Електронне наукове фахове видання **"Ефективна економіка"** включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)
www. economy.nayka.com. ua | № 5, 2018

УДК 368:330.131.7:004

В. П. Ільчук,
д. е. н., професор, завідувач кафедри фінансів, банківської справи та страхування, Чернігівський національний технологічний університет, м. Чернігів
О. М. Парубець,
д. е. н., доцент, професор кафедри фінансів, банківської справи та страхування, Чернігівський національний технологічний університет, м. Чернігів
Д. О. Сугоняко,
к. е. н., доцент , доцент кафедри публічного управління та менеджменту організацій, Чернігівський національний технологічний університет, м. Чернігів

ІННОВАЦІЙНІ ПІДХОДИ ДО РОЗВИТКУ РИНКУ КІБЕРСТРАХУВАННЯ В УКРАЇНІ

V. P. Ilchuk,
Doctor of Economic Sciences, Professor, Head of the Department of Finance, Banking and Insurance, Chernihiv National University of Technology, Chernihiv
O. M. Parubets,
Doctor of Economic Sciences, Associate Professor, Professor of the Department of Finance, Banking and Insurance, Chernihiv National University of Technology, Chernihiv
D. O. Sugonyako,
Candidate Economic Sciences, Associate Professor, Associate Professor of the Department of Public Administration and Organizations Management, Chernihiv National University of Technology, Chernihiv

INNOVATIVE APPROACHES TO THE DEVELOPMENT OF CYBER-INSURANCE MARKET IN UKRAINE

Ринок кіберстрахування в Україні знаходиться в процесі свого становлення і стикається з інституційними, фінансовими, організаційними, інформаційними, маркетинговими та науково-методичними проблемами, які потребують поєднання державного, ринкового та інноваційного підходів до їх розв'язання.
У статті наведено рекомендації щодо практичного застосування запропонованих інноваційних підходів до формування і розвитку зазначеного ринку, головними серед яких є удосконалення інституційного механізму управління інноваційною діяльністю страхових компаній, сприяння розвитку взаємодії останніх з Департаментом кіберполіції, Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації, створення інституту страхових омбудсменів, застосування актуарного моделювання на основі використання персоналізованого маркетингу, індивідуального андерайтингу, впровадження на рівні страхових компаній новітніх технологій.

The cyber-insurance market in Ukraine is at the stage of its formation and faces institutional, financial, organizational, informational, marketing and scientific and methodological problems that require a combination of state, market and innovative approaches to their solution.

The article gives some recommendations on the practical application of the proposed innovative approaches to the formation and development of this market. The main suggestions are the following: improvement of the institutional mechanism for managing the insurance activity of innovative companies; promotion of interaction between the latter and the Department of Cyberpolicy, the National Commission, which carries out the state regulation in the field of communication and information; creation of the institution of insurance ombudsmen; use of actuarial modelling based on the application of personalized marketing, individual underwriting; implementation the latest technology at the level of insurance companies.

Ключові слова: *інноваційні підходи, кіберстрахування, кіберризики, попит, пропозиція, безпека, технології, збитки, розвиток.*

Key words: *innovative approaches, cyber-insurance, cyber-risk, demand, supply, security, technology, losses, development.*

Постановка проблеми. Розвиток процесів глобалізації та інтеграції в умовах інформаційної економіки приводить до появи нових видів ризиків, пов'язаних з кіберзагрозами й кібератаками, негативний вплив яких має транснаціональний і транскордонний характер та поширюється на декілька країн одночасно. У зв'язку з цим потребують негайного вирішення проблеми, пов'язані з удосконаленням системи кіберзахисту та розвитком інноваційних інструментів ризик-менеджменту, одним з яких є кіберстрахування. В Україні ринок кіберстрахування перебуває на початковому етапі становлення та потребує розробки інноваційних підходів до подальшого розвитку, враховуючи накоплений позитивний досвід зарубіжних країн у цьому напрямку.

Світовий ринок кіберстрахування розвивається швидкими темпами. За експертними оцінками обсяг операцій на такому ринку до 2020 р. може становити від 7,5 до 10 млрд дол. США., а загальна сума збитків від кібератак зросте до 2,1 трлн дол. США. Лідером за обсягами операцій на такому ринку є США [1]. Темпи розвитку кіберстрахування в кожній країні світу зумовлюються їхнім соціально-економічним та техніко-технологічним становищем, впровадженням ІТ-технологій, рівнем інформатизації суспільства.

В умовах розвитку штучного інтелекту, мережевих підприємницьких структур, хмарних технологій, ринку аутсорсингу вдосконалюються методи і прийоми хакерських атак, що призводить до зростання обсягів кіберзлочинів. У результаті цього зростає ймовірність настання кіберризиків, покриття яких потребує впровадження інноваційних підходів до продуктів страхування, чим і зумовлюється актуальність обраної теми дослідження.

Аналіз останніх досліджень і публікацій. Проблеми становлення та перспективи розвитку ринку кіберстрахування, впровадження інновацій у сфері страхування досліджені в наукових працях багатьох вітчизняних та зарубіжних вчених.

На думку В. П. Братюк кіберстрахування в Україні повинно стати новим видом страхування від кримінальних кіберризиків та загроз втручання в діяльність автоматизованих систем, оскільки країна перебуває в процесі інформатизації, інтенсивно впроваджує нові інформаційні технології в усіх сферах суспільної практики [2, с. 174].

Для активізації ролі кіберстрахування у зменшенні кіберризиків та поліпшенні кіберстійкості С. Ванг пропонує не просто передавати ризики від компаній до страховиків, а пом'якшити вимоги органів нагляду за страховою діяльністю на продукти кіберстрахування, розвивати взаємовигідне партнерство між страховими компаніями та фірмами з безпеки інформаційних технологій у напрямку надання інтегрованих послуг зі зменшення ризику та страхового захисту, що ґрунтується на угодах розподілу доходів у сферах надання консультаційних послуг зі страхування ризику, розслідування випадків та розгляду претензій, відшкодування збитків [3].

Дж. Кесен та К. Хейєс акцентують увагу на труднощах, пов'язаних з визначенням обсягів фінансових наслідків втрати даних, які є непередбачуваними, що робить ризик важким для страхування. Страховикам бракує комплексних актуарних даних, які інформують про інші види збитків, покритих страхуванням. Деякі страхові компанії реагують на цю невизначеність, стягуючи вищу премію, створюючи винятки та обмежуючи охоплення, але ці підходи можуть обмежувати ринок кіберстрахування [4].

Встановлюючи взаємозалежність моделей кіберризиків та кіберстрахування від моделей фінансового ризику, Й. Малкотра пропонує розглядати їхні складові в таких аспектах:

– кіберризики та кібератаки є економічними іграми, які впливають на економічну цінність конкретного об'єкта на цій одиниці аналізу, такого як нація, фірма чи індивід;

– в основі взаємодії кібер- та фінансової сфери повинна бути довіра;

– економічні витрати від настання кіберризиків та кібератак повинні отримати фінансову (економічну) оцінку [5].

Проводячи аналіз зарубіжного досвіду інноваційного розвитку страхової діяльності автори роботи [6] зазначають, що в останнім часом у багатьох країнах світу відбувається динамічний розвиток онлайн-страхування, інтернет-страхування, розвиток ІТ-інфраструктури страховиків, використання страховими компаніями телематичних технологій, інтернет-магазинів, інтернет-вітрин тощо.

Приказюк Н. В. та Моташко Т. П., досліджуючи напрямки впровадження інновацій у страховій системі України, пропонують запровадження нових інноваційних продуктів, послуг, технологій та рішень, серед яких особливе місце посідають страховий омбудсмен, електронний страховий поліс, банкострахування, використання Інтернету, телематика, мобільні, ігрові та відеотехнології, хмарні платформи, програмне забезпечення, блокчейн, страхування нестандартних ризиків та кіберстрахування. Останнє передбачає охоплення страховим захистом нового виду ризику – кіберризику [7, с. 184-188].

На необхідність використання кіберстрахування як елементу активної стратегії для пом'якшення ризику, пов'язаного з кіберзагрозою не тільки для власного конкурентного добробуту, але і для забезпечення критичної національної інфраструктури вказує С. Шекелфорд. На думку автора, кіберстрахування може допомогти кількісно оцінити ризик та допомогти захистити фірми від кібератак. При цьому страхові компанії повинні шукати найбільш вразливі для кібератак фірми, наприклад, телекомунікаційні, високотехнологічні компанії, засоби масової інформації та пропонувати їм відшкодування збитків, індивідуальний підхід до укладання страхових угод [8].

Основним завданням кіберстрахування є захист від наслідків великомасштабної хакерської атаки. Цей вид страхування забезпечує фінансовий механізм відновлення після великих збитків, допомагаючи підприємствам повернутися до нормального функціонування, збереження стабільності, платоспроможності та зниження втрат у результаті перерви у виробництві. Крім того, страхові компанії пропонують такі додаткові умови: відшкодування витрат на розслідування кіберзлочинів, антикризовий піар з метою відновлення репутації, витрати на захист у суді й відновлення роботи ІТ-систем [9].

Розрізненість теоретичних підходів до формування ринку кіберстрахування у вітчизняній і зарубіжній практиці та законодавча невизначеність основних понять, що входять до його структури зумовлюють необхідність проведення подальших досліджень у напрямку обґрунтування інноваційних підходів до його розвитку з урахуванням сучасних тенденцій зростання кіберзагроз.

Постановка завдання. Мета статті полягає у виявленні проблем становлення ринку кіберстрахування в Україні та обґрунтуванні інноваційних підходів стосовно його подальшого розвитку.

Виклад основного матеріалу дослідження. Масштабні хакерські атаки в Україні відбулися в період 2014-2017 років і за прогнозами експертів в умовах інформатизації корпоративного сектору й суспільства їх кількість у майбутньому буде зростати швидкими темпами. Розглянемо основні види хакерських атак, які здійснили найбільш потужний негативний вплив на економіку держави.

У 2014 р. здійснена DDoS-атака призвела до злому сайта Центральної Виборчої Компанії під час Президентських виборів в Україні. Наприкінці 2015 р. потужна хакерська атака вивела з ладу об’єкти критичної інфраструктури в Прикарпатті, Києві, Чернівцях. У грудні 2016р. було здійснено декілька хакерських атак, спрямованих на втручання до інформаційних систем Міністерства фінансів України, Державної казначейської служби, Пенсійного фонду, а також сайту Укрзалізниці та підстанції Північної компанії Укренерго. Влітку 2017 р. відбулася найбільш масштабна за наслідками і рівнем збитку хакерська атака за допомогою вірусної програми Petya.A, яка порушила роботу системи органів виконавчої влади, державних і приватних підприємств, банківських установ, мобільних операторів, засобів масової інформації. У жовтні того ж року була здійснена чергова атака на Міністерство інфраструктури України, Одеський аеропорт і київське метро з використанням нового вірусу-шифрувальника, який вимагав викуп у біткоїнах [10]. Стислий аналіз здійснених кібератак в Україні свідчить про їхню диверсифікацію, масштабність і охоплення різних аспектів економічної діяльності держави.

Основними видами кіберризиків у сучасних умовах виступають кріптовіруси, хакерські атаки на інформаційні системи об’єктів критичної інфраструктури, фінансово-кредитних установ, державних інституцій, крадіжки персональних даних, несанкціоновані транзакції, DDoS–атаки на DNS-сервери тощо. Це призводить до збільшення витрат суб’єктів господарювання на вдосконалення захисту інформаційних систем, які, на жаль, не завжди можуть протистояти та відбити можливі кібератаки. У цьому випадку зменшити рівень втрат від настання кібератак можливо за допомогою кіберстрахування.

Перш ніж визначити інноваційні підходи до розвитку ринку кіберстрахування в Україні, необхідно дослідити наявні проблеми його становлення і функціонування, які можна поділити на такі групи:

– інституційні – відсутність законодавчо-нормативної бази регулювання ринку кіберстрахування, діяльності страхових компаній, які можуть надавати послуги зі страхування кіберризиків;

– фінансові – недостатній обсяг фінансових ресурсів, що вкладаються у сферу забезпечення кібербезпеки на державному, регіональному, локальному рівнях; відсутність ефективних фінансових інструментів і важелів розвитку національної системи кіберстрахування;

– інформаційні – помилки в розробці й підтримці інформаційних систем страховиків і страхувальників; розвиток кібершпіонажу; перенесення персоналом підприємств, установ, організацій комерційної інформації в соціальні мережі;

– організаційні – відсутність кваліфікованого персоналу у сфері страхування кіберризиків; довіри юридичних і фізичних осіб до діяльності страхових компаній і ринку кіберстрахування; тимчасовий характер страхових відносин;

– маркетингові – низький попит на продукти кіберстрахування через їхню високу вартість; небажання клієнтів надавати необхідний для виявлення страхових випадків доступ до своїх інформаційних систем; відсутність досвіду страхових компаній з врегулювання ситуацій настання страхових подій, пов'язаних з втручанням в інформаційний простір держави, суб'єктів господарювання і населення; відсутність рекламування в засобах масової інформації, соціальних мережах переваг страхування кіберризиків у порівнянні з можливими збитками від кібератак; низький рівень конкуренції в сегменті кіберстрахування;

– науково-методичні – відсутність наукового обґрунтування методики визначення показників оцінювання та розрахунку кіберризиків, стандартів оцінки збитків від настання кібератак та суми їх відшкодування страхувальниками.

Особливістю кіберстрахування є те, що попит на нього формується в процесі виникнення кіберзагроз або після кібератак. Пропозиція залежить від індивідуальних особливостей настання кіберінцидентів у страхувальників, вартості страхових послуг, розміру прибутку страховиків та відшкодування збитків від настання страхових випадків, можливістю останніх укладати страхові договори через систему Інтернет (онлайн-поліси). Ринок кіберстрахування характеризується консервативною моделлю побудови, і страховим компаніям, насамперед, треба завоювати довіру страхувальників до інноваційних страхових продуктів у сфері інформаційної безпеки.

Сфера застосування кіберстрахування, як ефективного інструменту відшкодування значної суми збитків у результаті настання кібератак, у майбутньому розширюватиметься завдяки використанню біометричних методів ідентифікації в процесі здійснення фінансових, зокрема, страхових операцій; розширення сфери застосування чат-ботів суб'єктами страхової, банківської та бізнес сфер; збільшення кількості хакерських атак на провайдерів хмарних технологій та їхніх клієнт-серверних мереж.

Найбільш привабливими для кіберзлочинців є фінансово-кредитні установи, особливо банки, які широко використовують сучасні інформаційні технології. Несанкціоновані втручання в діяльність систем Інтернет-Клієнт-Банк та Інтернет-банкінгу, кіберкрадіжки даних із банківських рахунків та платіжних карток клієнтів є наслідком значної кількості кіберзлочинів у фінансовій сфері. За даними Національного банку України, у 2017 р. сталося 77,6 тисячі випадків шахрайства з банківськими картками, що призвело до втрати коштів на суму 163,7 млн грн. [11].

У зв'язку з цим інститут банківської таємниці стає більш вразливим і спричиняє втрату ділового іміджу й довіри фізичних і юридичних осіб до банківської системи країни загалом. На заваді ефективної взаємодії банківських установ і страхових компаній у напрямку зменшення негативного впливу кіберзлочинів постає низький рівень фінансової грамотності населення стосовно гарантування безпеки власних банківських рахунків і можливостей страхування від різного роду кіберризиків, що у випадку їх настання дасть змогу повернути значну суму коштів у вигляді страхового відшкодування за укладеними договорами. Необхідно створити сумісні інформаційно-просвітницькі ресурси, завдяки яким клієнти могли б чітко побачити, з яким банком співпрацює та чи інша страхова компанія і який спектр страхових послуг у сфері кіберстрахування надає.

Розвиток внутрішнього ринку кіберстрахування потребує також удосконалення інституційного механізму управління інноваційною діяльністю страхових компаній, який враховує вплив ендогенних і екзогенних факторів та поєднує інструменти державної підтримки диверсифікації інноваційних продуктів страхування з ринковими. Основними проблемами державного регулювання зазначеного ринку є недосконаліть нормативно-законодавчої бази, відсутність державних стандартів функціонування та державної фінансової підтримки.

Головними органами державного регулювання страхового ринку України є Національна комісія, що здійснює державне регулювання у сфері ринків фінансових послуг, Державна служба фінансового моніторингу України, Державна аудиторська служба України та ін. Розвиток ринку кіберстрахування потребує тісної взаємодії страхових компаній з Департаментом кіберполіції, Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації для об'єднання зусиль, спрямованих на моніторинг кіберзагроз та протидію кіберзлочинності. Важливим напрямком також є розвиток мережевої взаємодії національних страхових компаній між собою та страховиками інших країн з метою обміну позитивним досвідом у сфері страхування кіберризиків. Зазвичай збитки від кіберзлочинів становлять значну суму, і страхові компанії об'єднують свої зусилля шляхом перестрахування.

З метою захисту прав страхувальників необхідно створити інститут страхових омбудсменів, що сприятиме покращенню якості і прозорості надання послуг на ринку кіберстрахування. У 2015 р. була створена громадська спілка «Український страховий омбудсмен» (УСО) [12], головною метою діяльності якої є надання безплатної консультаційної допомоги у вирішенні спірних питань між страхувальниками і страховиками щодо виплати страхового відшкодування в основному за полісами «автоцивілки». Рішення омбудсмена є обов'язковими для страхових компаній, що входять до складу УСО, для інших страховиків вони мають рекомендаційний характер.

Впровадження інноваційних продуктів на ринку кіберстрахування потребує впровадження інформаційних технологій страховиками. Для того щоб страхувати різноманітні кіберризики та відповідати зростаючим вимогам клієнтів, до складу яких можуть входити високотехнологічні компанії, підприємства

критичної інфраструктури,телекомунікаційні фірми, фінансово-кредитні установи, бізнес-структури тощо, страхові компанії повинні тісно співпрацювати з постачальниками телематичного обладнання, мобільними операторами, провайдерами хмарних сервісів і т. ін. При цьому треба враховувати той факт, що страхові компанії, які надають послуги з кіберстрахування, також можуть стати об'єктами кібератак у випадку недостатнього забезпечення їхньої інформаційної безпеки. Несвоєчасне виявлення та затримка нейтралізації витоку конфіденційної інформації, втрата інтелектуальної власності можуть спричинити більш глобальні наслідки, пов'язаних із зростанням недовіри до страхового ринку, масового розірвання укладених договорів страхування, виплати страховиками значної суми коштів у вигляді страхового відшкодування наслідків кіберкрадіжки.

Виходячи з цього, страхові компанії, що здійснюють страхування кіберризиків, повинні забезпечити надійне зберігання конфіденційної інформації, що міститься на паперових або електронних носіях, створивши відповідні служби інформаційної безпеки. До функцій останніх необхідно передати ідентифікацію внутрішніх і зовнішніх загроз, які можуть призвести до випадкових або зловмисних витоків інформації. Для забезпечення стійкості від кіберзагроз необхідно налагодити тісну співпрацю між службами безпеки страховиків і страхувальників на основі застосування сучасних технологій та пристроїв запобігання витоку даних з їхніх інформаційних систем, мінімізувавши вплив людського фактора. Без суттєвої державної фінансової підтримки, розробки державних стандартів, індикаторів та граничних значень оцінки інформаційної безпеки у сфері страхування забезпечити надійний захист інформації на практиці дуже складно.

Розвиток кіберстрахування потребує прискорення інформатизації послуг зі страхування кіберризиків. Нині дуже складно знайти інформацію про страхові компанії, що пропонують укладання полісів кіберстрахування, спектр їхніх послуг, розмір відшкодування збитків та ін. Зважаючи на це, необхідна чітка регламентація механізмів взаємодії між страховиками і страхувальниками.

Конкурентну перевагу на ринку кіберстрахування отримають страхові компанії, які при розробці методології визначення страхових тарифів і ризиків кіберстрахування будуть застосовувати актуарне моделювання на основі використання персоналізованого маркетингу, що забезпечить індивідуальний підхід до кожного клієнта за допомогою використання інтерактивних комунікацій. Також прийняття кіберризиків на страхування неможливе без застосування індивідуального андерайтингу, який включає комплекс заходів, спрямованих на збалансування інтересів страхувальника і страховика в напрямку проведення експертної оцінки таких ризиків,прогнозування ймовірності розміру потенційних збитків від настання кіберінцидентів, визначення умов страхування, розміру страхового покриття і премій.

Висновки. Інформаційні технології, що стрімко проникають в економічні й соціальні процеси, зумовлюють необхідність інноваційних змін на ринку страхування України і розвитку такого сегмента, як кіберстрахування, який забезпечує необхідний страховий захист і відшкодування суми збитку в розмірі, необхідному для компенсації витрат, пов'язаних із втратою баз даних страхувальників та їх подальшим відновленням у разі виникнення масштабних кібератак. Оскільки ринок кіберстрахування України перебуває на початковому етапі свого становлення, під час розроблення інноваційних підходів щодо його подальшого розвитку треба широко використовувати накопичений позитивний досвід багатьох країн світу, який свідчить про диверсифікацію спектра послуг кіберстрахування і застосування окремих полісів страхування від комп'ютерних злочинів, хакерських атак та покритті збитків у процесі їх настання.

Поштовхом для розвитку зазначеного ринку стане прийняття відповідних законодавчих актів у сфері забезпечення кібербезпеки на рівні держави та окремих суб'єктів господарювання, чітке визначення в Законі України «Про страхування» сутності кіберстрахування, з віднесенням його до добровільного або обов'язкового виду страхування. Діапазон кіберзлочинів достатньо широкий і коливається від отримання доступу до інформаційних баз даних, об'єктів інтелектуальної власності, втручання в діяльність комп'ютерних систем до отримання фінансової вигоди. З одного боку, необхідність кіберстрахування виникає у зв'язку з розвитком інформаційних технологій та інноваційних продуктів у різних сферах економічної діяльності, що викликає появу різноманітних кіберризиків, з іншого – кіберзлочини переважно відбуваються шляхом крадіжки інновацій або новітніх технологій. З огляду на це можна зробити висновок, що в основі розвитку кіберстрахування і зростання кіберзлочинів, особливо у фінансовій сфері, є інновації і питання тільки в тому, хто скоріше ними скористується і з якою метою. У цьому аспекті при розвитку системи страхування кіберризиків необхідно практично повністю виключити вплив людського фактора на розкриття інформації про страхувальників, створивши відповідні служби інформаційної безпеки і встановивши обмежений доступ працівників до їхніх баз даних з персональною відповідальністю виконавців. На законодавчому рівні необхідно посилити кримінальну відповідальність, зокрема і працівників страхових компаній, за продаж інформаційних баз даних клієнтів, розкриття конфіденційної інформації. Запровадження запропонованих інноваційних підходів у сукупності із забезпеченням прозорості та розширенням меж взаємодії і співробітництва страхових компаній з іншими економічними агентами приведе до диверсифікації страхових послуг і розвитку ринку кіберстрахування, що дасть змогу суттєво зменшити обсяг збитків від настання випадків кібершахрайства.

Предметом подальших досліджень у напрямку розвитку ринку кіберстрахування України стануть питання класифікації видів страхування кіберризиків, розробки методики проведення актуарних розрахунків страховими компаніями для відновлення нормального функціонування діяльності економічних агентів, державних інституцій після масштабних кібератак.

Література.

1. Forbes [2016], “Cyber Crime Costs Projected To Reach $2 Trillion by 2019”. https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7885d6313a91.

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

3. Shaun S. Wang. Integrated Framework for Information Security Investment and Cyber Insurance https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674.

4. Jay P. Kesan & Carol M. Hayes Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment 102 Minn. L. Rev. 191 (2017), University of Illinois College of Law Legal Studies Research Paper No. 17-18.

5. Yogesh Malhotra (2015). Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at-Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era, Post-Doctoral Research Thesis on Finance, Risk, and, Quant Modeling Beyond the Global Financial Crisis, Suni Polytechnic Institute, New York. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547.

6. Пікус Р. Інноваційний розвиток страхової діяльності як основа підвищення її ефективності / Р. Пікус, В. Заколодяжний // Вісник Київського національного університету імені Тараса Шевченка. Економіка. – 2015. – Вип. 3. – С. 72-80.

7. Приказюк Н. В. Нові можливості для розвитку страхової системи України / Наталія Валентинівна Приказюк, Тетяна Петрівна Моташко // Український журнал прикладної економіки. – 2016. – Том 1. – № 4. – С. 177-192.

8. Scott J. Shackelford (2012) Should Your Firm Invest in Cyber Risk Insurance? Business Horizons, http://ssrn.com/abstract=1972307.

9. Кібер-страхування: новий інструмент ризик-менеджменту [Електронний ресурс]. – Режим доступу: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu.

10. Найбільші кібератаки в Україні з 2014 року. Інфографіка [Електронний ресурс] / Журнал Новое время. – Режим доступу: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html.

11. Національний банк України [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/

12. Український страховий омбудсмен [Електронний ресурс]. – Режим доступу: http://ombudsman.ua/.

References.

1. Forbes (2016), “*Cyber Crime Costs Projected To Reach $2 Trillion by 2019*”, available at: https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#7885d6313a91 (Accessed 10 May 2018).

2. Bratiuk, V. P. (2015), “Essence of cyber crimes and insurance protection from cyber risks in Ukraine”, *Aktualni problemy ekonomiky – Actual problems of economics*, vol. *9*, pp.421 - 427.

3. Wang, S. S. (2017), “*Integrated Framework for Information Security Investment and Cyber Insurance*”, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918674 (Accessed 10 May 2018).

4. Kesan, J. P. and Hayes, C. M. (2017), “Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment”, University of Illinois College of Law Legal Studies Research Paper, vol. 17-18.

5. Malhotra, Y. (2015), “Stress Testing for Cyber Risks: Cyber Risk Insurance Modeling beyond Value-at-Risk (VaR): Risk, Uncertainty, and, Profit for the Cyber Era, Post-Doctoral Research Thesis on Finance, Risk, and, Quant Modeling Beyond the Global Financial Crisis, Suni Polytechnic Institute, New York, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2553547 (Accessed 10 May 2018).

6. Pikus, R. and Zakolodiazhnyi, V. (2015), “Innovative Development of Insurance Activity as Basis of Increasing its Efficiency”, *Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Ekonomika – Bulletin of Taras Shevchenko National University of Kyiv. Economics*, vol. *3*, pp.72–80.

7. Prykaziuk, N. V. and Motashko, T. P. (2016), “New opportunities for development of the insurance system of Ukraine”, *Ukrains'kyj zhurnal prykladnoi ekonomiky – Ukrainian Journal of Applied Economics*, vol. *1*(4), pp.177–192.

8. Shackelford, S. J. (2012), “Should Your Firm Invest in Cyber Risk Insurance”, *Business Horizons*, available at: http://ssrn.com/abstract=1972307 (Accessed 10 May 2018).

9. Hladyshevskaia, O. (2017), “Cyber Insurance: A New Risk Management Tool”, available at: http://forbes.net.ua/ua/opinions/1426423-kiber-strahuvannya-novij-instrument-rizik-menedzhmentu (Accessed 10 May 2018).

10. Novoe Vremia (2017), “The largest cyberattacks in Ukraine since 2014. Infographics”, available at: https://nv.ua/ukr/ukraine/events/najbilshi-kiberataki-proti-ukrajini-z-2014-roku-infografika-1438924.html (Accessed 10 May 2018).

11. *National Bank of Ukraine* (2018), available at: https://bank.gov.ua/ (Accessed 10 May 2018).

12. *Ukrainian Insurance Ombudsman* (2018), available at: http://ombudsman.ua (Accessed 10 May 2018).

Стаття надійшла до редакції 18.05.2018 р.