УДК 34.09 DOI: 10.31249/iajpravo/2026.01.10

КРЫСАНОВА Н.В.[1] КИБЕРСТРАХОВАНИЕ В УСЛОВИЯХ РАСШИРЕНИЯ КИБЕРУГРОЗ (Обзор)

Аннотация. В последние несколько лет киберстрахование как альтернативная стратегия управления рисками демонстрирует быстрый рост по сравнению с другими видами страхования. В обзоре рассматриваются позиции ученых по политике киберстрахования и гарантии безопасности юридических и физических лиц от киберрисков и киберпреступлений. Модели киберстрахования – сравнительно новый институт в праве; его динамика позволяет выявить основные тенденции развития комплексных страховых услуг. В разных странах развитие киберстрахования идет разными темпами и в различных формах, что позволяет выявить общие тенденции и оптимальные модели его перспективного развития.

Ключевые слова: страхование; киберстрахование; киберриски; правовой институт; правовая политика.

KRYSANOVA N.V. Cyberinsurance in the context of expanding cyber threats (Review)

Abstract. In the last few years, cyber insurance as an alternative risk management strategy has shown rapid growth compared to other types of insurance. The review examines the positions of scientists on cyber insurance policy and guarantees for the security of legal entities and individuals from cyber risks and cybercrimes. Cyber insurance models are a relatively new institution in law; its dynamics make it possible to identify the main trends in the development of comprehensive insurance services. Cyber insurance is developing at different rates and in different forms in different countries, which makes it possible to identify common trends and optimal models for its future development.

[1] *Крысанова Нина Владимировна*, старший научный сотрудник отдела правоведения ИНИОН РАН, кандидат юридических наук.

Keywords: insurance; cyberinsurance; cyberrisks; legal institute; legal politics.

Для цитирования: Крысанова Н.В. Киберстрахование в условиях расширения киберугроз (Обзор) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 1. – С. 158–171. – DOI: 10.31249/iajpravo/2026.01.10

Введение

Появление и развитие искусственного интеллекта (ИИ), больших данных, облачных вычислений, Интернет вещей и беспилотных автомобилей, цифровизация экономики и общества повышают благосостояние. Однако растущая зависимость от ИТ-сектора и интеграция цифровых технологий практически во все сферы жизни создают значительные киберриски, развиваются подходы по борьбе с киберпреступностью. Наука и практика реагируют на вызовы киберугроз и риски в киберпространстве и ищут пути решения этих проблем, в том числе через развитие институтов страхования. В обзоре представлены история появления института киберстрахования, практика киберстрахования в Российской Федерации и в зарубежных странах.

Появление института киберстрахования

Как указывает Джозефина Вольф (Josephine Wolff), доцент кафедры политики кибербезопасности в Школе Флетчера при Университете Тафтса (США), рост рынка киберстрахования в значительной степени определялся нормативными правовыми актами и регулирующими органами, но само киберстрахование в значительной степени остается нерегулируемым. В отличие от других форм страхования, здесь нет требований, определяющих, какие риски полисы киберстрахования должны охватывать, кто должен их получать или кому они должны быть доступны [7, p. 28–29].

С начала 2000-х годов в ряде штатов США были приняты законы об уведомлении о нарушениях данных, например в штате Калифорния – Билль № 1386 (2002) (California Senate Bill 1386)[1] (далее – S.B. 1386), и Общий регламент ЕС по защите данных

[1] California Senate Bill 1386. – URL: http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (дата обращения: 23.11.2025).

(General Data Protection Regulation, GDPR) в Европе в 2016 г. (вступил в силу в мае 2018 г.); они способствовали росту спроса на киберстрахование и повлияли на то, какие виды потерь им покрываются, как это было, например, в случае решения Комиссии по ценным бумагам и биржам США (US Securities and Exchange Commission) о том, что компании должны раскрывать киберриски для акционеров в рамках их финансовых заявок.

Однако в США, в отличие от автострахования, киберстрахование не является обязательным. А по сравнению со страхованием от наводнений или терроризма оно не гарантируется правительством, или, в противоположность медицинскому страхованию, фактическое содержание полисов и расходы, которые они должны покрывать, не регулируются никаким законодательством ни на уровне штатов в США, ни на федеральном уровне. Такие подходы, по мнению Д. Вольф, понятны, учитывая небольшой размер и время существования рынка киберстрахования и тот факт, что исторически он охватывал довольно узкий набор относительно специфических угроз, таких, например, как утечка данных розничных продавцов и т.п. [7, p. 29].

Исторически сложилось так, что по мере роста популярности новых страховых продуктов или возникновения проблем, подобных тем, с которыми в настоящее время сталкиваются киберстраховщики, регулирующие органы часто вмешивались, чтобы стабилизировать рынок, защитить потребителей и предоставить необходимую помощь, данные или финансовую поддержку. Поскольку рынок киберстрахования продолжает расти, стоит проанализировать его развитие наряду с развитием других видов страховых продуктов, чтобы лучше понять роль, которую регулирующие органы могут играть на развивающихся страховых рынках, а также влияние, которое государственная политика оказывает на формирование различных форм киберстрахования [ibid.].

В 2025 г. в серии изданий Springer Nature «Международная серия Хюбнера о рисках, страховании и экономической безопасности» под редакцией Жоржа Дионна вышел в свет «Справочник по страхованию». Его авторы, А. Браун и Н. Хейсле, в частности подчеркивают, что в последнее время все больше персональных данных подвергается утечке, а вредоносные атаки и другие события приводят к значительным финансовым потерям [5, p. 251]. Новые технологии и, в частности, цифровые технологии, создали новые риски, которые представляют для страховщиков значительные проблемы. Исследования рисков и возможных стратегий управле-

ния рисками имеют решающее значение как для страховых компаний, так и для общества в целом.

Между тем, еще в 1990 г. Конгресс США выпустил доклад «Несбывшиеся обещания: банкротства страховых компаний», в котором, в частности, был сделан вывод о том, что деятельность страховщиков крайне слабо регулируется, и поэтому они могут регулярно вводить в заблуждение либо отказываться от своих обязательств перед клиентами. По мнению авторов доклада, система регулирования должна предвидеть и эффективно пресекать деятельность недобросовестных лиц, которые неизбежно будут вторгаться в такую привлекательную отрасль, как страхование, где клиенты передают крупные суммы наличных в обмен на обещание будущих выгод [7, p. 40]. Особенно подчеркивалось, что страховая отрасль имеет относительно низкие барьеры для «входа», поскольку новым страховым компаниям и продуктам не требуется вкладывать какой-либо значительный капитал: все, что нужно сделать, – это дать «обещания» потенциальным клиентам о будущей страховке. «Деньги поступают заранее, а выплата страховых возмещений может занять годы», – отмечается в докладе [ibid.].

Как подчеркивает Д. Вольф, ссылаясь на доклад Конгресса США, простота концепции страхования сочетается с чрезвычайной сложностью ее реализации. Правильное ценообразование, управление средствами, распределение рисков посредством перестрахования, создание адекватных резервов и рассмотрение претензий – все это требует должного уровня управления и даже определенного личного таланта; когда этого не хватает из-за недобросовестного отношения или некомпетентности, из страхового бизнеса, в отличие от других видов предпринимательства, можно очень легко уйти [ibid.]. В современных условиях это означает потребность в специальной правовой политике в сфере страхования вообще – и в сфере киберстрахования в особенности. Так, если на ранних этапах становления киберстрахования – с 1990-х годов – выпуск первых полисов страховыми компаниями сопровождался крайне тщательными проверками безопасности, и наличие полиса киберстрахования служило своего рода сигналом, что безопасность фирмы была тщательно проверена, а некоторые первые пользователи киберстрахования приобретали полисы только для того чтобы дать понять своим клиентам и деловым партнерам: они серьезно относятся к безопасности (например компания LockBox) [7, p. 44], в 2000-х годах многие компании – и большинство страховщиков – не имели доступа к специалистам в области

компьютерной безопасности, и страховые компании начали сотрудничать с технологическими фирмами, дабы снизить вероятность убытков своих клиентов, – тенденция, которая сохранялась и в последующие годы, поскольку все больше компаний приобретали киберстрахование, а все больше технологических компаний стали рассматривать страховщиков как потенциальный способ привлечения клиентов [7, p. 46].

Ситуация в сфере киберстрахования, например в США, стала меняться после того, как 5 апреля 2002 г. злоумышленники получили доступ к серверу дата-центра, в котором хранились личные дела, номера социального страхования и информация о заработной плате более 250 тыс. государственных служащих Калифорнии [7, p. 50]. В результате этого инцидента в 2002 г. и был разработан и принят вышеупомянутый Билль об уведомлении о нарушениях данных, который вступил в силу в 2003 г. и обязывал все компании, ведущие бизнес в Калифорнии, уведомлять клиентов о нарушениях в отношении их личной информации (персональных данных). На случаи взлома зашифрованной информации не распространялось требование об уведомлении, но в остальном закон – несмотря на то, что был принят только штатом Калифорния – применялся практически ко всем нарушениям во всех крупных компаниях США. Цель S.B. 1386 состояла в том, чтобы помочь частным лицам, таким как служащие штата Калифорния, чья информация была украдена с офисных компьютеров контролера, защитить себя от кражи личных данных и финансового мошенничества в случае кражи их данных. До принятия S.B. 1386 не существовало требования, согласно которому компании должны были уведомлять клиентов о нарушениях, и поэтому о многих инцидентах не сообщалось [7, p. 51].

Как указывает Дж. Вольф, принятие закона S.B. 1386 (а также других аналогичных ему нормативных правовых актов об уведомлении о нарушениях в сфере персональных данных) не только стимулировало продажи киберстрахования, но и изменило содержание полисов киберстрахования, сделав акцент на страховании от утечки данных [7, p. 54]. Это законодательство США привело к возникновению новых издержек для компаний, таких как расходы на уведомление жертв нарушений в соответствии с требованиями законов и т.п.

По мере распространения законов об уведомлении о нарушениях в различных странах, государства, часто с небольшими вариациями, которые усложняли обременительную задачу соблю-

дения разрозненного набора из десятков различных режимов уведомления, продолжали создавать новые финансовые риски для компаний и новые возможности для киберстрахования и т.д. [7, p. 54].

Вместе с тем, в то время как законы об уведомлении о нарушениях данных упростили подачу исков в суд на компании за неспособность защитить личную информацию своих клиентов, режимы ответственности, регулирующие эти инциденты, долгое время оставались далеки от ясности.

Д. Вольф приводит такой пример: в 2011 г., когда у компании Sony произошел взлом данных в системе PlayStation, шло отклонение нескольких коллективных исков о нарушении конфиденциальности данных. Есть и другие примеры. Как пишет Дж. Вольф, практика показала, что тот факт, что частные лица стали получать уведомления о нарушениях, затрагивающих их личную информацию, отнюдь не означало, что компании, допустившие эти нарушения, будут привлечены к ответственности за такие инциденты. Не было четкого набора стандартов или требований безопасности, на которые могли бы указать заявители, чтобы требовать ответственности компании, – другими словами, никто не был уверен, что представляет собой халатность, когда дело касалось кибербезопасности [7, p. 67].

Кроме того, во многих случаях утечка данных и другие виды инцидентов, сопряженных с кибербезопасностью, связаны с множеством различных взаимозависимых организаций. Производители программного и аппаратного обеспечения, дизайн веб-сайтов, операторы связи и хостинги, платежные системы и интернет-провайдеры – все они могут играть определенную роль в совершении взломов, например оставляя уязвимости в коде или будучи не в состоянии обнаружить и заблокировать преступников, действующих в их (цифровой) инфраструктуре. То есть решение о том, кто должен нести ответственность за взломы и утечку данных, во многом зависело от конкретных деталей того или иного инцидента [ibid.].

Тем не менее киберстрахование достаточно долго продолжало развиваться в рамках Страхования коммерческой гражданской ответственности (Commercial General Liability (CGL) Insurance). С появлением киберпреступлений и юридическим признанием их особенностей, полагает Д. Вольф, развитие такой формы, как страхование ответственности от компьютерного мошенничества и киберугроз в качестве разновидности киберстрахования, стал практически неизбежен [7, p. 87].

В разных страховых полисах страховщики предлагали разные определения того, что считается компьютерным мошенничеством, а суды (в США), в свою очередь, придерживались совершенно разных мнений о том, насколько ясны эти формулировки, что они означают и насколько данное преступление должно было совершаться с помощью компьютера, чтобы оно считалось компьютерным мошенничеством. Так, в одном из подходов из формулировок страхового полиса следует, что компьютерное мошенничество – это убытки, непосредственно связанные с использованием любого компьютера для осуществления денежного перевода мошенническим путем, и т.п. [7, p. 90].

Обобщая этапы становления институтов киберстрахования, Дж. Вольф подчеркивает, что если «ранние» полисы киберстрахования были в основном сосредоточены на страховании от утечек персональных данных, а затем в эту сферу добавилось страхование от компьютерного мошенничества, то в настоящее время, по мере расширения спектра онлайн-угроз предприятия, организации и частные лица во всех секторах экономики и повседневной жизни начали сталкиваться с новым набором дорогостоящих и серьезных рисков, начиная от программ-вымогателей и заканчивая перебоями в работе облачных сервисов, экономическим шпионажем и проч. [7, p. 111–112].

Разные государства разрабатывают собственные подходы в развитии киберстрахования – институт киберстрахования бурно развивается.

Далее остановимся подробнее на отдельных примерах его развития.

Опыт Российской Федерации в сфере киберстрахования

Российская компания «Позитивные технологии» приводит такие цифры: мировой показатель среднего совокупного ущерба от утечки данных вырос с 4,45 млн в 2023 г. до 4,88 млн долл. в 2024 г. В России средний ущерб от утечки информации в 2024 г. составил 11,5 млн рублей. Согласно экспертным оценкам, максимальный совокупный ущерб (включая затраты на расследование инцидента) может достигать 140 млн рублей[1].

[1] См.: Утечки конфиденциальных данных из организаций: второе полугодие 2024 года / Positive Technologies. – URL: https://www.ptsecurity.com/research/analytics/utechki-dannyh-aktualnye-ugrozy-vtorogo-polugodiya-2024-dlya-organizaczij/#id3 (дата обращения: 18.11.2025).

В России киберстрахование рассматривается как вид страхования, который защищает от финансовых потерь, связанных с кибератаками, кражей личных данных и другими рисками в цифровой среде [3, с. 38].

Киберугрозы признаются крайне актуальными для российских предприятий, а кибератаки рассматриваются как действенный способ нанести финансовый ущерб. В нашей стране, как отмечают Н.Н. Чибинев и Н.В. Ляшенко, исследователи из Южно-Российского государственного политехнического университета (НПИ) им. М.И. Платова (Новочеркасск), кибератаки происходят во всех сферах деятельности человека и направлены в основном на подрыв безопасности объектов экономики и информационных систем государственных учреждений. Здесь они ссылаются на цифры, которые привел вице-премьер РФ Д.Н. Чернышенко 6 февраля 2024 г., выступая на форуме «Цифровая экономика» в рамках выставки «Россия». Он сообщил, что в 2023 г. российские IT-специалисты отразили более 65 тыс. кибератак на критическую информационную инфраструктуру. При этом следует отметить, что в 2021 г. целью атак был финансовый сектор, а в 2022 г. – государственный сектор [6]. В последние два года ИБ-центр ФСБ регистрирует более 170 кибератак каждый день [4].

Кибератаки в настоящее время становятся самыми распространенными причинами возникновения различных видов преступлений, нередко приводящих к чрезвычайным ситуациям. Характерными примерами возможности возникновения техногенных и социальных чрезвычайных ситуаций от кибератак могут служить события в ряде регионов нашей страны. Это подчеркивает опасность киберугроз как потенциальных чрезвычайных ситуаций. Для борьбы с ними авторы предлагают разработать нормативно-правовые акты и использовать современные технологические решения. На государственном уровне в России они предлагают ввести понятие «киберчрезвычайная ситуация», «кибератака» и «кибербезопасность», хотя они установлены в ГОСТ Р 56205–2014 и ГОСТ Р 56498–2015, а в Уголовном кодексе РФ предусмотрены ст. 272–274 за преступления в сфере компьютерной информации [4].

Инициаторами киберпреступления могут выступать как отдельные лица и организованные группировки, так и правительственные структуры недружественных стран. Основные киберинциденты, с которыми сталкиваются представители бизнеса, – это шифрование данных на рабочих станциях, компрометация банковских счетов, кража или модификация данных о клиентах. Также

крайне актуальным является скрытый киберриск, который возникает при неопределенности в полисе киберстрахования, неразвитости рынка киберстрахования с точки зрения предложения или сложности проверки степени ущерба, вызванного киберсобытием [2, с. 13].

Директор по рискам «СберСтрахования», председатель рабочей группы Всероссийского союза страховщиков (ВСС) Владимир Новиков в рамках Уральского форума «Кибербезопасность в финансах» отметил, что в 2023 г. страховщики в сфере киберстрахования получили около 900 млн руб. По его оценке, это составляет меньше 1% от всех страховых премий. Тем не менее, как показывают статистические данные, объем российского рынка киберстрахования быстро растет, приближаясь к 1 млрд рублей в 2025 г. Рост обусловлен увеличением числа кибератак и утечек данных. Несмотря на это, доля компаний с киберстраховкой остается низкой (6% в 2022 г.). Это обусловлено низкой осведомленностью и непониманием киберстрахования со стороны бизнеса, а также сложностей с обеспечением стандартизированного покрытия со стороны страховщиков[1].

В 2023 г. в России был запущен в работу Центр исследования киберугроз Солар (Solar), который аккумулирует базу знаний о кибератаках. Новым инструментом борьбы с потерями от кибератак является страхование посредством иншуртеха (InsurTech) [3, с. 33] и децентрализованного финансирования, что позволяет предприятиям и организациям улучшить управление рисками. Российскими учеными предлагается выделение InsurTech в самостоятельное направление страхования и создание для него собственных регулятивных инструментов [3, с. 39].

По мнению Н.Н. Чибинева и Н.В. Ляшенко, для достижения целей защиты от киберугроз необходимо:

1) внести в единые нормативно-законодательные акты по безопасности в системе МЧС России понятие о киберчрезвычайной ситуации и порядок ее установления и классификации. Под *киберчрезвычайной ситуацией* они предлагают понимать обстановку на конкретных объектах жизнедеятельности или определенной территории, сложившуюся в результате разрушения их компьютерно-телекоммуникационной инфосферы и повлекшую за

[1] За 2023 год премии по киберстрахованию в России составили около 900 млн рублей // Коммерсантъ. – URL: https://www.kommersant.ru/doc/6510671 (дата обращения: 06.09.2025).

собой ущерб здоровью людей или окружающей среде, приостановку производственной деятельности, значительные материальные потери и нарушение условий жизнедеятельности людей;

2) выполнить Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации», запрещающего использование иностранного программного обеспечения на объектах критической инфраструктуры, принадлежащей госорганам;

3) использовать наиболее эффективный в настоящее время способ обеспечения информационной безопасности – модель Zero Trust, включающую в себя многие слои аутентификации, мониторинг сетевого трафика, криптографию и анализ поведения пользователей. Для реализации концепции Zero Trust используется шлюз кибербезопасности NGFW (NextGeneration Firewall) и применяются классические продукты класса IDM (Identity and Access Management), PAM (Privileged Access Management), EDR (Endpoint Detection and Response) и DLP (Data Loss Prevention);

4) развивать рынок киберстрахования в России как один из видов комплексной защиты от всевозможных киберугроз и др. [4].

Виды киберстрахования в практике зарубежных стран

«*Страхование по требованию*» – инновационная концепция, представленная сектором InsurTech. Этот вид страхования быстро набирает популярность, и некоторые эксперты прогнозируют, что этот развивающийся рынок может вырасти до 190 млрд долл. к 2026 г. Швейцарский исследователь А. Браун определяет страхование по требованию как покрытие эпизодических рисков, предлагающее потребителям индивидуальную защиту в определенные периоды, когда они или их имущество подвергаются риску [4, p. 226].

Страхование по требованию имеет две формы: краткосрочное страхование и страхование на основе универсального базового дохода (Universal Basic Income) (далее – UBI).

Краткосрочное страхование предназначено для защиты от рисков, которые ограничены во времени или повторяются и имеют известный или, по крайней мере, надежно предсказуемый характер воздействия. Распространенными примерами краткосрочных страховых продуктов являются страхование путешествий на одну по-

ездку, временное страхование от несчастных случаев, краткосрочное автострахование и др.

Страхование UBI подходит для ситуаций, когда подверженность потребителей риску меняется во времени. В рамках страхование UBI страховое покрытие активируется полностью автоматически, в зависимости от таких факторов, как местоположение, активность или контекст. По мнению А Брауна, полисы по требованию лучше соответствуют потребностям страховщиков, чем традиционные договоры. Таким образом, действующим страховщикам также следует внедрять инновации в этом направлении [5, p. 228].

Встроенное страхование представляет собой смену парадигмы в предложении и потреблении страховых услуг. Идея заключается в том, чтобы органично интегрировать страховое покрытие в стоимость при продаже нестраховых продуктов и услуг. С ростом популярности цифровых платформ встроенное страхование стало инновационным решением. Оно существенно упрощает процесс покупки страховки для клиентов, создавая единый центр обслуживания для всех их страховых и нестраховых потребностей, устраняя необходимость в многочисленных транзакциях. Хотя в 2020 г. доля встроенного страхования в общем объеме продаж страховых услуг в мире составила всего 6%, его потенциал считается огромным [5, p. 228].

Разновидностями встроенного страхования являются связанное встроенное страхование и пакетное встроенное страхование.

Связанное встроенное страхование подразумевает практику предложения страхования в качестве дополнения к основному продукту или услуге. В этой модели клиенты могут выбрать страховое покрытие, адаптированное к их конкретным потребностям наряду с покупкой основного предложения. Известным примером является покупка онлайн-страховки путешествий на сайтах авиакомпаний или туристических компаний.

Пакетное встроенное страхование подразумевает, что страхование является неотъемлемой частью продукта или услуги. В этом случае клиенты автоматически получают страховое покрытие как часть общего пакета, без необходимости отдельной покупки [5, p. 229].

Рынок киберстрахования в основном представлен коммерческим страхованием, в то время как решения по киберстрахованию на розничном рынке все еще находятся на начальном этапе развития. Так, стандартные полисы страхования имущества и ответст-

венности для коммерческого сектора доступны на большинстве страховых рынков по всему миру. Однако большинство полисов страхования имущества и ответственности покрывают только ущерб физическим активам, таким как производственные мощности, и не включают киберриски. Нередко в договорах страхования не содержится четкого указания о том, будут ли киберсобытия (киберриски) включены или исключены [1, с. 336].

Одной из причин неразвитости киберстрахования, по мнению швейцарского исследователя М. Элинга, может быть то, что как страховщикам, так и страхователям до сих пор неясно, каковы механизмы киберрисковых событий и какую ценность создают полисы киберстрахования [6, p. 215].

Нередки ситуации, когда страхователи полагают, что киберинциденты покрываются страховкой, в то время как страховщик предполагает обратное. Это ведет к юридическим спорам, судебной неопределенности, а судебные издержки увеличивают финансовый риск страховщиков. Судебные споры нередко возникают из того, что во многих случаях оказывается невозможным проверить, в какой степени ущерб связан с киберсобытием и кто должен нести ответственность в данных обстоятельствах.

Вследствие обозначенных проблем страховщики стремятся к более четкому изложению условий договоров двумя способами. Вопервых, страховые компании составляют договоры страхования, явно исключая киберриски из традиционных полисов, и предлагают специальные «отдельные киберполисы». Вовторых, страховые компании могут прямо включать условия киберстрахования в общий страховой полис и соответствующим образом корректировать премии, что приводит к появлению так называемых «позитивных киберполисов» или «пакетных полисов» [6, p. 217].

За последние десять лет, например, в США в сфере страхования сформировался специализированный рынок, предлагающий покрытие киберрисков. Однако, по мнению М. Эллинга, за пределами США киберстрахование применяется мало. Так, в Европе многие корпорации даже не знают о существовании этого вида страхования, и лишь единицы им пользуются [6, p. 210].

По состоянию на 2020 г. мировой рынок киберстрахования оценивается в 5 млрд долл. премий. Компании с покрытием в диапазоне от 100 до 199 млн долл. составляют лишь 25% мирового рынка (1,44 млрд долл. премий от примерно 500 компаний), компании с страховым покрытием более 200 млн долл. составляют

20% мирового рынка (1,1 млрд долл. премий от 250 компаний) [6, p. 210]

Рынок США гораздо более развит, чем европейский, отчасти потому, что в США достаточно давно действуют требования к отчетности о кибератаках с относительно высокими штрафами за нарушения. Новые правила отчетности значительно повысили осведомленность о киберрисках и увеличили спрос, особенно на страхование ответственности (третьих лиц) от киберугроз. Таким образом, на рынке США в основном доминирует страхование от третьих лиц, в то время как те немногие полисы, которые уже существуют в Европе, ориентированы на страхование от первой стороны. В 2018 г. в Европейском союзе также были введены обязательства по предоставлению отчетности об утечках данных, что стало важным фактором развития европейского рынка киберстрахования [6, p. 212].

Информации об азиатском рынке страхования у западных исследователей мало, но, по их оценкам, по сравнению с Европой и США многие азиатские страны по-прежнему отстают в политике и стратегиях киберстрахования. С учетом того, что на Азию приходится 25% мировых кибератак, а в Азиатско-Тихоокеанском регионе расположено 40% мировых центров обработки данных, следует ожидать, что со временем азиатские страны обгонят США и Европу в киберстраховании [6, p. 212].

Перестрахование. По оценкам швейцарских исследователей, в настоящее время около половины своих киберпремий страховые компании передают перестраховщикам. Согласно статистическим данным, только четыре компании перестраховщика принимают более 60% премий; более 75% перестраховщиков имеют премии менее 100 млн долл. [ibid.].

Средняя стоимость полиса киберстрахования в США составляет 1485 долл. в год. Страховые премии варьируются от 650 до 2357 долл. для полиса с ответственностью в один млн долл. Прогнозы динамики рынка киберстрахования исследователи дают неоднозначные [6, p. 212].

Заключение

Киберстрахование – перспективный институт страхования, который, однако, по мнению ученых, пока не получил широкого распространения и отчасти не оправдал ожиданий многих экспертов, а также практиков в сфере страхования. Одним из объяснений

этого может быть ошибочное восприятие киберрисков. Повышение осведомленности субъектов правоотношений в вопросах киберстрахования может способствовать повышению спроса на страхование от киберрисков. Невысокая распространенность киберстрахования связана с отсутствием экспертизы для предварительной оценки защищенности страхователей [6, p. 225]

В российской действительности, для того чтобы занять прочную нишу на рынке информационной безопасности, киберстрахованию потребуется время, в течение которого появятся новые и более доступные предложения, включая комплексные услуги в сфере страхования. На фоне роста киберугроз и более осознанного подхода к вопросам обеспечения информационной и кибербезопасности можно ожидать увеличение спроса на услуги киберстрахования. Отметим, что киберстрахование представляет собой комбинированный продукт, включающий в себя не только страхование рисков, но и сервисную составляющую, которая может включать в себя дополнительные услуги с привлечением партнеров. Опыт других стран может быть полезен России при регулировании проблем страхования киберрисков.

Список литературы

1. Жмурова С.С., Джафаров Д.И. Правовое регулирование страхования киберрисков в России: опыт зарубежных стран и перспективы развития // Право и государство: теория и практика. – 2025. – № 4. – С. 334–337.
2. Клишина Ю.Е., Углицких О.Н., Серафимова В.А. Страхование юридических лиц от киберрисков: проблемы и перспективы развития // Финансы и учетная политика. – 2023. – Вып. 2. – С. 11–14
3. Коданева С.И. InsurTech в России и за рубежом: проблемы и перспективы // Право и цифровая экономика. – 2023. – № 4 (22). – С. 33–41.
4. Чибинев Н.Н., Лященко Н.В. Кибератака как новый вид чрезвычайных ситуаций // Инженерный вестник Дона. – 2024. – № 7. – URL: file:///C:/Users/Администратор/Downloads/kiberataka-kak-novyy-vid-chrezvychaynyh-situatsiy%20(2).pdf (дата обращения: 11.11.2025).
5. Braun A., Haeusle N. Digital Insurance and InsurTech // Handbook of Insurance / ed. by Georges Dionne. – 3 ed. – Cham: Springer Nature: 2025. – Vol. I. – P. 225–251. – URL: https://link.springer.com/chapter/10.1007/978-3-031-69561-2_8 (дата обращения: 11.11.2025).
6. Eling M. Cyber Risk and Cyber Insurance // Handbook of Insurance / ed. by Georges Dionne. – 3 ed. – Cham: Springer Nature, 2025. – Vol. 1. – P. 199–225. – URL: https://link.springer.com/chapter/10.1007/978-3-031-69561-2_7 (дата обращения: 11.11.2025).
7. Wolff J. Cyberinsurance policy: Rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks. – Cambridge: MIT Press, 2022. – 291 p.