УДК 336.233.2
DOI 10.52575/2687-0932-2023-50-1-122-132

Обзор мировых тенденций развития киберстрахования

Канупа М.С., Степанова М.Н.
ФГБОУ ВО «Байкальский государственный университет»
Россия, 664003, Иркутская область, город Иркутск, ул. Ленина, д.11
E-mail: mkanupa@mail.ru, stepanovaMN@bgu.ru

Аннотация. Развитие информационных технологий неизбежно повлекло за собой распространение киберпреступности, приобретающей все больший масштаб как в мировом пространстве, так и в рамках отдельных стран и влекущей за собой колоссальные по размерам прямые убытки, возрастающие объемы расходов на обеспечение кибербезопасности. На этом фоне все более востребованным становится страхование, выполняющее не только компенсирующую функцию, но и превентивную. Становление и дальнейшее развитие рынка киберстрахования важно не только с точки зрения удовлетворения возрастающего спроса со стороны разработчиков и пользователей информационных систем, но и является значимым этапом трансформации мирового страхового пространства. Востребованность киберстрахования предопределена интенсификацией процесса цифровизации, однако его качественное развитие является достаточно сложным и сопровождается рядом объективных проблем, в первую очередь связанных со спецификой андеррайтинга информационных рисков и урегулирования страховых претензий, требующих поиска возможных вариантов решения, в том числе обращаясь к накопленному мировому опыту. Авторами было выделено и представлено пять основных мировых тенденций развития киберстрахования, определяющих тренды национальных рынков на ближайшую перспективу. Отмечено, что рост страховых тарифов при одновременном снижении объемов предлагаемой страховой защиты, расширении перечня ограничений и вовлеченности потребителей страховых услуг в самопокрытие рисков неизбежно приведет к перелому мировой тенденции увеличения спроса на продукты киберстрахования.

Ключевые слова: киберстрахование, страхование киберрисков, рынок киберстрахования, страхование информационных рисков, мировой страховой рынок, развитие страхового рынка

Для цитирования: Канупа М.С., Степанова М.Н. 2023. Обзор мировых тенденций развития киберстрахования. Экономика. Информатика, 50(1): 122–132. DOI 10.52575/2687-0932-2023-50-1-122-132

Overview of Global Trends in the Development of Cyber Insurance

Mariia S. Kanupa, Marina N. Stepanova
Baikal State University,
11 Lenina St., Irkutsk, 664003, Russia
E-mail: mkanupa@mail.ru, stepanovaMN@bgu.ru

Abstract. The development of information technologies has inevitably led to the spread of cybercrime, which is becoming increasingly widespread both in the global space and within individual countries and entails not only colossal direct losses, but also increasing amounts of cybersecurity costs. Against this background, insurance is becoming more and more in demand, performing not only a compensating function, but also a preventive one. At the same time, the formation and further development of the cyber insurance market is important not only from the point of view of meeting the increasing demand from developers and users of information systems, but also is a significant stage in the transformation of the global insurance space. The demand for cyber insurance is predetermined by the intensification of the digitalization process, but its qualitative development is quite complex and is accompanied by a number of objective problems. The authors identified and presented five major global trends in the development of cyber insurance, which determine the trends of national markets in the near future. It is noted that the growth of insurance tariffs with a simultaneous

decrease in the volume of insurance protection offered, the expansion of the list of restrictions and the involvement of consumers of insurance services in self-covering risks will inevitably lead to a reversal of the trend of increasing demand for cyber insurance products.

Keywords: cyber insurance, cyber risk insurance, cyber insurance market, information risk insurance, global insurance market, insurance market development

For citation: Kanupa M.S., Stepanova M.N. 2023. Overview of Global Trends in the Development of Cyber Insurance. Economics. Information technologies, 50(1): 122–132 (in Russian). DOI 10.52575/2687-0932-2023-50-1-122-132

Введение

В связи с цифровизацией общества и бизнес-процессов значительной части компаний, киберпреступность стала обретать все больший ареал воздействия, открывая для киберпреступников новые горизонты [Якимова, Нарутто, 2016; Осипенко, Соловьев, 2021; Ищенко, Кручинина, 2022]. Число вмешательств в данные, краж секретной информации и нарушений в работе систем компаний растет в геометрической прогрессии. «Кибернападениям» подвергаются самые разнообразные типы организаций: от мелкого бизнеса без привязки к отрасли и онлайн-сервисов до медицинских и государственных учреждений. Среди методов обеспечения информационной безопасности особое значение начинает приобретать киберстрахование, которое постепенно переходит в разряд одного из наиболее действенных и актуальных вариантов минимизации потерь, возникающих в результате кибersбоев и кибератак. При этом теоретическая база «киберстрахования» еще формируется: в научно-практической среде имеют место различные подходы к определению содержания киберстрахования и особенностей осуществления [Брызгалов, Цыганов, 2002; Русецкая, 2007; Иванов, 2016; Мамаева, Ларионов, 2018; Конявский, Хованов, 2000; Брызгалов, Грызенкова, Цыганов, 2020], но все так или иначе сводится к тому, что оно в первую очередь направлено на обеспечение страховой защиты специфического объекта страхования — информации [Степанова, Юсупова, 2021]. И это тот самый случай, когда практическая реализация отдельного направления страховой защиты существенно опережает его теоретически упорядоченное описание. Во многом это происходит благодаря высоким темпам развития национальных страховых рынков, откликающихся на чрезвычайную востребованность соответствующих продуктов со стороны носителей риска и при этом имеющих определенные национальные особенности их функционирования.

Объекты и методы исследования

Теоретической и методологической основой исследования послужили новейшие разработки ученых в области управления информационными рисками, а также национальные стандарты обеспечения информационной безопасности; информационной базой – аналитические отчеты и обзоры зарубежных агентств, затрагивающие отдельные аспекты развития киберстрахования как специфического сегмента рынка страховых услуг. Было применено структурирование и сравнение данных за сопоставимые периоды, а также методы системного, статистического и дедуктивного анализа. Цель исследования – выявление основных мировых тенденций развития киберстрахования на основе анализа соответствующих сегментов национальных рынков страховых услуг. Объектом исследования определено страхование рисков информационной безопасности, предметом исследования — экономические отношения, складывающиеся на международном и национальном рынке киберстрахования. Научная новизна работы состоит в обобщении мирового опыта киберстрахования, которое позволило выделить основные тенденции развития киберстрахования, общие для разных национальных рынков. По мнению авторов, представленные тенденции будут наблюдаться и на отечественном рынке страховых услуг, поскольку имеет место общая

природа угроз и единые задачи митигации их последствий, стоящие перед страховым сообществом.

Результаты и их обсуждение

Информационные риски становятся все более значимыми среди существующих рисков среды и более опасными для функционирования организаций, особенно работающих с огромным массивом информации. Однако их теоретическое описание, включая определение содержательных границ, еще в процессе разработки. Несмотря на то, что базовые понятия «информационная безопасность» и «кибербезопасность» в российской практике определены в качестве самостоятельных, очевидного разделения производных от них понятий «информационные риски» и «киберриски» до сих пор не произошло. Более того, за рубежом содержательно они воспринимаются как равноценные, поэтому в целях анализа мирового опыта их минимизации также были приняты в качестве взаимозаменяемых с общей методической основой обеспечения страховой защиты. В соответствии с этим под киберстрахованием допустимо понимать особое направление страхования, ориентированное на снижение убытков страхователей и бенефициаров, вызванных хакерскими атаками, уничтожением или кражей данных, вымогательством, а также минимизацию их потерь из-за перерывов в работе и возникающей ответственности перед третьими лицами, связанной с реализацией киберрисков.

Первые значимые для становления страхования в сфере информационной безопасности события (появление первых страховых продуктов, интенсивная наработка практики андеррайтинга и урегулирования страховых претензий) связываются с Великобританией и Северной Америкой, которые до настоящего времени остаются лидерами по уровню развития информационного страхования в мире.

Большинство наиболее востребованных страховых программ – это программы, разработанные страховыми компаниями США. Одним из крупнейших страховщиков, не только реализующим достаточно разнообразные страховые продукты в сегменте митигации киберрисков, но и оказывающим услуги по оценке потенциальных угроз, осуществляющим сбор и обработку данных, предоставляющих возможность страхователям и более мелким страховщикам проводить качественную политику управления информационными рисками, является компания AIG. Другой пример выхода за пределы исключительно осуществления страховых выплат при наступлении соответствующих страховых событий – пример крупнейшей страховой компании Chubb, имеющей как достаточно большой набор страховых продуктов в сегменте киберзащиты владельцев бизнеса, включая страхование киберответственности, так и ресурсы, дающие возможность страхователям максимально быстро реагировать на совершаемые кибератаки, тем самым минимизируя потенциальный ущерб.

Вклад в рост ценности и важности киберстрахования на территории Северной Америки также внесла Канада. В связи с резким ростом числа предприятий, пострадавших от кибератак в 2018 году, страна сделала все возможное для его активного развития – благодаря этому ее рынок в настоящее время представлен сразу несколькими достаточно крупными страховыми компаниями, работающими в сегменте киберстрахования: AXIS Canada, Beazley Canada, AIG Insurance Company of Canada, Zurich Canada и другими.

Достаточно развито киберстрахование и в Соединенном Королевстве: согласно результатам исследования Ovum, 9 из 10 британских компаний имеют соответствующую страховую программу, направленную на минимизацию потерь, связанных с киберрисками. Вместе с тем, британские брокеры по-прежнему рассматривают данный сегмент не только как «важный», но и все

еще «растущий рынок» [UK firms…, 2018], поскольку только 38% компаний имеют страховое покрытие, распространяемое на все виды киберугроз.

Крупнейшими мировыми лидерами сферы киберстрахования, выходящими за пределы обслуживания национальных страховых рынков, в настоящее время являются страховые компании Hiscox, Chubb, Hartford, AIG и др. (см. табл. 1).

Таблица 1
Table 1

ТОП-10 страховых компаний, лучших в сфере киберстрахования
TOP-10 of the best cyber insurance companies

Позиция	Страховая компания (расположение штаб-квартиры)	Рейтинговая оценка по 5-балльной шкале
1	Hiscox (Гамильтон, Бермудские острова)	4.9
2	Chubb (Цюрих, Швейцария)	4.8
3	The Hardford (Хартфорд (Коннектикут), США)	4.7
4	AIG (Нью-Йорк, США)	4.7
5	CNA (Чикаго, США)	4.6
6	Arch (Бермудские острова)	4.5
7	Hanover Вустер (Массачусетс, США)	4.5
8	Intact (Торонто, Канада)	4.4
9	Beazley (Лондон, Великобритания)	4.3
10	Axis (Бермудские острова)	4.3

Составлено по данным: [The Best Cyber Insurance Companies for 2022, 2022]
Source: [The Best Cyber Insurance Companies for 2022, 2022]

Отметим, что представленный в таблице 1 топ-лист лучших киберстраховщиков по версии AdvisorSmith [The Best Cyber Insurance Companies for 2022, 2022], не является единственным и не претендует на абсолютную точность оценки. Однако он максимально полно учитывает не только объем аккумулируемых в данном сегменте страховых сборов, но и другие, не менее важные показатели: рейтинговую оценку финансовой устойчивости от компаний AM Best и Standard & Poor's, данные об уровне удовлетворенности клиентов, представленные в исследованиях JD Power, рейтинги жалоб от Национальной ассоциации уполномоченных по страхованию, наполняемость страховых программ (доступные функции и опции), а также доступность информации для клиентов.

Что касается России, то развитие информационного страхования на ее страховом пространстве началось несколько позднее, чем в других странах [Брызгалов, Цыганов, 2002]. Первые попытки создания основ для реализации нового вида страхования на основе опыта иностранных коллег, подготовка условий его внедрения в страховые портфели были не удачны. Однако это способствовало формированию первооснов его нормативно-правового обеспечения, совершенствованию отдельных элементов страховой защиты на случай реализации информационных рисков и положило начало сотрудничеству между страховыми организациями и заинтересованными в становлении киберстрахования субъектами. Завершающим моментом

стало появление на российском страховом рынке первых страховых продуктов, способных составить конкуренцию зарубежному ассортименту, были сформированы планы на дальнейшее развитие и определены основные барьеры, мешающие более быстрому и эффективному внедрению киберстрахования в страховую практику. В настоящее время в России представлено лишь несколько компаний, занятых данным концептом, но при этом существует возможность выбора соответствующих страховых продуктов (хоть и относительно ограниченного). В то же время детально изучить содержание конкретных страховых программ и объемы их продаж практически невозможно: соответствующая информация не раскрывается с той степенью полноты, которая могла бы обеспечить качественный сравнительный анализ, статистический учет по данной нише страхового рынка и вовсе не ведется. В большинстве случаев неподготовленный пользователь сталкивается с формулировкой «условия в рамках индивидуального предложения», а аналитик имеет в арсенале инструментов анализа лишь правила страхования. Таким образом, на российском рынке роль страхования в обеспечении информационной безопасности пока крайне сдержанна [Самаруха, Сорокина, 2022].

Что касается мирового рынка киберстрахования, то он в данный момент переживает некий период перехода на новую ступень качественного развития [Степанова, Юсупова, 2022]. Количество киберпреступлений и их разнообразие растет, диверсификация кибератак становится все более широкой. Последствия от потери и хищения информации принимают форму убытков, средняя величина которых постоянно растет [Bhardwaj, 2020; Colonial Pipeline ransomware attack..; Cost of data breaches, 2022; Cyber Attacks Increased 50% Year over Year, 2022]. Достаточно сильным рычагом для активизации страхового рынка стала вспышка пандемии COVID-19. Ускорение перехода различных операций и процессов в режим онлайн спровоцировало мощный скачок кибератак, что в свою очередь заставило увеличить размеры выделяемые на митигацию киберрисков бюджетов и актуализировало необходимость трансферта рисков на страхование. Этим объясняются высокие темпы роста рынка киберстрахования в настоящее время. Развитие технологий, растущий спрос на оцифровывание, использование различных интеллектуальных достижений в IT-сфере создают прочную базу для развития различных способов защиты. Существуют различные платформы, защитные системы, программное обеспечение и другие инструменты, которые компании стараются объединить со страхованием для нивелирования рисков и управления ими. Учеными были сделаны выводы о том, что дальнейшие темпы роста страхования будут увеличиваться по всему миру, при этом самые высокие темпы роста ожидаются в Азиатско-Тихоокеанском регионе и Европе. Америка же в ближайшие несколько лет будет готовить своих клиентов к неустойчивым условиям рынка страхования.

Исторически рынок киберстрахования считался «мягким», что позволяло фирмам относительно легко получать страховое покрытие по относительно невысоким тарифам. Однако повышенные киберриски и экспоненциальный рост атак программ-вымогателей, особенно за последний год, привели к ужесточению входящих условий страхования и адаптации рынка под них. В результате анализа содержания аналитических отчетов экспертов разных стран [Sanjay, 2019; Schenkelberg, 2021; Sharply Rising Cyber Insurance…, 2021; Singleton, 2021; Statistics. Insurance…; ACA Aponix Cyber Insurance…, 2022; Statistique. Cyber assurance, 2021; Cyberinsurance provider coalition…] было выявлено 5 основных тенденций развития киберстрахования в ближайшее время.

1. Увеличение спроса на соответствующие страховые продукты.

С ростом числа и стоимости киберинцидентов во всем мире все больше фирм принимают факт того, что кибератак не избежать и в этом случае киберстрахование может быть весьма полезно в качестве инструмента минимизации связанных с ними финансовых потерь. По данным Национальной ассоциации уполномоченных по страхованию (NAIC), количество действующих договоров киберстрахования только в период с 2019 по 2020 год увеличилось более чем на 20 %, а в период с 2016 по 2020 год – почти в два раза (рис. 1).

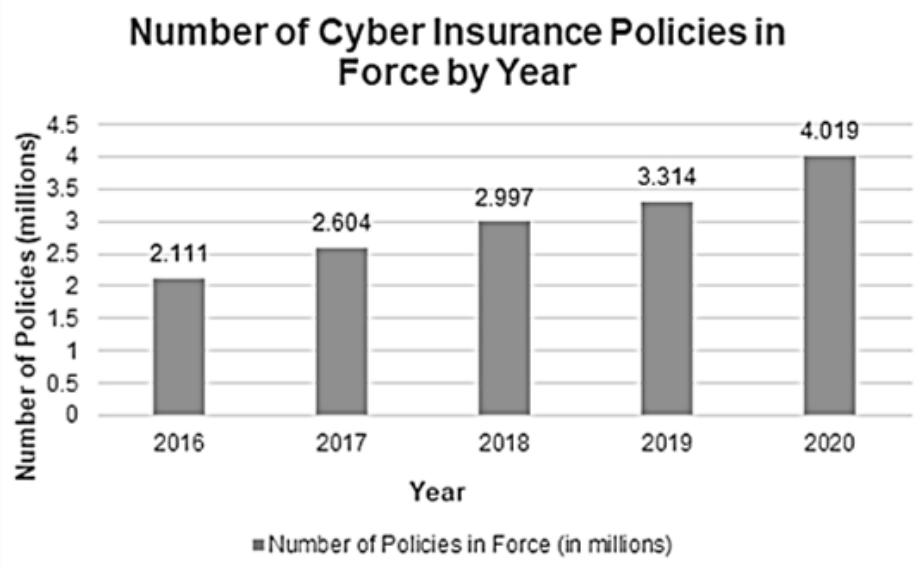

Рис. 1. Динамика количества действующих договоров киберстрахования за период с 2016 по 2020 гг., млн шт., всего в мире [Sanjay, 2019]
Fig. 1. Dynamics of the number of existing reinsurance contracts for the period from 2016 to 2020, million units, total in the world [Sanjay, 2019]

2. Ужесточение условий страхования и расширение числа исключений из страхового покрытия.

В то время как спрос на киберстрахование растет, количество предложений на соответствующих сегментах страхового рынка сокращается: страховщики и перестраховщики делают шаг назад, пересматривая свои ожидания от рисков и ужесточая входящие требования к страхователям и объектам страхования. С увеличением числа кибератак и поданных в связи с соответствующими убытками исков отрасль стала менее прибыльной. По оценкам кредитного рейтингового агентства FitchRatings, выплаты страховых компаний по претензиям существенно увеличились, а, следовательно, выросло и значение коэффициента прямых убытков – с 47 центов на каждый доллар заработанных премий в 2019 году до 73 центов в 2020 году (рис. 2).

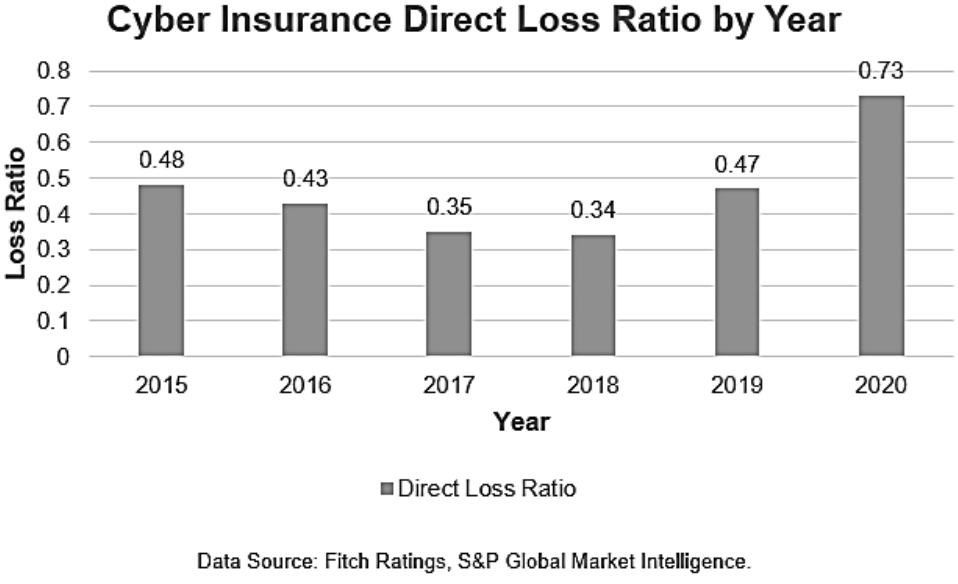

Рис. 2. Тенденция изменения среднего мирового значения коэффициента прямых убытков с 2015 по 2020 гг. [Schenkelberg, 2021]
Fig. 2. Trend of change in the average global value of the direct loss ratio from 2015 to 2020 [Schenkelberg, 2021]

В результате страховщики начинают уделять еще больше внимания экспертизе рисков, требуя от компаний больше информации об убытках от киберпреступлений для оценки киберпрограмм фирм. Один из способов реагирования — это установление более строгих требований к безопасности заявителей. Многофакторная аутентификация (MFA) становится ключевым требованием многих страховых компаний наряду с другими средствами контроля, такими как наличие решения для обнаружения конечных точек и реагирования, защищенные и зашифрованные резервные копии, управление привилегированным доступом, непрерывность бизнеса и планирование реагирования на инциденты, а также осведомленность о кибербезопасности.

Страховщики также опираются на дополнительные приложения, связанные с историей столкновения фирм с программами-вымогателями и громкими кибер-взломами, как на попытку собрать воедино информацию о присущих фирмам рисках. В ходе подобных «следственных» процессов страховые компании более тесно сотрудничают со специалистами по кибербезопасности, чтобы лучше понять в чем конкретно заключаются киберриски той или иной организации, как они проявляются и что способствует увеличению их вероятности. В конечном счете фирмы, не предоставляющие надлежащих сведений и/или не имеющие необходимых средств контроля, могут вообще не рассматриваться в качестве обеспечиваемых страховой защитой, страховаться под более высокие страховые тарифы и/или усеченные лимиты страхового покрытия, что позволяет страховщикам несколько нивелировать предполагаемый дополнительный риск, принимаемый вместе с «проблемным» получателем страховых услуг.

3. Рост среднего размера страховых премий за счет увеличивающихся страховых тарифов.

Дисбаланс спроса и предложения на рынке киберстрахования привел к резкому росту ставок страховых взносов. Наиболее значимо тарифы выросли после кибернападений на американскую трубопроводную систему «Colonial Pipeline» летом 2021 года [Sharply Rising Cyber Insurance…, 2021] – результат этого инцидента сказался на отрасли в целом и теперь фирмы нередко сталкиваются с увеличением размера расчетных базовых премий на 100–300%. По заключению исследователей, в сентябре 2021 года ставки по киберстрахованию для объектов с покрытием от 1 млн долларов выросли на 174% по сравнению с 12 месяцами ранее [Singleton, 2021]. Прогнозируется, что далее страховые компании будут продолжать претендовать на получение более высоких премий – так они реагируют на развивающиеся киберугрозы и увеличивающуюся вероятность реализации информационных рисков.

4. Снижение лимитов страхового покрытия.

Усиление контроля со стороны страховщиков и рост премий влияют на объем страхового покрытия, предлагаемого носителям риска. В то время как в прошлом для компании среднего размера не было редкостью иметь страховое покрытие в размере 10 млн долларов, то сегодня этой же фирме большинство операторов страхового рынка предложат программы с покрытием не более 5 млн долларов. Если фирмы считаются высокорискованными, страховщики с меньшей вероятностью установят для них более высокий лимит страхового покрытия или вообще откажут в страховом покрытии. Одновременно с этим, в связи с ростом страховых тарифов некоторые фирмы сами принимают решение сократить свое страховое покрытие в обмен на более доступные входящие ценовые условия. Эти факторы привели к общей тенденции к снижению пределов обеспечения страховой защитой. В сентябре 2021 года ведущий мировой страховой брокер и консультант по рискам «Marsh» сообщил, что 23% ее клиентов выразили добровольное желание уменьшить страховые суммы или столкнулись с вынужденным снижением размеров предлагаемого страхового покрытия [Statistics. Insurance…].

Наряду с более низкими лимитами страхового покрытия некоторые страховщики полностью пересматривают страховое покрытие для рисков совершения определенных кибератак, таких как воздействие программ-вымогателей. Так, страховая компания AXA объявила, что с мая 2022 года прекратит предоставлять соответствующее покрытие во Франции

[ACA Aponix Cyber Insurance…, 2022]. Решение AXA является ответом на растущие убытки, понесенные страховщиком в результате исполнения обязательств, связанных с последствиями атак программ-вымогателей на информационные системы страхователей, а также на давление со стороны правительства, указывающего на то, что подобные выплаты крайне негативно сказываются на информационном поле, так как способствуют росту числа атак программ-вымогателей. Несмотря на то, что в настоящее время решение AXA распространяется только на Францию, оно в любое время может выйти за ее пределы и потенциально «открыть двери» для других страховщиков, последующих этому примеру в будущем.

5. Увеличение уровня удержания риска на самостраховании.

В то время как лимиты покрытия снижаются, а премии растут, страховщики также ожидают, что их клиенты будут нести больший риск за счет применения положения об удержании. Подобно франшизе, положение об удержании определяет часть ущерба, за которую страхователи будут нести ответственность до вступления в силу договора страхования. В то время как страховщики часто требуют выполнения стандартного условия об удержании, некоторые страхователи при получении полиса охотно соглашаются на более высокие ставки удержания в надежде свести к минимуму размер начисляемых страховых премий. В 4 квартале 2021 года «Marsh» сообщила, что 60% ее клиентов приняли повышенные меры по удержанию в попытке сохранить страховую премию на низком уровне [Statistique. Cyber assurance, 2021]. Поскольку страхователи стремятся уменьшить свой риск и избежать крупных потерь, политика удержания может стать пунктом, на который они все чаще опираются при распределении риска между страховщиками.

Дискуссия

В рамках дискуссии представляется необходимым обсудить, что же оставляют фирмам пересматриваемые условия страхования, растущие страховые премии и снижающиеся при этом лимиты покрытия. По нашему мнению, в первую очередь – ориентир на более ранний собственный андеррайтинг, полноценный риск-менеджмент и более качественную систему превенций. Компаниям, уже обеспеченным программами киберстрахования и тем, кто впервые рассматривает возможность получения страхового покрытия, можно рекомендовать начинать процесс подготовки к взаимодействию со страховщиками как можно раньше: участие на ранних стадиях процесса планирования и подачи заявок на трансферт риска, потенциальные страхователи смогут лучше выявлять существующие пробелы в обеспечении собственной информационной безопасности и работать над их устранением, тем самым повышая шанс на доступ к страховым программам с более привлекательными тарифными ставками и охватом страховой защиты.

Заключение

В ходе исследования были выявлены следующие общие для активных в киберстраховании стран особенности его развития. Роль страхования в минимизации киберрисков стала более значимой, чем была в начале становления национальных рынков, условия страхования более прозрачными, но вместе с тем и менее лояльными в отношении потенциальных получателей страховых услуг. Прошел пик реализации максимально полных с точки зрения обеспечиваемого покрытия страховых программ – они также адаптируются под возрастающие риски киберсреды, что накладывает отпечаток и на ценовые условия страховых сделок – увеличиваются не только страховые тарифы, но и лимиты собственного удержания страхователей. Страхователи в стремлении сэкономить на страховых платежах вынуждены отказываться от полноценного страхового покрытия, страховые компании при этом также заходят в режим оптимизации расходов, обусловленный ростом осуществляемых выплат – главным образом это происходит за счет более тщательной селекции рисков и большего числа устанавливаемых ограничений. То и другое в конечном счете сказывается на

качестве страховой защиты, но пока не оказывает серьезного влияния на снижение темпов роста спроса на соответствующие страховые продукты. Однако, по нашему мнению, уже в ближайшее время, столкнувшись с реализацией рисков в рамках адаптированных программ, не обеспечивающих полного возмещения, страхователи изменят эту тенденцию, постепенно переориентируясь на более качественную превенцию рисков.

Несмотря на более позднее включение страховых компаний, работающих в России, в реализацию киберстрахования, уже сейчас можно наблюдать общие с общемировыми тенденции его развития. В первую очередь это касается увеличивающейся потребности в страховых продуктах и существующих ограничений в предлагаемых на рынке программах. Анализ мирового опыта позволит отечественным страховщикам своевременно и более гибко реагировать на последствия принимаемых в данной сфере решений, а также более качественно прогнозировать развитие данного сегмента с учетом существующих потребительских сценариев, наблюдаемых на иных национальных рынках.

Список источников

ACA Aponix Cyber Insurance: Top Five Trends for 2022. 2022. APONIX. URL: https://www.acaglobal.com/insights/cyber-insurance-top-five-trends-2022 (дата обращения: 10.11.2022).

Bhardwaj D. 2020. Nearly 7 lakh cyberattacks in 2020, IT Ministry tells Parliament. Hindustan Times. URL: https://www.hindustantimes.com/india-news/nearly-7-lakh-cyber-attacks-in-2020-it-ministry-tells-parliament/story-bOv6SuWSP9XxUwtF9uBTvK.html (дата обращения: 10.11.2022).

Colonial Pipeline ransomware attack. Wikipedia. URL: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack (дата обращения: 10.11.2022).

Cost of data breaches. 2022. IBM Security. New York. URL: https://www.ibm.com/ (дата обращения: 10.11.2022).

Cyber Attacks Increased 50% Year over Year. 2022. Checkpoint. Tel Aviv. URL: https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/ (дата обращения: 10.11.2022).

Cyberinsurance provider coalition acquires binaryedge: Cybersecurity News, Insights and Analisis. Security Week. URL: https://www.securityweek.com/cyber-insurance-provider-coalition-acquires-binaryedge (дата обращения: 10.11.2022).

Sanjay A. 2019. Capital One Data Breach and Why Asia Pacific Must Rethink Cloud Security. CDO Trends. URL: https://www.cdotrends.com/story/14493/capital-one-data-breach-and-why-asia-pacific-must-rethink-cloud-security (дата обращения: 10.11.2022).

Schenkelberg F. 2021. 4 Effective Risk Mitigation Strategies. Accendo Reliability. URL: https://accendoreliability.com/4-effective-risk-mitigation-strategies/ (дата обращения: 10.11.2022).

Sharply Rising Cyber Insurance Claims Signal Further Risk Challenges. 2021. FitchRatings. New York. URL: https://www.fitchratings.com/research/insurance/sharply-rising-cyber-insurance-claims-signal-further-risk-challenges-15-04-2021 (дата обращения: 10.11.2022).

Singleton C. 2021. X-Force Threat Intelligence Index 2021. IBM Security. New York. URL: https://www.ibm.com/downloads/cas/M1X3B7QG (дата обращения: 10.11.2022).

Statistics. Insurance. GlobalData. URL: https://www.globaldata.com/media/insurance/ (дата обращения: 10.11.2022).

Statistique. Cyber assurance. 2021. Eficiens. Paris. URL: https://www.eficiens.com/cyber-et-assurance/#quelques-chiffres (дата обращения: 10.11.2022).

The Best Cyber Insurance Companies for 2022. 2022. AdvisorSmith. URL: https://advisorsmith.com/business-insurance/cyber-liability-insurance/best-cyber-insurance-companies/ (дата обращения: 10.11.2022).

UK firms ahead of the curve for cyber insurance uptake. 2018. The Actuary, 08. URL: https://www.theactuary.com/news/2018/08/2018/08/16/uk-firms-ahead-curve-cyber-insurance-uptake (дата обращения: 10.11.2022).

Список литературы

Брызгалов Д.В., Грызенкова Ю. В., Цыганов А. А. 2020. Перспективы цифровизации страхового дела в России / Д. В. Брызгалов. Финансовый журнал. Т. 12, 3: 76-90.

Брызгалов Д.Н., Цыганов А. А. 2002. Страхование электронных рисков. Директор-Инфо, 47: 35—41.

Иванов И.К. 2016. Киберстрахование: как обеспечить информационную безопасность бизнесу. Большой портал для малого бизнеса, 16: 13-24.

Ищенко Е.П., Кручинина Н.В. 2022. Высокие технологии и криминальные вызовы. Всероссийский криминологический журнал. Т. 16, 2: 199–206.

Конявский В.А., Хованов В.Н. 2000. Страхование информационных рисков и обеспечение информационной безопасности. Управление защитой информации. Т. 4, 1.

Мамаева Л.Н., Ларионов В. И. 2018. Киберстрахование как способ обеспечения информационной безопасности. Экономическая безопасность и качество, 1 (30): 76-79.

Осипенко А.Л., Соловьев В.С. 2021. Основные направления развития криминологической науки и практики предупреждения преступлений в условиях цифровизации. Всероссийский криминологический журнал. Т. 15, 6: 681–691.

Русецкая Э.А. 2007. Система страхования как важнейший инструмент, обеспечивающий общую экономическую безопасность и стабильность в условиях глобализации мировой экономики. Дайджест-финансы: электронный журнал. URL: https://cyberleninka.ru/article/n/sistema-strahovaniya-kak-vazhneyshiy-ins-trument-obespechivayuschiy-obschuyu-ekonomicheskuyu-bezo-pasnost-i-stabilnost-v-usloviyah (дата обращения: 10.11.2022).

Самаруха В.И., Сорокина Т.В. 2022. Роль финансов в обеспечении экономической безопасности России в условиях геополитической трансформации мировой экономики. Известия Байкальского государственного университета. Т. 32, 3: 474–484.

Степанова М.Н., Юсупова М. Н. 2021. Генезис российской практики киберстрахования. Журнал прикладных исследований, 6-9: 874-881.

Степанова М.Н., Юсупова М. Н. 2022. Анализ ключевых характеристик современного мирового рынка киберстрахования. Журнал прикладных исследований, 1-1: 54-61.

Якимова Е.М., Нарутто С.В. 2016. Международное сотрудничество в борьбе с киберпреступностью. Криминологический журнал Байкальского государственного университета экономики и права. Т. 10, 2: 369–378

References

Bryzgalov D.V., Gryzenkova Yu. V., Tsyganov A. A. 2020. Prospects of digitalization of insurance business in Russia / D. V. Bryzgalov. Financial Journal. Vol. 12, 3: 76-90.

Bryzgalov D.N., Tsyganov A. A. 2002. Electronic risk insurance. Director-Info, 47: 35-41.

Ivanov I.K. 2016. Cyber insurance: how to ensure information security for business. Big portal for small business, 16: 13-24.

Ishchenko E.P., Kruchinina N.V. 2022. High technology and criminal challenges. All-Russian Journal of Criminology, vol. 16, 2: 199-206.

Konyavsky V.A., Khovanov V.N. 2000. Information risk insurance and information security assurance. Information Security Management. Vol. 4, 1.

Mamaeva L.N., Larionov V. I. 2018. Cyber insurance as a way to ensure information security. Economic security and quality, 1 (30): 76-79.

Osipenko A.L., Soloviev V.S. 2021. The main directions of development of criminological science and practice of crime prevention in the conditions of digitalization. All-Russian Journal of Criminology. Vol. 15, 6: 681-691.

Rusetskaya E.A. 2007. The insurance system as the most important tool ensuring general economic security and stability in the conditions of globalization of the world economy. Digest-finance: an electronic journal. URL: https://cyberleninka.ru/article/n/sistema-strahovaniya-kak-vazhneyshiy-ins-trument-obespechivayuschiy-obschuyu-ekonomicheskuyu-bezo-pasnost-i-stabilnost-v-usloviyah (дата обращения: 10.11.2022).

Samarukha V.I., Sorokina T.V. 2022. The role of finance in ensuring Russia's economic security in the context of the geopolitical transformation of the world economy. Proceedings of the Baikal State University. Vol. 32, 3: 474-484.

Stepanova M.N., Yusupova M. N. 2021. The genesis of Russian cyber insurance practice. Journal of Applied Research, 6-9:874-881.
Stepanova M.N., Yusupova M. N. 2022. Analysis of the key characteristics of the modern global cyber insurance market. Journal of Applied Research, 1-1:54-61.
Yakimova E.M., Narutto S.V. 2016. International cooperation in the fight against cybercrime. Criminological Journal of the Baikal State University of Economics and Law. Vol. 10, 2: 369-378.

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Канупа Мария Сергеевна, магистрант Байкальского государственного университета, г. Иркутск, Россия

Степанова Марина Николаевна, кандидат экономических наук, доцент, доцент кафедры финансов и финансовых институтов Байкальского государственного университета, г. Иркутск, Россия

ORCID: 0000-0001-9776-1129

INFORMATION ABOUT THE AUTHORS

Mariia S. Kanupa, Graduate Student of Baikal State University, Irkutsk, Russia

Marina N. Stepanova, Candidate of Economic Sciences, Associate Professor, Associate Professor of the Department of Finance and Financial Institutions, Baikal State University, Irkutsk, Russia

ORCID: 0000-0001-9776-1129