DOI: https://doi.org/10.18371/fp.1(33).2019.177102

УДК 368.3.06

СТРАХУВАННЯ В СИСТЕМІ УПРАВЛІННЯ КІБЕР-РИЗИКАМИ ПІДПРИЄМСТВА В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

НАГАЙЧУК Н.Г.
кандидат економічних наук, доцент
декан факультету управління та права
Черкаського навчально-наукового інституту
ДВНЗ «Університет банківської справи»
ORCID ID: 0000-0002-2014-3151
e-mail: nagaichuk_n@ukr.net

ТРЕТЯК Н.М.
кандидат економічних наук, доцент
доцент кафедри фінансів та банківської справи
Черкаського навчально-наукового інституту
ДВНЗ «Університет банківської справи»
ORCID ID: 0000-0002-9457-2645
e-mail: natali_m2008@ukr.net

ТКАЛЕНКО О.
здобувач вищої освіти освітнього ступеня магістр
спеціальності 073 Менеджмент
Черкаського навчально-наукового інституту
ДВНЗ «Університет банківської справи»

Анотація. У статті досліджено поняття кібер-ризику, теоретично описано процеси організації страхового захисту від кібер-ризиків. Розкрито методичні та практичні аспекти участі страхових компаній в розробці та реалізації програми страхового захисту підприємств від кібер-ризиків. Виявлено напрями активізації ролі страхових компаній у забезпеченні страхових інтересів громадян, бізнесу та держави від наслідків кібер-ризиків.

Ключові слова. Кібер-ризик, кібер-загроза, страхування кібер-ризиків, система управління ризиками на основі кібер-страхування, функція корисності.

Аннотация. В статье исследовано понятие кибер-риска, теоретически описаны процессы организации страховой защиты от кибер-рисков. Раскрыто методические и практические аспекты участия страховых компаний в разработке и реализации программы страховой защиты предприятий от кибер-рисков. Выявлены направления активизации роли страховых компаний в обеспечении страховых интересов граждан, бизнеса и государства от последствий кибер-рисков.

Ключевые слова. Кибер-риск, кибер-угроза, страхование кибер-рисков, система управления рисками на основе кибер-страхование, функция полезности.

Постановка проблеми. Розвиток сучасної економіки, заснованої на використанні новітніх цифрових технологій, створення нових матеріалів, аналізі великих масивів даних, розробці нових систем управління, призводить до зміни принципів конкурентних відносин.

Однак, незважаючи на безумовні переваги цифровізації економіки – поява Dig Data, штучного інтелекту, технології блокчейну, хмарних обчислень, з'являються і новітні ризики, генеровані їх використанням, що можуть негативно впливати на економічних суб'єктів та результати їхньої діяльності.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження різних аспектів страхування кібер-ризиків здійснили такі учені, як В.П. Братюк, Е.Д. Семенова, С. Волосович, Ю. Кожедуб, Н.В. Приказюк та інші. Однак, зважаючи на недостатню страхову активність потенційних потерпілих від наслідків кібер-ризиків (споживачів страхових послуг), розгляд сучасного стану та детермінант розвитку страхування кібер-ризиків є актуальним напрямом наукових досліджень.

Метою статті є виявлення напрямів активізації ролі страхових компаній у забезпеченні страхових інтересів громадян, бізнесу та держави від наслідків кібер-ризиків.

Результати дослідження. Світова економічна система знаходиться на постіндустріальній (інформаційній) стадії розвитку. Визначальною характеристикою цифрової економіки є модернізація факторів виробництва, основним із яких стають дані у цифровому форматі. Опрацювання значних обсягів даних та використання результатів їх аналізу дозволяють значно підвищити ефективність різноманітних виробництв, технологій та обладнання, зберігання, продажу і постачання товарів й послуг [1].

Сучасні тренди інтернет-середовища – це рух від об'єднання комп'ютерів і людей до об'єднання (розумних) об'єктів/речей. Така концепція отримала назву Інтернет речей (Internet of Thing – IoT) і стала невід'ємною частиною IT-інфраструктури та економіки в цілому. Вона пов'язана зі збільшенням кількості і типів пристроїв, підключених до мережі, оснащених вбудованими технологіями для взаємодії один з одним або з зовнішнім середовищем і розглядає організацію таких мереж як явище, здатне перебудувати економічні та суспільні процеси , що виключає з частини дій і операцій необхідність участі людини. Інтернетом речей можна назвати об'єднану мережу унікально ідентифікованих кінцевих точок (або «речей»), які можуть спілкуватися без участі людини, використовуючи IP-з'єднання. Екосистема, що підтримує Інтернет речей включає в себе складне поєднання технологій, що не обмежуються тільки модулями/пристроями, пов'язаністю, платформами Інтернету речей, зберіганням, серверами, безпекою, аналітичним програмним забезпеченням та IT-послугами [2, 3, 4].

«Розумні» пристрої та нові послуги можуть бути причиною непередбачених наслідків і вразливостей, що

зумовлює появу специфічних ризиків – кібер-ризиків. Розширення підключених до мереж машин і обладнання може привести до появи надскладних ризиків, таких як крадіжка даних, збої комунікації і навіть відмова цілих виробничих ліній та ланцюгів поставок.

Кібер-ризики названі одними із найнебезпечніших ризиків для провадження бізнесу, сумарні втрати світової економіки від їх реалізації становили у 2015 році близько 445 млрд дол США [5, с. 10], а вже у 2017 році – 600 млрд дол США [6]. За даними Страхового брокера «ІНСАРТ» понесений збиток українським бізнесом внаслідок кібер-атак склав 25 млн. дол. США, близько 50% вітчизняних компаній мали справу з кібер-атаками; більш ніж 125 тис. комп'ютерів було заражене внаслідок кібер-атаки вірусу Petya.A, а розмір збитків становив 466,3 млн. дол США [6]

Кібер-ризик – це ризик, пов'язаний з використанням комп'ютерного обладнання та програмного забезпечення, як в локальних мережах, так і в глобальній Інтернет-мережі; в розрахунково-платіжних системах, системах інтернет-торгівлі, промислових системах управління; а також ризик, пов'язаний з накопиченням, зберіганням і використанням особистих персональних даних.

У сучасній економічній літературі представлено достатню кількість різнопланових підходів до визначення суті поняття кібер-ризику (рис. 1).

Однак, наведені підходи не враховують сукупність специфічних особливостей, які розкривають зміст кібер-ризиків [14, 15, 16, 17, 18]:

по-перше, об'єктом зазіхань (потенційної втрати) є дані (інформація) (нематеріальні активи), що несанкціоновано видаляються, спотворюються, порушується їх конфіденційність або унеможливлюється доступ до них (неавторизоване розкриття, зміна або руйнування цифрових активів);

по-друге, підмножина сукупних ризиків, які відносяться одночасно до ризиків ІТ та інформаційної безпеки;

по-третє, це ризики реалізації навмисних злочинних дій за допомогою використання ІТ.

Врахування таких особливостей дозволило трактувати кібер-ризик як специфічний ризик, поява якого зумовлена діяльністю на електронному ринку та використанням ІТ-технологій.

Кібер-ризики виникають внаслідок настання таких подій:

1. Нецільові атаки (фішинг, кардинг, sms-шахрайство);
2. Цільові атаки (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки, вимагання);
3. Атаки зсередини (розкрадання, знищення інформації, сприяння цільовій атаці).

Результати настання кібер-ризиків можуть розглядатися з позиції видів завданих збитків (фінансовий і майновий) та суб'єктів наслідків їх реалізації (1-ша особа, 3-тя особа), наведені на рис. 2.

Отже, у світлі зростання кількості та серйозності кібер-злочинів ризик-менеджмент організацій змушений внести до свого списку ще одну

небезпеку – хакерські атаки. З такими ризиками необхідно працювати і шукати шляхи їх оптимізації, зокрема за трьома основними напрямами: технологічні рішення безпеки, просвітницька робота в сфері протидії та профілактики кібер-злочинів, а також кібер-страхування.

Рис. 1. Наукові підходи до визначення суті поняття «кібер-ризик»
Джерело: складено авторами на підставі опрацювання [7, 8, 9, 10, 11, 12, 13]

Узагальнюючи наведене вище, наслідки та прояви збитків внаслідок реалізації кібер-ризиків для суб'єктів підприємницької діяльності представлено в табл. 1.

Подією, що сприятиме зростанню, в першу чергу, європейського ринку кіберстрахування вважаємо набуття з 25 травня 2018 року чинності регламентного документа Європейського Союзу щодо захисту даних (General Data Protection Regulation, GDPR) внаслідок підвищення обізнаності компаній про ризики, викликаних порушеннями конфідентційності при обробці даних.

Нові правила надають громадянам ЄС більше прав на свою онлайн-інформацію і передбачають штрафні санкції, розмір яких досягає 4% річного доходу компанії при виявленні серйозних порушень.

На думку страхових експертів, цей директивний документ, а також наслідки таких великих кібератак, таких як WannaCry і NotPetya, будуть стимулювати попит на кіберстрахування у Європі. Так, кількість синдикатів Lloyd's, що пропонують кіберстрахування, тільки за 2016 рік збільшилася на 20%. На думку виконавчого директора Lloyd Інги Біль, щорічні прирости брутто-премії європейського кіберстрахування до 2020 року можуть скласти понад 2 млрд дол. США, що сумарно становитиме близько 9 млрд дол. США.

	Першої особи	***Третьої особи (3-ті особи можуть вимагати):***
Фінансові збитки	✓ Витрати на реагування (IT-розслідування, повідомлення клієнтів) ✓ Юридична допомога: консультації і захист від вимог третіх осіб ✓ PR: мінімізація репутаційного збитку ✓ Втрата прибутку через падіння системи/хмари ✓ Витрати на відновлення даних ✓ Кібер-шантаж (зняття загрози) ✓ Інтелектуальна власність	✓ Втрачену внаслідок кібер-інциденту вигоду; ✓ Витрати на відновлення ✓ Витрати на юридичну допомогу ✓ Збитки від втрати даних (персональні та інші) та інші фінансові втрати ✓ На них можуть бути накладені штрафи та санкції
Майнові збитки	✓ Крадіжка активів ✓ Поломка машин внаслідок кібер-інциденту ✓ Знищення або збиток будівлям/спорудам або іншому майну ✓ Перерва у діяльності (зупинка виробництва через фізичний збиток майну внаслідок кібер-інциденту) ✓ Збиток здоров'ю працівників	✓ Крадіжка активів третіх осіб ✓ Поломка машин третіх осіб внаслідок кібер-інциденту ✓ Знищення або збиток будівлям/спорудам або іншому майну 3-х осіб ✓ Шкода навколишньому середовищу ✓ Збиток здоров'ю третіх осіб

Рис. 2. Класифікація наслідків кібер-ризиків

Таблиця 1

Наслідки для підприємств від настання кібер-ризиків

Вплив	Збиток
Припинення або уповільнення бізнес-процесів	Втрата клієнтів та прибутку
Втрата конкурентної переваги	
Збиток для бренду та втрата репутації	Зниження вартості бізнесу
Судові розгляди та позови	Витрати на усунення наслідків, штрафи і санкції регулюючих органів

Джерело: розроблено авторами на основі [19].

Експерти відмічають, що крупні клієнти при прийнятті рішення про співпрацю однією з умов виставляють – наявність поліса страхування кібер-ризиків у своїх партнерів. Про перспективи даного виду страхування говорить і те, що найбільші страхові компанії світу вже мають подібні послуги в своєму портфоліо.

Світовий досвід свідчить, що розвиток страхового ринку сприяє росту національної економіки в цілому, а кібер-страхування – суб'єктів підприємницької діяльності, забезпечуючи їх стабільне функціонування і свободу у прийнятті рішень при здійсненні інвестиційної та інноваційної діяльності в умовах цифровізації економіки. Для конкурентної боротьби підприємствам необхідно впроваджувати нові перспективні технології з метою реалізації послуг нового покоління. Відбувається цифрова трансформація бізнесу, що тягне за собою появу нових ризиків.

Страховики пропонують послуги зі страхування ризиків, що спричиняють втрати економічних суб'єктів, зумовлені використанням ними обчислювальної техніки та мереж, так зване кібер-страхування.

Приходить і розуміння того, що набагато легше витратити частину коштів на страхування, ніж втратити не лише гроші, але й ділову репутацію. Інформаційні активи компаній дорожчають, відповідно і ймовірність втрат також стрімко зростає. Аналітики роблять прогнози про майбутнє значне зростання попиту на послуги даного виду страхування, зіставні з сьогоднішнім страхуванням майна.

Р. Беме та Г. Шварцем запропоноване наступне визначення кібер-страхування – це передача фінансового ризику, пов'язаного з мережевими та комп'ютерними інцидентами, третій стороні [20]. У табл. 2 згруповано критерії віднесення кібер-ризиків до страхових та види кібер-ризиків, що можуть бути застрахованими.

Специфічність кібер-ризиків, що можуть бути застраховані, проявляється у:

1. Відсутності у страхувальників і страховиків планів з реагування в подібних випадках.

2. Існуванні перспективи суброгації, оскільки більшість подій викликані умисними діями.

3. Доцільності залучення професійних консультантів на етапі укладення договору страхування та врегулювання збитку.

Кібер-страхування – це страховий продукт, що захищає компанію від ризиків, пов'язаних з використанням мережі Інтернет, а також із ризиками, що відносяться до інформаційних технологій, IT-інфраструктури та діяльності підприємства у кібер-просторі. Страховий захист від кібер-ризиків потребують компанії, які:

– здійснюють діяльність, яка безпосередньо пов'язана з мережею Інтернет;

– використовують банківські картки, розрахункові системи, а також віддалені системи доступу;

– відправляють через Інтернет конфіденційні особисті дані;

– застосовують інтернет-сайт для залучення покупців або надання і поширення даних про свою діяльність [22].

Договір кібер-страхування покриває збитки страхувальника завдані кібер-атакою, та понесені у результаті перерв у виробництві, втрати і відновлення даних, реагування на

інцидент, виплати викупної суми кріптолокерам, розслідування інциденту, а також кібер-злочину з метою фінансової вигоди (шахраї).

Таблиця 2

Умови прийняття кібер-ризиків на страхування та їх види

Критерії, що дозволяють ідентифікувати кібер-ризик як страховий:	Види кібер-ризиків, які частково або повністю можуть бути застраховані:
– випадковість виникнення втрат (проблемна для оцінки); – максимально можлива втрата (не проблематична для оцінки); – середня втрата на подію (не є проблематичною для оцінки); – експозиція втрат (не проблематична для оцінки); – ліміти покриття (проблемні для оцінки); – страхова премія (менш проблематична для оцінки).	– ризик привласнення та використання конфіденційної інформації співробітниками компанії; – ризик отримання хакером інформації про номери кредитних карт або рахунків клієнтів компанії; – ризик розкрадання грошових коштів з рахунків в банку або цінних паперів з рахунку в депозитарії; – ризик розкрадання даних кредитних карт і засобів з них; – ризик втрати або розголошення інформації через помилки співробітника; – перерва в роботі підприємства, його комп'ютерної мережі, сайту; – збитки, пов'язані з розміщенням на сайті страхувальника неправдивої інформації або інформації, що має характер дифамації (приниження честі, гідності та ділової репутації); – ризик втрати матеріального носія, що містить конфіденційну інформацію

Джерело: складено за [13, 21].

З метою підвищення привабливості страхової послуги, страховики додатково розширюють страхове покриття додаванням таких умов як:

– відшкодування витрат на розслідування кібер-злочинів;

– антикризовий піар з метою відновлення репутації;

– витрати на захист у суді і відновлення роботи ІТ-системи.

Таким чином, кібер-страхування надзвичайно вигідно при великомасштабному інциденті компрометації ІТ-системи, допомагаючи підприємствам зберігати фінансову стабільність, оперативно повернутися до нормального функціонування і зниження втрат.

Звернення до кібер-страхування спрямоване на досягнення основної мети – забезпечення підприємства компенсаційним ресурсом достатнього за обсягом і за прийнятну ціну, що досягається за рахунок виконання основних завдань, із дотриманням відповідних принципів (рис. 3).

В. Братюк зазначає, що страхування кібер-ризиків спрямоване на подолання наслідків втручання кібер-злочинців (відновлення функцій, інформації, комунікацій) та пов'язане з покриттям всіх необхідних для цього витрат, а також на відшкодування збитків, які є результатом простою комп'ютерних систем [24].

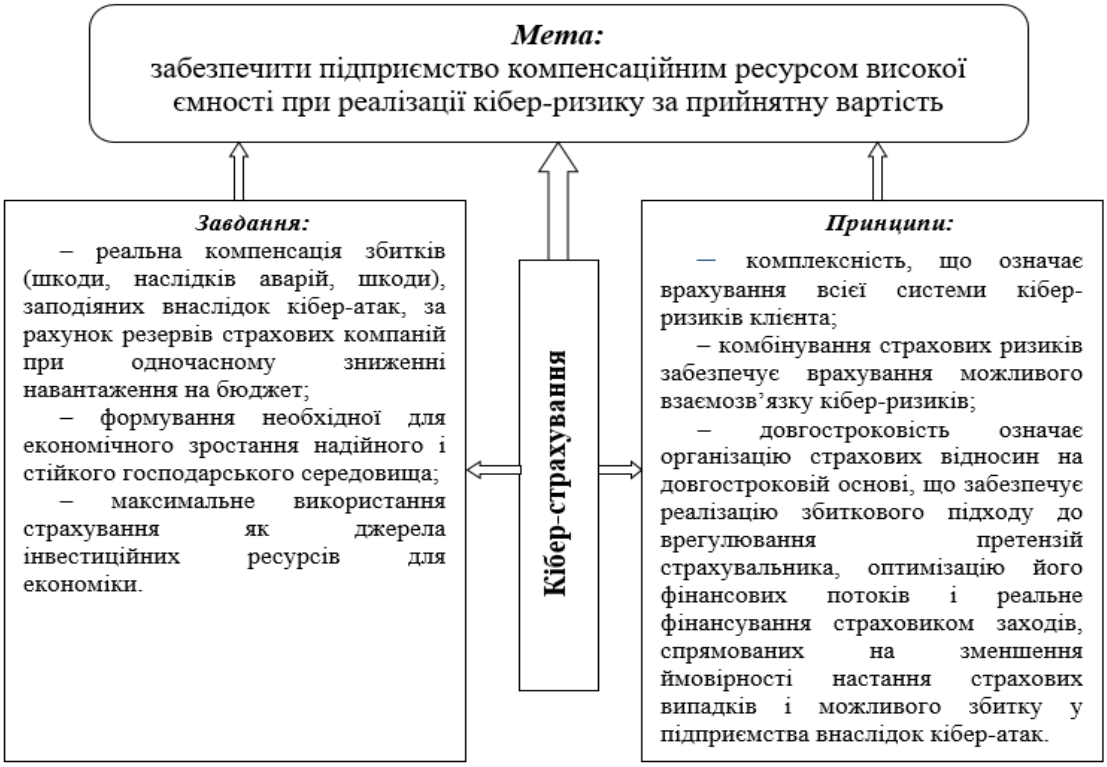

Рис. 3. Мета, завдання та принципи кібер-страхування
Джерело: складено за [23, с.61].

Є.С. Сєдов виокремив характерні особливості страхування кібер-ризиків (табл. 3).

Звичайно, у першу чергу, підприємство зацікавлене у збереженні своїх активів як виробничого, так і іншого призначення, а також у продовженні своєї діяльності навіть у випадку реалізації різного роду ризиків. Основні детермінанти кібер-страхування представлені у табл. 4.

Як бачимо, основним завданням кібер-страхування є захист від хакерських атак. Існують певні складнощі в доведенні наявності кібер-атаки. Клієнти матимуть велику спокусу звернутися за страховим відшкодуванням, навмисно, здійснивши атаку всередині компанії. Страховикові буде вкрай тяжко довести факт шахрайства. Також існує небезпека того, що компанії просто не будуть витрачати кошти на поліпшення систем безпеки, маючи страховий поліс – чекатимуть на виплату страхового відшкодування.

Врахування таких особливостей дозволило трактувати кібер-страхування як складову ризик-менеджменту підприємства, що представляє собою – фінансовий механізм відновлення після значних збитків, метою якого є допомога страхувальникам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити витрати, пов'язані з перервами у виробництві, викликаними дією кібер-ризиків. З позиції страхувальників кібер-страхування – метод управління ризиками й захист від різноманітних загроз, що виникають при здійсненні електронної комерції.

Таблиця 3

Особливості страхування кібер-ризиків

Риса (особливість)	Характеристика
Брак досвіду страховиків і відповідних стандартів	Кібер-страхування – це новий вид страхування, і страховики ще не мають чіткої стандартизованої процедури
Еволюціонування інформаційних систем	Комп'ютерні системи швидко еволюціонують, з'являються нові технології, які можуть змінити природу кібер-ризиків
Інформаційна асиметрія	Страховик не завжди має доступ до тієї ж самої інформації, що і страхувальник. Найчастіше ця інформація є засекреченою
Еволюція кібер-атак	Техніки і прийоми, які використовують кібер-злочинці, постійно змінюються, і ці зміни є непередбачуваними
Взаємозалежність безпеки	Рівень захисту однієї системи часто залежить від захисту інших: вірус може проникнути в систему через канал, створений з компанією-партнером
Нестача статистичних даних	Відсутність статистичних даних про інциденти не дає змоги страховикам визначити надійність їхніх полісів, так як ця інформація часто є конфіденційною і не підлягає розголошенню.
Складність оцінити збитки	Це пов'язано з природою інформаційних активів (вартість ноу-хау чи вартість репутації)
Проблеми з визначенням покриття	Важко визначити, від чого саме страхувальник хоче застрахуватися, а страховик у свою чергу не може точно визначити, чи готовий він це покрити
Винятки та обмеження	Поліси зі страхування кібер-ризиків містять безліч винятків та обмежень щодо покриття
Відповідальність	Коли була здійснена кібер-атака, необхідно встановити рівень відповідальності за збитки і визначити, хто несе відповідальність за шкоду. У деяких випадках це можуть бути власники систем, в інших – розробники програмного забезпечення тощо
Час для пред'явлення претензій	Багато атак відбуваються непоміченими. Порушення у роботі системи можуть бути виявлені вже після нападу. Крім того, деякі атаки є надзвичайно тривалими (наприклад, напади можуть зайняти кілька місяців). Питання про те, яким чином страховики повинні відшкодувати витрати, залишається відкритим

Джерело: складено за [25, 26]

Захист від кібер-ризиків може послідовно перетворюватися у важливу сферу бізнесу. Кібер-ризики становлять серйозну проблему для страхової галузі, оскільки вона володіє дуже обмеженими даними про довгострокові втрати від них, що унеможливлює проведення оцінки ризику з використанням звичайних моделей. Крім того, самі ризики змінюються в міру того, як бізнес оцифровується, що вимагає гнучких рішень, які включають набагато більше, ніж просто страхове покриття. Невідомі кібер-ризики можуть бути виявлені у багатьох існуючих традиційних страхових програмах для бізнесу, оскільки договірні умови або не виключають цих ризиків, або не формують виключень і обмежень з достатньою точністю. Доволі рано розглядати кібер-страхування в українських реаліях, оскільки його впровадження на сучасному етапі

розвитку страхового ринку України є неможливим, що в першу чергу зумовлено відсутністю потужно капіталізованих страховиків, здатних прийняти такі ризики на страхування.

Таблиця 4

Детермінанти кібер-страхування

Опис ризику, що покривається страховиком	– ризики, що виникають при використанні електронних даних та їх передачі, включаючи технологічні інструменти, такі як інтернет та телекомунікаційні мережі; – фізичний збиток, який може бути спричинений випадками порушення кібербезпеки, шахрайством, заподіяним зловживанням даними, будь-якою відповідальністю, що виникає внаслідок зберігання даних; а також доступності, цілісності та конфіденційності електронної інформації щодо приватних осіб, компаній чи урядів [28]
Прояв ризику	Хакерські атаки
Страхувальники	Підприємства реального сектору, банки, фінансові компанії, реєстратори цінних паперів, реєстратори прав власності та ін.
Переваги для страхувальників	– експертиза найбільш суттєвих ризиків; – розробка рекомендацій щодо мінімізації наслідків атаки
Ризики для страховиків	– складність доведення кібератаки (можливе внутрішньофірмове шахрайство); – відсутність у страхувальника потреби здійснювати витрати на покращення системи безпеки

Джерело: складено за [27]

По-друге, відсутня будь-яка нормативна база, що визначає природу кібер-ризиків, можливість та умови їх страхування, зокрема, жодна компанія не має ліцензії на такий вид страхування. По-третє, вітчизняні страховики ще не мають у своєму розпорядженні методик оцінки даного ризику, що унеможливлює встановлення ціни страхового захисту. І четверта, мабуть основна причина – відсутність платоспроможних страхувальників, які можуть дозволити собі придбати доволі недешеву програму страхування від кібер-ризиків.

На сьогодні на вітчизняному страховому ринку лише деякі страхові компанії можуть запропонувати якісний страховий захист від кіберзлочинності (кібер-ризиків). Відсутня необхідна статистика, законодавча база, судова практика. Недостатньо і кваліфікованих фахівців, що мають уявлення про даний вид ризику та його структуру [29].

Однак, на перспективу, вітчизняні страховики повинні стежити за світовими тенденціями, переймати західний досвід; збирати і аналізувати дані, статистику зарубіжних компаній і готувати платформу для створення власних продуктів із кібер-страхування. Варто звернути увагу на поліс CyberEdge від American International Group (AIG), адже на сьогоднішній день це вершина розвитку кіберстрахування.

Певний рух у цьому напрямі відбувається через страхових брокерів, які мають можливість виходу на світовий ринок кібер-страхування та розміщують ризики

вітчизняних підприємств-страхувальників.

Крім того, причинами, що стримують розвиток кіберстрахування в Україні є: невизначенність юридичного статусу цифрових активів; не розробленість методичних підходів до класифікації ризиків використання цифрових активів, відсутність методик оцінки кібер-ризиків та систем ризик-менеджменту адаптованих до потреб цифрової економіки. У розпорядженні страховиків є традиційні страхові продукти (види страхування технічних ризиків), які можуть бути модернізовані під потреби цифрової економіки: страхування машин від поломок, страхування від перерв у виробництві, страхування ризику введення технологічних інновацій, страхування електронного обладнання, страхування ризику втрати прибутку внаслідок поломок промислових машин і технологічного обладнання, страхування післяпускових гарантійних зобов'язань тощо.

Більшість компаній витрачають більшу частину свого часу та ресурсів, створюючи захист в середині компанії, що включає дані, системи та персонал. Це є відправною точкою, але периметр вже не стабільний, а система внутрішнього захисту вже не є достатньо сильною, щоб утримати нападників [3]. Кібер-ризики можуть призводити до прямих та непрямих грошових втрат суб'єктів господарювання. В першому випадку можна легко виміряти збитки в грошовому еквіваленті. В другому – необхідно залучати експерта або фахівця для якісної оцінки величини збитків від наслідків кібер-ризиків в організації [19].

Існують чотири варіанти обробки ризику:

– зниження ризику – рівень ризику повинен бути знижений шляхом вибору заходів та засоби контролю і управління так, щоб ризик який залишився міг бути повторно оцінений як допустимий;

– збереження ризику – рішення зберегти ризик, що не здійснюючи подальших дії, слід приймати в залежності від оцінки ризику;

– запобігання ризику – відмова від діяльності або умови, що викликає конкретний ризик;

– перенесення ризику – ризик повинен бути переданий на сторону, яка може найбільш ефективно здійснювати менеджмент конкретного ризику в залежності від оцінки ризику.

В результаті обробки повинні бути відібрані заходи і засоби контролю та управління для зниження, збереження, запобігання або перенесення ризиків.

У сучасній літературі основна увага приділяється організаційно-технічному забезпеченню інформаційної безпеки і, зокрема, апаратним і програмним засобам захисту інформації. Однак економічні методи забезпечення інформаційної безпеки не менш важливі, ніж технічні.

Мета системи управління ризиками підприємства на основі страхового захисту полягає у зниженні рівня ризиків супутніх діяльності компанії до прийнятного для акціонерів (власників) рівня шляхом передачі ризиків страховику і тим самим сприяння досягненню поставлених перед компанією цілей (рис. 4).

Управління кібер-ризиками на основі побудови страхового захисту підприємства організовується за результатами аналізу його діяльності з урахуванням факторів, що впливають на оцінку можливого збитку. Для ідентифікації ризиків суб'єкти господарювання складають карти ризиків. Структурно-функціональна модель організації процесу оцінки кібер-ризиків підприємства представлена на рис. 5.

Інструментами і методами моніторингу і управління ризиками є перегляд і аудит ризиків, аналіз відхилень і трендів, технічні вимірювання виконання, аналіз резервів [30].

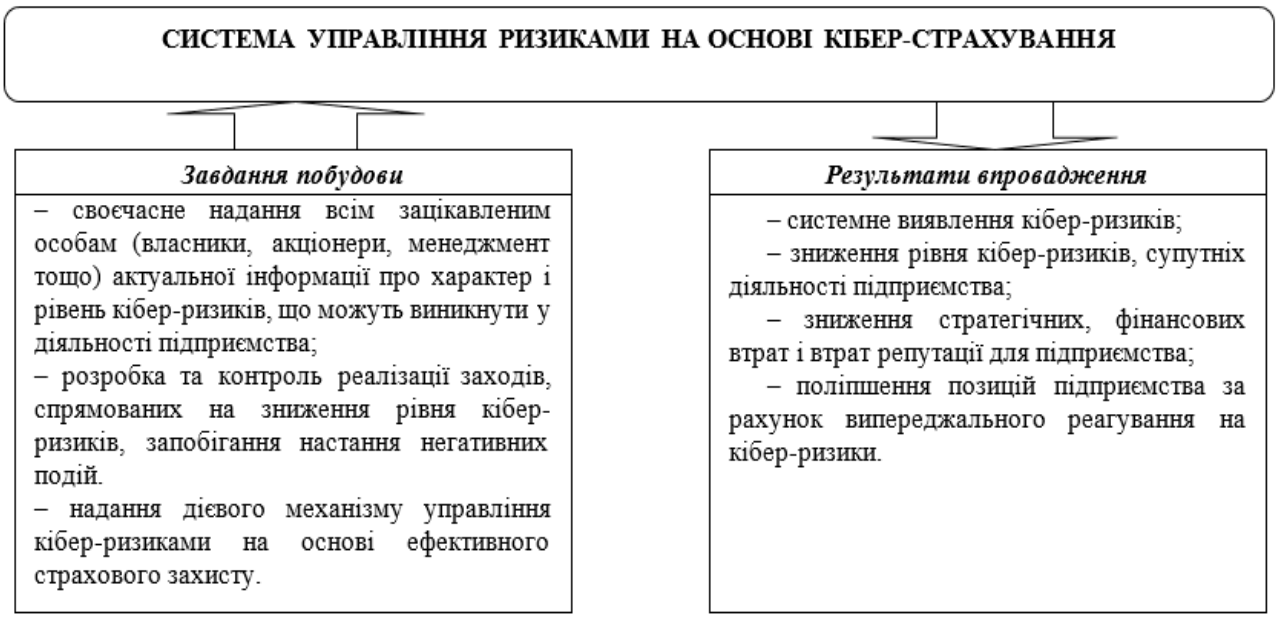

Рис. 4. Завдання побудови та результати впровадження системи управління ризиками на основі кібер-страхування

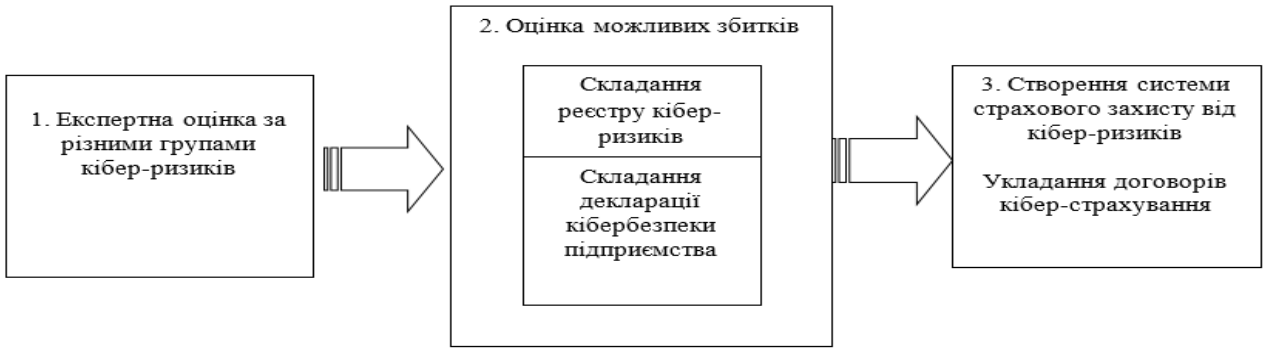

Рис. 5. Структурно-функціональна модель оцінки кібер-ризиків підприємства

Звернення підприємства до страхової компанії за страховим захистом передбачає усестороннє вивчення страховиком (сюрвеєром, оцінювачем) особливостей та специфіки бізнесу клієнтів з метою формування програми попереджувальних заходів і розробки пакетів страхових продуктів в рамках наявних програм страхового захисту, які найбільш повно

відповідають потребам того чи іншого підприємства з урахуванням ймовірності реалізації кібер-ризику виникнення збитків. Проведене дослідження наукових напрацювань українських та зарубіжних вчених дало змогу трактувати «кібер-страхування» як складову ризик-менеджменту підприємства, що представляє собою фінансовий механізм відновлення після значних збитків, метою якого є допомога страхувальникам повернутися до нормального функціонування, зберегти стабільність, платоспроможність та знизити витрати, пов'язані з перервами у виробництві, викликаними дією кібер-ризиків.

На даний момент складається ситуація, при якій вітчизняні страхові компанії поки не можуть розробити власний підхід до оцінки кібер-ризиків, що стримує зростання популярності цієї послуги в Україні. Вітчизняні страхові компанії, готуючи пропозицію для клієнта, оцінюють ризики компанії за допомогою непрямих ознак і характеристик, таких як: методи управління ризиком в компанії; способи зберігання даних; проведення чи тестування систем інформаційної безпеки та аудиту, а також оцінюють кількість співробітників зайнятих в IT. Слід очікувати, що найближчим часом почнуть формуватися більш детальні методики, які все-таки будуть відповідати на пряме запитання щодо оцінки ризиків кібер-страхування.

Список використаної літератури

1. Кешелава А.В. Введение в «Цифровую» экономику. ВНИИГеосистем, 2017. 28 с.

2. Тинькова А.А., Замотайкина А.А. Особенности и преимущества платформы Watson IoT для Интернета вещей. URL: http://nauka-rastudent.ru/39/4148/

3. Интернет Вещей: инновационные и перспективные технологии – IoT Russia 2015. URL: http://www.tmtconferences.ru/iot2015.html

4. Карачев О. Интернет вещей: что это такое и с чем его едят? URL: http://chezasite.com/news/chto-takoe-internet-veshei-82180.html

5. Ways to make global e-commerce easier for everyone. December, 2017. URL: https://www.weforum.org/agenda/2017/12/ecommerce-trade-wto-growth-opportunity6.2018.iforum.ua/ru/speakers/alexandra-gladyshevskaya

7. Calderon C., Marta E. (2007) A taxonomy of software security requirements. Avances en Sistemas e Informatica, 4 (3), pp. 47-56.

8. Cebula J., Young L. (2010) A taxonomy of operational cyber security risks. Software Engineering Institute, Carnegie Mellon University. Available at:

http://resources.sei.cmu.edu/ library/asset-view.cfm?AssetID=9395 [Accessed 12/04/16].

9. Firesmith D. (2004) Specifying reusable security requirements. Journal of object technology, 3 (1), pp. 61-75.

10. Donnelly C., Englund M., Nielsen J.P., Tangaard C. (2014) Asymmetric information, self-selection and pricing of insurance contracts: the simple no-claims case. Journal of risk and insurance, 81 (4), pp. 757-780.

11. Gerasimenko V.A. (1994) Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannykh [Data protection in data processing systems]. Moscow: Energoatomizdat Publ.

12. Ol'ga A. Mirsanova (2016) The Bonus-Malus System as the policyholders' classification method in cyber-insurance / Economics: Yesterday, Today and Tomorrow. 6`2016

13. Biener C., Eling M., Wirfs J.H. (2015) Insurability of cyber risk: an empirical analysis. Working papers on risk management and insurance, URL: http://www.ivw.unisg.ch/~/
media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf [Accessed 15/04/16].

14. Воронова Т. Безопасный интернет. *Calaméo*. URL: http://ru.calameo.com/books/002793881c6046eb0d2fb

15. Завгородний В.И. Парадигма информационных рисков. *Финансовый Университет при Правительстве РФ*. URL: http://www.fa-kit.ru/main_dsp.php?top_id=591

16. Зайцева О.Н. О необходимости введения понятия «риски адекватности информации». *Фундаментальные исследования*. 2013. № 1–3. С. 807–811.

17. Мишель М. Управление информационными рисками. *Финансовый директор*, 2003. № 9. С. 64–68.

18. Data scarce for insurers covering cyber risks. Business Insurance. URL: http://www.businessinsurance.com/article/20150610/NEWS06/150619981/1251

19. Віннікова І.І., Кібер-ризики як один із видів сучасних ризиків у діяльності малого та середнього бізнесу та управління ними. *Східна Європа: економіка, бізнес та управління.* 2018. № 5 (16).

20. Böhme R., Schwartz G. (2010) Modeling cyber-insurance: towards a unifying framework. WEIS. URL: http://econinfosec.org/archive/weis2010/papers/session5/weis2010_ boehme.pdf [Accessed 12/04/16].

21. Цена информационной безопасности и страховая защита откибер – рисков. URL: http://strahovkunado.ru/insur/strakhovan.

22. Страхование кибер-рисков. URL: https://www.arsenalins.ru

23. Пономарёв А. Н. Разработка модели процесса корпоративного страхования. Имущественное корпоративное страхование. *Вестник ВГУ. Серия: Экономика и управление*. 2009. №2. С.61-68.

24. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9. С. 421-427.

25. Сєдов Є. С. Деякі аспекти страхування кібер-ризиків. *Інноваційні напрямки розвитку страхового ринку України* : зб. матеріалів ІІІ Міжнар. наук.-практ. конф. м. Київ,19–20 квітня 2016 р., Київ, 2016. С. 288–291.

26. Marotta A. A Survey on Cyber-Insurance. Bologna, Italy: Unipol Gruppo Finanziario S.p.A., 2015. 52 p.

27. Курбанова О.Э., Ларионов В.И. Киберстрахование как способ обеспечения информационной безопасности. *Материалы Всероссийской заочной научно-практической конференции: Проблемы развития страхового бизнеса в Росии*., 2017. С. 55-58.

28. CRO Forum. The Cyber Risk Challenge and the Role of Insurance. December 2014. URL : http://www.thecroforum.org/cyber-resilience-cyber-risk-challenge-role-insurance.

29. Иващенко А.Н., Шарко И.А. Мировой рынок страхования кибер-рисков: перспективы и препятствия для развития в Республике Беларусь. Материалы IX Международной научно-практической конференции студентов «Национальная экономика Республики Беларусь: проблемы и перспективы развития» г. Минск, 2016. Минск, 2016. С. 196–202.

30. Кропотина О.Е. Страхование как метод управления рисками промышленных предприятий. *Экономика и управление народным хазяйством*, 2009. №11 /12. С. 12–14.