УДК 368.021.4:004

**Савченко Наталія Григорівна**
*доктор філософії з економіки,*
*доцент кафедри фінансів*
*Державний торговельно-економічний університет*
**Savchenko Nataliia**
*Doctor of Philosophy in Economics,*
*Associate Professor of the Finance Department*
*State University of Trade and Economics*
ORCID: 0000-0003-2972-5024

**Серажим Юліан Віталійович**
*доктор філософії з економіки,*
*доцент кафедри банківської справи*
*Державний торговельно-економічний університет*
**Serazhym Yulian**
*Doctor of Philosophy in Economics,*
*Associate Professor of the Banking Department*
*State University of Trade and Economics*
ORCID: 0000-0002-2295-7095

DOI: 10.25313/2520-2294-2025-11-11604

# УПРАВЛІННЯ РИЗИКАМИ СТРАХОВОЇ КОМПАНІЇ ПІД ЧАС ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

# RISK MANAGEMENT OF AN INSURANCE COMPANY DURING DIGITAL TRANSFORMATION

***Анотація.*** *Вступ. Сучасний страховий ринок перебуває в умовах активної цифрової трансформації, яка зумовлює перегляд традиційних підходів до управління бізнес-процесами, організації клієнтських взаємодій і системи ризик-менеджменту. Застосування штучного інтелекту (далі – ШІ) надає нові можливості для управління ризиками, але створює й додаткові виклики – етичні, правові та технологічні. Це зумовлює потребу вдосконалення системи ризик-менеджменту та адаптації її до цифрових викликів.*

*Мета. Метою статті є розкриття концептуальних засад управління ризиками страхової компанії з акцентом на його цифрову трансформацію.*

*Матеріали і методи. Матеріалами дослідження є наукові праці вітчизняних і зарубіжних дослідників. У роботі застосовано методи аналізу, синтезу, порівняння та логічного узагальнення для визначення впливу цифрових технологій на систему управління ризиками.*

*Результати. Узагальнено теоретичні й практичні аспекти управління ризиками в умовах цифровізації. З'ясовано, що цифрова трансформація зумовлює нові типи ризиків – кібернетичні, технологічні, операційні, регуляторні. Проаналізовано динаміку кількості кібератак в Україні (2022–2024 рр.) та роль цифрових інструментів у мінімізації їхнього впливу. Показано, що впровадження ШІ, Big Data та InsurTech підвищує точність оцінки ризиків, автоматизує реагування та зміцнює фінансову стійкість страхових компаній. Запропоновано багаторівневий підхід до трансформації системи ризик-менеджменту страхової компанії. Виокремлено основні проблеми управління ризиками страхової компанії під час цифрової трансформації.*

*Перспективи. Подальші дослідження доцільно спрямувати на розробку інтегрованої моделі ризик-менеджменту з урахуванням інструментів ШІ для прогнозування ризиків і підвищення стійкості страхових компаній у цифровій економіці.*

***Ключові слова:*** *ризик-менеджмент, кіберстрахування, штучний інтелект, кіберризики, диджиталізація, фінансова стійкість.*

***Summary.*** *Introduction. The modern insurance market is undergoing active digital transformation, which requires a review of traditional approaches to business process management, customer interaction, and risk management systems. The use of*

*artificial intelligence (hereinafter referred to as AI) provides new opportunities for risk management, but also creates additional challenges – ethical, legal, and technological. This necessitates the improvement of risk management systems and their adaptation to digital challenges.*

*Purpose. The purpose of this article is to reveal the conceptual foundations of risk management in insurance companies, with an emphasis on its digital transformation.*

*Materials and methods. The research materials are scientific works by domestic and foreign researchers. The work uses methods of analysis, synthesis, comparison, and logical generalization to determine the impact of digital technologies on the risk management system.*

*Results. The theoretical and practical aspects of risk management in the context of digitalization are summarized. It has been established that digital transformation gives rise to new types of risks – cybernetic, technological, operational, and regulatory. The dynamics of the number of cyberattacks in Ukraine (2022–2024) and the role of digital tools in minimizing their impact have been analyzed. It is shown that the introduction of AI, Big Data, and InsurTech increases the accuracy of risk assessment, automates response, and strengthens the financial stability of insurance companies. A multi-level approach to the transformation of an insurance company's risk management system is proposed. The main problems of risk management for insurance companies during digital transformation are highlighted.*

*Prospects. Further research should focus on developing an integrated risk management model that incorporates AI tools for risk forecasting and improving the resilience of insurance companies in the digital economy.*

***Key words:*** *risk management, cyber insurance, artificial intelligence, cyber risks, digitalization, financial stability.*

**Постановка проблеми.** Сучасний страховий ринок перебуває на етапі активної цифрової трансформації, що суттєво змінює бізнес-моделі, систему ризик-менеджменту та характер взаємодії між учасниками ринку. Впровадження цифрових технологій, зокрема автоматизації, великих даних (далі — Big Data), ШІ та блокчейну, надає нові можливості для підвищення ефективності управління ризиками, але водночас зумовлює низку викликів, пов'язаних із кіберзагрозами, технічними труднощами та ризиками витоку інформації.

Інтеграція ШІ в аналітичні процеси страхових компаній потребує розроблення нових підходів до моніторингу, прогнозування та оцінювання ризиків.

Водночас наявна практика ризик-менеджменту українського страхового сектору залишається недостатньо адаптованою до цифрових викликів, а чинна нормативно-правова база лише частково враховує управління ризиками страхових компаній та використання інтелектуальних технологій. Це зумовлює необхідність наукового обґрунтування напрямів трансформації цієї сфери в умовах цифрової економіки.

**Аналіз останніх досліджень і публікацій.** Проблематика розвитку системи ризик-менеджменту страхових компаній в умовах цифрової трансформації активно висвітлюється сучасними українськими та зарубіжними науковцями. Значний внесок у формування теоретико-методичних засад управління ризиками роблять В. Губа та С. Кісь, які досліджують особливості управління ризиками страхових компаній у процесі цифровізації та євроінтеграції, наголошуючи на необхідності підвищення прозорості й точності прогнозування [1].

Вплив ШІ на систему управління ризиками аналізують А. Чорновол, Я. Гончарук, Є. Хелемендик і С. Кисилиця, доводячи, що використання ШІ автоматизує оцінку ризиків і зменшує вплив людського фактору [2]. Подібну позицію поділяють Н. Заплатинський (N. Zaplatynskyi), П. Люб (P. Lub) і С. Запорожцев (S. Zaporozhtsev), які підкреслюють роль ШІ в підвищенні кібербезпеки та ранньому виявленні загроз [3].

Проблеми страхування кіберризиків розглядають Г. Нямещук і В. Біла, які визначають його як важливий елемент управління цифровими ризиками [4], та А. Шолойко, яка акцентує на необхідності оновлення нормативно-правового поля й розвитку актуарних методів [5]. На проблемах низької обізнаності бізнесу й недостатній актуарній базі наголошують Р. Пікус і Ю. Бабенко [6].

Інноваційні підходи до цифрової трансформації страхового менеджменту пропонує В. Другова, яка розробляє багаторівневу систему ризик-менеджменту з використанням ШІ, Big Data та моделювання ризиків [7]. Необхідність використання новітніх технологій у страхових компаніях з метою підвищення конкурентоздатності обґрунтовують Ю. Данько та С. Бровко, аналізуючи переваги та перспективи використання інноваційних продуктів на страховому ринку [8]. Чинником підвищення ефективності аналітики та тарифоутворення визначають цифрові технології Н. Євтушенко, Ю. Кривенко та Д. Стеценко [9]. Потребу адаптації ризик-менеджменту до викликів воєнного часу підкреслюють К. Бездітко і Д. Загорська [10].

Вплив воєнного стану на страхову галузь аналізують А Житар [11] та А. Марина й М. Пеценко [12], обґрунтовуючи необхідність розширення страхових продуктів, що покривають наявні ризики страхових компаній.

Отже, наукові джерела засвідчують зростання уваги до цифровізації страхового бізнесу, упровадження ШІ. Водночас потребують подальшої розробки практичні механізми інтеграції ШІ-рішень та методики оцінки кіберризиків у системі ризик-менеджменту страхових компаній.

**Метою статті** є розкриття концептуальних засад управління ризиками страхової компанії з акцентом на його цифрову трансформацію.

Для досягнення мети сформульовано такі завдання:

1) проаналізувати теоретичні засади управління ризиками в діяльності страхових компаній та визначити основні підходи до їх трансформації в умовах воєнного стану;
2) оцінити вплив воєнних ризиків і цифрових загроз на ефективність функціонування системи ризик-менеджменту страхового сектору України;
3) обґрунтувати напрями вдосконалення механізмів ризик-менеджменту страхових компаній з урахуванням сучасних технологічних інновацій та потреб післявоєнного відновлення страхового ринку.

**Матеріали і методи.** Матеріалами дослідження є наукові праці вітчизняних і зарубіжних дослідників щодо управління ризиками та застосування ШІ у фінансовому секторі загалом та страховому, зокрема.

У процесі дослідження використано такі наукові методи: порівняльного аналізу — для оцінювання впливу технологічних інновацій (ШІ, Big Data, блокчейн) на ефективність управління ризиками; системного підходу — для побудови моделі інтегрованої системи ризик-менеджменту; логічного узагальнення — для формулювання висновків і розробки практичних рекомендацій щодо вдосконалення ризик-менеджменту страхових компаній в цифровому середовищі.

**Виклад основного матеріалу.** Управління ризиками страхової компанії в умовах цифрової трансформації набуває стратегічного значення, оскільки ефективність бізнесу безпосередньо залежить від здатності організації передбачати, оцінювати та мінімізувати наслідки потенційних загроз. Страхування — одна з галузей фінансового сектору, що найбільш чутливо реагує на впровадження цифрових технологій, адже процеси збору, обробки й захисту інформації визначають конкурентоспроможність і стійкість суб'єкта страхового ринку. У цьому контексті страхова компанія повинна постійно аналізувати зміни зовнішніх і внутрішніх чинників, які впливають на її фінансові показники та ризиковий профіль [12, с. 46]. Для цього необхідно розвивати інтегровані комп'ютерні системи управління ризиками, що забезпечують аналітичну підтримку прийняття рішень та контроль за рівнем операційних, фінансових і кіберризиків.

За останні роки в Україні спостерігається стрімке зростання уваги до питань кібербезпеки, що зумовлено підвищенням частоти, масштабності та складності кібератак, які впливають як на бізнес-сектор, так і на державне управління. Аналітичні дослідження підтверджують стійку тенденцію до збільшення кількості кіберінцидентів і формування попиту на страхові продукти, здатні компенсувати цифрові втрати, збитки від простоїв та витрати на відновлення після атак. Як зазначають Г. Нямещук та В. Біла, у сучасних умовах страхування кіберризиків перетворюється на провідний елемент забезпечення фінансової стійкості підприємств, особливо в період воєнного стану [4, с. 281].

Кіберризик визначається як імовірність порушення функціонування IT-систем або цифрової інфраструктури організації через несанкціоноване втручання, знищення цифрових активів чи інші деструктивні дії, що призводять до фінансових втрат або репутаційної шкоди [13].

За офіційними підрахунками команд реагування CERT-UA, у 2022–2024 рр. спостерігалося стійке зростання кількості зареєстрованих кіберінцидентів в Україні: близько 2 194 випадки у 2022 р., 2 543 — у 2023 р. і ≈ 4 315 — у 2024 р. [14–17]. Водночас трансформується структура цільових кібератак, зокрема зростає частка атак на урядові установи та об'єкти критичної інфраструктури. Інциденти, що стосуються фінансового сектору (страхування) та IT-галузі, залишаються вагомими і в окремі періоди становлять помітну частку від загальної кількості зафіксованих випадків. Це підкреслює необхідність узгодженої реалізації превентивних та коригувальних заходів, до яких належить використання інструментів ШІ для раннього виявлення загроз і автоматизації дій у разі інциденту [14]. Динаміку кількості кібератак в Україні (2022–2024) та роль цифрових інструментів у мінімізації їхнього впливу наведено в таблиці 1.

Наведена динаміка свідчить про посилення кіберагресії, розширення спектра цільових об'єктів та зростання ризиків для провідних секторів економіки, зокрема фінансового й страхового.

Паралельно розвивається ще один важливий напрям — застосування ШІ у страхуванні. Українські дослідники зазначають, що інтеграція ШІ-технологій сприяє автоматизації процесів обробки даних, скорингу ризиків, прогнозування інцидентів та оптимізації тарифоутворення. Водночас наголошується на необхідності дотримання етичних стандартів, прозорості алгоритмів і узгодження з нормативними вимогами у сфері персональних даних [2; 3].

Результати сучасних досліджень в Україні свідчать, що застосування технологій машинного навчання та ШІ дозволяє суттєво підвищити швидкість виявлення кіберзагроз і скоротити час реагування на інциденти. Як зазначають Ю. Данько, С. Бровко [8], інтеграція ШІ в процеси страхування не лише зменшує вплив людського фактору під час оцінювання ризиків, але й підвищує ефективність андерайтингу, тобто оцінки страхових випадків та визначення страхових премій.

Інновації на основі ШІ мають потужний вплив на весь страховий ланцюг створення вартості. Завдяки ШІ страхові компанії можуть аналізувати великі масиви даних, виявляючи закономірності

*Таблиця 1*

**Динаміка кількості кібератак в Україні (2022–2024 рр.) та роль цифрових інструментів у мінімізації їхнього впливу**

| Рік | Зареєстровано/ оброблено | Роль цифрових інструментів у мінімізації впливу (конкретні застосунки) |
|---|---|---|
| 2022 | 2 194 оброблених інцидентів | ШІ-підтриманий моніторинг логів і мережевого трафіку для раннього виявлення; EDR/ XDR-платформи; базова кібергігієна (MFA, резервні копії); формування перших страхових продуктів для бізнесу |
| 2023 | 2 543 інциденти | Big Data + ШІ для підвищення точності скорингу ризиків; інтеграція кіберстрахування в договори (покриття реагування, відновлення даних, юридична допомога); автоматизація інцидент-менеджменту |
| 2024 | 4 315 інцидентів | Масштабніша інтеграція ШІ-рішень: динамічне тарифоутворення для кіберполісів на основі аналітики, автоматичні playbook-и реагування (ШІ-асистовані), побудова національних/локальних баз інцидентів для покращення актуарних розрахунків. |

*Джерело:* узагальнено автором на основі [14–17]

ризиків і тенденції збитковості, що дозволяє формувати більш точні моделі ціноутворення. Це не лише підвищує ефективність управлінських процесів, а й сприяє зменшенню невизначеності в прийнятті рішень. Як наслідок, страхові компанії отримують змогу оперативніше реагувати на зміни ринку, а власники полісів — більш персоналізовані пропозиції страхового захисту.

У ширшому контексті цифрової трансформації варто зазначити стрімкий розвиток технологій InsurTech, які стали рушійною силою оновлення страхового бізнесу. Під терміном InsurTech розуміють використання інноваційних технологій, таких як ШІ, машинне навчання, аналітика великих даних, блокчейн, інтернет речей та мобільні додатки, для оптимізації страхових процесів і зниження операційних ризиків [18]. В Україні цей напрям розвивається особливо активно після пандемії COVID-19 та в умовах воєнного стану, коли онлайн-сервіси страхування стали нормою для споживачів.

Водночас застосування ШІ в страхуванні передбачає розв'язання низки важливих завдань, зокрема забезпечення якості та релевантності даних, включно з анонімізацією та захистом персональної інформації; гарантування прозорості моделей (explainability) для прийняття страхових і регуляторних рішень; управління моделями (Model Risk Management) та їх адаптація до швидкоплинних кібертрендів; а також дотримання етичних і правових обмежень при автоматизованих рішеннях, наприклад у випадках відмови в страхових виплатах. Ці аспекти повинні бути інтегровані до внутрішніх політик страхових компаній і вимог до постачальників ШІ-рішень [3, с. 57].

Вітчизняні дослідження підкреслюють, що ефективна система ризик-менеджменту повинна базуватися на поєднанні цифрових технологій, нормативної відповідності та гнучкої архітектури управління [7; 19]. З огляду на це, доцільним є формування багаторівневої моделі трансформації

*Таблиця 2*

**Багаторівневий підхід до трансформації системи ризик-менеджменту страхової компанії**

| Рівень | Основні інструменти та заходи | Очікувані результати |
|---|---|---|
| Превентивний рівень (профілактика) | Упровадження ШІ-моніторингу (аналіз мережевого трафіку, поведінкової аналітики); встановлення вимог кібергігієни до клієнтів (багатофакторна автентифікація, резервне копіювання, план реагування). | Зниження ймовірності інцидентів, раннє виявлення аномалій, підвищення культури безпеки серед страхувальників. |
| Оцінка ризику й тарифоутворення | Використання Big Data та ШІ для формування динамічних скорингових моделей; облік інфраструктурних і галузевих характеристик клієнта; формування пулу ризиків і перестрахування частини експозиції. | Точніше ціноутворення, зниження страхових збитків, підвищення прибутковості та прозорості ризикових рішень. |
| Реагування та відшкодування | Застосування ШІ-асистованих процедур реагування (автоматична категоризація інцидентів, генерація рекомендацій); розробка стандартизованих процедур виплат з урахуванням часових і репутаційних чинників. | Оптимізація часу реагування, зменшення збитків, підвищення задоволеності клієнтів. |
| Управління моделями й відповідність | Створення процесів Model Risk Management; регулярне тестування й аудит моделей; виконання вимог регулятора щодо звітності про кіберінциденти. | Прозорість і надійність ШІ-рішень, відповідність регуляторним стандартам, мінімізація ризиків моделювання. |

*Джерело:* розроблено автором

ризик-менеджменту страхової компанії, яка враховує цифрові виклики та можливості використання ШІ (табл. 2).

Отже, ефективне управління ризиками страхової компанії в умовах цифрової трансформації потребує системного та багаторівневого підходу, який поєднує технологічну інноваційність і нормативну дисципліну. Використання інструментів Big Data, ШІ-моніторингу та управління ризиками моделей забезпечує не лише підвищення точності оцінки ризиків, а й створює основу для формування довіри клієнтів і партнерів. Цифрові технології розширюють можливості автоматизації андеррайтингу, оцінки ризиків і моніторингу кіберзагроз, водночас зумовлюючи нові виклики, для кращого розуміння яких доцільно візуалізувати основні проблеми управління ризиками страхової компанії в період цифрової трансформації (рис. 1).

Узагальнення представлених проблем свідчить, що управління ризиками страхової компанії в умовах цифрової трансформації потребує системного підходу, який поєднує технологічні, нормативні та аналітичні інструменти. Недостатня стандартизація полісів, відсутність достовірних даних для моделювання ризиків, висока вартість страхових продуктів та обмежене розуміння кіберзагроз суттєво стримують розвиток ринку кіберстрахування в Україні. Водночас упровадження ШІ та аналітики великих даних здатне суттєво змінити ситуацію, забезпечуючи більш точне оцінювання ризиків, ефективну тарифну політику й оперативне реагування на інциденти.

Страхові компанії, реагуючи на виклики цифрової епохи, активно розробляють нові поліси, що охоплюють широкий спектр послуг — від відшкодування збитків і компенсації витрат на відновлення даних до надання юридичної підтримки та залучення експертів із кібербезпеки. Проте український ринок кіберстрахування поки що суттєво відстає від європейського та американського за рівнем розвитку, кількістю актуарних даних і ступенем стандартизації страхових продуктів [6].

З огляду на специфіку вітчизняного ринку, перед Україною постає завдання розроблення ефективної стратегії розвитку кіберстрахування та адаптації до міжнародних стандартів. Першочергове значення має формування якісної профільної освіти та підвищення обізнаності населення й бізнесу щодо потенційних кіберризиків. Відкритий доступ до інформації про загрози, способи їх запобігання та методи захисту сприяє зменшенню ймовірності настання страхової події. У цьому контексті особливу роль відіграють урядові програми, освітні ініціативи для бізнесу, закладів освіти, а також масові інформаційні кампанії в медіа та соціальних мережах.

Наступним важливим напрямом є розвиток сучасної кіберінфраструктури, що передбачає впровадження технологій кіберзахисту, створення центрів обробки даних та реалізацію національної програми кібербезпеки. Інвестиції в ці сфери сприяють підвищенню рівня цифрової стійкості держави. Досвід країн Європи, зокрема Великої Британії, Німеччини, Франції та Швеції, підтверджує ефективність поєднання державних і приватних вкладень у сфері кіберзахисту.

Водночас ефективна стратегія запобігання кіберризикам вимагає тісної співпраці між державними установами, приватним сектором і громадськістю. Партнерство, взаємний обмін даними та спільні ініціативи у сфері реагування на кіберінциденти є невіддільними частинами національної системи кібербезпеки. Не менш важливим аспектом є вдосконалення правової бази, зокрема створення чітких норм відповідальності за порушення кіберзаконодавства, регламентація обігу інформації в цифровому середовищі та забезпечення прозорості страхових відносин.

Страхування кіберризиків становить важливий елемент загальної системи кібербезпеки, але не може замінити комплексну систему технічного


Рис. 1. Основні проблеми управління ризиками страхової компанії під час цифрової трансформації
*Джерело:* розроблено автором за джерелом [4]

та організаційного захисту. Ефективний захист потребує поєднання сучасних технологій, підготовлених фахівців і чітко відпрацьованих процедур. Водночас кіберстрахування дозволяє організаціям компенсувати фінансові втрати, пов'язані з кіберінцидентами, оперативно відновлювати бізнес-процеси, отримувати експертну допомогу з кібербезпеки та забезпечувати безперервність діяльності [11].

Для підвищення ефективності управління ризиками страхові компанії мають розробити стандартизовані вимоги до кібергігієни для страхувальників як обов'язкову умову отримання страхового поліса. Це сприятиме зменшенню кількості інцидентів, зумовлених недотриманням базових заходів безпеки, та формуванню культури відповідального використання цифрових технологій. Паралельно доцільно інвестувати у створення власних інтелектуальних інструментів на базі ШІ або співпрацювати з надійними технологічними провайдерами для вдосконалення систем виявлення кіберінцидентів і підвищення точності тарифоутворення.

Не менш важливим завданням є формування локальних баз даних кіберінцидентів і пов'язаних із ними збитків, що забезпечить можливість для більш точних актуарних розрахунків і прогнозування ризиків. Окрім цього, подальший розвиток нормативно-правової бази повинен ураховувати специфіку кіберстрахування та впровадження технологій ШІ, особливо в частині прозорості алгоритмів, захисту персональних даних і етичного використання ШІ у страхових процесах.

**Висновки і перспективи подальших досліджень.** Отже, управління ризиками страхової компанії в умовах цифрової трансформації потребує системного підходу, що поєднує технологічні, організаційні та нормативно-правові аспекти. Використання цифрових інструментів, зокрема технологій ШІ, аналітики великих даних та автоматизованих систем моніторингу, забезпечує підвищення точності оцінювання ризиків, оперативність реагування на інциденти й оптимізацію процесів страхового менеджменту.

У подальших наукових дослідженнях доцільно зосередити увагу на розробленні методичних підходів до інтеграції кіберстрахування в загальну систему управління ризиками страхової компанії, оцінюванні ефективності впровадження технологій ШІ в актуарну діяльність та моделюванні фінансової стійкості страхових організацій в умовах зростання кіберзагроз. Такий підхід сприятиме підвищенню конкурентоспроможності страхового сектору України та його адаптації до викликів цифрової економіки.

**Література**

1. Губа В. Р., Кісь С. Я. Управління ризиками страхових компаній в умовах цифровізації в контексті європейської інтеграції. *Розвиток бізнесу в контексті європейської інтеграції: глобальні виклики, стратегічні пріоритети, реалії та перспективи:* матеріали Міжнародної науково-практичної конференції (м. Київ, 07 червня 2024 р.). Київ, 2024. С. 61–63. DOI: 10.5281/zenodo.11913036

2. Чорновол А. О., Гончарук Я. М., Хелемендик Є. І., Кисилиця С. О. Використання штучного інтелекту в управлінні фінансовими ризиками банків і страхових компаній. *Актуальні питання економічних наук.* 2025. № 8. DOI: https://doi.org/10.5281/zenodo.14887306

3. Zaplatynskyi N., Lub P., Zaporozhtsev S. Improving cybersecurity with artificial intelligence. *Bulletin of Cherkasy State Technological University.* 2024. Vol. 29. № 4. P. 53–61. DOI: 10.62660/bcstu/4.2024.53.

4. Нямещук Г., Біла В. Страхування кіберризиків як складовий елемент системи ефективного менеджменту: кейс України. *Challenges and Issues of Modern Science*. 2024. № 2. С. 280–284. URL: https://cims.fti.dp.ua/j/article/view/117/156 (дата звернення: 04.11.2025).

5. Шолойко А. С. Актуалізація кіберстрахування в умовах цифровізації економіки. *Науковий вісник ОДЕУ.* 2023. № 9 (310). С. 98–106. DOI: 10.32680/2409-9260-2023-9-310-98-106

6. Пікус Р. В., Бабенко Ю. Л. Перспективи розвитку страхування від кібератак в Україні. *Економіка*. 2022. № 2. С. 134–140. DOI: https://doi.org/10.32702/2306-6806.2022.2.134

7. Другова В. Інноваційні підходи до страхового менеджменту в умовах цифрової трансформації. *Економіка та суспільство.* 2024. № 66. DOI: https://doi.org/10.32782/2524-0072/2024-66-123

8. Данько Ю. І., Бровко С. В. Вплив інноваційних технологій на розвиток страхового ринку. *Економіка та суспільство.* 2024. № 62. DOI: https://doi.org/10.32782/2524-0072/2024-62-8

9. Євтушенко Н., Кривенко Ю., Стеценко Д. Цифрові технології у страхуванні. *Грааль науки.* 2024. № 43. С. 105–114. DOI: https://doi.org/10.36074/grail-of-science.06.09.2024.011

10. Бездітко К., Загорська Д. Я. Управління ризиками у страхуванні. *Молодий вчений.* 2023. № 12 (124). С. 151–156. DOI: https://doi.org/10.32839/2304-5809/2023-12-124-6

11. Житар М. Тенденції розвитку страхового ринку України в умовах воєнного стану. *Економіка та суспільство.* 2024. № 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-24

12. Марина А., Пеценко М. Страховий ринок України в умовах війни. *Цифрова економіка та економічна безпека.* 2023. № 5 (05). С. 44–51. DOI: https://doi.org/10.32782/dees.5-7

13. Cyber risk and cybersecurity: a systematic review of data availability / F. Cremer et al. *Geneva Pap Risk Insur Issues Pract.* 2022. Vol. 47. P. 698–736. DOI: https://doi.org/10.1057/s41288-022-00266-6

14. У 2022 році урядова команда реагування на комп'ютерні надзвичайні події зареєструвала 2194 кібератаки, чверть з них на органи влади — держспецзв'язку. *Україна: медіацентр: вебсайт.* 2023. URL: https://mediacenter.org.ua/uk/u-2022-rotsi-uryadova-komanda-reaguvannya-na-komp-yuterni-nadzvichajni-podiyi-zareyestruvala-2194-kiberataki-chvert-z-nih-na-organi-vladi-derzhspetszv-yazku/ (дата звернення: 04.11.2025).

15. Урядова команда CERT-UA в 2023 році опрацювала 2543 кіберінциденти. *gov.ua: вебсайт. 2024.* URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti (дата звернення: 04.11.2025).

16. У другій половині 2024 року було зафіксовано 2576 кібератак рф, це майже в половину більше за попередні 6 місяців. *dev.ua: вебсайт*. 2025. URL: https://dev.ua/news/kiberataky-rf-na-ukrainu-za-pivrichchia-2024-roku-1745998713 (дата звернення: 04.11.2025).

17. Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber War. 2024. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20240916/2024%2008%20Cyber%20digest_ENG.pdf (дата звернення: 04.11.2025).

18. Руденко В. В., Мирончук В. М., Смагло О. В. InsurTach як драйвер розвитку страхування. *Економіка та суспільство.* 2024. № 70. DOI: https://doi.org/10.32782/2524-0072/2024-70-42

19. Дубина М. В., Середюк І. О., Білоус Н. В. Роль кіберстрахування в системі ризик-менеджменту банківських установ. *Проблеми і перспективи економіки та управління*. 2020. № 1 (21). С. 18–196. DOI: 10.25140/2411-5215-2020-1(21)-183-196

**References**

1. Huba, V. R., Kis, S. Ya. (2024). Upravlinnia ryzykamy strakhovykh kompanii v umovakh tsyfrovizatsii v kontekksti yevropeiskoi intehratsii [Risk management of insurance companies under digitalization in the context of European integration]. In: *Rozvytok biznesu v konteksti yevropeiskoi intehratsii: hlobalni vyklyky, stratehichni priorytety, realii ta perspektyvy*: materialy Mizhnar. nauk.-prakt. konf. (m. Kyiv, 07 chervnia 2024 r.) (pp. 61–63.). Kyiv. DOI: 10.5281/zenodo.11913036 [in Ukrainian].

2. Chornovol, A. O., Honcharuk, Ya. M., Khelemendyk, Ye. I., & Kysylytsia, S. O. (2025). Vykorystannia shtuchnoho intelektu v upravlinni finansovymy ryzykamy bankiv i strakhovykh kompanii [Use of artificial intelligence in managing financial risks of banks and insurance companies]. *Aktualni pytannia ekonomichnykh nauk*, № 8. Pp. 1–19. DOI: https://doi.org/10.5281/zenodo.14887306 [in Ukrainian].

3. Zaplatynskyi, N., Lub, P., Zaporozhtsev, S. (2024). Improving cybersecurity with artificial intelligence. *Bulletin of Cherkasy State Technological University*, № 29(4). Pp. 53–61. DOI: 10.62660/bcstu/4.2024.53 [in English].

4. Nyameshchuk, H., & Bila, V. (2024). Strakhuvannia kiber-ryzykiv yak skladovyi element systemy efektyvnoho menedzhmentu: keis Ukrainy [Cyber risk insurance as a component of effective management system: the case of Ukraine]. *Challenges and Issues of Modern Science*, № 2. Pp. 280–284. URL: https://cims.fti.dp.ua/j/article/view/117/156 [in Ukrainian].

5. Sholoiko, A. S. (2023). Aktualizatsiia kiberstrakhuvannia v umovakh tsyfrovizatsii ekonomiky [Actualization of cyber insurance in the context of digitalization of the economy]. *Naukovyi visnyk ODEU*, № 9 (310). Pp. 98–106. DOI: 10.32680/2409-9260-2023-9-310-98-106 [in Ukrainian].

6. Pikus, R. V., & Babenko, Yu. L. (2022). Perspektyvy rozvytku strakhuvannia vid kiberatak v Ukraini [Prospects for the development of cyberattack insurance in Ukraine]. *Ekonomika*, № 2. Pp. 134–140. DOI: https://doi.org/10.32702/2306-6806.2022.2.134 [in Ukrainian].

7. Druhova, V. (2024). Innovatsiini pidkhody do strakhovoho menedzhmentu v umovakh tsyfrovoyi transformatsii [Innovative approaches to insurance management in the context of digital transformation]. *Ekonomika ta suspilstvo*, № 66. Pp. 1–6. DOI: https://doi.org/10.32782/2524-0072/2024-66-123 [in Ukrainian].

8. Danko, Yu. I., & Brovko, S. V. (2024). Vplyv innovatsiinykh tekhnolohii na rozvytok strakhovoho rynku [The impact of innovative technologies on the development of the insurance market]. *Ekonomika ta suspilstvo*, № 62. DOI: https://doi.org/10.32782/2524-0072/2024-62-8 [in Ukrainian].

9. Yevtushenko, N., Kryvenko, Yu., & Stetsenko, D. (2024). Tsyfrovi tekhnolohii u strakhuvanni [Digital technologies in insurance]. *Hraal nauky*, № 43. Pp. 105–114. DOI: https://doi.org/10.36074/grail-of-science.06.09.2024.011 [in Ukrainian].

10. Bezdytko, K., Zahorska, D. Ya. (2023). Upravlinnia ryzykamy u strakhuvanni [Risk management in insurance]. *Molodyi vchenyi*, № 12(124). Pp. 151–156. DOI: https://doi.org/10.32839/2304-5809/2023-12-124-6 [in Ukrainian].

11. Zhytar, M. (2024). Tendentsii rozvytku strakhovoho rynku Ukrainy v umovakh voiennoho stanu [Trends in the development of Ukraine's insurance market under martial law]. *Ekonomika ta suspilstvo*, № 61. DOI: https://doi.org/10.32782/2524-0072/2024-61-24 [in Ukrainian].

12. Maryna, A., & Petsenko, M. (2023). Strakhovyi rynok Ukrainy v umovakh viiny [The insurance market of Ukraine in wartime]. *Tsyfrova ekonomika ta ekonomichna bezpeka*, № 5(05). Pp. 44–51. DOI: https://doi.org/10.32782/dees.5-6 [in Ukrainian].

13. Cremer, F., Sheehan, B., Fortmann, Kia A.N., Mullins M., … & Materne S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues Pract*, Vol. 47. Pp. 698–736. DOI: https://doi.org/10.1057/s41288-022-00266-6 [in English].

14. U 2022 rotsi uriadova komanda reahuvannia na kompiuterni nadzvychaini podii zareiestruvala 2194 kiberataky, chvert z nykh na orhany vlady — derzhspetszviazku [In 2022, the government's computer emergency response team registered 2,194 cyberattacks, a quarter of them against government agencies — state special communications] (2023). *Ukraina: mediatsentr: vebsait.* Retrieved from https://mediacenter.org.ua/uk/u-2022-rotsi-uryadova-komanda-reaguvannya-na-komp-yuterni-nadzvichajni-podiyi-zareyestruvala-2194-kiberataki-chvert-z-nih-na-organi-vladi-derzhspetszv-yazku/ [in Ukrainian].

15. Uriadova komanda CERT-UA v 2023 rotsi opratsiuvala 2543 kiberintsydenty [The government CERT-UA team processed 2,543 cyber incidents in 2023] (2024). *gov.ua: vebsait.* Retrieved from https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti [in Ukrainian].

16. U druhii polovyni 2024 roku bulo zafiksovano 2576 kiberatak rf, tse maizhe v polovynu bilshe za poperedni 6 misiatsiv [In the second half of 2024, 2,576 cyberattacks were recorded in the Russian Federation, which is almost half more than in the previous 6 months] (2025). *dev.ua: vebsait.* Retrieved from https://dev.ua/en/news/kiberataky-rf-na-ukrainu-zapivrichchia-2024-roku-1745998713 [in Ukrainian].

17. Review of cybersecurity news in Ukraine, tendencies, and world events related to the First World Cyber War. 2024. Retrieved from https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20240916/2024%2008%20Cyber%20digest_ENG.pdf [in English].

18. Rudenko, V.V., Myronchuk, V.M., & Smahlo, O.V. (2024). InsurTach yak draiver rozvytku strakhuvannia [InsurTach as a driver of insurance development]. *Ekonomika ta suspilstvo*, № 70. DOI: https://doi.org/10.32782/2524-0072/2024-70-42 [in Ukrainian].

19. Dubyna, M.V., Serediuk, I.O., & Bilous, N.V. (2020). Rol kiberstrakhuvannia v systemi ryzyk-menedzhmentu bankivskykh ustanov [The role of cyber insurance in the risk management system of banking institutions]. *Problemy i perspektyvy ekonomiky ta upravlinnia*, № 1(21). Pp. 183–196. DOI: 10.25140/2411-5215-2020-1(21)-183-196 [in Ukrainian].