КИБЕРРИСКИ: мнение участников рынка

Есть ли сегодня в России предпосылки для развития страхования киберрисков и что может быть препятствием для этого вида страхования? «Современные страховые технологии» представляют мнение ведущих игроков рынка.

Дмитрий Грузинцев

Руководитель отдела GrECo Russia

Большинство инновационных страховых продуктов в России основаны на западных практиках, которые адаптируются в соответствии с российским законодательством и особенностями рынка. Так было со страхованием ответственности директоров и руководителей (D&O), и сейчас аналогичные процессы происходят со страхованием киберрисков. В западных странах это активно развивающееся направление, а большинство крупных компаний уже имеет договор страхования. Также страхование киберрисков активно приобретают компании среднего и малого бизнеса. Совокупное проникновение страхования киберрисков можно оценить на уровне 70–80 %. Как следствие, за рубежом уже есть урегулированные страховые случаи и выплаты по договорам страхования.

В России все гораздо скромнее. Реальный интерес к страхованию киберрисков возник после серии хакерских атак с использованием вирусов Petya и Wannacry, произошедших во второй половине 2017 года. Развитию рынка страхования киберрисков будет способствовать изучение западного опыта, изменение российского законодательства по защите данных, формирование инфраструктуры, необходимой для страхования киберрисков – специализированные инсти-

Анастасии Селезнева

Независимый эксперт

Страхование перерывов в производстве от реализации киберрисков не существует отдельно, вне страхования киберрисков. Это одно из покрытий комплексного продукта. Продукт вызывает большой интерес на российском рынке. Но на данный момент заключенных договоров не так много. Яркий интерес к продукту возник после печально знаменитых атак 2017 года, когда бизнес увидел, что на самом деле этот риск существует, когда большое количество компаний пострадало. Но едва ситуация успокоилась, успокоились и менеджеры предприятий, отвечающие за безопасность. Ситуация характерная для России: пока гром не грянет, мужик не перекрестится.

Среди топовых компаний, как и среди компаний среднего и малого бизнеса, многие проявляют интерес к страхованию от киберрисков. Некоторые риск-менеджеры уже имеют представление, зачем этот продукт нужен. Раздумья о необходимости приобретения соответствующего страхового покрытия наблюдаются и у ИТ-специалистов. Раньше они считали единственным спасением от проблем наличие хороших антивирусных программ. Сейчас люди уже начинают понимать, что далеко не от всего антивирус может их защитить.

Я оцениваю текущую ситуацию как пограничную. Думаю, что интересный громкий инцидент, который выйдет в публичное пространство, подтолкнет большое количество предприятий к заключению договоров страхования. Если будет такой негативный толчок, то страхование от киберрисков приобретет массовый характер, так же, как это развивается на западе.

туты сюрвееров, аварийных комиссаров (loss adjusters) и т.п. Хорошим драйвером являются международные бизнес-форумы, в которых принимают участие и делятся своим опытом представители крупнейших компаний мира, в том числе из России. По данным отчета Всемирного экономического форума в 2018 году кибератаки находятся на 3-м месте из топ-10 по вероятности возникновения и на 6-м по размеру ущерба. В будущем значимость данных рисков будет расти. Описанные выше факторы способствуют развитию страхования киберрисков в России.

Одним из основных препятствий развития направления в России является слабое информирование российского бизнес-сообщества о возможности страхования таких рисков, о подходах к оценке рисков и урегулированию страховых случаев. Большинство компаний воспринимают киберугрозы как нечто, касающееся исключительно ИТ-специалистов. Многим не ясно, например, как будет проходить анализ риска или как будет считаться убыток от перерыва в деятельности в результате кибератаки. Во многом подходы к анализу рисков и урегулированию убытков по договорам страхования киберрисков схожи с классическими видами страхования. Наша задача как страхового брокера, используя международную практику и российский опыт, помочь компаниям понять возможность страхования киберрисков, а также консультировать на всех этапах от идентификации и оценки риска до урегулирования страховых случаев.