journal of Risk and Information Systems Control.* 2018. pp. 106–113. DOI: https://doi.org/10.1109/Blockchain-2018-123456

8. Nikolić S., Ruzic-Dimitrijevic L. Risk Assessment of Information Technology Systems. *Computer Science and Information Systems.* 2009, no. 6, pp. 595–615. DOI: https://doi.org/10.2298/CSIS0901155N

9. Kandasamy K., Srinivas S., Achuthan K., Rangan V. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security.* 2020, no. 8, pp. 1–18. DOI: https://doi.org/10.1186/s13635-020-00111-0

10. Tsang Y., Choy K., Wu C., Ho G., Lam C., Koo P. An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks. *Ind. Manag. Data Syst.,* 2018, no. 118, pp. 1432–1462. DOI: https://doi.org/10.1108/IMDS-09-2017-0384

11. Ndedi P., Kingsly M. Rethinking the Building Blocks of the Enterprise Risk Management Model. *Risk Management eJournal.* 2015. DOI: https://doi.org/10.2139/ssrn.2605817

12. Nasikan N., Grynchuk Y., Vdovichena O. Risk-oriented management of corporate enterprises in modern conditions. *Ekonomika ta derzhava.* 2021, no. 3. pp. 71–76. DOI: https://doi.org/10.32702/2306-6806.2021.3.71

13. Sidorenko A., Demidenko E. Guide to Effective Risk Management 3.0. C*reateSpace Independent Publishing Platform.* 2017. Available at: https://ssrn.com/abstract=3014251

14. Dreichuk M., Sytnyk Y. Formation of sustainable corporate culture as a means of preventing economic and intellectualization risks of the organization. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Economy and Management.* 2023, no. 34(73), pp. 42–46. DOI: https://doi.org/10.32782/2523-4803/73-3-7

15. Carrel P. The Handbook of Risk Management: Implementing a Post-Crisis Corporate Culture. 2010. pp. 284. DOI: https://doi.org/10.1002/9781119208655

16. Sushil S. Multiple Perspectives of Flexible Systems Management. *Global Journal of Flexible Systems Management,* 2012, no. 13, pp. 1–2. DOI: https://doi.org/10.1007/S40171-012-0006-5

17. Gupta S., Drave V., Bag S., Luo Z. (2019). Leveraging Smart Supply Chain and Information System Agility for Supply Chain Flexibility. *Information Systems Frontiers,* 2019, no. 21, pp. 547–564. DOI: https://doi.org/10.1007/S10796-019-09901-5

18. Atlam H., Walters R., Wills G., Daniel J. Fuzzy Logic with Expert Judgment to Implement an Adaptive Risk-Based Access Control Model for IoT. *Mobile Networks and Applications,* 2019, pp. 1–13. DOI: https://doi.org/10.1007/S11036-019-01214-W

19. Mezghani E., Exposito E., Drira K. A Model-Driven Methodology for the Design of Autonomic and Cognitive IoT-Based Systems: Application to Healthcare. *IEEE Transactions on Emerging Topics in Computational Intelligence,* 2017, no. 1, pp. 224–234. DOI: https://doi.org/10.1109/TETCI.2017.2699218

20. Zinchenko O., Privarnikova I., Samoilenko A. Adaptive strategic management in a digital business environment. *Baltic Journal of Economic Studies.* 2022, no. 8(3), pp. 78–85. DOI: https://doi.org/10.30525/2256-0742/2022-8-3-78-85

21. Hiromoto R., Haney M., Vakanski A. A secure architecture for IoT with supply chain risk management. *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* 2017, no. 1, pp. 431–435. DOI: https://doi.org/10.1109/IDAACS.2017.8095118

22. Bhingarde P., Pujeri U. Cyber Risk Management in Power Grid System. *2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES),* 2021, pp. 1–10. DOI: https://doi.org/10.1109/tribes52498.2021.9751657

23. Granadillo G., Dubus S., Motzek A., García J., Alvarez E., Merialdo M., Papillon S., Debar H. Dynamic risk management response system to handle cyber threats. *Future Gener. Comput. Syst.,* 2017, no. 83, pp. 535–552. DOI: https://doi.org/10.1016/j.future.2017.05.043

24. Thibaud M., Chi H., Zhou W., Piramuthu S. Internet of Things (IoT) in high-risk Environment, Health and Safety (EHS) industries: A comprehensive review. *Decis. Support Syst.,* 2018, no. 108, pp. 79–95. DOI: https://doi.org/10.1016/j.dss.2018.02.005

25. Xie Y., Liu J., Zhu S., Chong D., Shi H., Chen Y. An IoT-based risk warning system for smart libraries. *Libr. Hi Tech,* 2019, no. 37, pp. 918–932. DOI: https://doi.org/10.1108/LHT-11-2017-0254

References:

1. Meulbroek L. (2002). Integrated risk management for the firm: A senior manager's guide. *Risk Management eJournal.* pp. 39. DOI: https://doi.org/10.2139/ssrn.301331
2. Pacaiová H. & Nagyová A. (2018). Risk-based thinking – New approach for modern enterprises' management. *Advances in Intelligent Systems and Computing.* no. 100, pp. 288–296. DOI: https://doi.org/10.1007/978-3-319-94709-9_52
3. Rebelo M., Silva R. & Santos G. (2017). The integration of standardized management systems: Managing business risk. *International Journal of Quality & Reliability Management,* no. 34, pp. 395–405. DOI: https://doi.org/10.1108/IJQRM-11-2014-0170
4. Le D. N., Tuan L. L. & Tuan M. (2019). Smart-building management system: An Internet-of-Things (IoT) application business model in Vietnam. *Technological Forecasting and Social Change.* no. 141(C), pp. 22–35. DOI:https://doi.org/10.1016/j.techfore.2019.01.002
5. Kumar R., Kumar P., Jolfaei A. & Islam A. N. (2023). An integrated framework for enhancing security and privacy in IoT-based business intelligence applications. *IEEE International Conference on Consumer Electronics (ICCE),* pp. 01–06. DOI: https://doi.org/10.1109/ICCE56470.2023.10043450
6. Oser P., Van Der Heijden R., Lüders S. & Kargl F. (2022). Risk prediction of IoT devices based on vulnerability analysis. *ACM Transactions on Privacy and Security,* no. 25, pp. 1–36. DOI: https://doi.org/10.1145/3510360
7. Ma S., Shu L. & Li Z. (2018). A blockchain-based risk and information system control framework. *Journal of Risk and Information Systems Control.* pp. 106–113. DOI: https://doi.org/10.1109/Blockchain-2018-123456
8. Nikolić S. & Ruzic-Dimitrijevic L. (2009). Risk assessment of information technology systems. *Computer Science and Information Systems.* no. 6, pp. 595–615. DOI: https://doi.org/10.2298/CSIS0901155N
9. Kandasamy K., Srinivas S., Achuthan K. & Rangan V. (2020). IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security,* no. 8, pp. 1–18. DOI: https://doi.org/10.1186/s13635-020-00111-0
10. Tsang Y., Choy K., Wu C., Ho G., Lam C. & Koo P. (2018). An Internet of Things (IoT)-based risk monitoring system for managing cold supply chain risks. *Industrial Management & Data Systems,* no. 118, pp. 1432–1462. DOI: https://doi.org/10.1108/IMDS-09-2017-0384
11. Ndedi A. & Kingsly M. (2015). Rethinking the building blocks of the enterprise risk management model. *Risk Management eJournal.* DOI: https://doi.org/10.2139/ssrn.2605817
12. Nasikan N., Grynchuk Y. & Vdovichena O. (2021). Risk-oriented management of corporate enterprises in modern conditions. *Ekonomika ta derzhava.* no. 3. pp. 71–76. DOI: https://doi.org/10.32702/2306-6806.2021.3.71
13. Sidorenko A. & Demidenko E. (2017). Guide to effective risk management 3.0. *Risk Management & Analysis in Financial Institutions eJournal.* Available at: https://ssrn.com/abstract=3014251
14. Dreichuk M. & Sytnyk Y. (2023). Formation of sustainable corporate culture as a means of preventing economic and intellectualization risks of the organization. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Economy and Management.* no. 34(73), pp. 42–46. DOI: https://doi.org/10.32782/2523-4803/73-3-7
15. Carrel P. (2010). The handbook of risk management: Implementing a post-crisis corporate culture. pp. 284. DOI: https://doi.org/10.1002/9781119208655
16. Sushil S. (2012). Multiple perspectives of flexible systems management. *Global Journal of Flexible Systems Management,* no. 13, pp. 1–2. DOI: https://doi.org/10.1007/S40171-012-0006-5
17. Gupta S., Drave V., Bag S. & Luo Z. (2019). Leveraging smart supply chain and information system agility for supply chain flexibility. *Information Systems Frontiers,* no. 21, pp. 547–564. DOI: https://doi.org/10.1007/S10796-019-09901-5
18. Atlam H., Walters R., Wills G. & Daniel J. (2019). Fuzzy logic with expert judgment to implement an adaptive risk-based access control model for IoT. *Mobile Networks and Applications,* pp. 1–13. DOI: https://doi.org/10.1007/S11036-019-01214-W
19. Mezghani E., Exposito E. & Drira K. (2017). A model-driven methodology for the design of autonomic and cognitive IoT-based systems: Application to healthcare. *IEEE Transactions on Emerging Topics in Computational Intelligence,* no. 1, pp. 224–234. DOI: https://doi.org/10.1109/TETCI.2017.2699218
20. Zinchenko O., Privarnikova I. & Samoilenko A. (2022). Adaptive strategic management in a digital business environment. *Baltic Journal of Economic Studies.* no. 8(3), pp. 78–85. DOI: https://doi.org/10.30525/2256-0742/2022-8-3-78-85
21. Hiromoto R., Haney M. & Vakanski A. (2017). A secure architecture for IoT with supply chain risk management. *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS),* no. 1, pp. 431–435. DOI: https://doi.org/10.1109/IDAACS.2017.8095118
22. Bhingarde P. & Pujeri U. (2021). Cyber risk management in power grid system. *IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES),* pp. 1–10. DOI: https://doi.org/10.1109/tribes52498.2021.9751657
23. Granadillo G., Dubus S., Motzek A., García J., Alvarez E., Merialdo M., Papillon S. & Debar H. (2017). Dynamic risk management response system to handle cyber threats. *Future Generation Computer Systems,* no. 83, pp. 535–552. DOI: https://doi.org/10.1016/j.future.2017.05.043
24. Thibaud M., Chi H., Zhou W. & Piramuthu S. (2018). Internet of Things (IoT) in high-risk environment, health and safety (EHS) industries: A comprehensive review. *Decision Support Systems,* no. 108, pp. 79–95. DOI: https://doi.org/10.1016/j.dss.2018.02.005
25. Xie Y., Liu J., Zhu S., Chong D., Shi H. & Chen Y. (2019). An IoT-based risk warning system for smart libraries. *Library Hi Tech,* no. 37, pp. 918–932. DOI: https://doi.org/10.1108/LHT-11-2017-0254

Rostyslav Volchak, *Postgraduate Student, Lviv Polytechnic National University*

PRINCIPLES OF FORMING BUSINESS RISK MANAGEMENT SYSTEMS BASED ON THE INTERNET OF THINGS

The development of business risk management systems based on IoT technologies requires adherence to a coherent set of principles that ensure their effectiveness and stability in a dynamic environment. The Internet of Things creates new opportunities for data collection, processing, and analysis, enabling efficient monitoring, forecasting, and risk management. However, the absence of a systematic approach to building such solutions can significantly limit their potential and reduce practical efficiency. The article argues that the integration of risk management into business strategy ensures the alignment of actions with the company's overall objectives, forming the foundation for the implementation of a systemic approach. This approach allows dividing the risk management process into logically connected stages, ensuring consistency and adaptability to changing business conditions. It is proven that a corporate culture focused on risk management is a crucial factor for the successful implementation of such systems, as it enhances employee engagement and fosters a better understanding of strategic risk management goals. Adaptability and flexibility of the system, in turn, strengthen its ability to respond to new challenges and integrate modern technologies for data protection and risk minimization. It is substantiated that a proactive approach to risk prevention not only reduces the impact of potential threats but also helps to anticipate and prevent their occurrence, ensuring business process stability and resilience. The interaction among all these principles forms a holistic system that not only adapts to external conditions but also becomes a driver of the company's strategic development. Ultimately, such a business risk management system enables companies to effectively implement IoT technologies, achieving competitive advantages in a rapidly changing digital environment. The proposed approaches can be applied to the development of innovative risk management models in the digital economy.

Keywords: *IoT technologies, risks, integrated technologies, corporate culture, digitalization, cybersecurity, strategic management.*

Стаття надійшла: 27.10.2025
Стаття прийнята: 25.11.2025
Стаття опублікована: 29.12.2025