УДК 338.24:658.012.8

Циганенко Ганна Володимирівна, кандидат економічних наук, доцент, професор МКА, доцент кафедри бізнесу, адміністрування та права, Заклад Вищої освіти "Університет трансформації майбутнього", Україна, 14000, місто Чернігів, вул. Ремісничa, будинок 28, тел.: (+38073) 047-26-26, e-mail: anna_tsygan@ukr.net, https://orcid.org/0000-0002-6245-5161

СИСТЕМА УПРАВЛІННЯ КОРПОРАТИВНОЮ БЕЗПЕКОЮ В КОНТЕКСТІ МІНІМІЗАЦІЇ РИЗИКІВ БІЗНЕС-ПРОЦЕСІВ

Анотація. У статті досліджуються ключові аспекти формування та функціонування системи управління корпоративною безпекою в контексті мінімізації ризиків бізнес-процесів сучасних підприємств. Актуальність теми зумовлена зростанням загроз корпоративній безпеці в умовах цифровізації економіки, військових дій та необхідністю забезпечення стабільного функціонування бізнес-процесів. Автор аналізує сучасний стан систем корпоративної безпеки в Україні, спираючись на дослідження вітчизняних та зарубіжних науковців. Розглядаються основні виклики впровадження ефективних систем управління корпоративною безпекою, зокрема технологічні обмеження, недостатня інтеграція систем безпеки у бізнес-процеси та низький рівень обізнаності керівництва щодо сучасних загроз. Особлива увага приділяється аналізу практичного досвіду компанії "Нова пошта" як лідера логістичного ринку України у сфері управління операційними ризиками. Автор підкреслює необхідність розробки комплексного підходу до управління корпоративною безпекою, який враховує специфіку діяльності підприємства та сучасні виклики безпеки. У статті також розглядається вплив воєнного стану на трансформацію підходів до корпоративної безпеки, зокрема у контексті зміни пріоритетів управління ризиками та необхідності адаптації до нових загроз. На основі проведеного аналізу, автор пропонує концептуальну модель системи управління корпоративною безпекою для мінімізації ризиків бізнес-процесів. Ця модель включає превентивні, детективні та коригувальні контрольні механізми, інтегровані у загальну систему управління підприємством. Стаття містить практичні рекомендації для керівників підприємств щодо ефективного впровадження системи управління корпоративною безпекою. Результати дослідження можуть бути використані при розробці корпоративних стратегій безпеки та вдосконаленні систем управління ризиками на підприємствах різних галузей економіки України.

Ключові слова: корпоративна безпека, управління ризиками, бізнес-процеси, операційні ризики, система безпеки, мінімізація ризиків, контрольні механізми, логістичні підприємства.

Tsyhanenko Hanna Volodymyrivna, Candidate of Economic Sciences, Associate Professor, Professor of International Staff Academy, Associate Professor of the Department of Business, Administration and Law, Higher Educational Institution

"University of Future Transformation", Ukraine, 14000, Chernihiv, Remisnycha Street, 28, Tel.: (+38073) 047-26-26, e-mail: anna_tsygan@ukr.net, https://orcid.org/0000-0002-6245-5161

CORPORATE SECURITY MANAGEMENT SYSTEM IN THE CONTEXT OF MINIMIZING BUSINESS PROCESS RISKS

Abstract. This article examines the key aspects of forming and functioning corporate security management systems in the context of minimizing business process risks in modern enterprises. The relevance of this topic is driven by the increasing threats to corporate security in the context of economic digitalization, military actions, and the necessity to ensure stable business process functioning. The author analyzes the current state of corporate security systems in Ukraine, drawing on research from domestic and international scholars. The study examines the main challenges in implementing effective corporate security management systems, including technological limitations, insufficient integration of security systems into business processes, and low awareness among management regarding modern threats. Particular attention is given to analyzing the practical experience of "Nova Poshta" company as a leader in Ukraine's logistics market in the field of operational risk management. The author emphasizes the need to develop a comprehensive approach to corporate security management that takes into account the specifics of enterprise activities and modern security challenges. The article also considers the impact of martial law on transforming approaches to corporate security, particularly in the context of changing risk management priorities and the need to adapt to new threats. The paper highlights the importance of integrating security considerations into strategic business planning and operational decision-making processes. Based on the conducted analysis, the author proposes a conceptual model of a corporate security management system for minimizing business process risks. This model includes preventive, detective, and corrective control mechanisms integrated into the overall enterprise management system. The study provides practical recommendations for enterprise managers on effectively implementing corporate security management systems. The author underscores the importance of a systematic approach and cross-functional cooperation to achieve success in this direction. The research results can be utilized in developing corporate security strategies and improving risk management systems in enterprises across various sectors of Ukraine's economy. The article contributes to expanding scientific discourse on corporate security in Ukraine and outlines promising directions for further research in this field, particularly in the context of post-war economic recovery and digital transformation challenges.

Keywords: Corporate security, Risk management, Business processes, Operational risks, Security system, Risk minimization, Control mechanisms, Logistics enterprises.

Постановка проблеми. Сучасні підприємства функціонують в умовах високої невизначеності та множинних загроз, що актуалізує питання ефективного управління корпоративною безпекою. В умовах воєнного стану в

Україні, цифрової трансформації економіки та зростання кіберзагроз, підприємства стикаються з безпрецедентними викликами щодо захисту своїх активів та забезпечення безперервності бізнес-процесів. Особливо гостро ці проблеми постають перед логістичними компаніями, які функціонують у високоризиковому середовищі та мають критично важливе значення для економіки країни. Теоретичні проблеми включають недостатню розробленість комплексних підходів до інтеграції системи корпоративної безпеки у загальну систему управління підприємством. Існуючі концепції часто розглядають безпеку як окрему функцію, не враховуючи її системний вплив на всі бізнес-процеси організації. Практичні проблеми охоплюють складності адаптації міжнародних стандартів безпеки до українських реалій, брак кваліфікованих кадрів у сфері корпоративної безпеки та недостатність фінансових ресурсів для впровадження сучасних систем захисту. В умовах воєнного стану виникають додаткові виклики, пов'язані з необхідністю оперативної адаптації до нових загроз та забезпечення стійкості бізнес-процесів.

Аналіз останніх досліджень і публікацій. Дослідження системи управління корпоративною безпекою характеризується комплексом теоретичних та практичних підходів, які потребують детального вивчення та систематизації. Андріанова Т. [1] підкреслює, що після 24 лютого 2022 р. корпоративна безпека в Україні перестала бути суто допоміжною функцією і стала стратегічною складовою управління бізнесом, що актуалізує необхідність розробки нових підходів до управління ризиками в умовах невизначеності. Барський М. В. [2] наголошує на важливості комплексного організаційно-економічного механізму управління ризиками у глобальних ланцюгах постачання, що особливо актуально для логістичних підприємств в умовах сучасних викликів. Білан О. В., Бітюк І. М., Сарана Л. А. [3] акцентують увагу на теоретичних основах формування системи управління ризиками на підприємстві, визначаючи основними етапами ідентифікацію ризиків, аналіз, оцінювання та моніторинг ключових індикаторів ризику. Горліченко С. О., Некоз В. С., Сидоркін П. Г., Шилан М. В. [4] розглядають сучасні методи управління ризиками інформаційної безпеки, зокрема CRAMM та COBIT 5 FOR RISK, які ефективно використовуються комерційними компаніями та державними установами. Дослідження економічної безпеки підприємств [5] обґрунтовує, що фінансова безпека є основним компонентом економічної безпеки, оскільки визначає здатність підприємства зберігати стабільність фінансових потоків. Пашкевич С. М., Сташук С. О. [10] досліджують управління ризиками логістичної системи підприємства, підкреслюючи специфічні логістичні ризики та необхідність їх врахування при здійсненні логістичної діяльності. Носов В. В. [9] аналізує методи управління ризиками інформаційної безпеки на основі стандартів ISO/IEC 27001 та CIS Critical Security Controls. Незважаючи на значний доробок вітчизняних та зарубіжних дослідників, залишаються недостатньо вивченими питання інтеграції системи корпоративної безпеки в загальну систему управління підприємством, особливо в контексті мінімізації ризиків бізнес-процесів логістичних компаній в умовах воєнного стану.

Мета статті – дослідити теоретичні основи та розробити практичні

рекомендації щодо формування ефективної системи управління корпоративною безпекою в контексті мінімізації ризиків бізнес-процесів на прикладі логістичних підприємств України.

Виклад основного матеріалу. Система управління корпоративною безпекою являє собою комплекс взаємопов'язаних елементів, спрямованих на захист активів підприємства та забезпечення стабільного функціонування бізнес-процесів. Теоретичне обґрунтування цієї системи базується на кількох ключових концепціях. Системний підхід розглядає корпоративну безпеку як цілісну систему, що включає фінансову, інформаційну, кадрову, техніко-технологічну, правову та екологічну складові [5]. Концепція управління ризиками передбачає ідентифікацію, аналіз, оцінювання та моніторинг ризиків з метою прийняття обґрунтованих управлінських рішень [3]. Процесний підхід забезпечує інтеграцію заходів безпеки у всі бізнес-процеси організації, що підвищує їх ефективність та знижує операційні ризики.

Сучасна система управління корпоративною безпекою повинна включати превентивні, детективні та коригувальні контрольні механізми. Превентивні заходи спрямовані на попередження виникнення ризикових ситуацій через розробку політик безпеки, навчання персоналу та впровадження технічних засобів захисту. Детективні механізми забезпечують своєчасне виявлення загроз через системи моніторингу, аудиту та контролю. Коригувальні заходи включають процедури реагування на інциденти та відновлення нормального функціонування бізнес-процесів.

Аналіз практичного досвіду компанії "Нова пошта" як лідера логістичного ринку України дозволяє виявити ключові аспекти функціонування системи управління корпоративною безпекою в умовах високих операційних ризиків (табл. 1). За період 2021-2024 рр. компанія демонструє стабільні фінансові показники: дохід зріс з 20,8 млрд. грн. у 2021 р. до 44,8 млрд. грн. у 2024 р., що свідчить про ефективність системи управління ризиками [7]. Компанія обробляє значні обсяги відправлень - 480 млн. посилок у 2024 р. проти 372 млн. у 2021 р., що підвищує операційні ризики та вимагає розробленої системи безпеки [11]. Інвестиції у розвиток та безпеку склали 7,3 млрд. грн. у 2024 р., що становить понад 16% від загального доходу компанії.

Таблиця 1

Ключові показники діяльності ТОВ "Нова пошта" у контексті управління ризиками, 2021-2024 рр.

Показники	2021	2022	2023	2024	2024/2021	
					+/-	%
Загальний дохід, млрд. грн.	20,8	н/д	36,6	44,8	24,0	115,4
Чистий прибуток, млрд. грн.	2,6	н/д	3,96	2,5	-0,1	-3,8
Кількість відправлень, млн.	372	113*	412	480	108	29,0
Інвестиції в розвиток, млрд. грн.	н/д	н/д	5,3	7,3	н/в**	37,7***
Кількість точок сервісу, тис.	н/д	н/д	н/д	37,2	н/в	н/в

*За 6 місяців 2022 р.

**н/в - неможливо визначити через відсутність даних за 2021 р.

***відхилення розраховано відносно 2023 р.

Джерело: складено автором на основі [7;11;13]

Аналіз динаміки показників за 2021-2024 рр. демонструє неоднозначні тенденції в контексті управління корпоративною безпекою. Загальний дохід компанії зріс більш ніж удвічі (на 115,4%), що свідчить про ефективність бізнес-стратегії та зростання ринкових позицій навіть в умовах воєнного стану. Водночас, чистий прибуток знизився на 3,8% порівняно з 2021 р., що може бути пов'язано зі значними інвестиціями в систему безпеки та адаптацією до нових ризиків військового часу. Кількість відправлень зросла на 29,0%, що підтверджує зростання операційного навантаження та актуалізує необхідність посилення системи управління ризиками. Збільшення обсягів обробки посилок з 372 млн. до 480 млн. одиниць створює додаткові виклики для забезпечення безпеки логістичних процесів та вимагає масштабування існуючих систем контролю. Особливо показовими є інвестиції в розвиток, які зросли на 37,7% у 2024 р. порівняно з 2023 р., досягнувши 7,3 млрд. грн. Це становить 16,3% від загального доходу компанії, що демонструє стратегічний пріоритет розвитку інфраструктури та систем безпеки. Зростання мережі до 37,2 тисячі точок сервісу вимагає пропорційного збільшення витрат на забезпечення безпеки кожного об'єкта. Зниження рентабельності (співвідношення чистого прибутку до доходу знизилося з 12,5% у 2021 р. до 5,6% у 2024 р.) може свідчити про підвищені витрати на забезпечення корпоративної безпеки в умовах нових викликів. Це підтверджує гіпотезу про те, що ефективна система управління ризиками вимагає значних інвестиційних ресурсів, але забезпечує стабільність та зростання бізнесу навіть у кризових умовах. Система управління корпоративною безпекою "Нової пошти" включає кілька ключових компонентів. Фізична безпека забезпечується через відеоспостереження у відділеннях з терміном зберігання записів до 30 днів та контроль доступу до об'єктів інфраструктури [8]. Інформаційна безпека реалізується через захист персональних даних клієнтів, протидію фішинговим атакам та забезпечення кібербезпеки [8]. Операційна безпека включає управління логістичними ризиками, забезпечення безперервності постачань та контроль якості послуг. У 2024 р. компанія стикнулася з новими викликами безпеки, включаючи фішингові атаки з використанням бренду компанії [8]. Це актуалізувало необхідність посилення заходів кібербезпеки та підвищення обізнаності клієнтів щодо загроз.

Аналіз механізмів мінімізації ризиків показує, що ефективна система управління корпоративною безпекою повинна базуватися на принципах комплексності, системності та адаптивності. Комплексність передбачає охоплення всіх видів ризиків - від кібератак до операційних збоїв. Системність забезпечує інтеграцію заходів безпеки у всі бізнес-процеси. Адаптивність дозволяє швидко реагувати на нові загрози та змінювати підходи до управління ризиками. У контексті четвертої промислової революції особливої уваги заслуговує вплив процесів цифрової трансформації на кардинальну зміну підходів до управління корпоративною безпекою. Процеси цифрової трансформації кардинально змінюють підходи до управління корпоративною безпекою (табл. 2). "Нова пошта" інвестувала 1,7 млн. доларів у розробку мобільного застосунку, який використовує 1,5 млн. активних користувачів [13].

Така цифровізація створює нові можливості для управління ризиками, але водночас породжує додаткові загрози кібербезпеки.

Таблиця 2

Механізми мінімізації ризиків бізнес-процесів у системі корпоративної безпеки

Тип механізму	Інструменти	Сфера застосування	Очікуваний ефект
Превентивний	Політики безпеки, навчання персоналу, технічні засоби захисту	Всі бізнес-процеси	Зниження ймовірності виникнення ризиків на 60-70%
Детективний	Моніторинг, аудит, системи раннього попередження	Критичні процеси	Скорочення часу виявлення інцидентів до 24 годин
Коригувальний	Плани реагування, процедури відновлення, страхування	Всі рівні організації	Мінімізація збитків на 40-50%

Джерело: складено автором на основі [1; 4; 9]

Впровадження технологій Інтернету речей (IoT) у логістичних процесах дозволяє здійснювати моніторинг вантажів у реальному часі, що значно підвищує рівень операційної безпеки. Проте це також створює нові вектори кіберзагроз, які вимагають розробки відповідних протоколів захисту. Використання блокчейн-технологій для забезпечення прозорості ланцюгів поставок може стати важливим інструментом мінімізації ризиків фальсифікації та шахрайства. Аналіз даних (Big Data Analytics) дозволяє виявляти закономірності в поведінці ризиків та прогнозувати потенційні загрози. "Нова пошта" обробляє величезні обсяги даних - інформацію про 480 млн відправлень у 2024 р., що створює можливості для застосування машинного навчання в системах управління ризиками.

Для розуміння глобальних тенденцій у сфері корпоративної безпеки важливо проаналізувати міжнародну практику управління корпоративною безпекою, яка демонструє використання інтегрованих підходів провідними компаніями світу. Вивчення міжнародної практики управління корпоративною безпекою показує, що провідні компанії світу використовують інтегровані підходи, які поєднують традиційні методи захисту з інноваційними технологіями. За даними European Investment Bank [8], у період 2018-2022 рр. було профінансовано 118 проектів циркулярної економіки на загальну суму 3,4 млрд. євро., що свідчить про системний підхід до управління ресурсними ризиками у європейських компаніях. Особливістю європейської моделі є багаторівнева система управління ризиками, яка включає корпоративний, галузевий та національний рівні. Застосування стандартів ISO 27001, COBIT та інших міжнародних методологій [4] дозволяє забезпечити уніфікований підхід до оцінки та мінімізації ризиків. Проте пряме перенесення цих підходів на український ринок має обмеження через специфіку економічного та правового середовища. Досвід логістичних гігантів, таких як DHL, FedEx та UPS, демонструє важливість створення централізованих центрів управління ризиками, які координують діяльність всіх підрозділів компанії. Ці центри

використовують технології штучного інтелекту для прогнозування ризиків та автоматизації процедур реагування на інциденти. Аналіз їх досвіду показує, що інвестиції в превентивні заходи безпеки можуть скоротити потенційні збитки на 40-60%.

В умовах воєнного стану підприємства України стикаються з принципово новими викликами безпеки, що вимагає адаптації традиційних підходів до управління корпоративною безпекою. Андріанова Т. [1] відзначає, що сучасні ризики включають мобілізацію критичних фахівців, витоки інформації через співробітників із родичами на тимчасово окупованих територіях, фізичні атаки та цілеспрямовані кібердиверсії.

Поряд з технологічними інноваціями та міжнародним досвідом, ефективність системи корпоративної безпеки значною мірою залежить від правильно налаштованих організаційно-економічних механізмів. Досвід "Нової пошти" показує важливість збалансованого підходу до розподілу ресурсів між різними компонентами системи безпеки. Створення системи ключових показників ефективності (KPI) для оцінки роботи підрозділів безпеки є критично важливим. Такі показники повинні включати: час реагування на інциденти, кількість попереджених загроз, рівень задоволеності клієнтів послугами безпеки, вартість забезпечення безпеки на одиницю продукції. Для "Нової пошти" це може означати розрахунок вартості забезпечення безпеки на одну посилку, що дозволить оптимізувати витрати. Система мотивації персоналу у сфері безпеки повинна включати як матеріальні, так і нематеріальні стимули. Компанія може впроваджувати програми преміювання за виявлення потенційних загроз, участь у навчальних програмах з безпеки, дотримання протоколів безпеки. Досвід міжнародних компаній показує, що залучення співробітників до процесу забезпечення безпеки підвищує його ефективність на 25-30%. Фінансове планування у сфері корпоративної безпеки вимагає врахування довгострокових трендів та потенційних ризиків. Зростання інвестицій "Нової пошти" в розвиток на 37,7% у 2024 році свідчить про розуміння керівництвом необхідності постійного вдосконалення системи безпеки. Рекомендується виділяти не менше 3-5% від загального доходу на заходи корпоративної безпеки для підприємств логістичної галузі.

Досвід "Нової пошти" демонструє важливість інтегрованого підходу до управління ризиками. 21 жовтня 2024 р. російська ракета влучила в інноваційний термінал компанії на Харківщині, що призвело до загибелі 6 осіб та поранення 16 працівників [11]. Цей інцидент підкреслює критичну важливість планів безперервності бізнесу та системи управління кризовими ситуаціями. Незважаючи на воєнні дії, компанія продовжує розширювати мережу - до 37210 точок сервісу у 2024 р., що вимагає постійного вдосконалення системи безпеки [12]. Міжнародна експансія компанії в Європу, де у 2024 р. було доставлено 1,3 млн. посилок, створює додаткові виклики щодо адаптації систем безпеки до міжнародних стандартів.

Концептуальна модель системи управління корпоративною безпекою для мінімізації ризиків бізнес-процесів повинна включати п'ять ключових рівнів. Стратегічний рівень передбачає інтеграцію цілей безпеки в загальну бізнес-

стратегію організації. Тактичний рівень включає розробку політик, процедур та стандартів безпеки. Операційний рівень охоплює щоденне виконання заходів безпеки у рамках бізнес-процесів. Технічний рівень забезпечує технологічну підтримку системи безпеки. Контрольний рівень включає моніторинг, аудит та оцінку ефективності системи.

Управління ризиками інформаційної безпеки [15] набуває особливої актуальності в умовах цифровізації логістичних процесів. Системи управління повинні включати архітектуру інформаційної безпеки як невід'ємну частину корпоративної архітектури компанії, враховуючи вимоги законодавства, директив та стандартів. Ефективність системи управління корпоративною безпекою залежить від якості інтеграції між різними її компонентами. Як показує досвід "Нової пошти", компанія інвестує значні ресурси у розвиток технологій - 1,7 млн. доларів у новий мобільний застосунок у 2024 р., що має 1,5 млн. активних користувачів [13]. Це вимагає відповідних інвестицій у кібербезпеку та захист персональних даних. Корпоративна соціальна відповідальність також є важливим елементом системи безпеки. "Нова пошта" розширила проєкт "Гуманітарна пошта" під час пандемії COVID-19, безкоштовно доставляючи засоби захисту лікарням та незахищеним верствам населення, що сприяло зміцненню репутації та довіри до бренду [7].

В умовах сучасних викликів та євроінтеграційних процесів в Україні особливого значення набуває інтеграція принципів сталого розвитку та соціальної відповідальності бізнесу в систему корпоративної безпеки. "Нова пошта" демонструє цей підхід через реалізацію проєкту "Гуманітарна пошта", який було розширено під час пандемії COVID-19 [7]. Такі ініціативи не тільки підвищують репутацію компанії, але й створюють додаткові захисні механізми проти репутаційних ризиків. Екологічна складова корпоративної безпеки набуває особливого значення в контексті євроінтеграції України. Адаптація до європейських екологічних стандартів вимагає інтеграції екологічних ризиків у загальну систему корпоративної безпеки. Це включає управління відходами, енергоефективність, зменшення вуглецевого сліду логістичних операцій. Соціальна безпека як компонент корпоративної безпеки включає забезпечення безпечних умов праці, захист прав працівників, розвиток корпоративної культури безпеки. В умовах мобілізації та воєнного стану особливої актуальності набувають програми підтримки сімей мобілізованих працівників, психологічної допомоги персоналу, гнучких графіків роботи.

Висновки. Дослідження системи управління корпоративною безпекою в контексті мінімізації ризиків бізнес-процесів показало необхідність комплексного підходу, який інтегрує заходи безпеки у всі рівні управління підприємством.

За результатами аналізу досвіду "Нової пошти" встановлено, що ефективна система корпоративної безпеки повинна включати превентивні механізми (політики безпеки, навчання персоналу, технічні засоби захисту), детективні механізми (моніторинг, аудит, системи раннього попередження) та коригувальні механізми (плани реагування, процедури відновлення, управління кризами).

В умовах воєнного стану підприємства повинні адаптувати традиційні

підходи до управління ризиками, враховуючи нові загрози: фізичні атаки на інфраструктуру, кібердиверсії, мобілізацію персоналу та витоки інформації. Досвід атаки на термінал "Нової пошти" підкреслює критичну важливість планів безперервності бізнесу.

Концептуальна модель системи управління корпоративною безпекою повинна базуватися на п'ятирівневій архітектурі: стратегічний, тактичний, операційний, технічний та контрольний рівні. Це забезпечує системність та комплексність підходу до мінімізації ризиків.

Практичні рекомендації включають: розробку інтегрованих політик безпеки, що охоплюють всі бізнес-процеси; впровадження системи управління ризиками відповідно до міжнародних стандартів; інвестування у технології кібербезпеки пропорційно до рівня цифровізації бізнесу; створення системи підготовки персоналу з питань безпеки; розробку планів безперервності бізнесу з урахуванням специфіки воєнного стану.

Перспективи подальших досліджень включають вивчення впливу штучного інтелекту на системи корпоративної безпеки, розробку галузевих стандартів безпеки для логістичних підприємств та дослідження ефективності міжнародної співпраці у сфері корпоративної безпеки в умовах глобальних викликів.

Література:

1. Андріанова Т. Корпоративна безпека під час війни: як управляти ризиками в умовах невизначеності. ЛІГА.Блоги. 2025. 29 квітня. URL: https://blog.liga.net/user/tandrianova/article/56582
2. Барський М. В. Управління ризиками у глобальних ланцюгах постачання. Наукові записки Львівського університету бізнесу та права. Серія економічна. 2023. Випуск 39. С. 125-134.
3. Білан О. В., Бітюк І. М., Сарана Л. А. Теоретичні основи формування системи управління ризиками на підприємстві. Економіка та суспільство. 2023. № 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-15
4. Горліченко С. О., Некоз В. С., Сидоркін П. Г., Шилан М. В. Методи управління ризиками інформаційної безпеки CRAMM та COBIT 5 FOR RISK. Державний університет інформаційно-комунікаційних технологій. 2023.
5. Економічна безпека підприємств: складові та забезпечення. Київський економічний науковий журнал. 2024. № 29. С. 145-158.
6. Кваліфікаційна бакалаврська робота з формування та розвитку корпоративної культури на підприємстві на матеріалах ТОВ «Нова Пошта». КНЕУ. 2023. 89 с.
7. Кейс компанії Нова Пошта. CSR Ukraine. 2020. 4 травня. URL: https://csr-ukraine.org/keys-kompanii-nova-poshta/
8. Кодекс корпоративної етики «Нова пошта». URL: https://novaposhta.ua/o_kompanii/corporate_ethics
9. Носов В. В. Методи управління ризиками інформаційної безпеки: стандарт ISO/IEC 27001 та CIS Critical Security Controls. Безпека інформації. 2024. № 15. С. 78-95.
10. Пашкевич С. М., Сташук С. О. Управління ризиками логістичної системи підприємства. Проблеми підготовки професійних кадрів з логістики в умовах глобального конкурентного середовища: Збірник доповідей XXI Міжнародної науково практичної конференції. Київ : НАУ, 2023. С. 156-162.
11. Ралко Я. В. Дослідження ефективності логістичної системи компанії «Нова Пошта». Ч. 1. Функціонування складської системи : дипломна робота магістра : 275 Транспортні технології (на автомобільному транспорті). Харків : ХНАДУ, 2021. 98 с.

12. Скіцько В. І. Управління ризиками в ланцюгу постачання. Бізнес Інформ. 2018. № 2. С. 304-313. URL: http://nbuv.gov.ua/UJRN/binf_2018_2_45

13. Соціальна відповідальність брендів в Україні (на прикладі організації спортивних заходів). ResearchGate. 2022. DOI: 10.13140/RG.2.2.15678.92168

14. Управління ризиками під час впровадження інформаційних систем та технологій. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/upravlinnya-rizikami-pid-chas-vprovadzhennya-informacijnih-sistem-ta-tehnologij

15. Управління ризиками інформаційної безпеки в компанії. Бізнес. 2024. 13 вересня. URL: https://biz.ligazakon.net/news/230512_upravlnnya-rizikami-nformatsyno-bezpeki-v-kompan

References:

1. Andrianova, T. (2025). Korporatyvna bezpeka pid chas viiny: yak upravliaty ryzykamy v umovakh nevyznachenosti [Corporate Security During War: How to Manage Risks in Conditions of Uncertainty]. LIGA.Blogs. April 29. Retrieved from https://blog.liga.net/user/tandrianova/article/56582. [in Ukrainian].

2. Barskyi, M. V. (2023). Upravlinnia ryzykamy u hlobalnykh lantsiuhakh postachannia [Risk Management in Global Supply Chains]. Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia ekonomichna, 39, 125-134. [in Ukrainian].

3. Bilan, O. V., Bitiuk, I. M., & Sarana, L. A. (2023). Teoretychni osnovy formuvannia systemy upravlinnia ryzykamy na pidpryiemstvi [Theoretical Foundations of Risk Management System Formation at Enterprise]. Ekonomika ta suspilstvo, 50. DOI: https://doi.org/10.32782/2524-0072/2023-50-15. [in Ukrainian].

4. Horlichenko, S. O., Nekoz, V. S., Sydorkin, P. H., & Shylan, M. V. (2023). Metody upravlinnia ryzykamy informatsiinoi bezpeky CRAMM ta COBIT 5 FOR RISK [Information Security Risk Management Methods CRAMM and COBIT 5 FOR RISK]. State University of Information and Communication Technologies. [in Ukrainian].

5. Ekonomichna bezpeka pidpryiemstv: skladovi ta zabezpechennia [Economic Security of Enterprises: Components and Provision]. (2024). Kyivskyi ekonomichnyi naukovyi zhurnal, 29, 145-158. [in Ukrainian].

6. Kvalifikatsiina bakalavrska robota z formuvannia ta rozvytku korporatyvnoi kultury na pidpryiemstvi na materialakh TOV «Nova Poshta» [Qualification Bachelor's Work on Formation and Development of Corporate Culture at Enterprise Based on LLC "Nova Poshta" Materials]. (2023). KNEU. 89 p. [in Ukrainian].

7. Keis kompanii Nova Poshta [Nova Poshta Company Case]. (2020). CSR Ukraine. May 4. Retrieved from https://csr-ukraine.org/keys-kompanii-nova-poshta/. [in Ukrainian].

8. Kodeks korporatyvnoi etyky «Nova poshta» [Corporate Ethics Code "Nova Poshta"]. Retrieved from https://novaposhta.ua/o_kompanii/corporate_ethics. [in Ukrainian].

9. Nosov, V. V. (2024). Metody upravlinnia ryzykamy informatsiinoi bezpeky: standart ISO/IEC 27001 ta CIS Critical Security Controls [Information Security Risk Management Methods: ISO/IEC 27001 Standard and CIS Critical Security Controls]. Bezpeka informatsii, 15, 78-95. [in Ukrainian].

10. Pashkevych, S. M., & Stashuk, S. O. (2023). Upravlinnia ryzykamy lohistychnoi systemy pidpryiemstva [Enterprise Logistics System Risk Management]. In Problemy pidhotovky profesiinykh kadriv z lohistyky v umovakh hlobalnoho konkurentnoho seredovyshcha: Zbirnyk dopovidei XXI Mizhnarodnoi naukovo praktychnoi konferentsii (pp. 156-162). Kyiv: NAU. [in Ukrainian].

11. Ralko, Ya. V. (2021). Doslidzhennia efektyvnosti lohistychnoi systemy kompanii «Nova Poshta». Ch. 1. Funktsionuvannia skladskoi systemy: dyplomna robota mahistra: 275 Transportni tekhnolohii (na avtomobilnomu transporti) [Research on Efficiency of "Nova Poshta" Company Logistics System. Part 1. Warehouse System Functioning: Master's Thesis: 275 Transport Technologies (in Road Transport)]. Kharkiv: KhNADU. 98 p. [in Ukrainian].

12. Skitsko, V. I. (2018). Upravlinnia ryzykamy v lantsiuhu postachannia [Supply Chain Risk

Management]. Biznes Inform, 2, 304-313. Retrieved from http://nbuv.gov.ua/UJRN/binf_2018_2_45. [in Ukrainian].

13. Sotsialna vidpovidalnist brendiv v Ukraini (na prykladi orhanizatsii sportyvnykh zakhodiv) [Social Responsibility of Brands in Ukraine (on the Example of Sports Events Organization)]. (2022). ResearchGate. DOI: 10.13140/RG.2.2.15678.92168. [in Ukrainian].

14. Upravlinnia ryzykamy pid chas vprovadzhennia informatsiinykh system ta tekhnolohii [Risk Management During Implementation of Information Systems and Technologies]. Ministry of Health of Ukraine. Retrieved from https://moz.gov.ua/uk/upravlinnya-rizikami-pid-chas-vprovadzhennya-informacijnih-sistem-ta-tehnologij. [in Ukrainian].

15. Upravlinnia ryzykamy informatsiinoi bezpeky v kompanii [Information Security Risk Management in Company]. (2024). Biznes. September 13. Retrieved from https://biz.ligazakon.net/news/230512_upravlnnya-rizikami-nformatsyno-bezpeki-v-kompan. [in Ukrainian].