

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.
Ефективна економіка. 2026. № 5.
ISSN 2307-2105



Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>).

DOI: <http://doi.org/10.32702/2307-2105.2026.5.19>

УДК 368:004.9:351.86

О. І. Копилюк,

*д. е. н, професор, завідувач кафедри фінансів, економічної безпеки,
банківської справи та страхового бізнесу,*

Львівський торговельно-економічний університет

ORCID ID: <https://orcid.org/0000-0002-0977-1309>

С. С. Гаранко,

аспірант,

Львівський торговельно-економічний університет

ORCID ID: <https://orcid.org/0009-0006-3578-4695>

ІНТЕГРАЦІЯ СТРАХОВИХ ТА БЕЗПЕКОВИХ ТЕХНОЛОГІЙ ЯК ПРІОРИТЕТНИЙ НАПРЯМ РЕАЛІЗАЦІЇ КОНЦЕПЦІЇ РОЗВИТКУ СТРАХОВОГО РИНКУ

О. Копулюк,

*Doctor of Economic Sciences, Professor, Head of the Department of Finance,
Economic Security, Banking and Insurance Business,*

Lviv University of Trade and Economics

S. Haranko,

Postgraduate, Lviv University of Trade and Economics

INTEGRATION OF INSURANCE AND SECURITY TECHNOLOGIES AS A PRIORITY DIRECTION FOR IMPLEMENTING THE CONCEPT OF INSURANCE MARKET DEVELOPMENT

У статті відзначено, що InsurTech є стратегічною концепцією у страховому секторі, яка акцентує на цифрових технологіях, які були впроваджені для управління ризиками та обслуговування клієнтів і пов'язана з діяльністю фірм, які використовують цифрові технології, часто стартапів. InsurSec є інноваційним інтегрованим підходом, спрямованим на захист бізнесу, який поєднує проактивні послуги кібербезпеки з традиційним кіберстрахуванням та провідні технології у сфері страхування. Запропоновано основні елементи системи InsurSec, які охоплюють мету, завдання та структуру. Зокрема, в якості цільових орієнтирів визначено: уникнення фінансових втрат, мінімізацію ризиків, максимізацію рівня безпеки. Завданнями системи є наступні: запобігання та виявлення загроз безпеці, проактивне реагування на загрози, моніторинг ризиків на випередження, захист бізнесу від кіберзагроз, полегшення для бізнесу щодо виконання вимог для зниження кіберризиків та отримання необхідного покриття у разі атаки. Структурно у систему входять такі складові: керована профілактика, керована безпека, реагування та відновлення, страхування від ризиків.

The article notes that InsurTech is a strategic concept in the insurance sector that focuses on digital technologies that have been implemented for risk management and customer service and is associated with the activities of firms that use digital technologies, often startups.

Investment in InsurTech has contributed to greater accessibility, use and availability of insurance products, thereby potentially improving insurance inclusion. For InsurTech startups, sustainable growth and investment depend on a corresponding increase in demand for services and the share of the population participating in insurance. InsurTech acts as an institutional innovation, reducing transaction costs, improving contract enforcement and strengthening trust through digital transparency. Technologies such as advanced analytics, artificial intelligence, the Internet of Things, cloud computing and blockchain

allow for significant efficiency gains through automation, while revolutionizing processes such as risk assessment, underwriting and insurance claims management.

The most common Insurtech risks include: privacy, security, fraud, software failures, system, financial, regulatory, and the likelihood of insured events.

InsurSec is an innovative integrated approach aimed at protecting businesses, combining proactive cybersecurity services with traditional cyber insurance and leading technologies in the insurance sector. The main elements of the InsurSec system are proposed, which cover the goal, objectives, and structure. In particular, the following targets are defined as: avoiding financial losses, minimizing risks, maximizing the level of security. The system's objectives are: preventing and detecting security threats, proactively responding to threats, monitoring risks to stay ahead, protecting businesses from cyber threats, and making it easier for businesses to meet the requirements necessary to reduce cyber risks and obtain the necessary coverage in the event of an attack. Structurally, the system includes the following components: managed prevention, managed security, response and recovery, and risk insurance.

Ключові слова: *Insurtech, InsurSec, страхові інновації, страхові й безпекові технології, Insurtech-стартапи, безпека*

Keywords: *Insurtech, InsurSec, insurance innovations, insurance and security technologies, Insurtech startups, security.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В сучасних умовах страховий ринок відіграє важливу роль у функціонуванні економіки, забезпечуючи захист від численних ризиків і загроз через механізми компенсації збитків. Водночас, страхова галузь перебуває під впливом трансформацій, що зумовлено стрімким розвитком цифрових технологій та

зміною очікувань клієнтів. Поява передових технологій, таких як штучний інтелект, аналітика великих даних і блокчейн, прискорила інтеграцію технологій у страхуванні та розвиток Insurtech. Порівняно з традиційним страхуванням, Insurtech пропонує чіткі переваги, включаючи підвищену операційну ефективність, покращений клієнтський досвід та сприяння ширшому охопленню ринку. Однак ризики кібербезпеки, втрата даних або шахрайство можуть негативно вплинути на рівень економічної безпеки страхового ринку.

Цифрова еволюція страхового сектору фундаментально змінила операційні парадигми, створюючи нові виклики та можливості для безпеки. Цифрова трансформація – це не лише інтеграція технологій в усталені практики, але й фундаментальне переосмислення того, як формується споживча вартість для клієнтів, тому вимагає глибоких організаційних змін з акцентом на впровадженні передових технологій, стратегій, заснованих на даних та інноваційного мислення. Окрім того, необхідність надійних систем безпеки зумовлена зміною регуляторного середовища та його впливом на кіберстрахування. Формування сталої екосистеми цифрового страхування повинно ґрунтуватися на збалансуванні розвитку страхових технологій із захистом прав та інтересів користувачів, враховуючи ймовірність настання негативних подій, що сприяло появі новітніх систем, таких як InsurSec. З огляду на це, інтеграція страхових та безпекових технологій має стати основою концепції розвитку страхового ринку на засадах його конкурентоспроможності, інноваційності, сталого розвитку.

Аналіз останніх досліджень і публікацій. Впровадженню сучасних цифрових технологій у страхуванні, застосуванню можливостей штучного інтелекту присвячені наукові публікації закордонних та вітчизняних учених. Зокрема, U. Franke, A. Orlando досліджують механізми сприяння інвестування страховиками у безпеку між взаємозалежними фірмами, які отримують можливість інвестувати частку своїх страхових премій для покращення безпеки одна одної [1]. Sh. Gurjar висвітлює проблематику

кібербезпеки у хмарному страхуванні на основі комплексного аналізу ризиків та рішень [2]. S. Cosma, G. Rimo відзначають посилення впливу InsurTech, штучного інтелекту та блокчейну на страховий сектор [3]. F. Mushonga, S. Mishі висвітлюють вплив страхових технологій на інклюзію страхування з використанням кількісних та якісних підходів [4]. A. Braun, R. Jia розкривають особливості застосування цифрових технологій у страхуванні з використанням InsurTech [5]. I. Sosa, S. Sosa розглядають структурну конфігурацію екосистеми InsurTech з точки зору її ролі у зміні створеної вартості у страхуванні [6]. Р. Щур, І. Плєць, І. Кохан досліджують InsurTech як ключовий драйвер трансформації страхового ринку в умовах цифровізації та глобалізації економік [7]. A. Wei, Y. Abdul Talib, Z. Sharif акцентують на основних ризиках, з якими стикаються користувачі в секторі страхових технологій [8]. С. Holland, А Kavuri розробили теоретичну модель бізнес-інновацій у InsurTech, яка фіксує вплив цифрових технологій на страхові ринки, розглядаючи інновації як багатовимірну концепцію, що охоплює бізнес-процеси, нові страхові продукти та зміни у ланцюжку створення вартості страхування [9]. Водночас, підвищення інтенсивності та динамічності змін у сфері цифровізації, поява новітніх ризиків і загроз зумовлюють потребу окреслення ключових засад та напрямів інтеграції страхових та безпекових технологій на страховому ринку з врахуванням перспектив його розвитку.

Формулювання цілей статті (постановка завдання). Метою статті є обґрунтування ключових засад інтеграції страхових та безпекових технологій на основі дослідження Insurtech й InsurSec й окреслення напрямів їх використання як основи реалізації концепції розвитку страхового ринку.

Виклад основного матеріалу дослідження. Інтеграція безпекових та страхових технологій є необхідною вимогою сучасності. В умовах зростаючих загроз у сфері цифровізації страховики пропонують не лише розподіл ризиків, убезпечуючи клієнтів від потреби накопичувати капітал для нейтралізації наслідків катастрофічних подій, але й використання

проактивного скринінгу для забезпечення належного рівня кібербезпеки. При цьому основними превентивними заходами є такі як: моніторинг прихованих мереж, публічних веб-сайтів клієнтів на наявність застарілого програмного забезпечення, неправильних конфігурацій, поширення інформації про загрози, для яких слід впроваджувати засоби контролю кіберризиків, керовані рішення для виявлення та реагування тощо.

Відзначаючи переваги здійснення превентивних заходів з боку страховиків U. Franke, A. Orlando констатують, що, по-перше, це дає їм доступ до інших видів відповідних технічних даних у (майже) реальному часі, що є значним покращенням порівняно з традиційними формами щорічного збору даних, по-друге, це вагома підстава вважати, що вони покращують безпеку їх клієнтів, надаючи додаткову впевненість під час страхування кіберризиків [1].

Згідно з аналізом хмарної безпеки у страхуванні, проведеним Value Momentum, організації, що впроваджують багаторівневий підхід до безпеки, відзначили 40% покращення можливостей виявлення та реагування на загрози. Перетворення основних процесів страхування на хмарні платформи призвело до значних зрушень у підході страховиків до безпеки, при цьому багатохмарні середовища стали нормою для 65% страхових компаній. Проблеми інтеграції між застарілими системами та сучасною хмарною інфраструктурою стають дедалі складнішими, що вимагає формування комплексної системи безпеки, яка враховує як традиційні, так і новітні загрози. Дослідження Value Momentum показує, що страховики, які впроваджують трирівневий підхід до безпеки, який включає безпеку інфраструктури, додатків та даних, продемонстрували 35% зниження кількості інцидентів безпеки, пов'язаних з інтеграцією застарілих систем [2].

Відзначаючи можливості впливу Insurtech на сталий розвиток науковці S. Cosma та G. Rimo наголошують, що цифрові рішення Insurtech сприяють енергоефективності й скороченню викидів вуглецю у страховій галузі. Insurtech сприяє сталому розвитку на основі розробки спеціальних страхових

продуктів, які покривають ризики, пов'язані з екологічними або соціальними явищами. Крім того, дані технології визнані фактором, здатним сприяти досягненню цілей сталого розвитку Організації Об'єднаних Націй (ООН), процесу фінансової інклюзії та гарантувати більшу соціальну справедливість [3].

Інвестування в InsurTech сприяло більшій доступності, використанню та наявності страхових продуктів, тим самим потенційно покращуючи інклюзію страхування. Для InsurTech-стартапів стале зростання та інвестиції залежать від відповідного збільшення попиту на послуги та частки населення, яка бере участь у страхуванні. Отже, InsurTech діє як інституційна інновація, знижуючи трансакційні витрати, покращуючи забезпечення виконання контрактів та зміцнюючи довіру завдяки цифровій прозорості.

На думку F. Mushonga, S. Mishi зміна механізмів структурування стимулів та інформаційних потоків на основі InsurTech з боку інституцій підвищує рівень інклюзивності та ефективності ринку, особливо в країнах, де виражені інституційні прогалини. Автори вважають, що шлях до глибшої інклюзії страхування в цифрову епоху – це складне завдання, яке вимагає цілісного екосистемного підходу. Впроваджуючи адаптивне регулювання, створюючи подвійну цифрову та людську основу, відстоюючи відповідний дизайн продуктів та стратегічно спрямовуючи капітал, зацікавлені сторони можуть забезпечити, щоб у перспективі InsurTech перетворилися на відчутну, справедливу та сталу інклюзію для усіх [4]. Отже, InsurTech визначається як технологічно орієнтовані стартапи, що впроваджують інноваційні підходи до страхових продуктів, послуг та бізнес-моделей, формуючи новий тип бізнес-екосистеми, в якій ключова роль відводиться співпраці, цифровим платформам та клієнтоорієнтованим пропозиціям.

InsurTech-стартапи з їхніми гнучкими методологіями та клієнтоорієнтованими стратегіями виступають агентами змін, змушуючи традиційних страховиків переосмислювати свої бізнес-моделі, операції та тактику взаємодії з клієнтами [5].

I. Sosa, S. Sosa вважають, що екосистему InsurTech найкраще розуміти як мережу взаємозалежних учасників, яка розвивається, включаючи стартапи, існуючих страховиків, постачальників технологій та регуляторів, які спільно створюють цінність, генеруючи цінні товари та послуги, кожен з яких залежить від інших, щоб забезпечити взаємний успіх та сталий розвиток. Науковці представляють поетапну модель, яка описує еволюційну природу феномену InsurTech та містить п'ять взаємопов'язаних фаз (цифровізація та технології, клієнтоорієнтований підхід, дані та аналітика, бізнес-моделі на основі платформ та екосистемні партнерства) [6].

Схожий підхід простежується у вітчизняних науковців, які до ключових характеристик InsurTech-страхової послуги відносять: цифрові технології, гнучкість і масштабованість, клієнтоорієнтованість, інноваційні моделі, інтеграція екосистеми [7].

Машинне навчання оптимізує обробку претензій, зменшуючи кількість помилок та підвищуючи точність даних, тоді як смарт-контракти на основі блокчейну автоматизують бізнес-процеси, підвищуючи ефективність і прозорість. Крім того, аналітика великих даних дозволяє здійснювати персоналізовану оцінку ризиків та динамічне ціноутворення, підвищуючи якість страхових послуг. Однак, швидке зростання Insurtech, хоча й представляє інноваційні можливості, супроводжується низкою ризиків.

Ризики, пов'язані з Insurtech, впливають з аспектів безпеки даних, алгоритмічної справедливості та технічної прозорості. З точки зору користувачів, це такі ризики, як злом та витік даних, що загрожують безпеці особистої інформації, а також підривають їхню довіру до Insurtech. Більше того, інтеграція технологій у страхування створює нові виклики. Зокрема, малі та середні страхові компанії з обмеженими фінансовими та технологічними ресурсами, ризикують бути витісненими з ринку через труднощі в адаптації до цифрової трансформації. Навіть серед високоцифрованих страхових компаній системні збої або кібератаки загрожують безпеці даних користувачів та впливають на стан бізнес-

операцій. Це посилює тиск на страхові компанії, щоб ті підтримували репутацію свого бренду та залучали нових користувачів.

Виникнення негативних подій, пов'язаних з технологіями, може призвести до суворіших регуляторних вимог та вищих витрат на дотримання вимог для страхової галузі, що потенційно перешкоджатиме широкому впровадженню Insurtech [8].

До найбільш поширених ризиків Insurtech доцільно віднести наступні: конфіденційності, безпеки, шахрайства, збоїв у програмному забезпеченні, системні, фінансові, регуляторні, ймовірність настання страхових випадків.

Перспективна спрямованість Insurtech зумовлена тим, що по-перше, трансформація ланцюга створення вартості страхування надає можливості для покращення взаємодії з клієнтами та оптимізації операцій. Такі технології, як передова аналітика, штучний інтелект, Інтернет речей, хмарні обчислення та блокчейн, дозволяють значно підвищити ефективність завдяки автоматизації, водночас революціонізуючи такі процеси, як оцінка ризиків, андеррайтинг та управління страховими відшкодуваннями. Їх застосування підвищує рівень страхового захисту від багатьох ризиків, дозволяючи при цьому підвищити інклюзивність страхування. По-друге, цифрова перебудова основних систем створює базу для нових бізнес-моделей. До них належать суб'єкти ринку, які працюють за допомогою економних, технологічно орієнтованих стратегій, організатори екосистем, які інтегрують взаємопов'язані послуги для надання комплексних рішень та партнери, орієнтовані на профілактику, які прагнуть проактивно зменшувати ризики. Вплив InsurTech-стартапів багатогранний – від оснащення традиційних страховиків передовими інструментами до новаторських інноваційних бізнес-моделей, які переосмислюють взаємодію з клієнтами щодо надання послуг.

C. Holland, A. Kavuri розглядають структуру бізнес-інновацій у страхових технологіях в у розрізі 3 складових: 1) проєктування, виконання та управління бізнес-процесами у страхуванні, 2) розробка та впровадження

нових страхових послуг на основі продуктових інновацій, 3) інновації в конфігурації ланцюга створення вартості, пов'язані з концепцією клієнтоорієнтованості та маркетинговою стратегією каналів [9].

Отже, InsurTech є стратегічною концепцією у страховому секторі, яка акцентує на цифрових технологіях, які були впроваджені для управління ризиками та обслуговування клієнтів й пов'язана з діяльністю фірм, що використовують цифрові технології. Бізнес-моделі InsurTech можна розділити на різні типи, які варіюються від платформ спрощення доступу до страхових продуктів, цифрових брокерів як посередників, що оптимізують процеси закупівель до вбудованих страхових рішень, які інтегрують покриття безпосередньо в основний продукт або послугу, моделі peer-to-peer (P2P), пропозиції страхування на вимогу та повністю. Вони мають інноваційну та перспективну спрямованість.

Інноваційну спрямованість до консолідації страхових та безпекових технологій має InsurSec, який розглядається як інтегрований, комплексний підхід до захисту бізнесу від кіберзагроз, що об'єднує страхування та безпеку. Він базується на новітніх технологіях запобігання й виявлення, досвіді кіберфахівців та підтримці страхової компанії для захисту бізнесу. Це синергія, яка в межах їх страхової політики забезпечує безпеку, ідентифікацію загроз та досвід експертів у подоланні розриву в можливостях бізнесу. [10].

Дана технологія вперше була розроблена у 2023р. компанією At-By – страховим постачальником в сфері цифровізації з метою допомоги малому та середньому бізнесу у подоланні нестачі технологій безпеки та набуття навичок страхування кіберризиків. Ця технологічна проблема вирішується шляхом надання через єдиний страховий поліс послуг безпеки та управління ризиками.

Ефективні рішення InsurSec інтегрують такі заходи як:

– профілактика – виявлення недоліків у безпеці та можливостях зменшення ризиків, визначення пріоритетних проблем на основі реальних

знань про фактичні загрози та підтримка в усуненні наслідків із залученням експертів;

- виявлення – реалізація можливостей моніторингу, ідентифікації та реагування на загрози; адаптація до профілю ризиків компанії та технічного середовища;

- реагування та відновлення – доступ до експертів з реагування та відновлення, які допоможуть страхувальникам відновити роботу у разі настання страхового випадку;

- механізм аналізу ризиків – можливості запобігання, виявлення, реагування та відновлення повинні бути підкріплені системою аналізу даних із замкнутим циклом, яка вивчає рівень витрат за різними факторами безпеки, шахрайства, фінансових та ризикових факторів. Оптимізоване рішення з точки зору часу та кращих практик із зменшення ризиків для бізнесу повинно агрегувати дані за заявами та ризиками, щоб швидко виявляти нові загрози;

- єдиний постачальник – рішення має надаватися страховою компанією, яка може забезпечити критично важливий захист від фінансових та репутаційних втрат, з якими сьогодні стикаються малі й середні підприємства [11].

Прикладна значимість поєднання страхових та безпекових технологій відзначена у матеріалах World Economic Forum Annual Meeting, де акцентовано на новому виді компаній InsurSec (страхування + безпека), для яких сильна безпека є стандартом, а для споживачів – відсутні загрози, пов'язані з недоліками використання програмного забезпечення [12].

Приймаючи на себе ризики, страховики мають зобов'язання допомогти іншим компаніям покращити свою безпеку та уникнути кіберризиків. В окремих випадках страхова компанія може надавати програмне забезпечення з безпеки, сприяючи зменшенню втрат для клієнтів. Основні елементи системи InsurSec представлені на рис. 1.

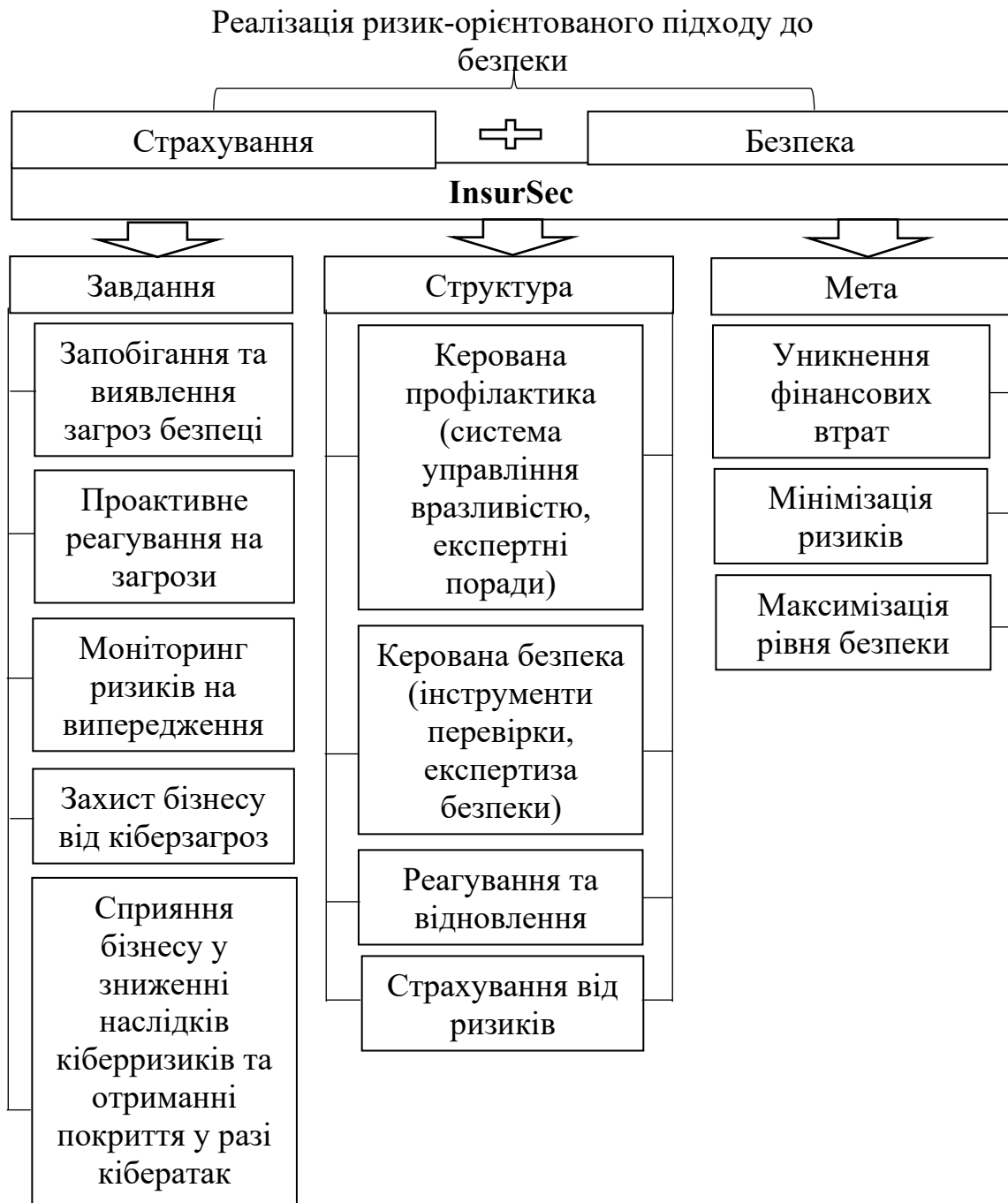


Рис. 1. Основні елементи системи InsurSec

Джерело: авторська розробка

Отже, InsurSec є перспективним інноваційним інтегрованим підходом спрямованим на захист бізнесу, який поєднує проактивні послуги кібербезпеки з традиційним кіберстрахуванням із задіянням провідних технологій та передового досвіду у сфері страхування. Він ґрунтується на застосуванні інструментів превентивного реагування на загрози та

зменшення ризиків для запобігання кібератакам, а не лише виключно на покритті збитків.

Інтеграція страхових та безпекових технологій, як засвідчує успішний досвід впровадження InsurTech та InsurSec є важливим стратегічним напрямом у реалізації концепції розвитку страхового ринку й впровадженні новітніх клієнтоорієнтованих страхових та безпекових продуктів і послуг.

Висновки та перспективи подальших розвідок у даному напрямі.

Формування сталої екосистеми цифрового страхування на основі збалансування розвитку страхових та безпекових технологій є важливою умовою зміцнення безпеки страхового ринку. InsurTech є стратегічною концепцією трансформації у страховому секторі, яка акцентує на цифрових технологіях управління ризиками та обслуговування клієнтів й формує новий тип бізнес-екосистеми, в якій ключова роль відводиться співпраці, цифровим платформам та клієнтоорієнтованим пропозиціям.

InsurSec є інноваційним інтегрованим підходом, спрямованим на захист бізнесу, який поєднує проактивні послуги кібербезпеки з традиційним кіберстрахуванням та провідні технології у сфері страхування. Такий підхід ґрунтується на застосуванні інструментів превентивного реагування на загрози та зменшення ризиків для запобігання атакам, а не лише виключно на покритті збитків.

Основні елементи системи InsurSec охоплюють мету, завдання та структуру. Структурно у систему входять такі складові: керована профілактика, керована безпека, реагування та відновлення, страхування від ризиків. В якості цільових орієнтирів визначено: уникнення фінансових втрат, мінімізацію ризиків, максимізацію рівня безпеки. До завдань системи віднесено: запобігання та виявлення загроз безпеці, проактивне реагування на загрози, моніторинг ризиків на випередження, сприяння бізнесу у зниженні наслідків кіберризиків та отриманні покриття у разі кібератак.

Подальші наукові дослідження в даному напрямі повинні стосуватися розробки інструментарію кількісного і якісного оцінювання ризиків й впливу

цифровізації на страховий сектор. Це дозволить сформувати й оцінити реальні та потенційні ризики і загрози, розробити напрями їх мінімізації, окреслити переваги і недоліки впровадження інноваційних технологій у страхування.

Література

1. Franke U., & Orlando A. Interdependent cyber risk and the role of insurers. *Research in Economics*. 2025. Vol. 79. No 3. DOI: <https://doi.org/10.1016/j.rie.2025.101059>.
2. Gurjar Sh. Cybersecurity in cloud-based insurance: A comprehensive analysis of risks and solutions. *World Journal of Advanced Research and Reviews*. 2025. Vol. 26. No 1. Pp. 2610-2619. DOI: <https://doi.org/10.30574/wjarr.2025.26.1.1320>.
3. Cosma S., & Rimo G. Redefining insurance through technology: Achievements and perspectives in Insurtech. *Research in International Business and Finance*. 2024. Vol. 70. DOI: <https://doi.org/10.1016/j.ribaf.2024.102301>.
4. Mushonga F. B., & Mishi S. The Impact of Insurtech on Insurance Inclusion: A Systematic Literature Review. *Risk and Financial Management*. 2026. Vol. 19. No 2. DOI: <https://doi.org/10.3390/jrfm19020122>.
5. Braun A., & Jia R. InsurTech: Digital technologies in insurance. *The Geneva Papers on Risk and Insurance - Issues and Practice*. 2025. Vol. 50(1). Pp. 1-7. DOI: <https://doi.org/10.1057/s41288-024-00344-x>.
6. Sosa I. & Sosa S. Building an InsurTech Ecosystem Within the Insurance Industry. *Risks*. 2025. Vol. 13(6). DOI: <https://doi.org/10.3390/risks13060108>.
7. Щур Р. І., Плєць І. І., Кохан І. В. Розвиток Insurtech як драйверу інновацій у страховому секторі. *Ефективна економіка*. 2025. № 10. DOI: <http://doi.org/10.32702/2307-2105.2025.10.18>.
8. Wei A., Abdul Talib Y. Y., & Sharif Z. Uncovering Risks in Insurtech From the Perspective of User-Perceived Risks: A Bibliometric Analysis and Future Research Agenda. *Sage Open*. 2026. Vol. 16(1). DOI: <https://doi.org/10.1177/21582440251414754>.
9. Holland C. P., & Kavuri A. S. Insurtech strategies: a comparison of incumbent insurance firms with new entrants. *The Geneva Papers on Risk and Insurance - Issues and Practice*. 2025. Vol. 50(1). Pp. 78-105. DOI:

<https://doi.org/10.1057/s41288-024-00341-0>.

10. Why Cybersecurity for SMBs is Broken and Only InsurSec Can Fix It. At-Bay. 2023. April 20. URL: <https://www.at-bay.com/articles/what-is-insursec> (Дата звернення: 15.04.2026).

11. At-Bay Introduces World's First InsurSec Solution to Address Growing Cybercrime Rates among U.S. Small Businesses. At-Bay. 2023. April 20. URL: <https://www.businesswire.com/news/home/20230420005373/en/At-Bay-Introduces-Worlds-First-InsurSec-Solution-to-Address-Growing-Cybercrime-Rates-among-U.S.-Small-Businesses> (Дата звернення: 15.04.2026).

12. Insurance may be the hero the cybersecurity industry needs. World Economic Forum Annual Meeting. 2024. Jan 8. URL: <https://www.weforum.org/stories/2024/01/insurance-hero-cybersecurity-industry-security> (Дата звернення: 16.04.2026).

References

1. Franke, U., and Orlando, A. (2025), “Interdependent cyber risk and the role of insurers”, *Research in Economics*, vol. 79, no 3. DOI: <https://doi.org/10.1016/j.rie.2025.101059>.

2. Gurjar, Sh. (2025), “Cybersecurity in cloud-based insurance: A comprehensive analysis of risks and solutions”, *World Journal of Advanced Research and Reviews*, vol. 26, no 1, pp. 2610-2619. DOI: <https://doi.org/10.30574/wjarr.2025.26.1.1320>.

3. Cosma, S., and Rimo, G. (2024), “Redefining insurance through technology: Achievements and perspectives in Insurtech”, *Research in International Business and Finance*, vol. 70. DOI: <https://doi.org/10.1016/j.ribaf.2024.102301>.

4. Mushonga, F. B., and Mishi, S. (2026), “The Impact of Insurtech on Insurance Inclusion: A Systematic Literature Review”, *Risk and Financial Management*, vol. 19, no 2. DOI: <https://doi.org/10.3390/jrfm19020122>.

5. Braun, A., and Jia, R. (2025), “InsurTech: Digital technologies in insurance”, *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 50(1), pp. 1-7. DOI: <https://doi.org/10.1057/s41288-024-00344-x>.

6. Sosa, I. and Sosa, S. (2025), “Building an InsurTech Ecosystem Within the Insurance Industry”, *Risks*, vol. 13(6). DOI: <https://doi.org/10.3390/risks13060108>.

7. Shchur, R. I., Plets', I. I., and Kokhan, I. V. (2025), "Development of Insurtech as a driver of innovations in the insurance sector", *Efektivna ekonomika*, vol. 10. DOI: <http://doi.org/10.32702/2307-2105.2025.10.18>.

8. Wei, A., Abdul Talib, Y. Y., and Sharif, Z. (2026), "Uncovering Risks in Insurtech From the Perspective of User-Perceived Risks: A Bibliometric Analysis and Future Research Agenda", *Sage Open*, vol. 16(1). DOI: <https://doi.org/10.1177/21582440251414754>.

9. Holland, C. P., and Kavuri, A. S. (2025), "Insurtech strategies: a comparison of incumbent insurance firms with new entrants", *The Geneva Papers on Risk and Insurance - Issues and Practice*, vol. 50(1), pp. 78-105. DOI: <https://doi.org/10.1057/s41288-024-00341-0>.

10. At-Bay (2023), "Why Cybersecurity for SMBs is Broken and Only InsurSec Can Fix It", available at: <https://www.at-bay.com/articles/what-is-insursec> (Accessed 15 April 2026).

11. At-Bay (2023), "At-Bay Introduces World's First InsurSec Solution to Address Growing Cybercrime Rates among U.S. Small Businesses", available at: <https://www.businesswire.com/news/home/20230420005373/en/At-Bay-Introduces-Worlds-First-InsurSec-Solution-to-Address-Growing-Cybercrime-Rates-among-U.S.-Small-Businesses> (Accessed 15 April 2026).

12. World Economic Forum Annual Meeting (2024), "Insurance may be the hero the cybersecurity industry needs", available at: <https://www.weforum.org/stories/2024/01/insurance-hero-cybersecurity-industry-security> (Accessed 16 April 2026).

Отримано редакцією журналу / Received: 29.04.26

Прорецензовано / Revised: 06.05.26

Дата публікації / Published: 26.05.26