

DOI: <https://doi.org/10.26565/1992-2337-2025-1-20>
УДК 351.862.1:007

Соболь Роман Георгійович,

кандидат наук з державного управління, доцент, доцент кафедри публічної політики
навчально-наукового інституту “Інститут державного управління”
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: sobol_roma@ukr.net <https://orcid.org/0000-0002-3176-3807>

Єфімов Юрій Вікторович,

доктор філософії, доцент, Перший заступник начальника
Державної екологічної інспекції у Харківській області, м. Харків,
вулиця Бакуліна, 6, м. Харків, 61166, Україна
e-mail: advokat977@ukr.net <https://orcid.org/0000-0003-2848-5583>

Бублій Максим Петрович,

кандидат наук з державного управління, доцент,
доцент кафедри управління персоналом та підприємництва
навчально-наукового інституту “Інститут державного управління”
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: mbubliy@gmail.com <https://orcid.org/0000-0003-1060-6404>

Серенок Артем Олексійович,

кандидат наук з державного управління, доцент, доцент кафедри публічної політики
навчально-наукового інституту “Інститут державного управління”
Харківського національного університету імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: artem.serenok@karazin.ua <https://orcid.org/0000-0002-5550-0921>

Соболь Марія Романівна,

студентка 4 курсу економічного факультету
Київського національного університету імені Тараса Шевченка,
вулиця Володимирська, 60, м. Київ, 01033, Україна
e-mail: maresobol@gmail.com <https://orcid.org/0009-0001-3584-4380>

ЦИФРОВІЗАЦІЯ СТРАХОВОГО РИНКУ ЯК ПІДХІД АНТИКРИЗОВОГО ПУБЛІЧНОГО УПРАВЛІННЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Як цитувати: Соболь Р. Г., Єфімов Ю. В., Бублій М. П., Серенок А. О., Соболь М. Р. Цифровізація страхового ринку як підхід антикризового публічного управління протидії гібридним загрозам. *Державне будівництво*. 2025. № 1 (37). С. 284–294. DOI: <https://doi.org/10.26565/1992-2337-2025-1-20>

In cites: Sobol, R.G., Yefimov, Yu.V., Bubliy, M.P., Serenok, A.O., Sobol, M.R. (2025). Digitalization of the insurance market as an approach of anti-crisis public management to counter hybrid threats. *State Formation*, no. 2 (36), 284–294. DOI: <https://doi.org/10.26565/1992-2337-2025-1-20> [in Ukrainian].

© Соболь Р. Г., Єфімов Ю. В., Бублій М. П., Серенок А. О., Соболь М. Р., 2025



This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0

Анотація. У статті досліджується роль цифровізації страхового ринку як інструменту антикризового публічного управління в умовах гібридних загроз. Аналізуються основні напрями цифрової трансформації страхового сектору, зокрема впровадження інноваційних технологій, таких як штучний інтелект, блокчейн та великі дані, для підвищення стійкості до кіберзагроз та інформаційних атак. Особлива увага приділяється ролі держави у формуванні нормативно-правової бази та стратегічного управління цифровими перетвореннями в страховій галузі.

Ключові слова: *цифровізація, страховий ринок, антикризове управління, публічне управління, гібридні загрози, кібербезпека, інноваційні технології.*

Постановка проблеми. На сьогодні цифровізація страхового ринку як підхід антикризового публічного управління протидії гібридним загрозам це вкрай актуальний й стратегічно важливий науковий напрямок досліджень, який поєднує цифрову трансформацію, страхування та сферу публічного управління в умовах нових викликів – зокрема, гібридних загроз (війна, кібератаки, дезінформація, економічний тиск тощо).

Зростаюча роль страхування у стабілізації економіки та соціального захисту – це важливий аспект сучасної системи публічного управління, особливо в умовах криз, війн, пандемій чи інших гібридних загроз [1]. Страховий ринок виступає не лише комерційною сферою, а й інструментом соціально-економічної безпеки [2].

Гібридні загрози, що поєднують традиційні та нетрадиційні форми впливу, зокрема кібернапади, інформаційні війни та економічні атаки, становлять серйозну небезпеку для національної безпеки. У цьому контексті цифровізація страхового ринку виступає важливим інструментом антикризового публічного управління, сприяючи підвищенню стійкості економіки та забезпеченню ефективного реагування на сучасні виклики.

Аналіз останніх досліджень та публікацій. Питання дослідження цифровізації страхового ринку як підхід антикризового публічного управління протидії гібридним загрозам є відносно молоді, однак уже немало науковців приділили свої роботи теоретичним дослідженням та практичним опрацюванням, а також розгляду впливу гібридних загроз на фінансову безпеку України. Це такі вчені, як: Барановський О., Внукова Н., Гончар М., Деркач О., Жук С., Зварич О., Максак Г., Мартинюк В., Чубик А. та інші.

Постановка завдання. Ціллю статті є розгляд процесу цифровізації страхового ринку як підходу антикризового публічного управління протидії гібридним загрозам та запровадження ефективних факторів щодо його вдосконалення.

Виклад основного матеріалу. У ХХІ столітті безпека держави, стабільність економіки та страхового ринку опинилися під тиском гібридних загроз – комплексних, багатовимірних дій, що поєднують військові, політичні, економічні, інформаційні та кіберінструменти [3]. Такі загрози не мають чітких кордонів, можуть бути анонімними та водночас потужними, що створює нові виклики як для державного управління, так і для бізнесу, зокрема страхового сектору.

Гібридні загрози – це поєднання традиційних і нетрадиційних форм впливу, спрямованих на підірив стабільності, економічної системи, довіри до влади та інституцій [3].

Дуже великим є вплив на державу у вигляді підриву інституційної спроможності: порушення функціонування державних органів через атаки на цифрову інфраструктуру. Ослаблення довіри громадян: інформаційні атаки й фейкові кампанії можуть зруйнувати легітимність державної політики. Підвищення тиску на бюджет: необхідність екстреного фінансування кризових заходів, компенсацій, ліквідації наслідків атак. Складність у прийнятті рішень: гібридні загрози часто не мають очевидного джерела, що ускладнює реагування [4].

Негативним є вплив на ринок і страховий сектор. Це зростання рівня ризиків. Традиційні моделі оцінки вже не завжди працюють, оскільки характер загроз непередбачуваний. Відчувається збільшення страхових випадків у вигляді атаки на ІТ-інфраструктуру, блокування ланцюгів постачання, пошкодження майна внаслідок диверсій. Виявляється необхідність впровадження нових страхових продуктів, таких як кіберстрахування, страхування від тероризму, політичних ризиків тощо. Інвестиційна невизначеність: через високий ризик компанії обережніше інвестують, особливо у довгострокові активи.

Важливим є спільна відповідальність, коли держава та бізнес повинні працювати спільно над системою національної стійкості. Важливо створювати єдину систему оцінки ризиків, інформаційного обміну, протоколів реагування на загрози. У страхуванні – це означає підтримку публічно-приватних партнерств, стимулювання розвитку InsurTech, захист критичної цифрової інфраструктури [5].

Гібридні загрози стають новою нормою у глобальній безпеці. Їхній вплив поширюється не лише на державні установи, а й на економіку загалом. У цих умовах страховий ринок виступає важливим інструментом стабілізації, однак потребує державної підтримки, цифрової трансформації та адаптації до нових викликів.

Важливо додати, що цифровізація страхового ринку – це процес впровадження цифрових технологій у всі етапи роботи страхових компаній: від продажу полісів до врегулювання страхових випадків і управління ризиками. Вона кардинально змінює традиційну модель бізнесу страхування, роблячи її більш зручною, прозорою та клієнтоорієнтованою [6].

Основні напрями цифровізації страхового ринку: онлайн-продажі страхових послуг, можливість купити поліс онлайн без відвідування офісу, платформи порівняння страхових продуктів (агрегатори), електронні поліси (наприклад, автоцивілка в Україні через МТСБУ). Мобільні додатки та персоналізовані сервіси, додатки для управління страховим полісом, подачі заявок, перегляду історії страхових випадків, штучний інтелект та big data для формування індивідуальних страхових пропозицій. Автоматизація та роботизація, використання чат-ботів та голосових асистентів для обслуговування клієнтів, автоматичне врегулювання страхових випадків (наприклад, виплати без

участі людини при простих випадках). Інтернет речей (IoT), впровадження телематики для автострахування (на основі стилю водіння), смарт-гаджети для страхування майна або здоров'я (фітнес-браслети, сигналізації). Блокчейн і кібербезпека, підвищення довіри до страхових угод через прозорі, незмінні блокчейн-записи, захист персональних даних клієнтів та запобігання шахрайству. InsurTech – технологічні стартапи в страхуванні. Нові гравці, які змінюють ринок, впроваджуючи інновації, часто співпрацюючи з традиційними компаніями або витісняючи їх.

Відмітимо переваги цифровізації для клієнтів:

- зручність і швидкість доступу до послуг;
- прозорість умов страхування;
- краще обслуговування та персоналізація;
- Переваги для страхових компаній:
- зниження операційних витрат;
- швидша обробка заяв;
- можливість точнішого оцінювання ризиків.
- Як гібридні загрози впливають на страховий сектор:
- зростання страхових ризиків;
- складність актуарного аналізу;
- підвищена потреба у кіберстрахуванні та страхуванні інфраструктури.

3. Роль публічного управління у цифровізації страхового ринку

Держава як регулятор і драйвер цифрових змін. Нормативно-правова база (електронний поліс, захист даних, RegTech). Публічно-приватне партнерство у створенні цифрової інфраструктури.

4. Напрями цифровізації страхового ринку в умовах гібридних загроз:

Цифрові платформи та відкриті дані для аналізу ризиків і забезпечення прозорості. Інтеграція штучного інтелекту для виявлення шахрайства та оцінки загроз. Кіберстрахування як нова форма захисту бізнесу і критичної інфраструктури. Використання блокчейн-технологій для захисту даних і договорів. Єдині державні реєстри та інтеграція з МВС, МЗС, МВС, ДПС тощо.

5. Виклики цифровізації в умовах гібридних загроз:

Ризики кібератак на страхову інфраструктуру. Брак кваліфікованих кадрів у сфері кібербезпеки та цифрових технологій. Недостатній рівень довіри з боку населення.

6. Приклади (український та міжнародний контексти)

Україна: запуск електронного поліса ОСЦПВ, Дія, впровадження кіберстрахування. НАТО, ЄС: створення кіберполісів та нормативів цифрового страхування інфраструктури. Ізраїль, Естонія – приклади цифрової стійкості держави.

Публічне управління має інтегрувати цифровізацію страхового ринку у стратегії національної безпеки. Необхідність створення національної програми кіберстрахування. Сприяння цифровій грамотності, кібергігієні та довірі до цифрових сервісів.

Цифровізація страхового ринку охоплює впровадження сучасних інформаційних технологій для автоматизації процесів, аналізу ризиків та взаємодії з клієнтами. Основні напрями цифрової трансформації включають:

Використання великих даних та штучного інтелекту для оцінки та прогнозування ризиків, що дозволяє оперативно реагувати на зміни в середовищі загроз.

Впровадження блокчейн-технологій для забезпечення прозорості та безпеки транзакцій, що знижує ризик шахрайства та підвищує довіру до страхових компаній.

Розвиток цифрових платформ та мобільних додатків для спрощення доступу до страхових послуг та покращення клієнтського досвіду [7].

Роль держави в антикризовому управлінні цифровими трансформаціями. Держава відіграє ключову роль у формуванні умов для ефективної цифровізації страхового ринку:

Розробка та впровадження нормативно-правової бази, що регулює використання цифрових технологій у страховій галузі та забезпечує захист прав споживачів.

Створення стратегічних ініціатив та програм, спрямованих на розвиток інфраструктури цифрових технологій та підтримку інноваційних стартапів у сфері страхування.

Забезпечення кібербезпеки через розробку стандартів та протоколів безпеки, а також проведення навчальних програм для підвищення кваліфікації кадрів у сфері цифрових технологій [3].

Роль держави в антикризовому управлінні цифровими трансформаціями є надзвичайно важливою, оскільки саме вона виступає як гарант стабільності, безпеки та сталого розвитку в умовах швидких технологічних змін. У сучасному світі цифровізація охоплює всі сфери суспільного життя – від економіки до освіти, охорони здоров'я та державного управління. Проте такі трансформації нерідко супроводжуються кризовими явищами: кібератаками, соціальними розривами, втратою робочих місць через автоматизацію, нерівним доступом до цифрових послуг тощо. У цьому контексті держава повинна виступати не лише як регулятор, а й як активний учасник процесу управління ризиками та пом'якшення негативних наслідків.

Антикризове управління цифровими трансформаціями з боку держави передбачає цілу низку дій: розробку нормативно-правової бази, що відповідає викликам цифрової епохи; створення інституцій, здатних оперативно реагувати на технологічні кризи; інвестування в цифрову інфраструктуру та освіту; захист прав громадян у цифровому середовищі. Особливої ваги набуває формування державної політики у сфері кібербезпеки, адже цифрові кризи часто пов'язані з витоком даних, зломом систем, порушенням приватності [7].

Крім того, держава відіграє ключову роль у забезпеченні цифрової інклюзії. Не всі соціальні групи мають рівний доступ до технологій, тому державне втручання необхідне для подолання «цифрової прірви» між різними верствами населення та регіонами. Це досягається шляхом підтримки освітніх

програм, цифрової грамотності, розвитку інтернет-інфраструктури в сільських районах.

Також важливою є функція держави як координатора між різними стейкхолдерами цифрової трансформації – бізнесом, наукою, громадянським суспільством. У кризових ситуаціях держава здатна об'єднати ресурси і зусилля для ефективного реагування, мобілізувати необхідні фінансові й організаційні інструменти.

Загалом, ефективне антикризове управління цифровими трансформаціями можливе лише за умови активної, відповідальної та стратегічно мислячої ролі держави. Це включає не лише реагування на виклики, а й випереджувальне планування, інноваційний підхід до формування політики та тісну взаємодію з усіма учасниками цифрової екосистеми.

Виклики та перспективи цифровізації страхового ринку. Цифровізація страхового ринку є важливим етапом розвитку фінансової сфери, що відкриває нові можливості для підвищення ефективності, прозорості та доступності страхових послуг. Водночас цей процес супроводжується низкою викликів, які потребують уваги як з боку держави, так і з боку страхових компаній. Одним із основних викликів є необхідність адаптації існуючих бізнес-моделей до нових умов функціонування. Традиційні підходи до оцінки ризиків, продажу полісів та обслуговування клієнтів поступово втрачають актуальність, поступаючись місцем автоматизованим і цифровим рішенням, що вимагає значних інвестицій у технології, аналітику та кібербезпеку [8].

Ще одним викликом є питання захисту персональних даних. Страховання оперує великою кількістю конфіденційної інформації, і з розвитком цифрових каналів її захист стає критично важливим. Кібератаки, витоки даних і шахрайство можуть не лише завдати фінансових збитків, але й серйозно підірвати довіру клієнтів до компаній. Окрім цього, цифрова трансформація страхового ринку може поглибити нерівність між клієнтами: ті, хто не володіє цифровими навичками або не має доступу до інтернету, можуть залишитися поза межами нових сервісів, що створює додатковий соціальний ризик.

Ще одним викликом цифровізації страхового ринку є питання захисту персональних даних. У процесі надання страхових послуг компанії збирають, обробляють і зберігають велику кількість чутливої інформації про своїх клієнтів – це медичні, фінансові, демографічні дані, історії страхових випадків тощо. Усі ці дані становлять серйозну цінність, і водночас – потенційну вразливість. З поширенням цифрових каналів обслуговування зростає ризик кібератак, несанкціонованого доступу, витоку інформації та її зловживання. Це створює серйозну загрозу не лише для конкретних осіб, а й для репутації страхової компанії, яка може втратити довіру клієнтів і понести фінансові збитки [5].

Крім технічних загроз, існує й нормативний аспект проблеми. Страхові компанії повинні дотримуватись вимог законодавства у сфері захисту персональних даних, зокрема міжнародних стандартів, таких як GDPR у Європейському Союзі, або відповідних національних регуляцій. Це передбачає

забезпечення прозорості обробки даних, надання клієнтам права на доступ і контроль над їхньою інформацією, а також впровадження надійних технічних і організаційних заходів захисту.

Захист персональних даних стає ще складнішим у зв'язку з впровадженням новітніх технологій, таких як штучний інтелект, машинне навчання та big data, що дозволяють здійснювати глибоку аналітику та прогнозування поведінки клієнтів. З одного боку, це дає змогу підвищити ефективність страхових послуг, але з іншого – створює ризик надмірного втручання в приватне життя і дискримінації на основі алгоритмічних рішень. Тому дуже важливо, щоб страхові компанії забезпечували баланс між інноваційністю та етичністю, розробляючи політики конфіденційності, підвищуючи обізнаність працівників і клієнтів щодо захисту інформації та впроваджуючи сучасні засоби кіберзахисту.

У сучасних умовах питання захисту персональних даних є не лише технологічним чи юридичним завданням, а й елементом довіри, на якій будується взаємодія між страховиком і клієнтом. Тому ефективне вирішення цього виклику є ключовим фактором успішної цифрової трансформації страхового ринку [7].

Кіберзагрози та ризики безпеки даних, що вимагає постійного вдосконалення систем захисту та реагування на інциденти.

Необхідність адаптації кадрового потенціалу, оскільки традиційні моделі управління потребують змін для ефективного використання цифрових технологій.

Необхідність адаптації кадрового потенціалу є одним із ключових аспектів цифровізації страхового ринку, оскільки традиційні моделі управління та організаційної структури вже не відповідають вимогам нової цифрової реальності. Умови швидкої технологічної трансформації потребують не лише оновлення інфраструктури, а й переосмислення ролі працівників, їхніх компетенцій та підходів до виконання обов'язків. Цифрові технології змінюють спосіб роботи: автоматизуються рутинні процеси, впроваджуються системи аналітики та штучного інтелекту, використовуються нові канали комунікації з клієнтами. Відтак виникає потреба у фахівцях, які не тільки добре розуміються на страховій справі, а й володіють цифровими навичками, аналітичним мисленням, здатністю працювати з великими масивами даних та адаптуватися до змін [8].

Однак, кадровий ресурс багатьох страхових компаній сформований переважно у традиційній парадигмі, де перевага надається досвіду, а не гнучкості чи цифровій компетентності. Це створює серйозний бар'єр на шляху трансформації, адже навіть найсучасніші цифрові рішення не будуть ефективними без персоналу, здатного з ними працювати. У зв'язку з цим постає завдання системного підходу до навчання та перепідготовки працівників, створення умов для безперервного професійного розвитку, стимулювання цифрової грамотності та культури інновацій.

Крім того, цифрова трансформація змінює вимоги до управлінських підходів. Традиційна ієрархічна модель управління поступово втрачає актуальність, натомість актуалізується потреба в гнучких, децентралізованих структурах, здатних швидко приймати рішення та адаптуватися до змін. Лідери нового покоління мають бути не лише фахівцями у сфері страхування, а й цифровими стратегами, що розуміють технологічні тенденції та вміють працювати з мультидисциплінарними командами. Таким чином, адаптація кадрового потенціалу передбачає не лише оновлення знань і навичок, а й зміну корпоративної культури, стилю лідерства та системи мотивації.

У підсумку, ефективна цифровізація страхового ринку неможлива без глибоких змін у підходах до управління людськими ресурсами. Інвестування в розвиток кадрів, підтримка інноваційного мислення та створення сприятливого середовища для змін стають необхідною умовою для досягнення конкурентоспроможності в цифрову епоху.

Інвестиційні бар'єри, пов'язані з високими витратами на впровадження новітніх технологій та необхідністю забезпечення їхньої сумісності з існуючими системами. Інвестиційні бар'єри, пов'язані з високими витратами на впровадження новітніх технологій та необхідністю забезпечення їхньої сумісності з існуючими системами, є одним із головних стримувальних факторів цифровізації страхового ринку. Цифрова трансформація потребує значних фінансових вкладень у модернізацію ІТ-інфраструктури, розробку програмного забезпечення, впровадження систем кібербезпеки, хмарних технологій, аналітичних платформ і рішень на базі штучного інтелекту. Для багатьох страхових компаній, особливо середнього та малого масштабу, такі витрати є надмірними та ризикованими, що змушує їх відкладати або обмежувати цифрові ініціативи [8].

Додаткову складність створює необхідність інтеграції нових цифрових рішень із вже наявними, часто застарілими системами, які були створені за традиційною логікою бізнес-процесів. Несумісність технологій, відсутність єдиних стандартів, складність переносу даних та адаптації персоналу призводять до затримок, зростання витрат і зниження ефективності цифрових проєктів. Крім того, модернізація старих систем часто потребує тимчасового зупинення частини бізнес-операцій, що також супроводжується фінансовими втратами та репутаційними ризиками.

Ще одним аспектом інвестиційних бар'єрів є невизначеність результатів цифровізації. Багато компаній побоюються, що великі вкладення у технології не принесуть очікуваного ефекту через відсутність досвіду, недостатню цифрову культуру або слабку ринкову готовність. В умовах високої конкуренції та швидкоплинності технологічного розвитку це створює ризик неефективного розподілу ресурсів і втрати інвестицій. Особливо це актуально в країнах із нестабільною економічною ситуацією, де пріоритет часто віддається короткостроковій стабільності, а не довгостроковим інноваціям.

Таким чином, подолання інвестиційних бар'єрів потребує стратегічного підходу, зокрема формування чітких цифрових дорожніх карт, пошуку партнерств із технологічними компаніями, залучення державної підтримки або

грантового фінансування. Страховий ринок має усвідомити, що цифровізація – це не просто витрати, а інвестиція в майбутню конкурентоспроможність, ефективність і стійкість до змін [7].

Попри ці виклики, цифровізація страхового ринку відкриває і значні перспективи. Однією з ключових переваг є підвищення клієнтоорієнтованості за рахунок використання big data, штучного інтелекту та мобільних додатків. Завдяки цифровим технологіям страховики можуть краще розуміти поведінку клієнтів, формувати персоналізовані пропозиції та надавати швидкий і зручний сервіс. Автоматизація процесів дозволяє скоротити витрати, зменшити ризик помилок і пришвидшити обробку заявок та виплат.

Перспективними також є такі напрями, як впровадження блокчейну для забезпечення прозорості угод, розвиток телемедицини в медичному страхуванні, використання телематики в автострахуванні, а також поява повністю цифрових страхових компаній – іншуртехів. Такі інновації здатні не лише змінити підходи до надання страхових послуг, а й сформувати нову культуру страхування в суспільстві.

Перспективи розвитку включають інтеграцію з іншими секторами економіки, розвиток міжнародного співробітництва у сфері цифрових технологій та створення умов для сталого розвитку цифрових інновацій у страхуванні.

Висновки з цього дослідження та перспективи подальших розвідок. Таким чином, цифровізація страхового ринку – це складний, але необхідний процес, що потребує комплексного підходу, модернізації нормативної бази, інвестицій у технології та розвиток цифрових компетенцій у працівників і споживачів. Успішна цифрова трансформація може стати потужним стимулом для зростання галузі, посилення її конкурентоспроможності та підвищення фінансової стійкості всього ринку.

Цифровізація страхового ринку є важливим елементом антикризового публічного управління, сприяючи підвищенню стійкості до гібридних загроз та забезпеченню ефективного функціонування економіки в умовах сучасних викликів. Успішна реалізація цифрових трансформацій потребує комплексного підходу, що включає розробку відповідної нормативно-правової бази, інвестиції в інфраструктуру та розвиток кадрового потенціалу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про правовий режим воєнного стану : Закон України. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text>
2. Страховики України збільшили збір чистих премій. URL: <https://interfax.com.ua/news/economic/948289.html>
3. Світова гібридна війна: Український фронт. Національний інститут стратегічних досліджень. Київ, 2017. 145с. URL: <http://www.niss.gov.ua/articles/2431/>
4. Сприяння розбудові можливостей України гарантувати безпеку суспільства в умовах гібридних загроз. результати експертного опитування. URL: https://geostrategy.org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf

5. Субачов І. І. Розвиток страхового ринку в Україні як фактору фінансової стабільності економіки. *Фінанси України*. 2020. № 11. С. 34.
6. Шелехов К. В. Страхування. Страхові послуги. Київ : ІЕУГП, 2020. 268 с.
7. Парубець О., Подоляк О. Трансформація механізму функціонування та розвитку страхового ринку в умовах цифровізації економіки. *Проблеми і перспективи економіки та управління*. 2024. URL: https://ppeu.stu.cn.ua/article/view/314105?utm_source=chatgpt.com
8. Брюховецька І. О., Кришталь Г. О. Аналіз впливу державної цифрової трансформації на страховий ринок України: нові можливості та ризики. *Наукові праці Міжрегіональної Академії управління персоналом. Економічні науки*. 2023. URL: https://journals.maup.com.ua/index.php/economics/article/view/2875?utm_source=chatgpt.com

Конфлікт інтересів.

Автори заявляють, що конфлікту інтересів щодо публікації цього рукопису немає.

Стаття надійшла до редакції 28.03.2025 р.

Стаття рекомендована до друку 02.04.2025 р.

Sobol R. G.,

PhD in Public Administration, Associate Professor of the Public Policy Department, Educational and Scientific Institute «Institute of Public Administration», V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine

e-mail: sobol_roma@ukr.net <https://orcid.org/0000-0002-3176-3807>

Yefimov Yu. V.,

Doctor of Philosophy, First Deputy Head of the State Environmental Inspectorate in Kharkiv Region, 6 Bakulina str., 6, Kharkiv, 61166, Ukraine

e-mail: advokat977@ukr.net <https://orcid.org/0000-0003-2848-5583>

Bublii M. P.,

PhD of Public Administration, Associate Professor, Associate Professor of Department of Personnel management and entrepreneurship, Educational and Scientific Institute «Institute of Public Administration», V.N. Karazin Kharkiv National University, 4 Svobody Square, Kharkiv, 61022, Ukraine

e-mail: mbubliy@gmail.com <https://orcid.org/0000-0003-1060-6404>

Serenok A. O.,

PhD of Science of Public Administration, Associate Professor, Associate Professor of the Public Policy Department, ESI "Institute of Public Administration" V.N. Karazin Kharkiv National University, 4 Svobody Square, Kharkiv, 61022, Ukraine

e-mail: artem.serenok@karazin.ua <https://orcid.org/0000-0002-5550-0921>

Sobol M. R.,

2nd year student of the Faculty of Economics of Taras Shevchenko National University of Kyiv, 60 Street Volodymyrska, Kyiv, 01033, Ukraine

e-mail: maresobol@gmail.com <https://orcid.org/0009-0001-3584-4380>

DIGITALIZATION OF THE INSURANCE MARKET AS AN APPROACH OF ANTI-CRISIS PUBLIC MANAGEMENT TO COUNTER HYBRID THREATS

Annotation. The article examines the role of digitalization of the insurance market as a tool of anti-crisis public management in the context of hybrid threats. The main directions of digital

transformation of the insurance sector are analyzed, in particular, the implementation of innovative technologies, such as artificial intelligence, blockchain and big data, to increase resilience to cyber threats and information attacks. Particular attention is paid to the role of the state in the formation of the regulatory framework and strategic management of digital transformations in the insurance industry.

Key words: *digitalization, insurance market, anti-crisis management, public management, hybrid threats, cybersecurity, innovative technologies*

REFERENCES

1. Pro pravoviy rezim voennogo stanu. Zakon Ukrainy. URL: <https://zakon.rada.gov.ua/laws/show/389-19#Text> [in Ukraine].
2. Strahoviki Ukrainy zbilshili zbir chistih premiy. URL: <https://interfax.com.ua/news/economic/948289.html> [in Ukraine].
3. Svitova hibrydna viina: Ukrainskyi front (2017). Natsionalnyi instytut stratehichnykh doslidzhen. Kyiv : URL: <http://www.niss.gov.ua/articles/2431/> [in Ukraine].
4. Spriannia rozbudovi mozhlyvosti Ukrainy harantuvaty bezpeku suspilstva v umovakh hibrydnykh zahroz. Rezultaty ekspertnoho opytuvannia. URL: https://geostrategy.org.ua/images/%D0%94%D0%BE%D1%81%D0%BB%D1%96%D0%B4%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F_%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%BE%D1%8E.pdf [in Ukraine].
5. Subachov, I.I. (2020). Rozvytok strakhovoho rynku v Ukraini yak faktor finansovoi stabilnosti ekonomiky. *Finansy Ukrainy, no. 11, 34* [in Ukraine].
6. Shelekhov, K.V. (2020). Strakhuvannia. Strakhovi posluhy. Kyiv: IEUH [in Ukraine].
7. Parubets' O., Podolyak O. (2024). Transformatsiya mekhanizmu funktsio-nuvannya ta rozvytku strakhovoho rynku v umovakh tsyfrovizatsiyi ekonomiky. *Problemy i perspektyvy ekonomiky ta upravlinnya*. URL: https://ppeu.stu.cn.ua/article/view/314105?utm_source=chatgpt.com [in Ukraine].
8. Bryukhovetska I.O., Kryshtal H.O. (2023). Analiz vplyvu derzhavnoyi tsyfrovoyi transformatsiyi na strakhovyy rynek Ukrayiny: novi mozhlyvosti ta ryzyky. Naukovi pratsi Mizhrehional'noyi Akademiyi upravlinnya personalom. *Ekonomichni nauky*. URL: https://journals.maup.com.ua/index.php /economics/article/view/2875?utm_source=chatgpt.com [in Ukraine].

Conflict of interest.

The authors declare that there is no conflict of interest regarding the publication of this manuscript.

The article was received by the editors 28.03.2025.

The article is recommended for printing 02.04.2025.