Oliynik L. A.
National University of Life and Environmental Sciences of Ukraine
Dobrivskyi V. H.
Separated Structural Subdivision of
National University of Life and Environmental Sciences of Ukraine
«Boyarka College of Ecology and Natural Resources»

FINANCIAL MONITORING FEATURES FOR EDUCATION AND RESEARCH FARMS OF AGRICULTURAL BUDGETARY INSTITUTIONS

Summary
The article highlights the financial monitoring features and offers the basic indicators of its implementation at education and research farms of agricultural budgetary institution. The case study for its peculiarities defined is Separated Subdivision of NULES of Ukraine «Velykosnytinske Education and Research Farm named after O. Muzychenka», the financial monitoring of which allowed offering the enterprise certain directions to improve efficiency under modern conditions. While carrying out financial monitoring of education and research farms, there should be awareness that such farms are based on self-supporting, being non-profit institutions that function as public institutions. Consequently, they make estimates. The specific features of financial statements and reports are due to the fact that revenues of educational and research farms are derived from the special fund. Financial monitoring for education and research farms of agricultural budgetary institution is proven to be implemented by using traditional analysis given the peculiarities of budgetary institutions.
Keywords: financial monitoring, education and research farm, budgetary institution, cost accounting, special fund, estimate.

УДК 368.8

Приказюк Н. В.
Кукурудзяк М. В.
Київський національний університет імені Тараса Шевченка

ПРОГРЕСИВНИЙ ДОСВІД ЗАРУБІЖНИХ КРАЇН У ВИРІШЕННІ ПРОБЛЕМ РОЗВИТКУ КІБЕРСТРАХУВАННЯ

Досліджено сутність кіберстрахування та визначено ризики, на випадок яких здійснюється кіберстрахування. Виявлено проблеми, що стримують розвиток кіберстрахування у світі. На основі прогресивного досвіду розвинених зарубіжних країн узагальнено способи вирішення виявлених проблем.
Ключові слова: кіберстрахування, кіберризики, безпека даних, державне регулювання у сфері безпеки особистих даних, повідомлення про порушення безпеки даних, перестрахування кіберризиків, інформаційне забезпечення кіберстрахування.

Постановка проблеми. Питання захисту конфіденційної інформації та особистих даних сьогодні стоїть як ніколи гостро. Будь-яка компанія, що здійснює обробку електронних персональних даних із використанням портативних пристроїв, комп'ютерів, серверів, Інтернет-ресурсів, піддається ризикам кібератак. У звіті Allianz Risk Barometeron Top Business Risks 2015 [1] кіберризики займають п'яте місце серед найнебезпечніших для бізнесу і водночас є найбільш недооціненими.

Страхування не може запобігти витоку інформації, але воно є важливим інструментом мінімізації негативного впливу кібератак на діяльність компаній.

Світовий ринок кіберстрахування перебуває на стадії становлення, оскільки в більшості країн ще не створено сприятливих умов для його розвитку.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження сутності страхової діяльності і різних видів страхових послуг та їхнього розвитку на сучасному етапі зробили такі вітчизняні науковці, як В.Д. Базилевич, Н.М. Внукова, О.О. Гаманкова, Ю.П. Гришан, О.М. Залєтов, А.Д. Заруба, С.С. Осадець, Р.В. Пікус, а також зарубіжні вчені: Дж. Арчі, К. Сарда, Дж. Фінкл. Разом із тим проблеми, які стосуються кіберстрахування, залишаються недостатньо вивченими.

Виділення невирішених раніше частин загальної проблеми. У наукових публікаціях часто проводиться аналіз ризиків у кіберстрахуванні та характеристика їхнього небезпечного впливу на діяльність компаній, види покриття, яке пропонують страховики, тенденції розвитку ринку. Існує потреба у визначенні проблем, які перешкоджають ефективному розвитку ринку кіберстрахування, та пошуку способів їхнього вирішення.

Мета статті полягає у виявленні проблем, що стримують розвиток кіберстрахування у світі, та визначенні способів їхнього вирішення на основі прогресивного досвіду зарубіжних країн.

Виклад основного матеріалу дослідження. Кіберстрахування являє собою спосіб управління ризиками щодо захисту персональних даних від наслідків їхнього витоку чи незаконного використання. Об'єктом такого страхування є майнові інтереси, пов'язані з ризиком настання відповідальності за порушення конфіденційності даних третіх осіб, ризиком сплати штрафних санкцій через таке порушення, недоотримання доходу у зв'язку з перериванням роботи компанії, пошкодження ІТ-інфраструктури компанії тощо.

Кіберризики – найскладніші та найбільш системні ризики, з якими стикаються компанії, що зберігають персональну інформацію, укладають угоди через мережу чи просто використовують

Інтернет у своїй діяльності. Вони можуть виникати в результаті дій держав, терористів, злочинців, інсайдерів. Інциденти, пов'язані з витоком даних, як правило, викликають ланцюгову реакцію і завдають значних репутаційних і фінансових збитків.

Кіберстрахування – швидкозростаюча галузь страхування. Згідно з прогнозом Price waterhouse Coopers, світовий ринок кіберстрахування до 2020 р. досягне в річному обсязі продажів 7,5 млрд. дол. США у порівнянні з 2,5 млрд. дол. США минулого року. У доповіді також зазначається, що кількість кібератак у 2015 р. досягла 42,8 млн., що на 48% більше, ніж у 2013 р., а кожен випадок порушення безпеки даних обійшовся американським компаніям у середньому 6,53 млн. дол. США, британським – 3,72 млн. дол. США. Ці витрати включали сплату штрафів, відновлення репутації, комерційні збитки, а також відновлення IT-інфраструктури компаній [9].

На сьогодні переважну більшість страхових платежів на світовому ринку кіберстрахування отримують компанії, зареєстровані у США (90–95%), а кількість застрахованих підприємств (великих і середніх за розміром) – близько 40%, тоді як у Великобританії ця частка складає лише 13% [10].

Розвиток кіберстрахування залежить від багатьох факторів.

На нашу думку, одна з основних проблем, що є бар'єром для ефективного функціонування ринку, – відсутність державного регулювання відносин, що лежать в основі кіберстрахування. Відносини, що лежать у основі кіберстрахування – це відносини між державою і суб'єктами господарювання щодо оперування (зберігання, використання, захисту, повідомлення про втрату, знищення) особистих даних. Державне регулювання таких відносин проявляється у вигляді прийняття державою нормативно-правових актів, визначення стандартів, установлення санкцій за порушення вимог.

На сьогодні США є лідером світового ринку кіберстрахування через налагоджену систему захисту приватної інформації та реагування на випадки порушення її конфіденційності.

До основних федеральних нормативних актів із питань кібербезпеки належать:

– Закон про фінансову модернізацію (Закон Гремма-Ліча-Блайлі), згідно з яким фінансові установи повинні захищати інформацію про клієнтів (1999 р.);

– Закон про уніфікацію й облік даних в області медичного страхування (HIPAA), де містяться рекомендації про повідомлення споживачів, коли безпека їхньої приватної медичної інформації була порушена (1996 р.);

– Закон про управління безпекою федеральної інформації (FISMA) – вимоги про захист інформації державними установами (2002 р.) [6].

Ці нормативні акти встановили, що медичні організації, фінансові установи та федеральні відомства повинні захищати інформацію, якою вони оперують.

Згодом із метою вдосконалення законодавства про кібербезпеку, федеральний уряд прийняв кілька нових законів, а також вніс зміни до тих, які були прийняті раніше, для покращання системи безпеки. Це, наприклад, Федеральний закон про порушення умов обміну даними від 2015 р., який зобов'язує біржу медичного страхування повідомляти кожного індивіда, чия персональна інформація була порушена або до якої був наданий несанкціонований доступ, якомога швидше, але не пізніше ніж через 60 днів після виявлення порушення.

Так, уперше страховий продукт у сфері кіберстрахування у США був запропонований ще в 1999 р. після внесення першого законопроекту щодо недоторканості приватного життя і захисту даних. Законодавче закріплення цих відносин створило попит на кіберстрахування, оскільки компанії передбачали, що будуть нести значні витрати, якщо порушать закон, а страхування – спосіб мінімізувати такий ризик.

Нині в 47 із 50 штатів ефективно діють і місцеві нормативні акти про захист даних, що містять положення про обов'язкове повідомлення компетентних органів у разі витоку даних. Закони про порушення умов обміну даними встановлюють стандарти, в яких визначаються:

- сторони, що повинні подати та отримати повідомлення;
- інформація, яка вважається особистою або конфіденційною;
- методи і терміни для подачі повідомлення;
- вимоги до змісту повідомлення;
- покарання за порушення закону.

Каліфорнія стала першим штатом, в якому було впроваджено закон про порушення умов обміну даними. Згідно з даним законом, будь-яка фізична або юридична особа, яка веде бізнес у штаті Каліфорнія і яка володіє або надає право використання автоматизованих даних, які включають у себе особисту інформацію, зобов'язана повідомляти про витік персональних даних. «Порушення безпеки системи» визначається як «несанкціоноване придбання автоматизованих баз даних, що ставить під загрозу безпеку, конфіденційність, або цілісність особистої інформації, яку використовує фізична або юридична особа». Повідомлення про порушення повинно бути здійснене в найбільш короткі терміни і без необґрунтованих затримок. Воно може бути подане у письмовому чи електронному вигляді, а також у вигляді «еквівалентного повідомлення». «Еквівалентне повідомлення» здійснюється, якщо вартість порушень перевищує 250 тис. дол. США або шкоди зазнало більше 500 тис. осіб. У такому випадку компанія зобов'язана повідомити через електронну пошту всіх осіб, безпека даних яких порушена, зробити заяву про інцидент на власному Інтернет-сайті і повідомити Головне управління засобів масової інформації [10].

Деякі штати встановлюють строгі часові обмеження щодо терміну подання повідомлення про витік даних. Так, законодавство штату Вермонт вимагає від постраждалих компаній робити попереднє подання про інцидент у Генеральну прокуратуру протягом 14 робочих днів із дня його виникнення. Законодавство штату Флорида встановлює термін у 30 днів, щоб повідомити осіб, безпека особистої інформації яких була порушена, та Управління з правових справ штату. Очевидно, що кожен нормативний акт містить жорсткі санкції в разі недотримання його положень.

Оскільки держава накладає значні фінансові санкції за втрату приватної інформації клієнтів, кіберстрахування стає важливим інструментом управління такими ризиками.

Ще однією запорукою успішного розвитку ринку кіберстрахування є встановлення державою конкретних стандартів щодо захисту даних. Стандарти кібербезпеки постійно розвиваються і

в деякій мірі специфічні для кожної галузі. Так, для медичних організацій це стандарти використання інформаційних технологій у галузі охорони здоров'я (HITECH), де визначаються вимоги до способу користування та рівня безпеки інформації про стан здоров'я; для компаній, які приймають кредитні та дебетові карти, – Стандарти захисту даних при використанні платіжних карт (PCI DSS) та ін.

Частина стандартів мають лише рекомендаційний характер (тобто не є обов'язковими). Однак страхові компанії, посилаючись на ці положення, можуть стимулювати прийняття та дотримання їх компаніями (наприклад, як обов'язкової умови отримання полісу страхування), що загалом покращить захищеність персональних даних.

Внутрішня безпека мережі будь-якої організації, яка зберігає особисту інформацію про клієнтів, відіграє чи не найважливішу роль при визначенні розміру покриття та вартості страхового продукту. Так, наприклад, страхова компанія American International Group пропонує максимальне кіберпокриття в розмірі 75 млн. дол. США тільки для провідних світових банків, що мають найкраще сформовані системи безпеки мереж та пом'якшення пливу кіберризиків [5].

Слід зазначити, що сектор фінансових послуг у США є однією з найбільш обізнаних і захищених галузей, які зіштовхуються з кіберзагрозами, але одночасно і найбільшою мішенню для злочинів [4].

Досвід США свідчить, що наявність державного регулювання у сфері порушення безпеки особистих даних сприяє ефективному розвитку кіберстрахування. Для страховика – окреслює стандарти, вимоги до захисту інформації, на які він посилається при визначенні умов страхування, а також у разі виявлення причини настання інциденту витоку даних. З іншого боку, значні санкції за порушення положень законодавства стимулюють організації придбати страховий захист.

Натомість поза межами США навіть у розвинених країнах державне регулювання відносин у сфері кіберстахування перебуває на стадії становлення. Часто існує законодавство про захист персональних даних, однак спеціальні норми щодо обов'язку інформувати уповноважені органи про кібератаку відсутні.

У 2013 р. ЄС прийняв стратегію кібербезпеки щодо реформування системи захисту персональних даних. Пакет реформ включає Загальне законодавство щодо захисту даних (The General Data Protection Regulation) та Директиву про захист даних для поліції та сектору кримінального правосуддя [8].

Загальне законодавство щодо захисту даних – це настанови, за допомогою яких Єврокомісія має намір посилити й уніфікувати захист даних для фізичних осіб у межах Європейського Союзу. Основними завданнями є надання громадянам можливості контролю своїх особистих даних і спрощення регуляторного середовища для міжнародного бізнесу шляхом уніфікації даного законодавства в межах ЄС.

Прийняття законодавства очікується в 2016 р. Положення вимагатимуть обов'язкової реєстрації в компетентному органі зламів баз даних для всіх учасників ринку. Згідно з проектом, компанії будуть зобов'язані повідомляти про кібератаку протягом 72 годин, а у випадку доведення, що витік інформації спричинений із вини самої компанії, накладатимуться штрафні санкції [8].

Важливим елементом реформи є можливість накладати значні штрафи в разі порушення закону – до 5% річного обороту організації. Так, нещодавно компанія Google була оштрафована на суму 900 тис. євро за порушення в Іспанії правил захисту даних, у той час як за новою реформою сума штрафу в такій ситуації досягла би 750 млн. євро.

На сьогодні обов'язок повідомлення про злам даних уже існує для операторів послуг зв'язку: компанія повинна відзвітуватись регулюючому органу про інцидент протягом 24 годин і «без невиправданої затримки» повідомити власників даних, коли це порушення «ймовірно може вплинути на порушення приватності цієї особи».

У США прийняття подібного законодавства стало поштовхом до стрімкого розвитку ринку кіберстрахування, і, ймовірно, після прийняття вищеописаної реформи на європейському ринку активізується як пропозиція продуктів кіберстрахування, так і попит на них.

Законодавство про обов'язкове повідомлення компетентних органів про інциденти витоку персональних даних уже ефективно впроваджене в Австралії (повідомлення Управління у сфері інформації (Office of the Australian Information Commissioner) відповідно до Закону про конфіденційність від 1988 р., Закону про свободу інформації від 1982 р. та ін.), Сінгапурі (повідомлення Комісії із захисту персональних даних (The Personal Data Protection Commission) відповідно до Закону про захист особистих даних від 2014 р.) та інших розвинених країнах.

Наступною проблемою, що стримує успішний розвиток кіберстрахування, є загроза концентрації кіберризиків.

Оскільки комп'ютерні системи є взаємозалежними і стандартизованими, вони особливо вразливі до корельованих утрат такого роду. Так звані «кібер-урагани» несуть невизначений ризик дуже великих утрат, не мають територіальних меж і важко піддаються прогнозуванню. Крім того, «кібер-урагани» піднімають бар'єр для виходу на страховий ринок, тому що страховику необхідно мати сформовані значні страхові резерви.

Як правило, страхові компанії використовують перестрахування в якості захисту від дуже великих потенційних виплат, і в таких випадках перестраховики допомагають запобігти концентрації ризиків. Однак ціна такого перестрахування висока, і це відображається на вартості полісів страхування.

Своєю чергою, перестраховики встановлюють відносно низькі ліміти для кіберстрахування, щоб обмежити свої ризики, тим самим не завжди дозволяючи компаніям придбати бажаний розмір покриття.

Держава може допомогти вирішити цю проблему, ставши перестраховиком для компаній, що здійснюють кіберстрахування. Це зробить їхні продукти більш прийнятним для клієнтів за рахунок зниження ціни, а зниження ціни призведе до зростання конкуренції на ринку.

У США існує основа для такого перестрахування – Закон про страхування від тероризму, прийнятий у 2002 р. Згідно з нормативним актом, держава протягом певного періоду компенсує частину страхових виплат страховикам, які зазнають значних витрат через виплату страхових відшкодувань, спричинених терористичним актом. Закон створив так звану федеральну «подушку безпеки» для страхових виплат у зв'язку з актами тероризму.

Програма реалізується після визнання страхового випадку терористичним актом (масш-

табні кібератаки підпадають під дану категорію). Утрати від такого випадку повинні перевищувати 100 млн. дол. США, розмір франшизи – 20%. У випадку реалізації програми федеральний уряд компенсує виплатити 85% застрахованих ризиків, що перевищує франшизу страховика, а страховик – 15%. Максимальний розмір такого страхового покриття становить 100 млрд. дол. на рік [6].

Таким чином, держава в ролі перестраховика допоможе страховим компаніям упоратись із ланцюговою реакцією кіберризиків. Окрім того, наявність гарантованого перестрахування з великими лімітами дасть можливість страховикам пропонувати програми страхування з більшим розміром покриття. Завдяки участі в державній програмі перестрахування страхові компанії сформують достатні власні резерви, щоб у подальшому впоратися з такими ризиками самостійно.

Нестача статистичної інформації для проведення актуарних розрахунків – наступна важлива проблема в кіберстрахуванні. Із цієї причини ризики, на випадок яких здійснюється страховий захист, важко піддаються кількісній оцінці, прогнозуванню, виникають проблеми при визначенні ціни та розміру страхового покриття.

На сьогодні у США ефективно діє Закон про обмін інформацією в області кібербезпеки (CISA) від 2015 р., головною метою якого є підвищення кібербезпеки за допомогою покращання обміну інформацією про кіберзагрози між урядом, технологічними та виробничими компаніями. Також Національна асоціація страхових комісарів (The National Association of Insurance Commissioners – NAIC) працює над розробкою нових вимог до звітності страхових компаній для полегшення оцінки ризиків у кіберстрахуванні (метою напрацювань є створення бази даних з інформацією від страховиків про деталі страхових випадків, з якими довелось зіштовхнутись). Підвищення обізнаності та здатності аналізувати ризик допоможе страховим компаніям формувати оптимальну цінову політику, пропонувати різноманітні види покриття.

Ризики, з якими стикаються страхові компанії в питаннях власної кібербезпеки, безумовно, є значними, ураховуючи характер та обсяг даних, необхідних для ведення бізнесу. Оскільки більшість персональних даних користувачів у фінансовому секторі та медичні дані (у медичному страхуванні) усе частіше зберігаються в електронному вигляді, організація ризик-менеджменту у страхових компаніях обов'язково повинна містити управління кіберризиками.

Порушення умов обміну даними, які набули широкомасштабного характеру, змусили законодавців сприяти удосконаленню умов захисту страховиків проти кібератак.

Так, Національна асоціація страхових комісарів сформувала Цільову групу з питань кібербезпеки в листопаді 2014 р. [2]. Це була перша спроба створити державний регулятор в області кібербезпеки страхових компаній. Діяльність NAIC зосереджена у трьох напрямках:

- захист власних даних;
- стимулювання страховиків захищати свої дані належним способом;
- нагляд за розвитком ринку кіберстрахування.

У 2015 р. Цільова група з питань кібербезпеки прийняла Принципи ефективного регулювання страхування кіберризиків (Principles for Effective Cybersecurity Insurance Regulatory Guidance) [3]. Положення містить 12 принципів, які служать основою для захисту конфіденційної інформації про осіб, що зберігається у страховиків, а також є настановами для страховиків і державних регуляторів щодо створення безпечних умов ведення справ.

Зміст принципів можна узагальнити наступним чином:

- Страхові компанії повинні включити управління кіберризиками в систему ризик-менеджменту підприємства.
- Рада директорів повинна детально вивчати всі матеріали, отримані в результаті внутрішнього аудиту IT-системи компанії.
- Страховики повинні бути інформовані щодо існуючих кіберзагроз через спеціальні організації обміну такою інформацією.
- Низка принципів стосується обов'язків страхових регуляторів, зокрема забезпечення належної нормативної бази, яка буде «гнучкою, практичною і послідовною» у взаємодії з національними стандартами.
- Поряд зі зміцненням принципів збереження конфіденційності даних при їхньому зборі, зберіганні, використанні та знищенні основним принципом визначається планування способу реагування на інциденти порушення середовища кібербезпеки [7].

Дані принципи допоможуть страховикам удосконалити внутрішні системи і процеси для захисту від витоку даних і втрати інтелектуальної власності, оскільки страхова галузь знаходиться під постійною загрозою кібернападів.

Висновки. Проаналізувавши проблеми, що стримують розвиток кіберстрахування у світі, узагальнено зарубіжний досвід їхнього вирішення.

По-перше, проблему невизначеності регулювання відносин у кіберстрахуванні можна вирішити шляхом прийняття в державі законодавства, яке регулює відносини у сфері захисту особистих даних, регламентації вимог щодо способу зберігання, рівня захисту цих даних і визначення відповідних санкцій у разі їхнього порушення (для страховика воно окреслить стандарти, вимоги до захисту інформації, на які він посилається при визначенні умов страхування, при розслідуванні інциденту витоку даних; для компаній – стане стимулом придбати кіберстрахування, щоб захистити себе від сплати значних штрафів, компенсації збитків третім особам за рішенням суду, судових витрат тощо).

По-друге, проблему нестачі інформації для проведення актуарних розрахунків у кіберстрахуванні можна вирішити шляхом утворення Бюро даних щодо кібербезпеки. Держава може сприяти утворенню такого Бюро, що значно допомогло б страховим компаніям та ризик-менеджерам управляти ризиками, створювати актуарні моделі для кіберризиків, тим самим скоротивши вартість полісів страхування і зробивши кіберстрахування більш привабливим для компаній.

По-третє, проблему концентрації кіберризиків у разі настання страхового випадку можна вирішити, якщо держава протягом певного часу буде забезпечувати перестрахування кіберризиків для страхових компаній. Це допоможе становленню ринку кіберстрахування за рахунок впевненості страховиків у можливості виконати свої зобов'язання в разі настання страхових випадків, зниження цін на поліси (високі тарифи перестраховиків прямо впливають на вартість страховки) і зростання конкуренції серед страховиків.

Таким чином, усунення даних бар'єрів сприятиме успішному розвитку ринку кіберстрахування в країнах, де поки воно нерозвинене чи взагалі відсутнє, а наведений зарубіжний досвід може слугувати прикладом вирішення зазначених проблем.

Список літератури:

1. Allianz Risk Barometer Top Business Risks 2015. Allianz SE and Allianz Global Corporate & Specialty SE survey [Електронний ресурс]. – Режим доступу : http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2015_EN.pdf.
2. Cybersecurity. National Association of Insurance Commissioners official site. [Електронний ресурс]. – Режим доступу : http://www.naic.org/cipr_topics/topic_cyber_risk.htm.
3. Insurance Industry Outlines Cyber Security Guidelines. Fortscale official site [Електронний ресурс]. – Режим доступу : http://fortscale.com/blog/insurance-industry-outlines-cyber-security-guidelines/.
4. Jennifer Archie Cybersecurity regulation and best practice in the US and UK . Latham & Watkins survey [Електронний ресурс]. – Режим доступу : https://www.lw.com/thoughtLeadership/Cybersecurity-regulation-and-best-practice.
5. Jim Finkle Cyber insurance premiums rocket after high-profile attacks. Multimedia news agency Thomson Reuters [Електронний ресурс]. – Режим доступу : http://www.reuters.com/article/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012.
6. Kriti Sarda A Glance At The United States Cyber Security LawsSecurity Laws. Appknox [Електронний ресурс]. – Режим доступу : https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/.
7. Mitigating cyber risk for insurers. Ernst & Young Global Limited survey. [Електронний ресурс]. – Режим доступу : http://www.ey.com/Publication/vwLUAssets/EY_-_Insights_into_cybersecurity_and_risk_(Part_2)/$FILE/ey-mitigating-cyber-risk-for-insurers.pdf.
8. Protection of personal data. European Commission Directorate-General for Justice and Consumers official site [Електронний ресурс]. – Режим доступу : http://ec.europa.eu/justice/data-protection/index_en.htm.
9. Turnaround and transformation in cybersecurity. Key findings from The Global State of Information Security® Survey 2016. PricewaterhouseCoopers survey [Електронний ресурс]. – Режим доступу : https://www.pwc.ru/ru/riskassurance/publications/assets/gsiss2016-report.pdf.
10. What Every CISO Needs to Know About Cyber Insurance. Symantec Corporation report [Електронний ресурс]. – Режим доступу : https://www.symantec.com/content/en/us/enterprise/white_papers/what-every-ciso-needs-to-know-cyber-insurance-21359962-wp.pdf.

Приказюк Н. В.
Кукурудзяк М. В.
Киевский национальный университет имени Тараса Шевченко

ПРОГРЕССИВНЫЙ ОПЫТ ЗАРУБЕЖНЫХ СТРАН В РЕШЕНИИ ПРОБЛЕМ РАЗВИТИЯ КИБЕРСТРАХОВАНИЯ

Резюме
Исследована сущность киберстрахования и определены риски, на случай которых осуществляется киберстрахование. Выявлены проблемы, сдерживающие развитие киберстрахования в мире. На основании прогрессивного опыта развитых зарубежных стран обобщены способы решения выявленных проблем.

Ключевые слова: киберстрахование, киберриски, безопасность данных, государственное регулирование в сфере безопасности личных данных, сообщение о нарушении безопасности данных, перестрахование киберрисков, информационное обеспечение киберстрахования.

Prikaziuk N. V.
Kukurudziak M. V.
Taras Shevchenko National University of Kyiv

PROGRESSIVE EXPERIENCE OF FOREIGN COUNTRIES IN SOLVING PROBLEMS OF CYBER INSURANCE

Summary
The essence of cyber security and identified risks, which cyber insurance policies coverage are provided for are studied. The problems which constrain the development of cyber insurance in the world are defined. On the basis of the progressive experience of developed foreign countries the solutions to existing problems are generalized.

Keywords: cyber insurance, cyber risks, data security, government regulation of personal data security, mandatory data breach notification, cyber insurance reinsurance, information support of cyber insurance.