

УДК 330:101.368.02.477

DOI: 10.31673/2415-8089.2019.030412

Гудзь О.Є., д.е.н., проф.,
Державний університет
телекомунікацій

РОЗВИТОК СТРАХУВАННЯ: НОВІ ІНСТРУМЕНТИ ТА МЕТОДИ УПРАВЛІННЯ РИЗИКАМИ В ЦИФРОВІЙ ЕКОНОМІЦІ

Розглянуто значення нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки, окреслено нові загрози та ризики економічних суб'єктів, які генеруються в умовах цифрової економіки, виявлено чинники що стримують розвиток кібер-страхування та впровадження insurtech-рішень, розкрито передумови їх активізації та визначено напрями й запропоновано заходи щодо їх розширення, обґрунтовано доцільність впровадження та використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки.

Ключові слова: страхування, нові інструменти та методи страхування, управління ризиками, цифрова економіка, кібер-страхування, insurtech-рішення.

Постановка проблеми. Незважаючи на безумовні переваги цифровізації економіки (розвиток ІКТ, Dig Data, штучного інтелекту, технології блокчейну, хмарних обчислень, створення сучасних матеріалів, впровадження нових дифузних моделей управління), з'являються і новітні ризики, генеровані використанням новітніх цифрових технологій, що можуть негативно впливати на результати функціонування економічних суб'єктів. Це зумовлює впровадження та використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки. Саме тому питання, пов'язані з активізацією та розширенням можливостей нових інструментів та методів страхування їх адаптації до інноваційних перетворень в економічному просторі, набувають сьогодні особливої актуальності.

Аналіз останніх досліджень та публікацій. Окремі теоретичні положення щодо проблем впровадження та використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки розкрито у наукових розвідках таких відомих вчених, як Л. Алексеєнко, В. Базилевича, В.П. Братюк, О. Вірбулевської, С. Волосович, О.О. Гаманкової, В. Геєць, В. Диби, І. Зеліско, Ю. Кожедуб, Р. Пікус, О. Пономарьової, Н. Приказюк, Н. Прокопенко та інших учених. Проте, зважаючи на важливість та актуальність окресленої проблематики, існує необхідність більш глибокого її розкриття та розробки пропозицій щодо передумов активізації та розширення переліку нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки.

Метою статті є розгляд значення нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки, окреслено нові загрози та ризики економічних суб'єктів, які генеруються в умовах цифрової економіки, виявлено чинники що стримують розвиток кібер-страхування та впровадження insurtech-рішень, розкрито передумови їх активізації та визначено напрями й запропоновано заходи щодо їх розширення, обґрунтовано доцільність впровадження та використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки.

Виклад основного матеріалу. Визначальною ознакою цифрової економіки вважається трансформація структури та вагомості факторів виробництва, ключовим із

яких стає інформація. „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” [11].

Відбувається digital - трансформація бізнесу, що зумовлює генерування нових ризиків. „Розумні” пристрої та інноваційні послуги можуть спровокувати непередбачені негативні наслідки та появу специфічних надскладних загроз (крадіжка інформації, збої комунікацій та цілих виробничих комплексів і логістичних ланцюгів). Так, за звітними даними Міжнародного економічного форуму (World Economic Forum) по глобальним ризикам, віртуальні (кібер) ризики означені, найголовнішими комерційними ризиками. Підтверджують таке ствердження і аналітичні дані компанії Global Corporate & Specialty, які аналізували ризики щодо ведення бізнесу.

Їх дані демонструють, що кібер-ризик є найнебезпечнішими для провадження бізнесу. Так, сумарні втрати світової економіки від їх реалізації становили у 2015 році близько 445 мільярдів доларів [16, с. 10], а вже у 2017 році – 600 мільярдів доларів [18]. За аналізом Страхового брокера „ІНСАРТ” – 25 млн. дол. США – понесений збиток українським бізнесом в результаті кібер-атак, близько 50% вітчизняних компаній мали справу з кібер- атаками; більш ніж 125000 комп’ютерів було заражене внаслідок кібер-атаки вірусу Petya.A, а розмір збитків склав 466,3 млн. доларів США [18]

Більшість вчених, вважають, що кібер-ризик – це ризик, що генерується використанням: телекомунікаційного обладнання, програмного забезпечення, локальних і Інтернет-мереж, розрахунково-платіжних систем, систем інтернет-торгівлі, промислових систем менеджменту, а також це ризик, що пов’язаний з накопиченням, зберіганням, передачею і використанням персональних даних.

Змістове наповнення кібер-ризиків розкривається через їх особливості [5]:

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

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

це ризики реалізації навмисних злочинних дій за допомогою використання ІТ;

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).

Кібер-ризик проявляються внаслідок настання таких подій:

нецільові атаки (фішинг, кардинг, sms-шахрайство);

цільові атаки (фінансове шахрайство, розкрадання баз даних, промислове шпигунство, DDoS атаки, вимагання);

атаки зсередини (розкрадання, знищення інформації, сприяння цільовій атаці).

Отже, у контексті збільшення чисельності кібер-злочинів, економічним суб’єктам необхідно розробляти шляхи їх мінімізації. Для цього використовують: технологічні рішення, просвітницьку діяльність щодо протидії кібер-злочинів, профілактичні заходи та кібер-страхування.

Кібер-страхування за ствердженням Р. Беме і Г. Шварца: це передача фінансового ризику, пов’язаного з мережевими та комп’ютерними інцидентами, третій стороні [17]. Фактично, кібер-страхування – це страховий продукт, який захищає економічні суб’єкти від ризиків, що відносяться до інформаційно-комунікаційних технологій, використання Інтернет - мережі, ІКТ-інфраструктури та діяльності у кібер-просторі.

Страховий ринок змушений адекватно реагувати на окреслені digital – трансформації і широке генерування кібер-ризиків, „зادля максимального задоволення потреб і побажань своїх клієнтів з метою їх страхового захисту в частині удосконалення підходів до ведення бізнесу, розробки інноваційних каналів реалізації продуктів і надання послуг та технологій обслуговування” [9, с. 49].

Нині, рівень розвитку вітчизняного страхового ринку окреслюється: соціально-економічними реаліями в країні, готовністю економічних суб'єктів до споживання якісно нових страхових послуг, а також державною підтримкою. „Порівняно з європейськими країнами, де страхування охоплено понад 94% страхового поля, в Україні страхові послуги користуються значно меншим попитом (10–15% страхового поля), особливо у галузі майнового та окремих видів особистого страхування, що зумовлено як низькою довірою економічних суб'єктів до страховиків, так і низьким рівнем їхньої обізнаності у сфері страхування” [14]. Так, за ствердженням аналітиків, „частка страхових платежів за особистим страхуванням в Україні становить усього 4-5%, тоді як у Західній Європі та США цей вид послуг займає близько 60%, у Японії – 80%, у Великобританії – 70%, а у світі в середньому – 58,3%. Загальний обсяг страхових послуг на фінансовому ринку України в останньому десятиріччі за зібраними преміями дорівнював 0,06% світового обсягу і був меншим у 400 разів порівняно із США, у 60 разів – із Німеччиною, у 50 разів – із Францією” [7, с. 413].

Останні роки спостерігається тенденція щодо зменшення кількості страхових компаній: на початок 2018 року їх кількість склала 294, з них 33 займаються страхуванням життя (СК „Life”) та 261 ризиковими видами страхування (СК „non-Life”) [13].

Коефіцієнт концентрації страхового ринку (CR-3) по СК „Life” сягає 54,3%, а по ризиковому страхуванню – 21,3%. У Франції цей коефіцієнт по „non-life” страхуванню становить 43,37%, по страхуванню життя – 38,54%; у Великобританії – 29,83% та 18,24%; у Нідерландах – 47,36% та 48,23% відповідно [10, с. 78]. Така висока концентрація страхового ринку України вказує на те, що вітчизняна економіка переобтяжена великою кількістю страхових компаній, частка з яких навіть не здатна надавати якісні страхові послуги, розраховуватися за власними зобов'язаннями та взагалі конкурувати за хоча б невеликий сегмент ринку [3, с. 5]. Для розвитку нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки страховий ринок варто очистити від недобросовісних страховиків та запровадити жорсткіші вимоги до показників їх ліквідності, платоспроможності, розміру мінімального капіталу, що сприятиме виконанню зобов'язань у періоди кризових деформацій.

Індекс Герфіндаля-Гіршмана (ННІ) характеризує рівень конкуренції на ринку через призму його концентрації і показує розподіл „ринкової влади” між суб'єктами ринку [1, с. 302]. Для оцінки ринкової концентрації використовуються наступні діапазони даного показника: ННІ<1000 – ринок оцінюється як неконцентрований; 1000< ННІ<1800 – ринок оцінюється як помірно концентрований; ННІ>1800 – ринок оцінюється як висококонцентрований [6, с. 83-84]. В Україні по Life-страхуванню у 2017 році цей індекс склав 1417,52 (у 2016 р. – 1079,59), а по non-Life-страхуванню, відповідно – 305,27 та 280,74. Загалом по страховому ринку індекс Герфіндаля-Гіршмана у 2017 р. становив 272,07, а у 2016 р. – 245,09.

Іншим ключовим показником вважається індекс щільності страхування. Страховий захист в країні вважається належним, якщо цей показник перебільшує 140 дол. США. Акцентуємо, що „для України характерним є низький рівень поширеності страхових послуг, адже витрати однієї особи на страхування в середньому становлять 65,4 дол. США, в той час, як в Польщі показник щільності страхування має значення 140 дол. США, в Німеччині – 1482 дол. США, в Японії – 5-6 тис. дол. США” [21].

За таких умов, подією, що сприятиме зростанню 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 конфіденційності при обробці даних. Регламентні нововведення надають економічним суб'єктам ЄС більше прав на свою онлайн-інформацію і передбачають штрафи обсягом до 4% річного доходу підприємств при виявленні грубих порушень. За ствердженням страхових аналітиків, цей регламент, а також широво відомі наслідки кібератак WannaCry і NotPetya сприятимуть попиту на послуги кібер-страхування.

Так, кількість синдикатів Lloyd's, що пропонують кібер-страхування за 2016 рік зросла на 20%. За переконанням виконавчого директора Lloyd Інги Біль, щорічні прирости бруто-премії європейського кіберстрахування до 2020 року можуть скласти понад \$ 2 млрд, що сумарно становитиме близько \$ 9 млрд. Аналітики зазначають, що великі підприємства при ухваленні рішень щодо співробітництва, вимагають наявності поліса кібер-страхування у своїх контрагентів, оскільки інформаційні ресурси дорожчають, диджиталізація набирає оберти, відповідно і ймовірність фінансових і репутаційних втрат стрімко підвищується. Перспективність розвитку кібер-страхування, підтверджується і тим, що світові потужні страхові компанії вже пропонують його продукти.

Задля зростання привабливості кібер-страхування, страхові компанії розширюють страхове покриття та надають додакові послуги:

- відшкодування витрат на розслідування кібер-злочинів;
- антикризовий піар з метою відновлення репутації;
- витрати на захист у суді і відновлення роботи ІТ-системи.

Тобто використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки є вигідним при великомасштабному інциденті збою чи компрометації ІКТ-системи, та сприяє економічним суб'єктам підтримувати економічну стабільність і мінімізувати втрати.

В. Братюк акцентує, 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 [4].

Н. Приказюк вважає, що розвитку кібер-страхування заважає: невизначеність регулювання відносин у кіберстрахуванні; нестача інформації для проведення актуарних розрахунків; концентрація ризиків у разі настання страхового випадку [15]. Окрім того, відсутня необхідна статистика, законодавча база, судова практика, недостатньо і кваліфікованих фахівців, що мають уявлення про даний вид ризику та його структуру [8].

Проведені дослідження дозволяють стверджувати, що в Україні розвиток кібер-страхування гальмується:

- відсутністю фінансово потужно страхових компаній здатних прийняти кібер-ризик;
- браком належної нормативної підтримки;
- відсутність адекватних методик щодо ідентифікації, оцінки та систематизації кібер-ризиків;
- браком достатньої статистичної та інформаційної бази для проведення актуарних розрахунків, що унеможливорює встановлення тарифів на продукти кібер-страхування;
- відсутність платоспроможних страхувальників, які мають можливість придбати продукти кібер-страхування;
- нормативна невизначеність статусу цифрових активів.

Нині, вітчизняні страхові компанії оцінюють кібер-ризик економічних суб'єктів за допомогою непрямих ознак, показників і характеристик, серед них: наявність ризик-менеджменту, наявність служб економічної та інформаційної безпеки, способи і технології зберігання конфіденційних даних, частота проведення тестування та аудиту безпеки інформаційних потоків та комунікаційних ланцюгів, кількість ІТ-спеціалістів тощо.

Водночас, у цій площині, як позитив, слід відмітити диджиталізацію страхових компаній, що дозволяє їм надавати персоналізовані послуги через зручні канали для страхувальників та ширше використання програм лояльності.

За даними Gartner „Hyper cycle for property & casualty (P&C) insurance” хмарні обчислення (cloud computing) входять до п'ятірки найбільш пріоритетних ІТ-рішень серед страхових компаній. А, за даними Gartner, 41% страхових компаній вже використовують хмарні обчислення в своїй діяльності, ще 41% впроваджує чи планує впровадити хмарні технології в наступні 6-12 місяців. За прогнозами Gartner хмарні технології будуть широко використовуватися в страховій галузі в наступні 5-10 років [20, с.7].

25% страхувальників бажає купити страхове покриття онлайн. Нині, характерна пряма залежність між рівнем розвитку страхового ринку та часткою каналу онлайн-продажів страхових послуг серед інших каналів збуту. На розвинутих ринках частка агентського каналу складає 50-60%, на середньорозвинутих – 60-70%, на нерозвинутих – 80-90% [12].

Варто виділити наступні ключові тенденції щодо розширення каналів продажу страхових продуктів:

зростання ролі Інтернет-мережі;

широке використання різних соціальних мереж, як альтернативних каналів дистрибуції;

використання хмарних технологій, SaaS рішень тощо;

автоматизація бізнес-процесів (андерайтингу, врегулювання збитків тощо) та збільшення частки прямих продажів.

Серед ключових чинників, що сприяють нарощенню частки онлайн страхування є:

можливість обрання персоніфікованих страхових продуктів;

низька вартість страхового продукту з високою якістю;

можливість порівняння страхових продуктів страхувальниками;

зручність для споживачів.

У Великобританії понад 20% акумульованих страхових премій приходиться на онлайн-канал [2].

Водночас, слід зауважити, що вітчизняним страховим компаніям варто переймати світовий досвід для розробки пропозицій із кібер-страхування. Так, цікавим у цій площині є поліс CyberEdge від American International Group (AIG), який нині вважається вершиною розвитку кібер-страхування. Визиває інтерес, те що за даними TechCrunch, компанії Apple і Cisco уклали угоду про партнерство із страховою компанією Allianz. І тепер економічні суб'єкти, які використовують технології Apple і Cisco, мають можливість укладати більш вигідні договори з кібер-страхування з Allianz.

І сьогодні, завдяки диджиталізації страхового сегменту економічного простору генерується якісно нова сфера – insuretech, як синтез сучасних цифрових технологій і традиційного страхування. Insuretech – це технології, які зосереджені на розробці страхових IT-рішень. До них відносять сервіси для споживачів та нові інструменти для роботи страховиків.

За інформацією IBM – 81% потужних успішних страхових компаній вже співпрацюють з insuretech-проектами, і 45% інших страховиків. Це підтверджує тезу, що для розвитку і успішного функціонування, страховим компаніям необхідні сучасні цифрові технології.

За ствердженням McKinsey, найбільш популярними технологічними рішеннями в insuretech-проектах є: мікрострахування (3%), блокчейн (4%), P2P (4%), робо-едвайзер (10%), гейміфікація (10%), страхування для IoT-сфери (12%), страхування на основі використання (13%), великі дані і машинне навчання (20%).

У звіті 2018 року, Edelman Trust Barometer експерти 2017 рік означають роком кризи довіри, а 2018 рік – роком битви за правду. Вірогідно, insuretech допоможе у цій битві.

Штучний інтелект, машинне навчання та аналіз великих даних — мають великий потенціал щодо поліпшення страхового захисту економічних суб'єктів. Big data допоможе страховикам краще ідентифікувати й оцінити ризики. Робо-едвайзер на основі AI і machine learning допоможуть з рутинними завданнями: консультування, підбір пропозицій і рішень, оформлення необхідних документів. Нині, об'єктом страхування стає не лише майно, а й інформація. Саме це є прикметною ознакою трансформації страхового сегменту. За дослідженнями PwC, від кіберзлочинів світова економіка втрачає 400 млрд дол на рік, і цей показник буде зростати. Для порівняння (за інформацією Time з посиланням на SpaceX): запуск ракети Falcon 9 коштує 62 млн дол, а Falcon Heavy – 90 млн дол. Вочевидь, що захищати свої бізнесові та приватні інтереси економічні суб'єкти без нових інструментів та

методів страхування для управління ризиками в умовах цифрової економіки та без insuretech-рішень не зможуть.

Адаптація страхового ринку до змін, пов'язаних із диджиталізацією економічних суб'єктів, зміною дизайну страхових інструментів, впровадженням цифрових технологій в організацію страхової індустрії і кібер-страхування, сприятиме підвищенню якості страхового захисту й стабільному прибутковому функціонуванню економічних суб'єктів, стимулюванню впровадження нових інструментів, методів, технологій і insuretech-рішень, урізноманітненню спектру страхових продуктів, удосконаленню форм і методів страхового нагляду тощо.

Висновки. У статті розглянуто значення нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки, окреслено нові загрози та ризики економічних суб'єктів, які генеруються в умовах цифрової економіки, виявлено чинники що стримують розвиток кібер-страхування та впровадження insuretech-рішень, розкрито передумови їх активізації та визначено напрями й запропоновано заходи щодо їх розширення, обґрунтовано доцільність впровадження та використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки. Зокрема, наголошено, що Адаптація страхового ринку до змін, пов'язаних із диджиталізацією економічних суб'єктів, зміною дизайну страхових інструментів, впровадженням цифрових технологій в організацію страхової індустрії і кібер-страхування, сприятиме підвищенню якості страхового захисту й стабільному прибутковому функціонуванню економічних суб'єктів, стимулюванню впровадження нових інструментів, методів, технологій і insuretech-рішень, урізноманітненню спектру страхових продуктів, удосконаленню форм і методів страхового нагляду тощо.

Надані пропозиції дозволять сформуванню передумови для активізації та розширення обсягів використання нових інструментів та методів страхування для управління ризиками в умовах цифрової економіки, що сприятиме підвищенню якості страхового захисту й конкурентоспроможності та нарощенню конкурентних переваг на вітчизняних та світових ринках усіх економічних суб'єктів.

Список використаної літератури

1. Абакуменко О.В. Моделирование рівня конкуренції на фінансовому ринку України. *Бізнесінформ*. 2013. № 5. С. 302–310.
2. Аккозов Б. Страховщики РК готовы к online-страхованию, а законодательство – нет: URL: http://www.kursiv.kz/news/details/finansy/strakhovshchiki_rk_gotovy_k_online_strakhovaniyu_a_zakonodatelstvo_net/
3. Базилевич В.Д. Новітні тенденції та протиріччя на страховому ринку України. *Вісник Київського національного університету імені Тараса Шевченка. Економіка*. 2012. Вип. 133. С. 5- 8.
4. Братюк В.П. Сутність кібер-злочинів та страховий захист від кібер-ризиків в Україні. *Актуальні проблеми економіки*. 2015. № 9. С. 421-427.
5. Воронова Т. Безопасный интернет URL: <http://ru.calameo.com/books/002793881c6046eb0d2fb>
6. Гаманкова О.О. Інформаційні вади дослідження ступеня монополізації ринку страхових послуг України. *Актуальні проблеми економіки*. 2009. № 10. С. 80 – 87.
7. Золотарьова О.В. Ключові тенденції та пріоритети розвитку ринку страхових послуг в Україні *Економіка і суспільство*. 2017. №11. С. 413-420.
8. Ивашенко А.Н., Шарко И.А. Мировой рынок страхования кибер-рисков: перспективы и препятствия для развития в Республике Беларусь. «*Национальная экономика Республики Беларусь: проблемы и перспективы развития*» материалы IX междунар. науч.-практ. конф. студентов. г. Минск: БГЭУ, 2016. С. 196–202.

9. Кулина Г. Світовий ринок страхових послуг в умовах зміни парадигми глобального економічного розвитку. *Світ фінансів*. 2017. № 3(52). С. 48-59.
10. Малікова І.П. Оцінка концентрації страхового ринку України, її зв'язок з процесами монополізації та конкуренції. *Науковий вісник Херсонського державного університету. Серія «Економічні науки»*. 2017. Вип. 23. С. 76-79.
11. На порозі «цифрового майбутнього». / за ред. А.В. Кешелава, В.Г. Буданов, В.Ю. Румянцев и др. ВНИИГеосистем, 2017. 28 с.
12. Павлова О. Страховий бізнес берет курс на інновації URL: <http://www.pcweek.ru/idea/article/detail.php?ID=123103>.
13. Підсумки діяльності страхових компаній за 2017 рік. URL: https://www.nfp.gov.ua/files/OgliadRinkiv/SK/2017_rik/sk_%202017.pdf
14. Пономарьова О.Б. Визначення проблем страхового ринку та їх вирішення. *Глобальні та національні проблеми економіки*. 2015. №5. URL: <http://global-national.in.ua/issue-5-2015>
15. Приказюк Н.В. Прогресивний досвід зарубіжних країн у вирішенні проблем розвитку кіберстрахування. *Вісник Одеського національного університету. Серія: «Економіка»*. 2016. Вип. 2. С. 164-168.
16. Allianz Risk Barometer Top Business Risks 2016. URL: <http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf>
17. Böhme R., Schwartz G. (2010) Modeling cyber-insurance: towards a unifying framework. WEIS. URL: http://econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf.
18. 2018.iforum.ua/ru/speakers/alexandra-gladyshevskaya/ Marotta A. A Survey on Cyber-Insurance. Marotta A., Martinelli F., Nanni S., Yautsiukhin A. Bologna, Italy: Unipol Gruppo Finanziario S.p.A.
19. The digital insurer. A new era in insurance: Cloud computing changes the game. *Accenture*.
20. World insurance in 2015: steady growth amid regional disparities. URL: http://media.swissre.com/documents/sigma_3_2016_en.pdf.

REFERENCES

1. Abakumenko, O.V. (2013) Modeluvannya rivnya konkurencii na finansovomu rynku Ukrainy [Modelling the level of competition at the financial market of Ukraine]. *Businessinform*, (5), 302–310.
2. Akkozov, B. Strahovschiki RK gotovy k online-strahovaniu, a zakonodavstvo – net [LCD Insurance ready for online-strahovaniu, and legislation-no]. Retrieved from http://www.kursiv.kz/news/details/finansy/strakhovshchiki_rk_gotovy_k_onlin_e_strahovaniyu_a_zakonodatelstvo_net/
3. Bazilevich, V.D. (2012) Novitni tendencii ta protyrichchya na strahovomy rynku Ukrainy [New trends and contradictions at the insurance market of Ukraine]. *Bulletin of Taras Shevchenko National University of Kyiv. Economy*, (133), 5- 8.
4. Bratuk, V.P. (2015) Sutnist kiber-zlochyniv ta strahovyi zahyst vid kiber-ryzykiv v Ukraini [The essence of cyber crimes and the insurance coverage against cyber risks in Ukraine]. *Actual problems of economics*, (9), 421-427.
5. Voronova, T. Bezopasnyi internet [Safe internet]. Retrieved from <http://ru.calameo.com/books/002793881c6046eb0d2fb>
6. Gamankova, O.O. (2009) Informaciini vydy doslidzhennya stupenya monopolizacii rynku strahovyh poslug Ukrainy [Information issues of the degree of monopolization of the insurance services market of Ukraine]. *Actual problems of economics*, (10), 80 – 87.
7. Zolotareva, O.V. (2017) Kluchovi tendencii ta priorityty rozvytku rynku strahovyh poslug v Ukraini [Key trends and priorities of the insurance market development in Ukraine]. *Economy and society*, (11), 413-420.
8. Ivaschenko, A.N., Sharko I.A (2016) Mirovoi rynek strahovaniya kiber-riskov: perspektivy I prepyatstviya dlya razvitiya v Respublike Belarus [The global cyber risk insurance market: perspectives and obstacles for development in the Republic of Belarus].

prospects and obstacles for development in Republic Belarus. *Materials of the IX International Scientific and Practical Conference of Students "National Economy of Republic Belarus: Problems and Prospects for Development."* Minsk: BGAU.

9. Kutlina, G. (2017) Svitovyi rynek strahovyh poslug v umovah zminy paradygmy globalnogo ekonomichnogo rozvytku [The insurance market in the context of changing the paradigm of global economic development]. *World of Finance*. (3(52)), 48-59.
10. Malikova, I.P. (2017) Ocinka koncentracii strahovogo rynku Ukrainy, ii zvyazok z procesamy monopolizacii ta konkurencii [Estimation of concentration of insurance market of Ukraine, its connection with monopolization and competition processes]. *Kherson State University Scientific Herald. Series "Economic Sciences"*, (23), 76-79.
11. Na poroge "cyfrovogo budushchego" [On the cusp of a "digital future"]. A. V. Keshelava, V.G. Budanov, V.U. Romyancev and other (2017). VNIIGeosystem.
12. Pavlova, O. Strahovoi biznes beret kurs na innovacii [The insurance business directs to innovations]. Retrieved from <http://www.pcweek.ru/idea/article/detail.php?ID=123103>.
13. Pidsumky diyalnosti strahovyh kompanii za 2017 rik [Results of insurance companies activity for 2017 year]. Retrieved from https://www.nfp.gov.ua/files/OgliadRinkiv/SK/2017_rik/sk_%202017.pdf.
14. Ponomareva, O.B. (2015) Vyznachennya problem strahovogo rynku ta ih vyrishennya [Defining the problems of the insurance market and solving them]. *Global and national problems of the economy*, (5). Retrieved from <http://global-national.in.ua/issue-5-2015>
15. Prykazuk, N.V. (2016) Progresyvnyi dosvid zarubighnyh krain u vyrishenni problem rozvytku kiberstrahuvannya [Progressive experience of foreign countries in solving problems of cyber insurance]. *Bulletin of the Odessa National University. Series: "Economics"*, (2), 164-168.
16. Allianz Risk Barometer Top Business Risks 2016. Retrieved from <http://www.agcs.allianz.com/assets/PDFs/Reports/AllianzRiskBarometer2016.pdf>
17. Böhme, R., Schwartz, G. (2010) Modeling cyber-insurance: towards a unifying framework. WEIS. Retrieved from http://econinfosec.org/archive/weis2010/papers/session5/weis2010_boehme.pdf.
18. 2018.iforum.ua/ru/speakers/alexandra-gladyshevskaya/ Marotta A. A Survey on Cyber-Insurance. Marotta A., Martinelli F., Nanni S., Yautsiukhin A. Bologna, Italy: Unipol Gruppo Finanziario S.p.A.
19. The digital insurer. A new era in insurance: Cloud computing changes the game. *Accenture*.
20. World insurance in 2015: steady growth amid regional disparities. Retrieved from http://media.swissre.com/documents/sigma_3_2016_en.pdf.

ГУДЗЬ ЕЛЕНА ЕВГЕНЬЕВНА. РАЗВИТИЕ СТРАХОВАНИЯ: НОВЫЕ ИНСТРУМЕНТЫ И МЕТОДЫ УПРАВЛЕНИЯ РИСКАМИ В ЦИФРОВОЙ ЭКОНОМИКЕ. Рассмотрены значение новых инструментов и методов страхования для управления рисками в условиях цифровой экономики, определены новые угрозы и риски экономических субъектов, которые генерируются в условиях цифровой экономики, выявлены факторы которые сдерживают развитие кибер-страхования и внедрение insuretech-решений, раскрыты предпосылки их активизации и определены направления и предложены меры по их расширению, обоснована целесообразность внедрения и использования новых инструментов и методов страхования для управления рисками в условиях цифр вой экономики.

Ключевые слова: страхование, новые инструменты и методы страхования, управления рисками, цифровая экономика, кибер-страхование, insuretech-решения.

GUDZ OLENA. INSURANCE DEVELOPMENT: NEW INSTRUMENTS AND METHODS OF RISK MANAGEMENT IN THE DIGITAL ECONOMY. *The importance of new insurance tools and methods for risk management in the digital economy is considered, new threats and risks of the economic entities that are generated in the digital economy are identified, factors that constrain the development of cyber insurance and implementation of insuretech solutions are revealed, the preconditions for their recognition are revealed directions and proposed measures to expand them, the feasibility of introducing and using new insurance tools and methods for risk management in digital terms is substantiated in economy.*

Key words: *insurance, new tools and methods of insurance, risk management, digital economy, cyber insurance, insuretech solutions.*