

<https://doi.org/10.26565/1992-2337-2026-1-04>

УДК 351

Соболь Роман Георгійович,

кандидат наук з державного управління, доцент,
доцент закладу вищої освіти кафедри публічної політики
навчально-наукового інституту «Інститут державного управління»
Харківський Національний університет імені В.Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: sobol_roma@ukr.net <https://orcid.org/0000-0002-3176-3807>

Козлов Костянтин Іванович,

кандидат наук з державного управління, доцент, доцент кафедри публічної політики,
навчально-наукового інституту «Інститут державного управління»
Харківський національний університет імені В. Н. Каразіна,
майдан Свободи, 4, м. Харків, 61022, Україна
e-mail: kostyk_1975@ukr.net <https://orcid.org/0000-0001-5688-6638>

Єфімов Юрій Вікторович,

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

Соболь Марія Романівна,

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

КІБЕРСТРАХУВАННЯ ЯК АНТИКРИЗОВИЙ ПІДХІД ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ПУБЛІЧНОГО УПРАВЛІННЯ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ СУСПІЛЬСТВА ТА ГІБРИДНИХ ЗАГРОЗ

Анотація. У статті розглядається кіберстрахування як інструмент антикризового управління в інформаційній політиці органів публічної влади. В умовах цифрової трансформації суспільства значно зростають ризики кібератак, витоку даних та порушення критичної інформаційної інфраструктури.

Як цитувати: Соболь Р. Г., Козлов К. І., Єфімов Ю. В., Соболь М. Р. Кіберстрахування як антикризовий підхід інформаційної політики публічного управління в умовах цифрової трансформації суспільства та гібридних загроз. *Державне будівництво*. 2026. № 1 (39). С. 48–60. <https://doi.org/10.26565/1992-2337-2026-1-04>

In cites: Sobol, R.G., Kozlov, K.I., Yefimov, Yu.V., Sobol, M.R. (2026). Cyberinsurance as an anti-crisis approach to information policy of public administration in the context of digital transformation of society and hybrid threats. *State Formation*, no. 1(39), 48–60. <https://doi.org/10.26565/1992-2337-2026-1-04> [in Ukrainian].

© Соболь Р. Г., Козлов К. І., Єфімов Ю. В., Соболь М. Р., 2026



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

Проаналізовано роль кіберстрахування у забезпеченні інформаційної безпеки, мінімізації фінансових втрат та формуванні стійкості до кіберзагроз у системі публічного управління. Наведено рекомендації щодо інтеграції кіберстрахування в стратегічне планування цифрової політики держави.

У статті зроблено огляд сучасного стану впливу гібридних загроз на розвиток механізму регулювання страхової діяльності у контексті підвищення національної безпеки в Україні. Чітко ідентифіковано гібридний вплив на економіку країни та визначні заходи протидії. Виділені слабкі місця (небезпеки) і гібридні загрози національній фінансовій безпеці України та суспільства на сучасному етапі.

Ключові слова: *кіберстрахування, публічне управління, цифрова трансформація, інформаційна політика, кібербезпека, ризик-менеджмент.*

Постановка проблеми. На сьогодні 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).

Цифрова трансформація суспільства призвела до значного зростання обсягів даних, що обробляються органами публічної влади, та впровадження цифрових технологій в управлінські процеси. Разом із цим зростає й вразливість до кіберзагроз. В таких умовах постає необхідність у нових інструментах захисту – як технічних, так і організаційно-фінансових. Одним із перспективних підходів є кіберстрахування, яке дозволяє компенсувати збитки від кібератак, знижувати навантаження на державний бюджет та підвищувати довіру до цифрових сервісів.

Аналіз останніх досліджень та публікацій. Питання дослідження розвитку кіберстрахування як антикризового підходу інформаційної політики публічного управління в умовах цифрової трансформації суспільства та гібридних загроз є відносно молоді, однак уже чимало науковців приділили свої роботи теоретичним дослідженням та практичним опрацюванням. До отаких вчених варто віднести: Андрущенко В., Бондарчук В., Возовик О., Кивлюк О., Кришталь Г., Максак Г., Мартинюк В., Парубець О., Подоляк О., Шиманська К. та ін.

Так О. Кивлюк у своїй статті «Теоретико-методологічні засади інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів» аналізує концептуальні підходи до взаємодії людини, суспільства та цифрових технологій, акцентуючи увагу на необхідності інтеграції кіберстрахування в загальну стратегію кібербезпеки [1]. Це дослідження підкреслює важливість розробки правових та етичних норм для ефективного управління кіберризиками в публічному секторі.

У статті «Cyber risk modeling using a two-phase Hawkes process with external excitation» автори пропонують розширену модель оцінки кіберризиків, яка враховує не лише внутрішні фактори, а й зовнішні шоки, такі як публікації про вразливості [2]. Цей підхід дозволяє більш точно прогнозувати ймовірність кіберінцидентів, що є важливим для розробки страхових продуктів у сфері кібербезпеки.

Дослідження «Розвиток цифрової економіки України» аналізує процеси цифровізації економіки на макро- та мікрорівнях, вказуючи на необхідність створення цифрового середовища, яке б задовольняло потреби держави, громадян та бізнесу [3]. Це підкреслює важливість інтеграції кіберстрахування в стратегії цифрової трансформації для забезпечення стійкості до кіберзагроз.

У дисертаційному дослідженні «Удосконалення механізмів антикризового публічного управління в економічній сфері» запропоновано модель оптимізації антикризового управління, яка включає створення централізованих баз даних, розвиток систем бізнес-аналітики та моніторингу, а також використання штучного інтелекту та інших інноваційних інструментів [4]. Ці елементи можуть бути адаптовані для впровадження кіберстрахування в публічний сектор.

Стаття «Кіберзагрози в умовах цифрової економіки» розглядає основні типи кіберзагроз, з якими стикаються державні установи та підприємства в умовах цифровізації [5]. Це дослідження підкреслює необхідність розробки ефективних механізмів кіберстрахування для мінімізації фінансових та репутаційних втрат від кіберінцидентів.

Метою статті є розгляд процесу кіберстрахування як антикризового підходу інформаційної політики публічного управління в умовах цифрової трансформації суспільства та гібридних загроз, а також запровадження ефективних факторів щодо його вдосконалення.

Застосована методологія і методи. Дослідження ролі кіберстрахування як антикризового підходу інформаційної політики публічного управління в умовах цифрової трансформації суспільства та гібридних загроз виконано на основі системного підходу, який дозволив комплексно проаналізувати взаємозв'язок між публічністю, кіберстрахуванням та інформаційною політикою в умовах воєнного стану, євроінтеграційних прагнень і гібридних загроз.

Використано загальнонаукові методи, зокрема аналіз і синтез, для узагальнення наукової літератури та виявлення теоретичних прогалин у вивченні антикризового підходу інформаційної політики публічного управління. Порівняльний метод застосовано для зіставлення міжнародного досвіду кіберстрахування із українськими реаліями, що сприяло формулюванню рекомендацій щодо адаптації ефективних практик.

Ці методи дозволили вирішити пошукові завдання: визначити потенціал інструментів кіберстрахування, виявити виклики його реалізації та розробити рекомендації для вдосконалення, досягнувши головної мети статті – розгляд процесу кіберстрахування як антикризового підходу інформаційної політики публічного управління в умовах цифрової трансформації суспільства та гібридних загроз, а також запровадження ефективних факторів щодо його вдосконалення.

Виклад основного матеріалу. Кіберстрахування – це механізм передання ризиків, пов'язаних із кіберінцидентами, страховим компаніям, який передбачає покриття збитків від зламу систем, витоку персональних даних, порушення роботи цифрових сервісів тощо [6].

У публічному управлінні цей інструмент набуває особливого значення, оскільки:

- забезпечує фінансову компенсацію втрат;
- стимулює впровадження стандартів кібербезпеки;
- створює додатковий мотиваційний механізм для підвищення рівня інформаційного захисту.

Сучасні цифрові системи публічного сектору – реєстри, портали електронного урядування, системи державних закупівель – становлять критичну інфраструктуру [7]. Їх порушення або компрометація можуть спричинити:

- втрату контролю над суспільними процесами;
- розголошення конфіденційної інформації;
- зниження легітимності органів влади.

У цьому контексті кіберстрахування відіграє роль антикризового інструменту, що забезпечує:

- оперативне реагування на кіберінциденти;
- зменшення негативних наслідків для громадян та бізнесу;
- збереження функціонування ключових систем.

Кіберстрахування є важливим елементом антикризової інформаційної політики в умовах цифрової трансформації [8]. Для ефективного впровадження цього інструменту в систему публічного управління доцільно:

1. Розробити нормативно-правову базу для регулювання кіберстрахування в публічному секторі. Розроблення нормативно-правової бази для регулювання кіберстрахування в публічному секторі є важливим елементом формування ефективної інформаційної політики держави в умовах зростаючих кіберзагроз та цифрової трансформації. Цей процес потребує системного підходу, який передбачає поетапне формування законодавчих, підзаконних та методичних документів із врахуванням міжнародного досвіду та національних особливостей. Насамперед, необхідно законодавчо визначити понятіно-категоріальний апарат, зокрема закріпити такі базові терміни, як «кіберстрахування», «кіберризик», «страховий випадок у сфері кібербезпеки», «об'єкт кіберстрахування» тощо. Чіткість термінології є фундаментом для побудови ефективної нормативної системи та унеможливлення правової колізії при реалізації страхових механізмів.

Наступним напрямом є встановлення правового статусу кіберстрахування у публічному секторі – зокрема, визначення умов, за яких укладання договорів кіберстрахування є обов'язковим для органів державної влади, органів місцевого самоврядування та державних підприємств, що працюють з критичною інформаційною інфраструктурою або обробляють великі обсяги персональних даних. У законодавстві також доцільно передбачити можливість добровільного страхування іншими суб'єктами публічного сектору із наданням відповідних рекомендацій та стандартів.

Важливо також розробити єдині стандарти та методики ідентифікації, оцінки та класифікації кіберризиків, які можуть бути об'єктом страхування. Це передбачає створення нормативів, що визначатимуть допустимі рівні ризику, критерії віднесення інцидентів до страхових випадків, вимоги до захисту інформаційних систем, а також процедури внутрішнього та зовнішнього аудиту кібербезпеки. Така уніфікація є необхідною для ефективної взаємодії між страховими компаніями та державними органами, а також для забезпечення прозорості процесів страхування.

Окрему увагу слід приділити врегулюванню процедур укладання та виконання договорів кіберстрахування, визначенню порядку фіксації кіберінцидентів, доказування страхового випадку, проведення експертизи, а також врегулювання страхових виплат. Необхідно розробити типові форми договорів, рекомендації щодо їх умов, а також положення щодо врегулювання спорів, що виникають у процесі реалізації страхових зобов'язань.

Регулювання діяльності страхових компаній у сфері кіберстрахування також потребує удосконалення. Зокрема, варто запровадити спеціальні ліцензійні вимоги для таких компаній, які передбачатимуть наявність фахівців з кібербезпеки, технічних засобів оцінювання ризиків, захисту даних клієнтів, а також обов'язок звітності перед державними регуляторами. Це дозволить забезпечити якість та надійність страхових послуг у сфері кібербезпеки.

Значущим елементом нормативної бази має стати інтеграція кіберстрахування у загальнонаціональну стратегію кібербезпеки та цифрової трансформації. Це передбачає, зокрема, розробку програм державної підтримки для впровадження страхових механізмів у публічному секторі, створення національного фонду кіберстрахування для компенсації втрат у разі масштабних або системних атак, а також стимулювання державно-приватного партнерства у сфері кіберзахисту.

Крім того, у процесі розроблення нормативно-правової бази необхідно враховувати вимоги законодавства про захист персональних даних, зокрема забезпечити правові гарантії нерозголошення інформації про користувачів під час розслідування кіберінцидентів та реалізації страхових механізмів. Усі дії страховиків, що стосуються обробки персональних даних, мають бути чітко регламентовані.

Завершальним компонентом нормативної бази має стати впровадження ефективних механізмів моніторингу, контролю та звітності. Органи публічного управління повинні регулярно інформувати відповідні державні інституції про наявність страхового покриття, кількість та види страхових випадків, ефективність використання страхових механізмів. Доцільно також створити централізовану базу даних про інциденти, що стали предметом страхового регулювання.

Таким чином, розроблення нормативно-правової бази для регулювання кіберстрахування в публічному секторі є багаторівневим процесом, що вимагає комплексного підходу, тісної міжвідомчої координації, адаптації міжнародного досвіду та постійного моніторингу актуальних кіберзагроз. Формування такої

бази сприятиме зміцненню кіберстійкості публічної адміністрації, зменшенню фінансових втрат від кібератак та підвищенню загальної довіри до цифрового урядування.

2. Створити механізми державного стимулювання участі органів влади у програмах кіберстрахування. Створення механізмів державного стимулювання участі органів влади у програмах кіберстрахування є важливим завданням для підвищення рівня кіберстійкості публічного сектору в умовах постійного зростання кількості та складності кіберзагроз. Участь органів державної влади у системі кіберстрахування дозволяє не лише зменшити фінансові наслідки потенційних кіберінцидентів, а й забезпечити системний підхід до управління кіберризиками. Водночас, з огляду на обмеженість бюджетних ресурсів, відсутність достатнього рівня обізнаності та нормативну невизначеність, публічні інституції часто не готові самостійно впроваджувати кіберстрахові механізми. У зв'язку з цим постає необхідність розроблення інструментів державного стимулювання, які б заохочували органи влади до участі у програмах кіберстрахування.

Одним із ключових напрямів стимулювання є запровадження фінансових інструментів підтримки, зокрема часткове субсидування витрат на укладання договорів кіберстрахування або повне покриття страхових внесків для державних органів, які виконують функції з підвищеним рівнем кіберризиків. Це може здійснюватися за рахунок спеціального бюджету кібербезпеки або створення державного фонду підтримки кіберстрахування, який функціонуватиме у межах реалізації національної стратегії цифрової трансформації. Такий підхід дозволить зняти основний бар'єр – фінансову недосяжність – та стимулюватиме органи влади до практичного впровадження страхових механізмів.

Другим важливим інструментом є регуляторне стимулювання, що передбачає створення умов, за яких участь у програмах кіберстрахування стає елементом виконання загальнообов'язкових вимог до інформаційної безпеки. Наприклад, в умовах оновлення нормативно-правових актів можна передбачити включення страхового захисту до переліку мінімальних критеріїв кібербезпеки для публічних органів, особливо тих, що працюють з критичною інформаційною інфраструктурою або персональними даними. Участь у програмі кіберстрахування також може бути додатковим критерієм під час оцінки діяльності органу влади або при проходженні аудитів безпеки.

Крім того, доцільно застосовувати інституційні стимули, зокрема створення спеціальних рекомендаційних програм, методичних матеріалів, шаблонів договорів страхування, а також проведення інформаційно-роз'яснювальної роботи серед керівників державних установ. Це дозволить підвищити рівень обізнаності про переваги кіберстрахування, пояснити механізми його дії та зменшити організаційний спротив. Важливим є й створення державного органу або підрозділу при існуючих структурах (наприклад, при Національному координаційному центрі кібербезпеки), який би супроводжував публічні органи у питаннях впровадження кіберстрахування, проводив оцінку доцільності укладання договорів та надавав консультативну допомогу.

Ще одним дієвим заходом стимулювання може бути запровадження пілотних проєктів з кіберстрахування для окремих міністерств, служб або територіальних громад. Позитивний досвід таких пілотів, за підтримки держави, може стати прикладом для масштабування практики на всю систему публічного управління. За результатами реалізації таких проєктів доцільно формувати аналітичні звіти з оцінкою ефективності, ризиків та рекомендацій щодо удосконалення страхових механізмів.

Крім того, на рівні урядової політики важливо запровадити систему рейтингів або індексів кіберстійкості органів влади, одним із компонентів яких буде наявність страхового покриття кіберризиків. Такі індекси можуть бути використані для публічного звітування, формування політики кібербезпеки, а також для прийняття рішень щодо розподілу фінансування на розвиток цифрової інфраструктури.

У перспективі, важливим напрямом є створення умов для державно-приватного партнерства у сфері кіберстрахування, де держава виступає не лише як замовник або контролер, а й як партнер для страхових компаній. Наприклад, може бути створена спеціальна державна програма співфінансування страхових продуктів у партнерстві з акредитованими страховиками, які відповідатимуть встановленим вимогам до якості та надійності послуг.

Таким чином, створення ефективної системи стимулювання участі органів влади у програмах кіберстрахування повинно базуватись на поєднанні фінансових, регуляторних, інформаційних та організаційних заходів. Такий підхід дозволить забезпечити поступовий перехід від декларативної інформаційної безпеки до реального механізму управління кіберризиками в системі публічного управління, що є надзвичайно актуальним у контексті цифрової трансформації держави та підвищення рівня національної кіберстійкості.

3. Запровадити систему сертифікації цифрових сервісів з урахуванням страхових критеріїв. Запровадження системи сертифікації цифрових сервісів з урахуванням страхових критеріїв є одним із перспективних напрямів розвитку комплексної політики у сфері кібербезпеки та кіберстрахування в публічному секторі. У сучасних умовах цифрової трансформації державного управління, коли органи влади активно впроваджують електронні сервіси для надання адміністративних, соціальних та інформаційних послуг, питання їх надійності, стійкості до кіберзагроз і відповідності вимогам страхових компаній стає критично важливим [9].

Суть ініціативи полягає у створенні такої нормативно врегульованої системи, яка б дозволяла оцінювати цифрові сервіси не лише з технічної та функціональної точки зору, а й з погляду ризиків, що мають значення для страхового покриття. Така сертифікація має поєднувати стандарти кібербезпеки (зокрема вимоги до захисту персональних даних, резервного копіювання, журналювання дій користувачів, багаторівневої автентифікації) із критеріями оцінки страхових ризиків, що використовуються страховими компаніями під час укладення договорів кіберстрахування.

Запровадження цієї системи дозволить, по-перше, створити прозорий механізм оцінки надійності цифрових сервісів, який буде зрозумілим як для державних замовників, так і для страхових компаній, розробників програмного забезпечення та аудиторів. По-друге, це забезпечить єдину базу для прийняття рішень про надання страхового покриття, оскільки наявність сертифіката відповідності певним рівням кіберстійкості може стати підставою для укладання договору кіберстрахування або зниження страхових тарифів. По-третє, сертифікація стимулюватиме розробників цифрових сервісів до підвищення рівня інформаційної безпеки, оскільки відповідність страховим критеріям ставатиме конкурентною перевагою при участі в державних тендерах чи реалізації цифрових проєктів у публічному секторі.

Реалізація такої системи сертифікації потребує створення нормативно-правової основи, яка визначатиме:

- категорії цифрових сервісів, що підлягають обов'язковій або добровільній сертифікації;
- вимоги до рівнів захисту, які мають бути забезпечені відповідно до типу даних, що обробляються сервісом;
- порядок оцінки ризиків і розрахунку страхових критеріїв;
- процедуру проведення сертифікації, перелік уповноважених органів або акредитованих організацій, що можуть здійснювати таку оцінку;
- терміни дії сертифікатів та процедуру їх поновлення чи відкликання у разі виявлення критичних вразливостей.

Крім того, доцільно передбачити створення державного реєстру сертифікованих цифрових сервісів, доступного для органів влади, страховиків та громадськості. Такий реєстр слугуватиме не лише джерелом інформації про рівень безпеки цифрових сервісів, а й інструментом державного контролю та планування заходів із підвищення кіберстійкості.

Важливо також інтегрувати цю систему з уже наявними в Україні або міжнародними стандартами, такими як ISO/IEC 27001 (управління інформаційною безпекою), ISO/IEC 27005 (управління ризиками інформаційної безпеки), а також рекомендаціями Європейського агентства з кібербезпеки (ENISA) щодо сертифікації ІКТ-продуктів і послуг.

Запровадження сертифікації цифрових сервісів з урахуванням страхових критеріїв забезпечить не лише підвищення якості електронного урядування, а й сприятиме формуванню зрілої системи управління кіберризиками, в якій страхування відіграватиме не формальну, а практичну роль у забезпеченні безперервності державних функцій. Це також зміцнить довіру громадян до державних цифрових сервісів, оскільки їх використання базуватиметься на перевірених, захищених і застрахованих рішеннях. У довгостроковій перспективі така сертифікаційна система стане важливою частиною інфраструктури кібербезпеки держави та дієвим інструментом забезпечення національної цифрової стійкості.

4. Розвивати партнерство між державою, страховими компаніями та ІТ-сектором. Розвиток партнерства між державою, страховими компаніями та ІТ-сектором є ключовим чинником формування ефективної системи кіберстрахування в публічному управлінні. У сучасному цифровому середовищі, де кіберзагрози стають дедалі складнішими й масовішими, жоден сектор – ані державний, ані приватний – не здатен самотійно забезпечити повноцінний захист від кіберінцидентів. Відтак, міжсекторна співпраця є стратегічно важливою для створення стійкої моделі управління кіберризиками, у якій кожна зі сторін виконує свою роль: держава – як регулятор і гарант безпеки суспільства, страхові компанії – як фінансовий інструмент ризик-менеджменту, а ІТ-сектор – як поставачальник технологічних рішень і експертних знань.

Партнерство має розвиватися на основі прозорого діалогу між усіма учасниками процесу та спільного формування політики у сфері кібербезпеки і страхування. З боку держави важливим є створення сприятливого нормативно-правового середовища, яке стимулює страхові компанії до розробки спеціалізованих продуктів у сфері кіберстрахування, а ІТ-компанії – до впровадження рішень, що відповідають високим стандартам безпеки. Зокрема, держава може ініціювати створення міжвідомчих робочих груп за участю представників регуляторних органів, страхового бізнесу та технологічних компаній для спільної розробки критеріїв оцінки кіберризиків, методик аудиту, шаблонів страхових договорів, а також механізмів реагування на кіберінциденти.

Крім того, ефективною формою партнерства може стати запуск пілотних проєктів кіберстрахування, у яких публічні установи виступатимуть як клієнти, страховики – як надавачі послуг, а ІТ-сектор – як технічні аудитори або розробники відповідних захисних систем. Це дозволить протестувати різні моделі страхового покриття, виявити проблеми на ранніх етапах, а також створити базу емпіричних даних для формування страхових тарифів і оцінки ризиків.

Також важливою складовою партнерства є обмін інформацією та аналітикою між сторонами. ІТ-компанії можуть надавати страховикам дані про типові вектори атак, рівень загроз і частоту інцидентів, що дозволить більш точно оцінювати ризики й формувати актуальні страхові продукти. Водночас, страхові компанії можуть інформувати державу та ІТ-сектор про найбільш вразливі сегменти публічної інфраструктури, що потребують додаткового захисту або змін у підходах до управління безпекою.

Держава, у свою чергу, може виступати каталізатором партнерства, створюючи умови для державно-приватного співробітництва: зокрема, через грантові програми, податкові стимули, субсидування премій кіберстрахування або пільгове регулювання для компаній, що надають сертифіковані ІТ-рішення для держсектору [10]. Крім того, державні органи можуть ініціювати розробку Єдиної цифрової платформи взаємодії, яка дозволить обмінюватися інформацією про сертифіковані сервіси, поточні ризики, страхові інциденти та рекомендації з протидії загрозам у режимі реального часу.

Не менш важливо налагодити співпрацю в сфері навчання та підвищення кваліфікації, зокрема через спільні освітні програми, тренінги для державних службовців, страхових андеррайтерів і фахівців з кібербезпеки. Це дозволить формувати спільну експертну базу та підвищувати рівень компетентності у сфері кіберризиків, що є необхідним для якісної реалізації страхових механізмів.

У довгостроковій перспективі партнерство між державою, страховими компаніями та ІТ-сектором має трансформуватись у екосистему кіберстійкості, у якій страхування є не лише способом компенсації втрат, а й дієвим елементом управління ризиками, планування безпеки та підвищення довіри до цифрової інфраструктури. Такий підхід сприятиме створенню ефективного механізму колективної відповідальності за безпеку цифрового середовища, у якому кожен учасник – держава, бізнес і технології – відіграє активну та координовану роль [11].

Інформаційна політика держави має охоплювати не лише питання відкритості, доступності та захисту інформації, а й розробку механізмів фінансової стійкості до інформаційних загроз [12].

Кіберстрахування може бути інтегроване у стратегії інформаційної політики через:

- встановлення обов’язкових вимог щодо наявності страхового покриття для держорганів;
- розробку стандартів оцінки кіберризиків;
- створення національного фонду кіберстрахування;
- стимулювання розвитку страхового ринку у сфері кібербезпеки.

У країнах ЄС, США та Ізраїлі кіберстрахування активно використовується як у приватному, так і в публічному секторах [10]. Наприклад:

У США деякі штати вимагають від постачальників державних цифрових послуг мати кіберстрахування.

У Великій Британії уряд співпрацює з приватними страховиками для оцінки кіберризиків у держсекторі.

Цей досвід може бути адаптований в Україні з урахуванням специфіки національного законодавства та рівня розвитку цифрової інфраструктури.

Висновки з цього дослідження та перспективи подальших розвідок у цьому напрямі. Таким чином, кіберстрахування є важливим елементом антикризової інформаційної політики в умовах цифрової трансформації. Для ефективного впровадження цього інструменту в систему публічного управління доцільно:

- розробити нормативно-правову базу для регулювання кіберстрахування в публічному секторі;
- створити механізми державного стимулювання участі органів влади у програмах кіберстрахування;
- запровадити систему сертифікації цифрових сервісів з урахуванням страхових критеріїв;
- розвивати партнерство між державою, страховими компаніями та ІТ-сектором.

Перспективи подальших розвідок у напрямі кіберстрахування як інструменту антикризового управління в інформаційній політиці органів публічної влади є надзвичайно широкими й актуальними у зв'язку зі стрімким ускладненням кіберзагроз, зростанням цифрової залежності публічного управління та потребою в системному забезпеченні кіберстійкості. Кіберстрахування поступово переходить із категорії факультативних фінансових інструментів у розряд стратегічно важливих компонентів антикризового менеджменту, здатних забезпечити безперервність функціонування публічної влади навіть у випадках масштабних кібератак чи системних збоїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кивлюк О. Теоретико-методологічні засади інформаційної та кібернетичної безпеки в умовах цифровізації суспільних процесів. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2024. № 4. С. 125–131. URL: <https://doi.org/10.32782/IT/2024-4-15>
2. Alexandre Boumezoued, Yousra Cherkaoui, Caroline Hillairet Cyber risk modeling using a two-phase Hawkes process with external excitation. [Submitted on 27 Nov 2023]. URL: <https://arxiv.org/abs/2311.15701>
3. Шиманська К., Бондарчук В. Пріоритетні напрями та механізми розвитку цифрової економіки в Україні. *Економіка, управління та адміністрування*. 2021. № 1(95). С. 19–22. URL: [https://doi.org/10.26642/ema-2021-1\(95\)-17-22](https://doi.org/10.26642/ema-2021-1(95)-17-22)
4. Вozовик О. Удосконалення механізмів антикризового публічного управління в економічній сфері. URL: <http://etnuir.tnu.edu.ua/handle/123456789/170>
5. Кіберзагрози в умовах цифрової економіки. 2024. URL: fnpu.cibs.ubs.edu.ua
6. Андрущенко В. П. Кібербезпека у публічному управлінні: виклики та перспективи. Київ: НАДУ, 2021. URL: <https://ipacs.knu.ua/pages/osn/2/news/2039/files/e8f052a9-3ca2-4574-ad95-ec8638583c7f.pdf>
7. European Union Agency for Cybersecurity (ENISA). Cyber Insurance: Recent Developments. (2023). URL: <https://www.enisa.europa.eu/search?keys=Cyber%20Insurance#contentList>
8. Smith R., Jones A. Public Sector Cyber Risk Management. Oxford University Press. 2020. URL: <https://www.emerald.com/books/edited-volume/12545/Public-Sector-Leadership-in-Assessing-and?redirectedFrom=PDF>
9. Кабінет Міністрів України. Концепція розвитку цифрової економіки та суспільства. 2023. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text>
10. National Cyber Security Centre (UK). 2022. Cyber Insurance Guidance for Public Bodies. URL: <https://www.ncsc.gov.uk/>
11. 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>
12. 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. № 1 (73). С. 31–37. URL: <https://doi.org/10.32689/2523-4536/73-5>

Конфлікт інтересів.

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

Стаття надійшла до редакції 13.02.2026 р.

Стаття рекомендована до друку 20.03.2026 р.

Опубліковано 30.05.2026 р.

Sobol R. G.,

*PhD of Science of Public Administration, Associate Professor,
Associate Professor of the Public Policy Department,
Educational and Scientific Institute «Institute of Public Administration»
of V. N. Karazin Kharkiv National University,
4 Svobody Square, Kharkiv, 61022, Ukraine
e-mail: sobol_roma@ukr.net <https://orcid.org/0000-0002-3176-3807>*

Kozlov K. I.,

*PhD in Public Administration, Associate Professor,
Associate Professor of the Public Policy Department,
Educational and Scientific Institute «Institute of Public Administration»
of V. N. Karazin Kharkiv National University,
4 Svobody Square, Kharkiv, 61022, Ukraine
e-mail: kostyk_1975@ukr.net <https://orcid.org/0000-0001-5688-6638>*

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 <http://orcid.org/0000-0003-2848-5583>*

Sobol M. R.,

*4th year student of the Faculty of Economics
of Taras Shevchenko National University of Kyiv,
60 Volodymyrska str, Kyiv, 01033, Ukraine
e-mail: maresobol@gmail.com <https://orcid.org/0009-0001-3584-4380>*

CYBERINSURANCE AS AN ANTI-CRISIS APPROACH TO INFORMATION POLICY OF PUBLIC ADMINISTRATION IN THE CONTEXT OF DIGITAL TRANSFORMATION OF SOCIETY AND HYBRID THREATS

Annotation. The article considers cyber insurance as a tool for anti-crisis management in the information policy of public authorities. In the context of the digital transformation of society, the risks of cyber attacks, data leakage and disruption of critical information infrastructure are significantly increasing. The role of cyber insurance in ensuring information security, minimizing financial losses and building resilience to cyber threats in the public administration system is analyzed. Recommendations are given for integrating cyber insurance into the strategic planning of the state's digital policy.

The article reviews the current state of the impact of hybrid threats on the development of the mechanism for regulating insurance activities in the context of improving national security in Ukraine. The hybrid impact on the country's economy and significant countermeasures are clearly identified. Weaknesses (dangers) and hybrid threats to the national financial security of Ukraine and society at the present stage are highlighted.

Key words: *cyber insurance, public administration, digital transformation, information policy, cybersecurity, risk management.*

REFERENCES

1. Kyvliuk, O. (2024). Theoretical and methodological foundations of information and cyber security in the context of digitalisation of social processes. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 4, 125–131. <https://doi.org/10.32782/IT/2024-4-15> [in Ukraine].

2. Boumezoued, A., Cherkaoui, Y., Hillairet, C. (2023). Cyber risk modeling using a two-phase Hawkes process with external excitation. [Submitted on 27 Nov 2023]. URL: <https://arxiv.org/abs/2311.15701>
3. Shymanska, K., & Bondarchuk, V. (2021). Priority directions and mechanisms of digital economy development in Ukraine. *Economics, Management and Administration*, (1(95), 17–22. [https://doi.org/10.26642/ema-2021-1\(95\)-17-22](https://doi.org/10.26642/ema-2021-1(95)-17-22) [in Ukraine].
4. Vozovyk, O. Improving Mechanisms for Crisis-Response Public Management in the Economic Sphere. URL: <http://etnuir.tnu.edu.ua/handle/123456789/170> [in Ukraine].
5. Cyber Threats in the Digital Economy. 2024. URL: fnpu.cibs.ubs.edu.ua [in Ukraine].
6. Andrushchenko, V.P. (2021). Cybersecurity in Public Administration: Challenges and Prospects. Kyiv: NADU. URL: <https://ipacs.knu.ua/pages/osn/2/news/2039/files/e8f052a9-3ca2-4574-ad95-ec8638583c7f.pdf> [in Ukraine].
7. European Union Agency for Cybersecurity (ENISA). (2023). Cyber Insurance: Recent Developments. URL: <https://www.enisa.europa.eu/search?keys=Cyber%20Insurance#contentList>
8. Smith, R., & Jones, A. (2020). Public Sector Cyber Risk Management. Oxford University Press. URL: <https://www.emerald.com/books/edited-volume/12545/Public-Sector-Leadership-in-Assessing-and?redirectedFrom=PDF>
9. Cabinet of Ministers of Ukraine. Concept for the Development of the Digital Economy and Society.. (2023). URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text> [in Ukraine].
10. National Cyber Security Centre (UK). (2022). Cyber Insurance Guidance for Public Bodies. URL: <https://www.ncsc.gov.uk/>
11. Parubets O., Podolyak O. (2024). The Transformation of the Insurance Market's Operating and Development Mechanisms in the Context of Economic Digitalization. *Challenges and Prospects for the Economy and Management*. URL: <https://ppeu.stu.cn.ua/article/view/314105> [in Ukraine].
12. Bryukhovetska, I.O., Kryshchal, H.O. (2023). Analysis of the impact of state digital transformation on the insurance market of Ukraine: new opportunities and risks. *Scientific Works of Interregional Academy of Personnel Management. Economic Sciences*, no. 1 (73), 31–37. <https://doi.org/10.32689/2523-4536/73-5> [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 13.02.2026.

The article is recommended for printing 20.03.2026.

Published 30.05.2026.