УПРАВЛІННЯ РИЗИКАМИ НА ПІДПРИЄМСТВІ
RISK MANAGEMENT AT THE ENTERPRISE

Стаття присвячена підвищенню рівня розуміння та ефективності управління ризиками на підприємстві для забезпечення його стійкості, конкурентоспроможності та успішного розвитку. Надано визначення понять управління ризиками підприємства та структура управління ризиками підприємства. Досліджено історичні передумови виникнення процесу управління ризиками на підприємстві. Розглянуто типологію ризиків, з якими можуть зіткнутися окремі галузі. Досліджено ряд ризиків з якими стикаються підприємства фінансового сектору та підприємства які працюють в IT секторі та в інтернеті. Досліджено існуючі кіберзагрози для сучасного підприємства. Визначено, що ефективний механізм управління ризиками допомагає підприємствам підвищити стійкість до негативних впливів та забезпечити стабільність у складних умовах.
Ключові слова: *ризик, ризик-менеджмент, підприємство, управління ризиками, кіберзагрози.*

Ukrainian scientists and entrepreneurs consider risk management as an important function, but this function often remains limited and fragmented. The main goal of this management is to prevent or reduce possible losses. In particular, risk managers are often associated with the insurance industry, and this limits their approach to risks. In recent decades, the topic of enterprise risk management has attracted considerable attention in scientific research. This is confirmed by a number of relevant and interesting scientific works that focus on various aspects of risk management. The article is devoted to increasing the level of understanding and effectiveness of risk management at the enterprise to ensure its stability, competitiveness and successful development. The definitions of the concepts of enterprise risk management and the structure of enterprise risk management are provided. The historical prerequisites for the emergence of the risk management process at the enterprise were studied. It is proven that in order to achieve financial and other success, an enterprise must be aware of potential risks that may affect safety, reputation, profits, operations, etc. A business that ignores risks and how to mitigate them can potentially face catastrophic consequences. The typology of risks that individual industries may face is considered. A number of risks faced by companies in the financial sector and companies working in the IT sector and on the Internet have been studied. The existing cyber threats for the modern enterprise have been studied. The topic of enterprise risk management remains very relevant and important for the modern business environment. Recent scientific research confirms the need for an integrated approach to risk management, as well as a focus on new types of risks, such as cyber security and climate change. An effective risk management mechanism helps enterprises increase resistance to negative impacts and ensure stability in difficult conditions. Therefore, further development and research in this area are extremely important for the successful functioning of enterprises in the modern world.
Key words: *risk, risk management, enterprise, risk management, cyber threats.*

УДК 657.6-051
DOI: https://doi.org/10.32782/dees.8-4

Білоус С.П.[1]
д.е.н., доцент,
Черкаський національний університет
імені Б. Хмельницького
Власенко А.Ю.
студент,
Черкаський національний університет
імені Б. Хмельницького

Bilous Svitlana, Vlasenko Amina
Cherkasy National University
named after B. Khmelnytskyi

Постановка проблеми. Українські науковці та підприємці розглядають управління ризиками як важливу функцію, але ця функція часто залишається обмеженою і фрагментарною. Головною метою цього управління є запобігання або зменшення можливих збитків. Особливо часто ризик-менеджери пов'язані з галуззю страхування, і це обмежує їхній підхід до ризиків.

Проте ризики, з якими стикаються підприємства в Україні, дуже різноманітні, і вони вимагають більш інтегрованого підходу до управління ними. Це означає, що головною метою ефективного ризик-менеджменту повинно стати використання знань з різних галузей для зменшення ризиків.

Важливо підкреслити, що покращення результатів діяльності підприємств в Україні вимагає уваги до проблеми управління ризиками в сучасних умовах. Це свідчить про важливість проведення досліджень щодо вивчення механізмів ризик-менеджменту та проблем, пов'язаних з підвищенням його ефективності в країні.

Аналіз останніх досліджень та публікацій. За останні десятиліття тема управління ризиками на підприємстві привернула значну увагу в наукових дослідженнях. Це підтверджується рядом актуальних і цікавих наукових робіт, які зосереджуються на різних аспектах управління ризиками. Серед авторів, які розкривали ці питання в своїх працях можна виділити: Н.Ю. Захарову [1], Т.В. Цвігуна [2], О.В. Михайленка, С.М. Ніколаєнка, О.О. Насіканову [3], В. Бутенка, М. Байдацького [4], С.А. Назаренка, Н.С. Носань [5] та інших провідних науковців.

Формування цілей статті. Мета дослідження полягає в підвищенні рівня розуміння та ефективності управління ризиками на підприємстві для забезпечення його стійкості, конкурентоспроможності та успішного розвитку.

Виклад основного матеріалу дослідження. Управління ризиками підприємства – це сфера, яка постійно розвивається, і зосереджена на виявленні та мінімізації ризиків, з якими стикаються підприємства. Ці ризики можуть бути специфічними для галузі або ризиками, з якими стикається практично кожна організація в 21 столітті, як-от кіберзагрози [6].

Структура управління ризиками підприємства – це інструмент, який може допомогти підприємству

[1] ORCID: https://orcid.org/0000-0002-0303-7453

ідентифікувати, перерахувати та ранжувати потенційні ризики для певних підрозділів організації [6].

Щоб досягти фінансового та іншого успіху, підприємство має знати про потенційні ризики, які можуть вплинути на безпеку, репутацію, прибуток, діяльність тощо. Підприємство, яке ігнорує ризики та способи їх зменшення, потенційно може зіткнутися з катастрофічними наслідками.

Підприємництво зіткнулося з ризиками з початку розвитку комерції. Крадіжки, стихійні лиха та численні інші зовнішні чинники становили загрозу для бізнесу на початку і продовжують нести ризики і сьогодні. Однак до 20-го століття ризики для організацій та підприємств стали більш витонченими, а результати потенційно жахливішими [6].

За словами Джеррі Дікінсона в його серії в «Financial Times» і в його книзі «Enterprise Risk Management: The Way Ahead for DRDC Within the DND Enterprise», корпоративне управління ризиками, як ми його знаємо, почалося після Другої світової війни, коли професіонали визначили певні ризики, як-от стихійні лиха, які страхові компанії будуть розглядати та покривати [7].

У 1963 році Роберт І. Мер і Боб Хеджес написали книгу «Управління ризиками на підприємстві». У цій книзі було сформульовано ідею про те, що підприємства повинні не лише страхувати ризики, з якими вони стикаються, але й виявляти та керувати ними в масштабах підприємства, маючи видимість від керівників [8].

Дікінсон пише, що в 1970-х роках зросли фінансові ризики (результат зростання популярності деривативів і хедж-фондів), і великі компанії зрозуміли, що їм слід керувати як страховими, так і фінансовими ризиками. Більше того, у міру розвитку галузей і створення абсолютно нових галузей, бізнес-лідери почали стикатися з проблемами відповідності та регулюванням, що створювало загальні та галузеві ризики. Усі ці ризики можуть вплинути на репутацію, ефективність і прибутковість підприємства [7]. Саме так і народилася сучасна концепція управління ризиками підприємства.

Сьогоднішнє бізнес-середовище є складним і динамічним. Багато підприємств працюють по всьому світу, де можуть застосовуватися різні закони та правила. Оскільки все більше підприємств ведуть свій бізнес через Інтернет, кібербезпека стала загрозою практично для кожної організації. Розглянемо деякі типи ризиків, з якими можуть зіткнутися окремі галузі [6].

– Фінансовий: Майже кожен тип ризику може вплинути на прибутки підприємства. Неспроможність реагувати на стихійне лихо, крадіжки зсередини та проблеми з репутацією впливають не лише на ці конкретні операції, але потенційно на фінансовий стан підприємства в цілому.

– Процентна ставка. Коливання процентних ставок може вплинути на різноманітні галузі, включаючи банківську справу та кредитування, фондовий ринок, нерухомість тощо.

– Юридичні проблеми. Підприємства можуть зіткнутися з юридичними санкціями, якщо вони не дотримуються букви чи духу закону, будь то

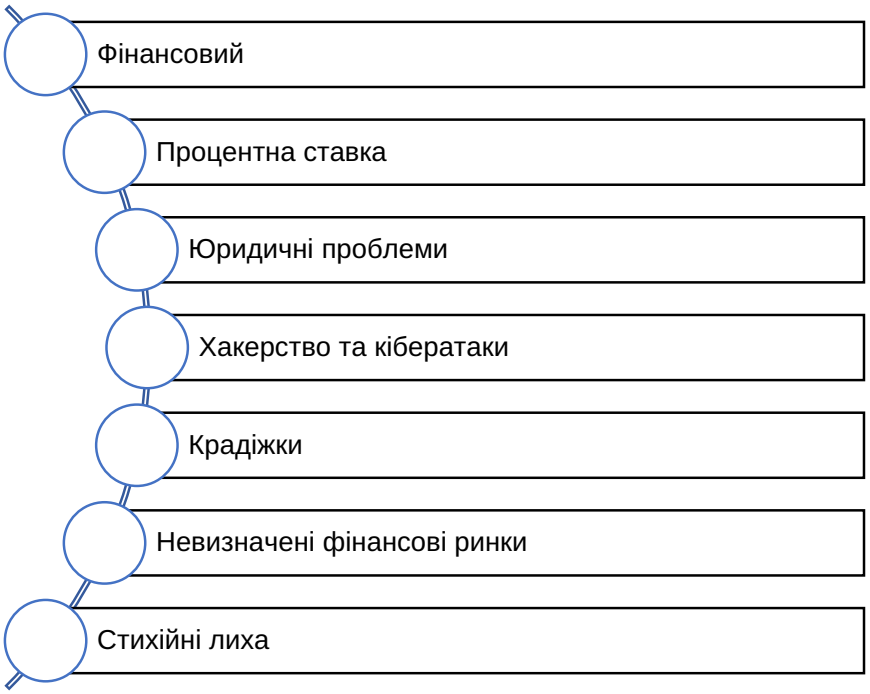

Рис. 1. Типологія ризиків на підприємстві

Джерело: складено авторм за [6]

місцеві, національні чи навіть міжнародні норми. Вони також можуть зіткнутися з цивільними позовами через уявну недбалість, дискримінацію тощо.

– Хакерство та кібератаки: будь-яка компанія, яка веде свій бізнес в Інтернеті, може зіткнутися з величезними ризиками для безпеки своїх даних, фінансових рахунків тощо.

– Крадіжки: одним із найбільших ризиків, з якими стикаються підприємства, є крадіжки з боку постачальників, продавців і співробітників. Це може варіюватися від того, щоб взяти додому гамбургери наприкінці зміни фаст-фуду, до розкрадання мільйонів доларів.

– Невизначені фінансові ринки: нестабільність глобального та національного фінансового ринку є ризиком для будь-якого підприємства. Акції компанії можуть раптово впасти не з вини самої компанії.

– Стихійні лиха: такі стихійні лиха, як землетруси та урагани, можуть настільки спустошити регіони, що вплинуть на доставку постачальником і виконання замовлень, іноді на тривалий період [6].

Також додатково можна виділити ще декілька типів ризиків, серед них:

– Державні та регуляторні органи: Дотримання нормативних вимог у кількох галузях, особливо у фінансах і охороні здоров'я, є критично важливим фактором ризику для бізнесу. Відповідність вимогам і нормативним актам, які постійно вдосконалюються, зобов'язують підприємства бути в курсі всіх відповідних норм і дотримуватися їх.

– Нещасні випадки: аварія, наприклад, із вантажем, може поставити діяльність підприємства під загрозу. Так само може статися нещасний випадок за участю працівника, якщо правова система визначає, що відповідальність несе підприємство.

– Глобальна та політична нестабільність: невизначеність геополітичної арени впливає на міжнародну торгівлю та підприємства, які в ній беруть участь [6].

Деякі галузі стикаються з більшими ризиками, ніж інші, особливо фінансовий сектор. Інвестиційна банківська діяльність, управління капіталом, іпотечна індустрія та інші види фінансових послуг стикаються з кількома потенційно шкідливими ризиками. Серед них:

Інвестиційні ризики: жодна інвестиція не є абсолютно безризиковою, і фінансові установи, пайові фонди тощо, можуть зазнати серйозних збитків, якщо інвестиції не окупляться.

Безпека: фінансові установи повинні захищати не лише власні гроші та прибутки, а й своїх інвесторів і клієнтів. Клієнти повинні знати, що їхні депозити та транзакції безпечні та захищені.

Перерви в безперервності бізнесу: коли підприємства зливаються, закриваються або переривається в роботі, підприємства фінансового сектору можуть постраждати прямо чи опосередковано [6].

За останні кілька років корпоративні ризики, пов'язані з IT та Інтернетом, зросли експоненціально. По суті, існує два типи проблем IT-ризику. Перший стосується технологічної та IT-індустрії, де зловмисники можуть проникнути у власне програмне забезпечення підприємства або сервери електронної пошти. Другий включає практично всі підприємства, оскільки майже кожне з них має значну присутність в Інтернеті та використовує електронну пошту для здійснення операцій і спілкування.

Кожна організація вразлива до кіберризиків, особливо в умовах, коли хакери та зловмисне програмне забезпечення стають все більш досконалими. Компрометовані компанії можуть завдати шкоди своїм продуктам, репутації, обслуговуванню клієнтів, розвитку, співробітникам та іншим сферам. Підприємства, які стикаються з хакерськими атаками або витоком даних, повинні діяти якомога швидше та прозоріше, зв'язуючись із клієнтами, щоб повідомити, як вони планують виправити ситуацію [6].

Сучасні підприємства стикаються з різними кіберзагрозами, які можуть становити серйозну загрозу їхній інформаційній безпеці та функціонуванню в цифровому середовищі. Деякі існуючі кіберзагрози включають [9]:

1. Кібератаки**:** Вони можуть бути в різних формах, таких як деніал-сервіс атаки (DDoS), віруси, троянські коні, різноманітні види злому та вторгнення, що спрямовані на отримання несанкціонованого доступу до інформації або завдають шкоду інфраструктурі.

2. Фішинг**:** Атаки фішингу намагаються обманом вивести користувачів на веб-сайти або надіслати шкідливий вміст через електронну пошту, щоб витягти конфіденційну інформацію, таку як паролі або фінансові дані.

3. Розкрадання даних: Злочинці можуть вкрасти конфіденційну інформацію компанії, включаючи клієнтські дані, корпоративні секрети, фінансову інформацію тощо.

4. Розповсюдження шкідливого програмного забезпечення (малваре): Включає в себе програми-вимоги викупу (рансомваре), шпигунське програмне забезпечення (шпіони), ботнети та інше шкідливе програмне забезпечення, яке може завдати шкоди або використовувати ресурси комп'ютерів підприємства.

5. Соціальний інжиніринг: Зловмисники можуть використовувати маніпулювання соціальними інтеракціями, щоб отримати доступ до інформації або здійснити атаки. Наприклад, вони можуть обдурити співробітників компанії, щоб надати доступ до системи або витягти конфіденційну інформацію.

6. Кібершпигунство: Державні актори або конкуруючі компанії можуть використовувати

кібершпигунство для викрадання важливої інформації або націльованих атак з метою зниження конкурентоспроможності.

7. Сек'юріті апдейти та програмні вразливості: Зловмисники можуть використовувати вразливості в програмному забезпеченні або обладнанні, які не були оновлені або забезпечені необхідною кібербезпекою [9].

Для захисту від цих кіберзагроз підприємства повинні розвивати і впроваджувати комплексні стратегії кібербезпеки, здійснювати регулярні аудити та оновлення систем і надавати навчання співробітникам щодо безпеки в інтернеті.

Керівники найвищого рівня повинні знати про всі кіберзагрози для своєї організації. ІТ-відділ не може самостійно боротися з цими досвідченими зловмисниками. Потужний, поширений характер кіберзагроз підкреслює потребу в системі управління ризиками для всього підприємства.

Кожне підприємство, незалежно від галузі, повинне розвивати та підтримувати міцні зв'язки між ІТ-ризиками, активами, процесами та засобами контролю, визначаючи їх відповідно до опису, категорії, ієрархії, власності та видимості. Підприємства повинні надати ІТ-відділам повноваження для оцінки, кількісного визначення, моніторингу та управління ІТ-ризиками. Має бути сформована політика управління проблемами та їх усунення, включаючи протоколи розслідування та аналіз першопричин. Нарешті, для ІТ-керівників та інших бізнес-лідерів повинні бути доступні моніторинг ризиків і показники, щоб вони могли швидко визначати ризики та вживати заходів, якщо це необхідно [6].

Висновки та перспективи подальших досліджень. Тема управління ризиками на підприємстві залишається дуже актуальною і важливою для сучасного бізнес-середовища. Останні наукові дослідження підтверджують необхідність інтегрованого підходу до управління ризиками, а також зосередження уваги на нових видах ризиків, таких як кібербезпека та зміна клімату. Ефективний механізм управління ризиками допомагає підприємствам підвищити стійкість до негативних впливів та забезпечити стабільність у складних умовах. Тому подальший розвиток та дослідження в цій області є надзвичайно важливими для успішного функціонування підприємств у сучасному світі.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Захарова Н.Ю. Управління ризиками на підприємстві: сутність, підходи та методи. *БІЗНЕС ІНФОРМ*. 2023. № 1. С. 203–209.

2. Цвігун Т.В. Механізм управління ризиками в системі управління підприємством. *Науковий вісник Міжнародного гуманітарного університету. Серія «Економіка і менеджмент».* 2017. Вип. 23. Ч. 2. С. 9–13.

3. Михайленко О.В., Ніколаєнко С.М., Насіканова О.О. Управління ризиками діяльності підприємства. *Проблеми системного підходу в економіці*. 2017. Вип. 6. С. 144–147.

4. Бутенко В., Байдацький, М. Теоретичні основи формування системи управління ризиками на підприємстві. *Економіка та суспільство*. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-35 (дата звернення: 20.08.2023).

5. Назаренко С.А., Носань Н.С. Ризик-менеджмент у господарській діяльності малих підприємств: сучасні імперативи. *Електронне наукове фахове видання з економічних наук «Modern Economics»*. 2020. № 23. С. 143–147. URL: https://www.mnau.edu.ua (дата звернення 10.08.2023).

6. Marker A. Enterprise Risk Management 101: Programs, Frameworks, and Advice From Experts. June 26, 2017. URL: https://www.smartsheet.com/enterprise-risk-management-guide (дата звернення 13.08.2023).

7. Dickinson G. Enterprise Risk Management Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance*. 2001. Vol. 26. No. 3. P. 360–366.

8. Robert Irwin Mehr, Robert Atkinson Hedges Risk Management in the Business Enterprise. Paperback, 2012. 664 p.

9. Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology.* 2022. DOI: 10.22541/au.166385207.73483369/v1 (дата звернення: 18.08.2023).

REFERENCES:

1. Zakharova N.Yu. (2023) Upravlinnya ryzykamy na pidpryyemstvi: sutnist, pidkhody ta metody [Risk management at the enterprise: essence, approaches and methods]. *BIZNES INFORM-BUSINESS INFORMATION*, no. 1, pp. 203–209.

2. Tsvihun T.V. (2017) Mekhanizm upravlinnia ryzykamy v systemi upravlinnia pidpryiemstvom [The Mechanism of Risk Management in the System of Enterprise Administration]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu – Scientific Bulletin of the International Humanitarian University*, vol. 23, part 2: pp. 913.

3. Mykhailenko O.V., Nikolaienko S.M., and Nasikanova O.O. (2017) Upravlinnia ryzykamy diialnosti pidpryiemstva [Risk Management of Enterprise Activity]. Problemy systemnoho pidkhodu v ekonomitsi – Problems of the systemic approach in economics, vol. 6. pp. 144–147.

4. Butenko V., Baydatskyi, M. (2023) Teoretychni osnovy formuvannya systemy upravlinnya ryzykamy na pidpryyemstvi [Theoretical foundations of the formation of the risk management system at the enterprise]. *Ekonomika ta suspilstvo – Economy and society*, no. (50). DOI: https://doi.org/10.32782/2524-0072/2023-50-35 (accessed August 20, 2023).

5. Nazarenko S.A., Nosan N.S. (2020) Ryzyk-menedzhment u hospodarskiy diyalnosti malykh pid-pryyemstv: suchasni imperatyvy [Risk management in the economic activity of small enterprises: modern imperatives]. *Elektronne naukove fakhove vydannya z ekonomichnykh nauk «Modern Economics» – Electronic scientific publication on economic sciences «Mo-dern Economics»*, no. 23, pp. 143–147. Available at: https://www.mnau.edu.ua (accessed August 10, 2023)

6. Marker A. (2017) Enterprise Risk Management 101: Programs, Frameworks, and Advice From Experts. June 26, 2017. Available at: https://www.smartsheet.com/enterprise-risk-management-guide (accessed August 13, 2023).

7. Dickinson G. (2001) Enterprise Risk Management Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance*, vol. 26, no. 3, pp. 360–366.

8. Robert Irwin Mehr, Robert Atkinson Hedges (2012) Risk Management in the Business Enterprise. *Paperback*. 664 p.

9. Diptiben Ghelani. Cyber Security, Cyber Threats, (2022) Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*. DOI: 10.22541/au.166385207.73483369/v1 (accessed August 18, 2023).