DOI: https://doi.org/10.30970/fp.4(58).2025.718182

УДК 368.029:004.056.5

КІБЕРРИЗИКИ ТА СТРАХУВАННЯ ІТ-ВІДПОВІДАЛЬНОСТІ: МІЖНАРОДНИЙ ТА УКРАЇНСЬКИЙ ДОСВІД

ЗАДОРОЖНА Анна Володимирівна
кандидатка фізико-математичних наук, доцентка,
доцентка кафедри цифрової економіки та бізнес-аналітики
Львівського національного університету імені Івана Франка
ORCID ID: https://orcid.org/0000-0002-9258-1679

Анотація. *У статті досліджуються питання кіберризиків та страхової відповідальності в сфері ІТ. Указано основні невизначеності, які можуть ускладнювати процес розробки програмного забезпечення. Розглянуто типові види полісів, які використовуються для страхування ІТ-сфери в Україні, охарактеризовано основних гравців на ІТ-ринку та послуги, які вони пропонують. Дано якісну оцінку ринку страхування ІТ-сфери в Україні, а також розглянуто стан ринку страхування ІТ-відповідальності та кіберризиків в США та ЄС. Зроблено висновок, що ринок страхування ІТ-відповідальності в Україні має фрагментарний характер та перебуває у початковому стані.*

Ключові слова: *страхування, страхування ІТ-відповідальності, кібербезпека, кібератака, захист інформації, виток даних, кіберстрахування, актуарні розрахунки, поліс, інформаційні технології, проєкт, інновації, програмний продукт, програмне забезпечення, бізнес.*

Постановка проблеми. Сучасна економіка все більше починає залежати від інформаційних технологій, цифрових платформ та онлайн-сервісів. Розробка нових програмних продуктів (ПП) стає одним із значущих напрямків економіки, а ці продукти починають сприйматися як один із різновидів товарів. Великий спектр ризиків, якими супроводжується процес розробки програмного забезпечення (ПЗ), та його впровадження в організаціях обумовлюють потребу в захисті як інтересів замовників, так й ІТ-розробників. Разом із тим із кожним роком зростає кількість кібератак та спроб порушення конфіденційності інформації, що висуває більш жорсткі вимоги до якості та захищеності розроблюваних ПП.

У сучасному світі існує тенденція до мінімізації фінансових та репутаційних ризиків шляхом укладання страхових договорів. Особливо актуальним це є для сфери ІТ, де процес створення та впровадження ПП може призводити до катастрофічних наслідків для організацій. Це, а також специфіка ІТ-галузі – особливі види ризиків, недостатня статистика щодо втрат у сфері ІТ, особливо в Україні, недостатні розробки страхових послуг та страхових нормативів – обумовлюють інтерес до проблеми страхування в сфері ІТ.

Аналіз останніх досліджень та публікацій. Питанню вивчення різних видів страхової відповідальності присвячено низку праць, наприклад [1; 2]. Проте поява новітніх технологій та їх впровадження у різні сфери людської діяльності обумовила потребу враховувати також нові види ризиків і здійснювати їх страхування. Вивчаючи

проблему страхування в контексті появи інноваційних технологій (таких, наприклад, як штучний інтелект), автор праці [3] дійшов висновку, що, попри всю складність в оцінці страхових премій та встановленні умов поліса відповідальності, роль страхування в сфері інновацій буде зростати та сприяти подальшому розвитку науково-технічного прогресу. Питанням відповідальності за розробку якісного ПЗ займався, зокрема, Д. В. Вудс [4], який дослідив, як змінювалися норми права зі зміною розуміння ПП від позиції послуги до позиції товару. Він проаналізував можливі ризики для розробників і постачальників ІТ-послуг та з'ясував, які втрати можуть бути заподіяні наданням неякісного ПП, оцінив страхові послуги для ІТ-сфери та зробив висновок, що традиційні страхові поліси не здатні повністю покрити всі можливі ситуації. Тому, на думку Д. В. Вудса, потреба в складанні спеціальних страхових полісів для ІТ-сфери буде постійно зростати, а страхування буде посередником у будь-якому майбутньому режимі відповідальності за ПЗ [4]. Крім того, він висунув пропозицію, яка надасть страховикам можливість стягувати з постачальників компенсацію збитків за виробництво ними небезпечного ПЗ. Ця система, за його словами, забезпечить компенсацію постраждалим за допомогою страхування, водночас дозволяючи режиму відповідальності за ПЗ перешкоджати розробці небезпечного забезпечення. При цьому важливішим стане стримувати розробку неякісного ПЗ, ніж обмежуватися виключно компенсацією постраждалій стороні [4].

Дослідженню важливості страхування відповідальності, що пов'язане з використанням ШІ в медичній галузі, присвячена праця [5]. У ній автори зазначають, що страхування відповідальності сприяє використанню високоякісного ШІ, оскільки ринок страхування зацікавлений у безпечних та ефективних продуктах, і, відповідно, підтримує розвиток інновацій, а також, що страхування покращує результати лікування та зменшує його вартість.

Інше важливе питання, яке порушується при розгляді проблеми якості ПП – питання захисту ПП від несанкціонованого доступу та кібератак. Про це згадує Д. В. Вудс, це ж питання розгянуто в праці [6]. У ній автори наголосили, що кіберстрахування слід розглядати як стратегію управління ризиками, які можуть виникати при роботі з інформаційними системами, та дослідили практику страхування кібербезпеки.

Проте, на нашу думку, питанням оцінки та подальшого страхування ризиків у сфері розробки та впровадження ПП та послуг, дослідження ринку страхових компаній, що надають такі послуги у світі, і, зокрема в Україні, не було приділено належної уваги.

Мета статті. Полягає в дослідженні особливостей нового виду страхування відповідальності в сфері ІТ, виявленні та урахуванні ризиків, які можуть виникати цій в сфері, вивченні стану ринку страхування ІТ-відповідальності в Україні та світі. Реалізація цієї мети здійснюватиметься із використанням методів аналізу і синтезу, а також компаративного аналізу.

Виклад основних результатів. Процес розробки програмного забезпечення та його подальше впровадження в організаціях замовників хоча багато в чому є систематизованим та сформованим, проте часто містить ряд невизначеностей, які можуть бути обумовлені:

–недостатньо якісними плануванням процесу та контролем за його дотриманням. Це може призводити до зриву термінів виконання робіт та проєкту в цілому, перевищення бюджету проєкту, неякісного виконання або неврахування складності деяких видів робіт;

–недостатньо чітким формулюванням вимог замовника, що може спричинити

створення продукту із дещо іншими характеристиками або викликати складності на етапах його розробки, збільшувати терміни виконання та бюджет проєкту;

−змінами в обсягах проєкту та збільшенні його складності;

−нестачею того чи іншого виду ресурсів;

−недостатньо гнучким реагуванням на зміни при розробці ПЗ;

−невдалим вибором методу управління розробкою ПЗ;

−технічними проблемами, які можуть бути пов'язані з пошуком та виправленням багів, захистом продукту від кібератак, витоком даних, ін.;

−низкою зовнішніх факторів, які впливають на ринок ІТ-послуг (конкуренція, економічні зміни, юридичні обмеження тощо) та ін. [7].

Окрім указаних ризиків, якими може супроводжуватися процес розробки ПП та надання ІТ-послуг, існують ризики, що пов'язані зі злочинним або недбалим виконанням робіт, а також ризики витоку конфіденційної інформації внаслідок доступу до неї розробників та постачальників ПП та послуг [8].

Такий широкий спектр ризиків, яким супроводжується створення ПП або надання послуг, інноваційність ПП, обумовили розвиток страхування даної сфери. Слід зауважити, що особливість ІТ-сфери часто потребує оформлення комбінованих полісів, які включають не тільки професійну відповідальність (Professional Indemnity) за неробочий або неякісний продукт, неякісне надання послуг, але й відповідальність перед громадськістю та продукцією (General Liability) [9]. Це дозволяє уникати багатьох неврахованих ризиків.

Загалом на ринку страхування пропонують такі типові ІТ-поліси:

– Professional Indemnity / Errors & Omissions (E&O) – по суті є полісом професійної відповідальності, який дозволяє покривати фінансові втрати клієнта через недосконалу роботу розробників ІТ-продуктів та постачальників послуг, наприклад, професійної помилки розробника, збою ПЗ, недотримання договору SLA (угоди про рівень послуг);

– Product / Service Liability – поліс, який більше орієнтується на дефекти, низьку якість продукту або послуги. Він передбачає фінансову та юридичну відповідальність за збитки, які завдали постачальники ПП або послуги. Поліс спонукає підприємців більше орієнтуватися на створення (або надання) більш безпечного ПП (послуги);

– Cyber (cyber insurance) – поліс, який ураховує збитки, що можуть бути заподіяні такими інцидентами, як технічні збої, помилки програмування та відмови роботи ІТ-систем, нецільові та таргетовані, а також внутрішні атаки [10];

– Third-party / General Liability – поліс, який призначений для покриття збитків застрахованої сторони в результаті її юридичної відповідальності перед третьою стороною. Поліс покриває лише шкоду чи збитки, завдані іншим особам через дії чи недбалість застрахованої особи;

– Legal defence costs, costs to remediate – передбачають витрати на юридичний захист, витрати на відшкодування і можуть бути окремими секціями.

Із огляду на особливості розробки та впровадження конкретного ПП, виокремлюють [11] страхові поліси за багатьма контрактами на рік або за одним конкретним проєктом, як, наприклад, пропонує Colonnade та BIS Ukraine [11, 12], за типом покриття – ліміт на тип відповідальності (професійна або загальна). Не практикується покриття моральних збитків або недоотриманих прибутків. Такі компанії, як Colonnade, надають покриття кіберризиків та репутаційних ризиків виключно для ІТ-компаній (а не для фрилансерів) та додають їх у пакет страхування ІТ-бізнесу. Також передбачено страхування відповідальності великих компаній або

стартапів, проте для страхування роботи останніх страхові компанії убезпечують себе інформацією про досвід роботи цих команд чи їх керівництва [12]. Умови страхування ІТ-відповідальності в Україні наведені в табл. 1. Як бачимо, деякі страхові компанії розглядають можливість покриття для таких перспективних компаній в США та Канаді; також українські страхові компанії не обмежуються індивідуальними полісами, а можуть пропонувати пакетні пропозиції. Укладання страхових полісів ІТ-відповідальності дозволяє українським компаніям підвищувати рівень довіри до їх роботи з боку клієнтів, а також наявність полісів звичайно є обов'язковою вимогою співпраці із закордонними партнерами [13].

Розглядаючи питання страхування ІТ-відповідальності, слід зауважити, що цей сегмент страхового ринку в Україні має фрагментарний характер, через що він не є виділений в окремий сектор страхового ринку і дані по ньому в Україні не є агрегованими. Крім того, статистичні дані по цьому напрямку страхування часто є комерційною таємницею. Тому видається доцільним розглянути стан страхового ринку загалом по Україні без конкретизації предмета страхування. Так, протягом 2023 р. – перше півріччя 2025 р. страховий ринок України демонстрував зростання загальних обсягів страхових премій [18]. Загальний обсяг премій за ризиковим страхуванням у 2023 р. становив 41,8 млрд грн, що на 20 % більше, ніж значення цього показника в 2022 р. та всього на 5 % менше довоєнного в 2021 р., що свідчить про відновлення динаміки ризикового страхування в 2023 р.

У 2024 р. загальний обсяг премій за ризиковим страхуванням в Україні становив 47,3 млрд грн., що на 13,2 % більше порівняно з 2023 р.

Таблиця 1

Українські компанії та брокери, що надають продукти й послуги страхування ІТ-відповідальності

Компанія/ брокер	Тип продукту	Спосіб придбання	Тариф/ціна	Переваги	Недоліки
Colonnade Ukraine	IT professional indemnity	Онлайн (ФОП) та брокер	$10k проєкт / ліміт $500k	Онлайн-калькулятор, підходить для фрилансерів. Можливість покриття на США та Канаду	Потреба в брокері для складних корпоративних випадків
СК «Еталон»	Професійна відповідальність	брокер / офіс	На вимогу	Продукт для юр.осіб, індивідуальні умови	Ціни – за запитом
BIS Ukraine	Liability (у т.ч. IT)	Через сайт/агента	На вимогу	Пакетні рішення	Індивідуальний підхід
INGO	Professional liability	На вимогу (онлайн форма)	На вимогу	Велика компанія, корпоративні продукти	Індивідуальний розрахунок
Allianz Ukraine	Liability / PI	Через брокера	На вимогу	Стабільність, міжнародний рейтинг	Вимагає перемовин, індивідуалізація
Брокери (Finevolution, Brit-Mark)	Пакетні рішення / підбір страховика	Консультація, підбір	Консультації платні/безкоштовні	Можливість отримати кращі умови і вести перемовини	Брокерська комісія / підготовка документів

Джерело: складено за [11–17]

За перше півріччя 2025 р. значення цього показника перевищило 30 млрд грн, що на 42 % більше порівнянно з аналогічним періодом 2024 р. [18]. Ураховуючи, що ІТ-сфера в Україні продовжує розвиватися та що ІТ-компанії активно співпрацюють з передовими країнами-постачальниками ПП, можна очікувати зростання страхування в

ІТ-сфері разом із розвитком страхового ринку України.

Загальний стан та тенденції розвитку ринку страхування ІТ-відповідальності можна прослідкувати на прикладах уже давно функціонуючих страхових ринків США та ЄС. Слід зазначити, що в США кіберстрахування (cyber insurance) та страхування ІТ-відповідальності (IT liability insurance) не відокремлюють одне від одного та статистичні дані по них подають у межах одного спільного сегмента ринку – Cyber Liability Insurance. Тому надалі будемо розглядати кіберстрахування як таке, що включає також дані зі страхування ІТ-відповідальності. Так, ринок кіберстрахування США у 2023 р. збільшився в 4,3 рази порівняно з 2016 р. (табл. 2), на що вплинули:

– тенденція поступового зростання у 2016–2019 рр. прямих премій із окремих полісів;

– тенденція різкого зростання (іноді у 2 рази) прямих премій із окремих полісів протягом 2020–2023 рр.;

– тенденція поступового зростання у 2016–2023 рр. прямих премій із пакетних (комбінованих) полісів [19–23].

Як видно з табл. 2, основний внесок до сумарних прямих нарахованих премій на ринку кіберстрахування США дають премії з окремих полісів, причому останніми роками частка їх зросла. Слід зазначити, що ринок кіберстрахування Північної Америки (США та Канади) у 2023 р. становив 56 %, а у 2024 р. – 63 % світового обсягу премій, що дозволяє говорити про зрілість та сформованість ринку кіберстрахування в цих країнах [24].

Таблиця 2

Нараховані прямі премії на ринку кіберстрахування США, 2016–2023 рр.

Рік	Прямі нараховані премії з окремих полісів		Прямі нараховані премії з пакетних полісів		Сумарні прямі нараховані премії з внутрішнього ринку, млрд дол. США
	розмір, млрд дол. США	До сумарних прямих премій з внутрішнього ринку, %	розмір, млрд дол. США	До сумарних прямих премій з внутрішнього ринку, %	
2016	1,00	59,9	0,67	40,1	1,67
2017	0,99	52,4	0,90	47,6	1,89
2018	1,11	54,7	0,92	45,3	2,03
2019	1,26	55,8	1,00	44,2	2,26
2020	1,62	58,9	1,14	41,5	2,75
2021	3,20	66,3	1,68	34,8	4,83
2022	5,17	71,6	2,05	28,4	7,22
2023	5,07	69,9	2,18	30,1	7,25

Джерело: складено за [19–23].

Примітка: дані щодо кіберстрахування в США включають дані про страхування ІТ-відповідальності як одного з підвидів кіберстрахування.

Підвищення інтересу у світі до полісів кіберстрахування можна пояснити низкою факторів, таких як:

– поширення Інтернет-технологій у різних сферах людської діяльності;

– надзвичайно швидке зростання обсягів даних, особливо конфіденційних;

– обставини, що пов’язані з передовими технологіями – недостатня грамотність користувачів, нестача кваліфікованого персоналу в організаціях;

– поява широкого спектра інструментів, у т. ч. використання штучного інтелекту для здійснення атак та ін.;

– значне зростання кібератак, через що виникає потреба у врахуванні кіберризиків, для чого й укладаються страхові поліси;

– високі втрати, які несуть кіберризики, у тому числі фінансові, для користувачів ПП та послуг;

– небезпека порушення стійкості бізнесу (електронна комерція, Інтернет-аукціони і т. д.) через масову цифровізацію, впровадження ШІ та ін. [25].

Слід відмітити,що подальше посилення цифровізації економіки може призвести до ще більшого зростання глобального ринку кіберстрахування протягом найближчих 10 років [26]. Останнє пов'язують із суттєвим зростанням кількості кібератак, у тому числі тих, які будуть спровоковані ШІ, як, наприклад, запитами платформ ШІ до конфіденційної і службової інформації та надання її стороннім особам [27]. Ще однією причиною поширення кібератак вважають ланцюг постачальників ПЗ, через що вразливість ПЗ одного постачальника буде поширюватися на всіх клієнтів даного ПЗ [27]. На жаль, опитування показують, що організації часто нехтують засобами кібербезпеки, наприклад, такими, як резервне копіювання даних або багатофакторна аутентифікація користувача мережі (MFA), що також сприяє зростанню кібератак [28].

Прогнозується, що потреби в кіберстрахуванні (та страхуванні ІТ-відповідальності як його складової) будуть настільки значними, що у 2025 р. розмір світового ринку кіберстрахування може досягнути 16,3 млрд дол. США, а до кінця десятиліття – до 30 млрд дол. США [28]. При цьому більш катастрофічних загроз будуть зазнавати малі та середні компанії, оскільки вони не мають таких можливостей виявлення та протистояння кібератакам, як великі, і, відповідно, будуть нести більш суттєві збитки. Продемонструвати це можна на прикладі атак програм-вимагачів, які заподіяли витоки даних для малих та середніх підприємств на 88 %, тоді як для великих – лише на 39 %.

Щодо ринку кіберстрахування в Європі, то він продовжує розвиватися, про що свідчить запроваджене з квітня 2025 р. у Великій Британії та ЄС покриття кіберризиків Tech E&O, яке дозволить клієнтам забезпечувати відповідальність, яка виникає внаслідок використання технологічних продуктів і послуг. Слід зазначити, що в Європі також спостерігається тенденція, аналогічна наявній у США, – великі компанії вкладають більше коштів у кіберзахист, ніж малі та середні компанії [29].

Наскільки важливим є кіберзахист для компаній, стає зрозумілим, якщо звернутися до результатів опитувань – для 72 % респондентів основною проблемою було переривання бізнесу через кібератаки, а 38 % компаній подали претензії [29]. Зауважимо, що проблема відповідальності за якість продукції не обмежується тільки увагою до організації технічної та програмної кібербезпеки. Так, зміни також стосуються нормативно-законодавчої бази, для якої у 2024 р. було розроблено та прийнято директиву ЄС про відповідальність за якість продукції (Product Liability Directive, PLD) [30]. Ці зміни запроваджуються не тільки для виробників споживчих товарів, але й для технологічних та програмних компаній. Особливістю цієї директиви є те, що поняття продукту значно розширюється і включає також:

– ПЗ, його оновлення та штучний інтелект (ШІ);

– файли цифрового виробництва;

– цифрові послуги [30].

Директива також передбачає збільшення терміну відповідальності за якість продуктів – до 10 років, а тягар доведення перекладається на відповідачів через

презумпції дефектності та причинно-наслідкового зв'язку [30]. При цьому зазначено умови, при яких ПП буде вважатися дефектним – несправність, втрата інформації, що викликана роботою цього ПП та ін. Більше того, передбачено ІТ-відповідальність не лише розробників цілого ПП, а й виробника конкретного компонента ПП. Директива також ураховує фактори глобалізації виробництва та постачання ПП – у разі виробництва ПП поза межами ЄС, позивачі можуть висувати претензії до імпортера, представника виробника в ЄС або постачальника послуг з виконання замовлень [30]. Розширюється перелік нових видів збитків – психологічна шкода та пошкодження/втрата персональних даних. Такі положення директиви дозволяють враховувати новий вид товарів та послуг – програмних та цифрових, а також нові тенденції, які виникли в сфері кібербезпеки із появою Інтернету.

Відповідно до звіту [31], в ЄС спостерігається подальший розвиток E&O-страхування, зростання кількості полісів, що пов'язані зі страхуванням цифрових послуг, технологічних та професійних помилок. Цікавим нововведенням на ринку кіберстрахування від Lloyd's (м. Лондон) стало страхування ризиків, які пов'язані з помилками ШІ [32].

Висновки. Страхування ІТ-ризиків належить до досить нових напрямків у страховій діяльності. Ринки кіберстрахування (які включають також страхування ІТ-відповідальності) США та ЄС уже добре розвинені та демонструють постійне зростання. При цьому в країнах Північної Америки (США та Канаді) ринок кіберстрахування становить значну частку світового ринку кіберстрахування – до 63 % світового обсягу премій. В ЄС відбувається систематизація ринку кібестрахування, запроваджуються Tech E&O поліси та нормативно-законодавчі заходи щодо розгляду ПП як одного з різновидів продукції, запроваджуються нові види страхування, пов'язані з розвитком ІТ-галузі, як, наприклад, страхування помилок ШІ.

Щодо страхування ІТ-відповідальності в Україні, то відповідний ринок відносно нещодавно почав розвиватися та поки що перебуває в зародковому стані. Статистичні дані по ньому поки що не агреговані. Проте вже зараз існує ряд страхових компаній, які пропонують послуги зі страхування ІТ-відповідальності та кіберризиків, стандартні поліси. Зважаючи на дедалі більшу діджиталізацію всіх сфер людського життя, а також ураховуючи тенденцію зростання обсягів створення ІТ-продуктів в Україні, можна очікувати, що ринок страхування ІТ-відповідальності буде зростати надалі й Україна набуде статусу країни з європейською культурою страхування.

Список використаної літератури

1. Liability Insurance. URL : https://www.sciencedirect.com/topics/social-sciences/liability-insurance

2. Remond-Gouilloud M. Insurance, liability and compensation. Marine Policy. 1990. Vol. 14. Is. 3. P. 236–242.

3. Anat Lior. Innovating Liability: The Virtuous Cycle of Torts, Technology, and Liability Insurance. Yale Journal of Law & Technology. 2023. Vol. 25. Is. 2. URL : https://yjolt.org/innovating-liability-virtuous-cycle-torts-technology-and-liability-insurance

4. Woods D. W. Software liability and insurance. Lawfare. 2024. P. 1–20. URL : https://www.lawfaremedia.org/article/software-liability-and-insurance

5. Stern A. D., Goldfarb A., Minssen T., and Nicholson Price II W. AI Insurance: How Liability Insurance Can Drive the Responsible Adoption of Artificial Intelligence in Health Care. New England Journal of Medicine Catalyst. 2022. Vol. 3, No. 4. DOI: https://doi.org/10.1056/CAT.21.0242

6. Tsohou A., Diamantopoulou V., Gritzalis S., Lambrinoudakis C. Cyber insurance: state of the art, trends and future directions. International Journal of Information Security. 2023. Vol. 22. P. 737–748. doi : 10.1007/s10207-023-00660-8

7. Основні ризики розробки програмного забезпечення та як їх усунути. URL : https://stfalcon.com/uk/blog/post/top-software-development-risks-and-how-to-remove-them

8. Страхування IT ризиків – що потрібно знати. URL : https://insa.com.ua/korporatyvne-strahuvannya/strahuvannya-vidpovidalnosti-it-spetsialistiv/

9. Чому українським IT-компаніям потрібно страхувати свою професійну чи громадянську відповідальність. URL : https://polis24.ua/news/articles/pochemu-ukrainskim-it-kompaniyam-nuzhno-strahovat-svoyu-pofessionalnuyu-otvetstvennost

10. Кіберстрахування: характеристика та особливості. URL : https://www.lawfirm-pryadko.com/articles/kiberstrahovanie _harakteristika_i_osobennosti

11. Сайт BIS Ukraine. URL : https://bisukraine.com/en/individuals/liability-insurance-c/

12. Сайт Colonnade. URL : https://colonnade.com.ua/

13. Сайт Etalon. URL : https://www.etalon.ua/press_centre/news/2021/12/861/

14. Сайт ІНГО. URL : https://ingo.ua/

15. Сайт Allianz Ukraine. URL : https://www.allianz.ua/uk_UA/korporativnim-klientam/strahovanie-otvetstvennosti.html

16. Сайт брокера Finevolution. URL : https://finevolution.com.ua/

17. Сайт брокера Brit-mark. URL : https://brit-mark.com/

18. Огляди страхового ринку України. URL : https://nasu.com.ua/oglyady-rynku/

19. NAIC. Cyber Supplement (2017 report). URL : https://content.naic.org/sites/default/files/inline-files/cmte_ex_ittf_180921_cyber_supplement_report_2018.pdf

20. NAIC. 2019 Cyber Supplement (2018 report). URL : https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final%20%281%29.pdf

21. NAIC. Cyber Supplement (2021 report). URL : https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf

22. NAIC. Final Cyber Report (2022 report). URL : https://content.naic.org/sites/default/files/inline-files/Final%202023%20Cyber%20Report.pdf

23. NAIC. Cyber Supplement (2023 report). URL : https://content.naic.org/sites/default/files/inline-files/Final%202023%20Cyber%20Report.pdf

24. An Overview of the Global Cyber (Re)Insurance Market. URL : https://actuary.org/wp-content/uploads/2025/08/Toolkit-GlobalCyber-8-25.pdf

25. 10 найбільших кібер-ризиків для бізнесу у 2022. URL : https://spilno.org/article/10-naibilshykh-kiber-ryzykiv-dlya-biznesu-u-2022

26. Cyber Insurance Market Outlook for 2024-2034: Coverage & Capital Managing. URL : https://beinsure.com/cyber-insurance-market-outlook/

27. Weak Governance of Artificial Intelligence Raises Risks of Cyber Attacks: Moody's. URL : https://www.carriermanagement.com/news/2025/10/16/280455.htm

28. Cyber Insurance: Risks and Trends 2025. URL : https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2025.html

29. Resilience Launches Tech E&O For UK & EU Enterprises. URL : https://www.prnewswire.com/news-releases/resilience-launches-tech-eo-for-uk--eu-enterprises-302425084.html

30. Ten things to know about the European Union's new product liability directive. URL : https://www.reuters.com/legal/legalindustry/ten-things-know-about-european-unions-new-product-liability-directive-2025-04-11/

31. Report Description. Errors and Omissions Insurance Market Outlook. URL : https://growthmarketreports.com/report/errors-and-omissions-insurance-market

32. Worried about AI errors? Lloyd’s has insurance for that. URL : https://www.spiceworks.com/security/worried-about-ai-errors-lloyds-has-insurance-for-that/

Дата надходження статті: 21.10.2025
Дата прийняття статті: 05.11.2025
Дата публікації статті: 25.12.2025