По оценке Allied Market Research, к 2022 г. глобальный рынок страхования киберрисков достигнет $14 млрд, а по оценке Allianz, в 2025 г. он будет составлять $20 млрд. В 2016 г. рынок страхования киберрисков в США увеличился на 35%, говорится в исследовании Fitch, до $1,35 млрд, но там считают, что в реальности он больше.

Но премии за киберриски – это капля в море для общего рынка страхования. В 2015 г. страховщики США собрали $1,5–3 млрд таких премий, говорится в февральском исследовании Deloitte (компания ссылается на оценки регуляторов и рейтинговых агентств). А общий размер премий, собранных в США в 2015 г., составил $505,8 млрд. В октябре 2016 г. полис страхования киберрисков был лишь у 29% компаний США.

Всплеск спроса на страхование киберрисков отмечается каждый раз, когда происходит громкая хакерская атака, отмечают эксперты, опрошенные WSJ. Так было, например, после атаки на серверы Yahoo в 2014 г., когда хакеры взломали 500 млн паролей пользователей; кибератаки на Национальный комитет Демократической партии США в июне 2016 г. и взлома IT-системы бюро кредитных историй Equifax, в результате которого в руки злоумышленников могли попасть личные данные 300 млн человек.

В 2017 г. от программ-вымогателей Wannacry и Petya пострадали сотни тысяч компьютеров по всему миру. Одной из жертв стал датский промышленный конгломерат Moller-Maersk, владеющий крупнейшим в мире бизнесом контейнерных перевозок, его убытки составят $200–300 млн, пишет WSJ. У страховой компании AIG после атак Wannacry спрос на страхование киберрисков вырос в Азии на 87%, а в глобальном масштабе – на 38%, сообщает FT.

Tryg, крупнейшая датская страховая компания, ожидает, что через пять лет страховать киберриски будет 90% ее клиентов. «Не бывает сейчас корпоративных клиентов, которые не страхуют здания и автомобили, – сказал Reuters гендиректор Tryg Мортен Хюббе. – Думаю, через несколько лет станет столь же очевидно, что нужно страховать киберриски».

Продать кота в мешке

Рынок страхования киберрисков мог бы расти и быстрее – потенциальный спрос достаточно велик, – если бы не его незрелость. Страховщики не понимают, что именно они продают, а их клиенты – что именно они покупают. «Появилось так много новых страховых продуктов, которые еще не испытаны, – сказал WSJ вице-президент страховой компании Travelers Тим Фрэнсис, – что в один прекрасный день начнут поступать обращения о страховых случаях, и тогда мы узнаем, значат ли слова, которые мы использовали в полисах, именно то, что мы имели в виду». Но зачастую разбираться с этим приходится юристам, добавляет он.

«Что будет, если завтра некий веб-хостинг подвергнется DDoS-атаке или его взломают хакеры и компании, которые пользуются им, не смогут обслуживать своих клиентов? Откуда нам знать, что купившие у нас полис страхования киберрисков не хранят все в одной корзине – облачный сервис, веб-хостинг, почтовый сервер, SaaS (программное обеспечение как услуга)?» – отмечает один из страховщиков, участвовавший в исследовании Deloitte.

Несколько респондентов Deloitte сравнивали риски, связанные с кибератаками, с рисками терактов: в обоих случаях группа лиц намеренно пытается нанести ущерб, такие атаки могут произойти когда угодно, где угодно и пострадать от них может кто угодно. Из-за страха получить огромные убытки многие страховые и перестраховочные компании после 11 сентября 2001 г. перестали страховать риски, связанные с терроризмом. «В конечном итоге все сводится к тому, что мы не понимаем, какие риски мы берем на себя, – сказал Deloitte еще один страховщик. – У нас недостаточно информации о том, где источник риска, чтобы мы могли его сократить».

В мире происходит настоящая гонка вооружений в киберсекторе и возможность совершить масштабную кибератаку есть у несколько десятков стран, отмечает Брюс Боланд, IT-директор в странах Азии компании FireEye, занимающейся вопросами безопасности. «Страховые полисы обычно не покрывают военные действия. А это значит, что чрезвычайно важным становится определение кибератак: кто знает, кто за ними стоит?» – говорит он.

Но даже если страховой полис от киберрисков есть, не факт, что в случае взлома он покроет все убытки. Тем более что, например, репутационный ущерб сразу может и не

проявиться. В июне 2014 г. работающая в США сеть ресторанов China Bistro, платившая за такую услугу $134 000 в год, узнала, что хакеры украли у нее номера кредиток 60 000 клиентов. Страховщик выплатил China Bistro $1,7 млн в качестве компенсации за расследование и судебные издержки, но самой сети пришлось заплатить $1,9 млн компании, которая занимается процессингом карт, пишет WSJ.

Россия только начинает

Страхование информационных рисков является неизвестным и непонятным для большинства потребителей этой услуги, говорится в материалах правительственной программы «Цифровая экономика» на 2017–2020 гг.» (с проектом документов ознакомились «Ведомости»). В России заключено менее 20 договоров страхования, большинство оформлено предприятиями с иностранным участием в «дочках» иностранных страховщиков. По словам зампреда ЦБ Владимира Чистюхина, проблема есть и на рынках других стран: страховые компании и регуляторы говорят, что этот вид развивается, но устойчивым тренд назвать нельзя.

Содержание страховой услуги по киберстрахованию не стандартизовано, в мировой практике варьируется от страны к стране и зависит от законодательной среды, говорится в материалах программы. «Калька» с американского или западноевропейского продукта практически не отвечает потребностям предприятий в российской юрисдикции. В ней предлагается с участием государства формировать тарифы, стандарты и привлекать для работы Российскую национальную перестраховочную компанию. А также введение обязательного страхования от киберугроз с 2020 г. для большинства стратегических отраслей. Однако с этим пока не согласен ЦБ (см. врез).

Есть проблемы и с выделением этого вида страхования в отдельный класс – в отличие от страхования для защиты «физических» активов предприятия расходы на страхование киберрисков не могут быть исключены из налоговой базы компаний, что снижает экономический интерес к такому страхованию. В программе предусмотрены изменения в страховом законодательстве, уравнивающие страхование информационных и «физических» активов.

Пока гром не грянул

Многие крупные и средние банки страхуют риски электронных и компьютерных преступлений в рамках договора комплексного банковского страхования от преступлений, говорит начальник управления страхования финансовых институтов и партнеров компании «Ингосстрах» Дмитрий Шапошников. В нефинансовом секторе, по его словам, активный интерес к страхованию киберрисков начал появляться только в последнее время. В «Ингосстрах» нередко обращаются крупные компании, опасающиеся приостановки основной деятельности, если выйдут из строя IT-системы.
Владимир Чистюхин, зампред ЦБ: Мое отношение к тому, чтобы придать страхованию киберрисков обязательный характер, отрицательное. В настоящее время мы не разобрались с предметом – что такое киберриски, из чего они состоят, мы в принципе не знаем практику страховых компаний – готовы они страховать киберриски либо нет. Для меня вопрос звучит не в том, чтобы придавать обязательность, а в том, чтобы начинать страховать киберриски.

У компании «Альфастрахование» на начало сентября было несколько десятков корпоративных клиентов, страхующих киберриски с общей суммой покрытия 100 млн евро, рассказал руководитель управления страхования финансовых рисков компании Андрей Макаренцев. Он также отмечает, что чаще всего киберстрахование как дополнительное покрытие к основному полису выбирают банки. По словам Макаренцева, клиенты недооценивают многие киберриски, включая вывод из строя оборудования в результате хакерских атак, организацию взрывов, пожаров, ложного срабатывания сигнализаций в результате взлома и нарушения систем безопасности через внешний доступ. Но он также отмечает, что спрос на страхование киберрисков постепенно растет.

«РЕСО-гарантия» не страхует от киберугроз, говорит заместитель гендиректора компании Игорь Иванов. По его словам, у компании нет данных для корректного расчета такого риска. «Видимо, таких данных пока недостаточно даже у крупнейших мировых страховщиков, хотя в последнее время запрос на такие или связанные частично с кибербезопасностью страховые услуги появляется», – добавляет он. Но «РЕСО-гарантия» участвует в страховании рисков международных клиентов AXA, которая является одним из ее акционеров.

Рынок страхования киберрисков только начинает формироваться и не все хорошо представляют, как осуществлять расчет потенциального ущерба, согласен старший менеджер департамента по управлению рисками компании Deloitte Анатолий Остроглазов. Однако «продукты по киберрискам уже у многих страховщиков готовы, поэтому новым игрокам будет несложно адаптироваться», отмечает он. Хотя пока

киберриски не реализуются, многие организации не готовы рассматривать их всерьез и надеются на собственную защиту, добавляет Остроглазов, в первую очередь страховые продукты по киберрискам будут рассматривать банки, поскольку там участились случаи вывода активов.

Источник: Ведомости, 08.11.2017