Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України від 11.07.2019 № 975)
www. economy.nayka.com.ua | № 9, 2020 | 24.09.2020 р.

DOI: 10.32702/2307-2105-2020.9.68

УДК 656.07

JEL Classification: L91; D81

С. М. Семенова,
к. е. н., доцент, доцент кафедри обліку та оподаткування,
Київський національний торговельно-економічний університет, м. Київ
ORCID ID: 0000-0001-7250-7482

КЛЮЧОВІ ТЕНДЕНЦІЇ В УПРАВЛІННІ РИЗИКАМИ ПРОВІДНИХ КОМПАНІЙ ЄС ЗА ОЦІНКАМИ ВНУТРІШНІХ АУДИТОРІВ

S. Semenova
PhD in Economics, Associate Professor,
Associate Professor of the Department of Accounting and Taxation,
Kyiv National University of Trade and Economics, Kyiv

KEY TRENDS IN RISK MANAGEMENT OF LEADING EU COMPANIES ACCORDING TO INTERNAL AUDITORS

Стаття присвячена дослідженню ключових тенденцій у визначенні найбільших ризиків, які впливають на функціонування підприємств, виявленні проблем та шляхів їх подолання, використовуючи досвід внутрішніх аудиторів провідних компаній ЄС. Зміни умов функціонування підприємств спричиняють трансформацію ризиків. Одним з завдань внутрішнього аудиту виступає об'єктивна оцінка ефективності процесів управління ризиками та сприяння їхньому постійному удосконаленню. Розвиток технологій та інновацій посилює ризики, пов'язані з використанням інформації у все більш цифровому світі. Кібербезпека та захист даних виступають об'єктами з найвищим рівнем ризиків. Кожен господарюючий суб'єкт, які і кожна країна для захисту національних інтересів піклується про безпеку інформаційних мереж та систем, створюючи служби захисту конфіденційних даних. Спостерігається тенденція до зростання ризиків, пов'язаних зі змінами законодавства і правил нормативно-правового регулювання, ризиків аутсорсингу і процесів постачання, ризиків з боку фінансової сфери, макроекономічної та політичної нестабільності. Особливої уваги вимагають ризики у сфері використання людських ресурсів, інтелектуального капіталу, корпоративного управління і культури, репутації, комунікації. Економічна нестабільність підсилює ризики злиття, поглинання, корупцію з різним ступенем прояву залежно від країни. Невпинно посилюються ризики зміни клімату, погіршення екології, набуваючи характеру глобальності та непередбачуваності для всіх сфер життя. Ризики і загрози здоров'ю та безпеці перебувають у тренді активного зростання під впливом covid-19, зважаючи на критичні наслідки пандемії для економіки, охорони здоров'я і суспільства в цілому. Аналізуючи ефективність протидії підприємства найбільшим ризиками необхідно враховувати специфіку і сферу діяльності, середовище і

взаємодію з іншими сторонами, регламент управління ризиками та готовність до кожного їхнього виду.

The article is devoted to the study of key trends in identifying the biggest risks that affect the functioning of enterprises, identifying problems and ways to overcome them, using the experience of internal auditors of leading EU companies. Changes in the operating conditions of enterprises cause a transformation of risks. One of the tasks of internal audit is to objectively assess the effectiveness of risk management processes and promote their continuous improvement. The development of technology and innovation increases the risks associated with the use of information in an increasingly digital world. Cybersecurity and data protection are the highest risk targets. Every business entity and every country to protect national interests cares about the security of information networks and systems, creating confidential data protection services. There is a growing trend of risks associated with changes in legislation and regulations, risks of outsourcing and supply processes, risks from the financial sector, macroeconomic and political instability. Particular attention needs to be paid to risks in the use of human resources, intellectual capital, corporate governance and culture, reputation, communication. Economic instability increases the risks of mergers, acquisitions, corruption with varying degrees depending on the country. The risks of climate change and environmental degradation are constantly increasing, becoming global and unpredictable for all spheres of life. Risks and threats to health and safety are on the rise under the influence of covid-19, given the critical consequences of the pandemic for the economy, health and society as a whole. Because internal auditors focus on areas of activity that may involve latent or undetected risks, their assessments and advice in identifying the greatest risks, possible ways to measure them, and analyzing countermeasures are of great practical value to businesses. Internal audit allows you to identify the company's reactions to growing risks and assess the quality of risk management of the company as a whole. Analyzing the effectiveness of the company to counteract the greatest risks, it is necessary to take into account the specifics and scope of activities, environment and interaction with other parties, risk management regulations and readiness for each of their types.

Ключові слова: *ризики; управління ризиками; ключові ризики; кібербезпека; внутрішній аудит.*

Key words: *risks; risk management; key risks; cybersecurity; internal audit.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В системі управління ризики пов’язують з загрозами й небезпекою настання негативних або несприятливих подій. Чим вищі ризики, тим більший рівень небезпеки та масштабу можливих втрат. Ризик означає необхідність нести відповідальність за будь-яку шкоду, втрату або труднощі. Робити щось, що може бути небезпечним, мати небажані наслідки, також означає ризикувати. Таким чином, в узагальненому розумінні ризик представляє собою можливі втрати, поразку, небезпеку, несприятливі події або наслідки. У зарубіжній практиці слово «*ризик*» має багато аспектів застосування і розуміння. Англійською мовою *risk* є одночасно дієсловом, що означає процес – ризикувати, тобто бути, перебувати в небезпеці, робити щось або обрати бездіяльність, прийняти рішення, яке супроводжують ризики, і слідувати йому, або опинитися в ситуації, яка має ймовірність спричинити втрати, шкоду, збитки, несприятливі наслідки. Разом з цим, *risk* є прикметником у значенні – ризикований, як певна характеристика явищ, процесів, дій, активів, зобов’язань підприємства, які потенційно можуть принести негативні результати за несприятливих обставин. Також *risk* виступає іменником, виражаючи безпосередньо можливість того, що трапиться щось погане або небезпечне. У фінансовому менеджменті поняття ризику використовується переважно в розумінні іменника, тобто як потенційна можливість негативних наслідків, втрати коштів або бізнесу в цілому. У сфері страхування ризик пов’язують з можливістю того, що щось буде пошкоджено, втрачено або визначеному об’єкту чи суб’єкту буде заподіяно шкоду. Проте ризик як стримуючий фактор є невіддільним від ведення бізнесу загалом і особливо прибуткових операцій, зокрема. Більший зиск, вищі відсотки винагороди приховують в собі більші ризики, тому вміння виявляти, аналізувати, оцінювати ризики є дуже важливим для кожного підприємства в сучасних динамічних умовах гострої конкурентної боротьби для прийняття зважених і ефективних рішень. Ключові ризики – це сукупність ризиків, які мають найбільший вплив на функціонування підприємства та досягнення

ним стратегічних цілей. Для забезпечення ефективності економічних процесів, дієвості внутрішнього аудиту, своєчасної підготовки і реалізації превентивних заходів дуже важливою є оцінка тенденцій впливу ключових ризиків на діяльність компанії. Тому визначення трендів найбільш суттєвих ризиків для господарюючих суб'єктів має практичну та наукову цінність для зосередження уваги на найважливіших аспектах управління ризиками компаній.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спирається автор, виділення не вирішених раніше частин загальної проблеми, котрим присвячується означена стаття. Аналіз наукових публікацій свідчить про значний інтерес до визначення ключових ризиків, які потребують посиленої уваги з боку ризик-менеджменту та внутрішнього аудиту. Так, у своїй праці М. Мартініс та К. Хоутон [1] досліджують питання ефективності аудиту ділових ризиків на основі тестування та матеріалів опитування провідних експертів великих компаній, пропонуючи розроблені робочі документи аудиторів для оцінки процесів з вищим і нижчим бізнес-ризиком таким чином, щоб аспекти діяльності, які містять вищий рівень ризику були досліджувані внутрішніми аудиторами більш ретельно, а ті, які містять менші ризики не забирали надмірну увагу і час. У підсумку це повинно забезпечити створення аудиторської ефективності. У своїй праці П. Колодзей [2] оцінює взаємозв'язок ключових ризиків діяльності, на думку польського автора, – операційний ризик, комплаєнс та ризики внутрішнього аудиту найбільше впливають на конкурентні позиції підприємства на ринку. При цьому основна увага приділяється визначенню найважливіших областей моніторингу та формуванню рекомендацій для зменшення ризиків й дотримання функції відповідності.

Висвітлюючи аспекти оцінювання ризиків при проведенні аудиту Н.І. Дорош [3] розкриває сутність підприємницького ризику та описує методи управління ризиками суб'єкта господарювання, проте представлені результати більше орієнтовані на проведення зовнішнього незалежного аудиту, наслідки не виявлення значних ризиків і їх вплив на подальшу діяльність підприємства, достовірність звітності та репутацію аудитора, не розкриваючи при цьому особливості управління ризиками на рівні підприємства.

У своїй праці О. Бойко [4] розглядає стурбованість аудиторів різних країн світу основними ризиками в сучасних умовах господарювання, зокрема, особлива увага приділяється захисту інформації, ризикам кібератак та досвіду світової спільноти у протидії загрозам. Проблеми управління ризиками підприємств в секторі ІТ-послуг для підвищення їх конкурентоспроможності аналізують І.А. Нечаєва та Є.А. Дьордій [5].

Важливі питання захисту мережевих та інформаційних систем, критичної інфраструктури й внутрішнього ринку країн ЄС від ризиків у своїй праці висвітлюють бельгійські та нідерландські вчені Д. Маркопоулу, В. Папаконстантину та П. де Герт [6]. Країни ЄС зацікавлені у створенні безпечних умов ведення бізнесу та функціонування критично важливих об'єктів у сучасному інформаційному середовищі. Тому підкреслюється важливість стратегічного міжнародного співробітництва у галузі кібезбезпеки, протидії кіберзагрозам, класифікації та виявлення ризиків. Загальні аспекти управління ризиками представлені в монографії О.Б. Данченко та О.В. Занори [7]. Ризики взаємодіють і здатні посилювати один одного, створюючи емерджентність або синергетичні ефекти [8]. Тому природа економічних ризиків, їх властивості і прояви є важливим об'єктом дослідження [9].

Актуальний огляд основних ризиків, визначених на основі опитування керівників відділів внутрішнього аудиту провідних європейських компаній, представляють у спільній роботі європейські інститути внутрішніх аудиторів Франції, Німеччини, Італії, Нідерландів, Іспанії, Швеції та Великобританії [10-12]. Представлена інформація є дуже корисною у розумінні сучасних проблем та посиленні вагомості окремих видів ризиків у при проведенні внутрішнього аудиту. Поряд з цим необхідним залишається поглиблення аналізу ключових ризиків, які впливають на діяльність всіх господарюючих суб'єктів. Всебічний аналіз поглядів науковців і практиків дозволить сформулювати актуальні тенденції в управлінні ризиками, їх виявленні, протидії та ефективному управлінні.

Формулювання цілей статті (постановка завдання). Метою даної статті є дослідження ключових тенденцій у визначенні найбільших ризиків, які впливають на функціонування підприємств, виявленні проблем, причин та можливих шляхів їх подолання для покращення показників ефективності діяльності господарюючих суб'єктів, використовуючи досвід внутрішніх аудиторів провідних компаній ЄС.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Відповідно до Міжнародних стандартів професійної практики внутрішнього аудиту [13], аудиторські послуги передбачають оцінювання доказів з метою формування висновків про підприємство, його операційну діяльність, функції, процеси, системи та інші питання. На основі реалізації систематичного, послідовного та ризик-орієнтованого підходу функцією внутрішнього аудиту є оцінювання ефективності й сприяння удосконаленню процесів корпоративного управління, управління ризиками та контролю на підприємстві [13]. Цінність і довіра до внутрішнього аудиту зростає тоді, коли їхні оцінки спираються на сучасні погляди і враховують майбутні тенденції [13], що надзвичайно важливо в сучасних умовах динамічних змін, посилення нових викликів і загроз. Зокрема, в питаннях управління ризиками, внутрішній аудит повинен забезпечувати об'єктивну оцінку ефективності процесів управління ризиками та їхньому постійному удосконаленню.

На основі всебічного збирання та аналізу інформації про діяльність підприємства формується судження про ефективність управління ризиками відповідно до оцінки виконання наступних положень: а) цілі сприяють та відповідають місії підприємства; б) суттєві ризики виявляються та оцінюються; в) обираються форми

реагування на ризики згідно з рівнем ризик-апетиту підприємства; г) всі відомості про ризики своєчасно і в повному обсязі надаються відповідним підрозділам підприємства, що дозволяє працівникам, керівникам та дирекції виконувати свої обов'язки [13]. Крім того, до обов'язкових завдань внутрішнього аудиту входить визначення впливу ризиків у сфері корпоративного управління, операційної діяльності та інформаційних систем. Внутрішній аудитор оцінює, чи є достовірною і цілісною інформація про господарську діяльність організації, чи відповідають фактичні показники ефективності та продуктивності запланованим, чи досягаються стратегічні цілі підприємства, чи належним чином здійснюється захист активів і їхнє раціональне використання, чи присутні відхилення від вимог законів, нормативних документів, політик, процедур, договірних зобов'язань тощо. Окремим аспектом діяльності внутрішнього аудиту є викриття і недопущення шахрайства, оцінка ризиків, пов'язаних з можливим шахрайством чи їх наслідками, а також надання консультацій керівництву у розробці або управлінні ризиками.

Оцінка ризиків та їхньої структури є невід'ємною частиною загального висновку (звіту) внутрішнього аудиту. Керівник внутрішнього аудиту не несе відповідальності за усунення ризику, проте він зобов'язаний повідомити про наявні ризики, рівень їх прийнятності відповідно до типу управління, виявлені можливі недоліки і порушення, рекомендації для їх усунення та моніторинг за виконанням прийнятих заходів. Відповідно до ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови» [14], метою управління ризиками компанії є створення та захист цінності, прийняття рішень для встановлення та досягнення цілей і підвищення ефективності. Для покращення процесу управління ризиками на підприємствах практичну цінність має врахування досвіду внутрішніх аудиторів щодо виявлення і оцінювання найбільших ризиків, які актуальні для всіх господарюючих суб'єктів.

Для встановлення динаміки та характеристики найбільш вагомих ризиків, які впливають на діяльність великих і найбільш успішних підприємств країн ЄС, інформативним є огляд результатів опитування внутрішніх аудиторів Франції, Німеччини, Італії, Нідерландів, Іспанії, Швеції та Великобританії [10-12]. На підставі якого було виявлено, що базовими ризиками для кожного господарюючого суб'єкта в сучасних умовах ведення бізнесу є: ризики кібер-атак; ризики, пов'язані з захистом та управлінням даними; ризики, спричинені конкуренцією, темпами розвитку та результатами інновацій, змінами законодавства, економічної і політичної невизначеності; ризики аутсорсингу та постачання; ризики фінансового сектору, корпоративного управління і культури; ризики у використанні людських ресурсів; ризики, спричинені корупцією, кліматичними змінами. Зміна рейтингу найбільших ризиків за оцінками, проведеними у 2018-2020 рр. очевидна – все більшої ваги набувають кіберризики та загрози, пов'язані в захистом даних (рис. 1). Рейтинг складався за прогнозними оцінками внутрішніх аудиторів на найближчий рік, тобто показники 2020 р. відображають результати опитування у 2019 р. і очікування експертів щодо того, які ризики будуть впливати на діяльність компанії у плановому році. Проте вже зараз, зважаючи на основні події 2020 року, загострення глобальних проблем через пандемію covid-19, питання екології, проблеми використання людських ресурсів, посилення цифровізації та віртуалізації суспільно-економічних процесів будуть впливати на подальші оцінки найбільших ризиків підприємств та змінювати інструментарій ризик-менеджменту.

У представленому на рис. 1 рейтингу ризиків у відсотках зазначено відповіді опитаних експертів у сфері внутрішнього аудиту щодо того, які саме п'ять найвагоміших ризиків вони визначають як найбільш впливові у функціонуванні та досягненні запланованих результатів діяльності підприємств. Можна помітити, що самі ризики, їхні групи трансформуються протягом 2018-2020 рр. Так, ризики, пов'язані з захистом даних у 2018 р. домінували з 51%, порівняно з кіберризиками, в той час, як у 2019 р. кібербезпека зайняла 66% відповідей опитаних, а захист даних – 58%. І у 2020 р. даний вид ризику розглядається об'єднано і має найвищий рівень актуальності – 78%.

Рис. 1. Динаміка визначення найбільших ризиків провідних компаній ЄС за оцінками внутрішніх аудиторів, (% - питома вага ризику у відповідях експертів)

* У 2018 р. рейтинг ризиків складений на основі оцінок, представлених в дослідженні [12, с.5-7], узагальнені цифрові дані в [10] присутні не по всіх видах ризиків, оскільки деталізовані по секторах діяльності та країнах

Джерело: складено автором на основі [10-12]

Кібербезпека є важливою частиною інформаційної безпеки підприємства. Зважаючи на зростаючі темпи цифровізації економічного та суспільно-політичного життя, ризики, пов'язані з кібербезпекою, залишаються ключовими бізнес-ризиками. Джерелами ризиків в даному процесі виступають як хакерські атаки, дії кіберзлочинців, так і необережні чи навмисні дії самих працівників та внутрішніх користувачів інформаційних систем підприємства, які не дотримуються встановлених процедур, правил й спричиняють негативні наслідки. Ще у 2017 р. глобальна атака Wannacry заразила понад 2 мільйони комп'ютерів у 150 країнах світу і вивела питання кібербезпеки та ризиків використання сучасних інформаційних систем у центр уваги [10, с.8]. Також яскравим прикладом слугував вірус-вимагач Petya, який завдав значних збитків та шкоди критичним підприємствам й приватному сектору в усьому світі, у тому числі і в Україні.

Уряди країн намагаються на державному рівні подолати ризики у даній сфері, створюючи відповідні державні органи, експертні центри, наприклад: Національний центр кібербезпеки Великобританії (UK's National Cyber Security Centre), Іспанський національний криптологічний центр (Spain's National Cryptologic Centre) [11], Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони в Україні [15]. Наприклад, Мережа CSIRTs складається з Комп'ютерної групи реагування на надзвичайні ситуації для установ, агентств та органів ЄС (the Computer Emergency Response Team for the EU institutions, agencies and bodies – CERT-EU) [6], основними завданнями якої є обмін інформацією про послуги, можливості та співпрацю, що стосується інцидентів і пов'язаних з ними ризиків, вироблення скоординованої реакції на інцидент й надання підтримки державам-членам ЄС у вирішенні транскордонних інцидентів.

Проте ризики пов'язані з інформацією не обмежуються кіберзагрозами. Кожна компанія працює з великими масивами інформації, вагома частина якої – це особисті персональні дані працівників, клієнтів, партнерів. Для підприємства значні ризики пов'язані з втратою цієї інформації, що тягне за собою збитки у вигляді штрафів, шкоду для репутації, іміджу надійної та стабільної компанії. Конфіденційність даних є доволі новою сферою управління, в тому числі для ризик-менеджменту. З одного боку, завдання захисту та збереження інформації вимагає вживати заходи верифікації доступу до баз даних, обмеження можливості вносити зміни, обробляти та передавати інформацію, удосконалення засобів збереження даних, потребує інвестиції у відповідне програмне забезпечення, кваліфікований персонал, технічні ресурси. Поряд з цим, логістика інформаційних потоків також вимагає оптимізації й покращення взаємодії між відділами, співробітниками у наданні необхідної, якісної та своєчасної інформації для прийняття рішень. У цьому процесі задіяні всі ланки підприємства, проте вагома роль належить обліковій інформації, оскільки саме вона виступає ядром всіх інформаційних потоків. Тому питання кібербезпеки виходить за рамки захисту персональних даних співробітників і клієнтів підприємства від злому, ризиків зараження вірусними програмами, витоку даних.

Кібербезпека стосується також того, як суб'єкти господарювання організовують процес збирання, обробки, накопичення, представлення й зберігання інформації. На практиці великі підприємства, які у штаті налічують понад 250 працівників мають створювати службу захисту даних, на яку покладається відповідальність щодо протидії ризикам в управлінні даними і підзвітність вищому керівництву.

Закон України «Про основні засади забезпечення кібербезпеки України» [15] визначає кібербезпеку як «захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». При цьому кіберпростір представляє собою певний віртуальний простір або середовище, яке дозволяє здійснювати комунікації, суспільні взаємовідносини, та формується з використанням з'єднаних комунікаційних систем та електронних комунікацій за допомогою мережі Інтернет або інших глобальних мереж передачі даних [15].

Для виявлення та реагування на кіберзагрози застосовуються так звані індикатори – показники, технічні дані. Закон України «Про основні засади забезпечення кібербезпеки України» визначає такі поняття, як кіберзлочинність, кіберрозвідка, кіберінцидент, кібершпигунство [15]. Ризики розглядаються з позиції кіберзагрози, що являє собою наявні або потенційні можливі явища і чинники, які створюють небезпеку національним інтересам України у кіберпросторі, чинять негативний вплив на кіберзахист і кібербезпеку її об'єктів.

У всьому світі представники держави та бізнесу вже давно працюють спільно, щоб різними способами нейтралізовувати кіберзагрози [4]. Власні кроки для захисту даних та регулювання питань кібербезпеки реалізовує Китай. Зокрема, ще у 2017 р. в Китаї було прийнято Закон «Про кібербезпеку Китайської Народної Республіки», де серед інших заходів передбачено необхідність одержання згоди для збору даних та захисту від втрати шляхом шифрування. Цей Закон також зобов'язує підприємства подавати на перевірку регуляторним органам відомості про операції перш ніж надавати великі обсяги персональних даних закордон. Крім того, об'єкти критичної інфраструктури, такі як, банки, транспортні і комунальні підприємства, повинні зберігати персональну інформацію, зібрану в Китаї в середині країни, що може вимагати репатріації даних з закордонних хмарних сервісів.

Загальноприйнятим є девіз про те, що краще запобігати ризикам, ніж ліквідовувати наслідки. Через кібератаки бізнес втрачає шалені кошти. За оцінками Стіва Лангана, генерального директора Hiscox Insurance (Великобританія), впродовж 2016 року світовий бізнес втратив 450 млрд доларів США внаслідок кібератак [4]. Виграти в битві із кіберзлочинцями можна, створивши всередині компанії центри безпеки (Security Operation Centres). Крім спеціалістів з інформаційних технологій, ризик-менеджерів, фінансистів, у таких центрах мають працювати внутрішні та зовнішні аудитори для забезпечення комплексного і ефективного захисту бізнесу від небезпечних кібератак [4]. До посилення систем кібербезпеки активно залучають різних фахівців, у зв'язку з чим їхні знання мають постійно удосконалюватися, зокрема, у сфері інформаційних технологій, управління ризиками та прогнозування можливих ситуацій розвитку подій.

Для подолання ризиків у кіберпросторі, їхнє зменшення до прийнятного рівня, нейтралізації потрібна низка важливих і взаємопов'язаних дій: 1) інвестицій в досконалі технічні засоби безпеки, їхнє належне обслуговування і оновлення; 2) навчання кадрів, як користувачів інформаційних систем, проведення тренінгів, встановлення суворих регламентів і процедур поводження з інформацією та ІТ системами. На це також вказують міжнародні експерти, додаючи, що для зменшення кіберризиків важливо одночасно інвестувати ресурси в засоби контролю і технічного захисту даних, наприклад, сучасні брандмауери, також важливо впроваджувати кіберкультуру через навчання і підвищення обізнаності на всіх рівнях організації [10]. І оскільки технології змінюються швидко, все більш стрімкими темпами, відповідно і засоби захисту не повинні відставати в даному прогресі.

Протидія ризикам у сфері використання інформаційних технологій, які набувають все більшої актуальності, залишається гострим питанням протягом всього періоду аналізу. Процеси оцифровування, автоматизації тісно пов'язані з впровадженням інновацій, зокрема, таких, як новітні комп'ютерні програми, роботизація, штучний інтелект. Поряд з позитивними проявами, інноваційні процеси можуть містити ризики і в площині корпоративної культури, опору, необхідності перекваліфікації персоналу, зміни організаційної структури, додаткових витрат, особливо на етапі впровадження. Одним з рішень пом'якшення ризиків може бути тестування пілотних інноваційних проектів для поетапного інтегрованого впровадження інновацій, виявлення слабких місць та їх своєчасне усунення.

Аналізуючи динаміку визначення найбільших ризиків, можна помітити, що інновації у 2019 р. у списку були доповнені ризиками, пов'язаними з діджиталізацією (відповідно 28% і 36%) і в оцінках внутрішніх аудиторах на 2020 р. вони вже показувались однією позицією – цифровізація та інновації, яка одержала 58% питомої ваги у відповідях експертів як одного з п'яти ключових ризиків, очікуваних на найближчий рік [11-12]. Що свідчить про посилення актуальності даного виду ризиків в діяльності сучасних компаній.

Ризики, пов'язані за складністю регулювання та невизначеністю, з 2018 р. трансформувались у ризик змін нормативної бази, який за прогнозними оцінками на 2020 р. зайняв 59% [10-12]. Зокрема, у складі цих ризиків можна виділити несприятливі зміни в законодавстві, нові умови, вимоги, податки, ускладнене адміністрування, впровадження нових стандартів та внесення змін до діючих. Як наприклад, це відбулось у 2018 р. з набуттям чинності МСФЗ 9 «Фінансові інструменти», МСФЗ 15 «Дохід за контрактами з клієнтами»,

МСФЗ 17 «Договори страхування», та подальші зміни національних і міжнародних стандартів обліку і звітності (МСФЗ та НП(С)БО). В свою чергу це впливає на порядок формування показників фінансової звітності, відображення його ресурсів, структуру капіталу, обчислення фінансових результатів та оцінювання фінансового стану підприємства.

Оцінка ризиків має базуватись на врахуванні регіональних та національних особливостей, зокрема, для Великобританії ризики для бізнесу посилює політична невизначеність та загрози, пов'язані з Brexit, для Іспанії – розширення транснаціонального бізнесу, який поширився на Мексику і зіткнувся з впливом США. На фінансовому ринку для компаній Франції, Італії, Нідерландів та Іспанії збільшення повноважень Єдиного наглядового механізму Європейського центрального банку (European Central Bank's Single Supervisory Mechanism – SSM) також розглядається як окреме джерело ризиків.

Нідерланди є єдиною країною, яка визначала саме культуру як один з найбільших ризиків організації [11, с.3], що пов'язано з впровадженням культури як складової ефективного корпоративного управління в даній країні та прийняттям Кодексу корпоративного управління, який було введено в дію у 2018 р. Провідні компанії Голландії висловлюють занепокоєння ризиками, пов'язаними з корпоративною стійкістю, природним навколишнім середовищем, кліматичними змінами і соціальною етикою працівників для забезпечення створення довготривалої цінності. Компанії у Франції більше ніж серед інших країн ЄС серед ризиків виділяють пріоритетними саме ризики, спричинені корупцією і підкупом, та вказують на необхідність розвитку і вдосконалення системи протидії корупції. Поряд з цим дані окремих країн також відрізняються між собою за секторами економіки і сферою діяльності.

Ризики, пов'язані з використанням людських ресурсів, зростають через недосконалий механізм управління талантами, нестачу висококваліфікованих працівників, технічні розробки, вплив демографічних факторів, зміну організаційних моделей підприємств. Автоматизація, ранні застосування штучного інтелекту вимагають перегляду традиційних підходів до використання персоналу, загострення проблем безробіття і працевлаштування, перекваліфікацію фахівців. Найбільш перспективним навичками працівників будуть ті, які неможливо відтворити та замінити програмно-апаратними засобами, - креативність, оригінальність, ініціативне критичне мислення, переконання і переговори, комплексне вирішення проблем та емоційний інтелект. Вже зараз в Європі спостерігається невідповідність між навичками і талантами, як наслідок, зростання незайнятих вакансій, зокрема в Чехії – на 38% у 2018 р., Італії – на 32%, Австрії – 28% [12, с.49-51]. Для подолання цих ризиків успішні компанії повинні чітко розуміти майбутні потреби свого бізнесу, особливо в кадровому плані, компетентності і знання своїх працівників, їх продуктивність. Для цього повинні бути прийняті обґрунтовані програми прийому та звільнення працівників, передбачені можливості кар'єрного зростання, управління талантами, розвиток креативності, інноваційність і гнучкість в питаннях управління людським капіталом. Прикладом успішного досвіду можна назвати впровадження Кодексу корпоративного управління у Великобританії та Німеччині.

Отже, як бачимо, спостерігаються значні зміни у визначенні найбільш впливових ризиків, які можуть завдати шкоди функціонуванню підприємства й потребують ретельного аналізу готовності компаній протидіяти цим видам ризиків для збереження конкурентних позицій і забезпечення сталого розвитку.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Динамічні зміни умов функціонування підприємств спричиняють трансформацію ризиків, які найбільше впливають на їх діяльність. Для забезпечення досягнення показників ефективності і стабільного розвитку кожне підприємство має аналізувати ризики та вибирати відповідні заходи протидії й реагування. Вплив технологій та інновацій на процеси економічного розвитку посилює ризики, пов'язані з використанням інформації у все більш цифровому світі. Кібербезпека та захист даних визнані сферами з найвищим рівнем ризиків у 2020 р. Діджиталізація визначалась як один з найбільших ризиків у 2019 р, проте ризики пов'язані з оцифровуванням у 2020 р. приймаються як факт, невіддільний від сучасного ведення бізнесу. Кожне підприємство і кожна країна піклується про безпеку інформаційних мереж та систем, захист даних, створюючи служби захисту великого обсягу конфіденційних даних. Поряд з цим зростають ризики, пов'язані зі змінами законодавства та правил нормативно-правового регулювання, ризики аутсорсингу, процесів постачання, фінансові ризики та ризики макроекономічної й політичної нестабільності. Посилюються ризики і у використанні людських ресурсів, інтелектуального капіталу, корпоративного управління та культури, ризики внаслідок змін стандартів обліку і звітності. Серед основних тенденцій спостерігається також зростання ризиків, пов'язаних з комунікацією та репутацією, фінансовим контролем. Економічна нестабільність підсилює ризики злиття і поглинання, корупцію. Тривожні наслідки зміни клімату, забруднення природного середовища дедалі більше висувають екологічні ризики поміж інших на перший план, підкреслюючи їх глобальність та непередбачуваність для всіх сфер життя. Ризики, пов'язані зі здоров'ям і безпекою також у тренді активного зростання, особливо через covid-19, зважаючи на критичні наслідки і загрози для економіки, охорони здоров'я та суспільства.

Оскільки внутрішні аудитори при проведенні перевірок зосереджують свою увагу на сферах діяльності, які можуть містити приховані або невиявлені ризики, їхні оцінки і поради у визначенні найбільших ризиків, можливих способів їх вимірювання, аналізу шляхів протидії мають велику практичну цінність для підприємств. Внутрішній аудит дозволяє виявити реакції підприємства на зростаючі ризики та оцінити якість ризик-менеджменту компанії загалом. Аналізуючи ефективність протидії підприємства найбільшим ризиками необхідно враховувати специфіку і сферу діяльності компанії, її розмір, середовище та взаємодію з внутрішніми і зовнішніми користувачами, регламент управління ризиками загалом та готовність до кожного

їхнього виду зокрема. Таким чином, внутрішній аудит оцінює ефективність процесів управління ризиками та сприяє їх удосконаленню.

Перспективи подальших досліджень полягають у визначенні властивостей та складових найбільш вагомих ризиків, що впливають на діяльність підприємств, запозичення досвіду успішних компаній країн ЄС, для формування інструментів і заходів ефективного управління, зменшення та нейтралізації негативного впливу ризиків у сучасних умовах господарювання.

Список літератури.

1. Martinis, M. and Houghton, K. (2019), "The Business Risk Audit Approach and Audit Production Efficiency". December 2019. Abacus (A Journal of Accounting, Finance and Business Studies), 55(4):734-782. https://doi.org/10.1111/abac.12178.
2. Kolodziej, P. (2016), "Operational Risk, Compliance Risk & Auditing", January 2016, DOI: 10.13140/RG.2.1.3200.5205.
3. Дорош Н.І. Оцінювання ризиків при проведенні аудиту. Науковий вісник Національної академії статистики, обліку та аудиту, 2017. № 4. С. 40-47.
4. Бойко О. Чим сьогодні занепокоєні аудитори різних країн світу: міжнародний досвід, на який варто звернути увагу. Вісник МСФЗ. 2017. № 8 (серпень). https://msfz.ligazakon.ua/ua/magazine_article/FZ001292.
5. Нечаєва І. А., Дьордій Є. А. Управління ризиками підприємства в секторі іт-послуг як інструмент підвищення його конкурентоспроможності. *Ефективна економіка*. 2018. № 12. DOI: 10.32702/2307-2105-2018.12.120.
6. Markopoulou D., Papakonstantinou V., P. de Hert (2019), "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", Computer Law & Security Review, Vol. 35, Issue 6, 105336, https://doi.org/10.1016/j.clsr.2019.06.007.
7. Данченко О.Б., Занора В.О. Проектний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень : монографія. Черкаси, 2019. 278 с.
8. Семенова С.М. Емерджентність у застосуванні системного підходу до управління підприємством. The International scientific and practical conference "A new view on the economy – the trend of innovative development", July 25, 2014 Kiev. Budapest. Vienna. Scientific.-inf. publ. center based on The Association of students and pedagogues "The Economist" Budapest: 2014, 196 p. P. 35-38.
9. Ілляшенко С.М. Економічний ризик: Навчальний посібник. 2-ге вид., доп. перероб. К.: Центр навчальної літератури, 2004. 220 с.
10. Risk in Focus 2018: Hot topics for internal auditors. Chartered Institute of Internal Auditing. URL: https://global.theiia.org/knowledge/Public%20Documents/Risk-in-Focus-Hot-Topics-2018.pdf.
11. Risk in Focus 2019: Hot topics for internal auditors. ECIIA, Chartered Institute of Internal Auditing, September 2018. URL: http://iap.work/wp-content/uploads/2018/12/risk-in-focus-2019.pdf.
12. Risk in Focus 2020: Hot topics for internal auditors. ECIIA, European Confederation of Institutes of Internal Auditing. The Corporate Governance House, Brussels, Belgium, September 2019. URL: https://www.eciia.eu/wp-content/uploads/2019/09/Risk-in-Focus.pdf.
13. Міжнародні стандарти професійної практики внутрішнього аудиту (стандарти) (*International Standards for the Professional Practice of Internal Auditing (Standards)*). URL: http://iia-ua.org/wp-content/uploads/2013/08/IPPF-Standards-2017-Ukrainian.pdf.
14. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (*Risk management – Guidelines*). URL: https://www.iso.org/ru/standard/65694.html.
15. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

References.

1. Martinis, M. and Houghton, K. (2019), "The Business Risk Audit Approach and Audit Production Efficiency". December 2019. *Abacus (A Journal of Accounting, Finance and Business Studies)*, 55(4): pp. 734-782. https://doi.org/10.1111/abac.12178.
2. Kolodziej, P. (2016), "*Operational Risk, Compliance Risk & Auditing*", January 2016, DOI: 10.13140/RG.2.1.3200.5205.
3. Dorosh, N.I. (2017), "Risk assessment during the audit", *Scientific Bulletin of the National Academy of Statistics, Accounting and Auditing*, vol. 4. pp. 40-47.
4. Boyko, O. (2017), "What are the concerns of auditors around the world today: international experience that is worth paying attention to". *Bulletin of IFRS*, Vol. 8, August. available at: https://msfz.ligazakon.ua/ua/magazine_article/FZ001292.
5. Nechayeva, I. and Dordiy, E. (2018), "Risk management of the enterprise in the it service sector as an instrument for improving it competitiveness", *Efektyvna ekonomika*, [Online], vol. 12, available at: http://www.economy.nayka.com.ua/?op=1&z=6797. DOI: 10.32702/2307-2105-2018.12.120
6. Markopoulou D., Papakonstantinou V., P. and de Hert (2019), "The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation", *Computer Law & Security Review*, Vol. 35, Issue 6, 105336, available at: https://doi.org/10.1016/j.clsr.2019.06.007.

7. Danchenko, O.B. and Zanora, V.O. (2019), "*Project management: risk management and change in management decision-making*": a monograph, Cherkasy, P. 278.

8. Semenova, S.M. (2014), "Immergence in applying the system approach to enterprise management", *The International scientific and practical conference "A new view on the economy – the trend of innovative development"*. The Association of students and pedagogues "The Economist", July 25, 2014 Kiev. Budapest. Vienna. Scientific.-inf. publ. center based on The Association of students and pedagogues "The Economist" Budapest, 196 p. P. 35-38.

9. Ilyashenko, S.M. (2004), "*Economic risk*": a textbook, 2nd ed., Ext. rework. Kyiv, Center for Educational Literature. 220 p.

10. *Risk in Focus 2018*: Hot topics for internal auditors. Chartered Institute of Internal Auditing. available at: https://global.theiia.org/knowledge/Public%20Documents/Risk-in-Focus-Hot-Topics-2018.pdf.

11. *Risk in Focus 2019*: Hot topics for internal auditors. ECIIA, Chartered Institute of Internal Auditing, September 2018. available at: http://iap.work/wp-content/uploads/2018/12/risk-in-focus-2019.pdf.

12. *Risk in Focus 2020*: Hot topics for internal auditors. ECIIA, European Confederation of Institutes of Internal Auditing. The Corporate Governance House, Brussels, Belgium, September 2019. available at: https://www.eciia.eu/wp-content/uploads/2019/09/Risk-in-Focus.pdf.

13. *International Standards for the Professional Practice of Internal Auditing (Standards).* URL: http://iia-ua.org/wp-content/uploads/2013/08/IPPF-Standards-2017-Ukrainian.pdf.

14. *ISO 31000:2018. Risk management. Guidelines*. available at: https://www.iso.org/ru/ standard/65694.html.

15. The Verkhovna Rada of Ukraine (2017), The Law of Ukraine "On the basic principles of cybersecurity in Ukraine". available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

Стаття надійшла до редакції 20.09.2020 р.