Рабочая группа по страхованию киберрисков критической инфраструктуры формирует предложения по введению в РФ обязательного или вмененного вида страхования в рамках проекта "Цифровая экономика", сообщила заместитель председателя правления Российской национальной перестраховочной компании (РНПК) Наталья Карпова, выступая на ноябрьских встречах перестраховщиков.

"Пока в рабочей группе обсуждается принятие закона об обязательном страховании от киберугроз объектов критически значимой инфраструктуры, в том числе предприятий оборонного комплекса, гидро-, электро— и теплостанций, ключевых объектов социального назначения. Введение такого страхования в обязательном виде потребует разработки специального закона", — сообщила она.

По словам Н.Карповой, в рабочую группу входят представители двух компаний — РНПК и "Сбербанк страхование". Альтернативным вариантом реализации страховой защиты от киберугроз в стране могла бы стать система вмененного страхования таких рисков для объектов критической инфраструктуры.

"Согласно планам правительства, в 2020 году в России должны быть внедрены индустриальные стандарты по обязательному аудиту информационной безопасности. Предполагается, что объекты, включенные в соответствующий список, должны будут в обязательном порядке проводить аудит информационной безопасности своих систем. Приобретение договора страхования киберрисков может быть включено как составляющая часть такой процедуры. При этом предприятия, покупающие такую защиту, могут относить подобные расходы на себестоимость", — высказала предположение Н.Карпова.

В отношении коммерческих структур, в значительной степени подверженных киберугрозам, таким как предприятия интернет-коммерции, можно было бы вести речь о следующем. Пока в полисах страхования имущества ущерб от кибератак всегда является исключением из страхового покрытия, выплат ждать не приходится. Разработка системных подходов, стандартов принятия рисков на страхование, а также правил выплат, определение самих страховых событий в результате могут позволить включить в продаваемые полисы имущественного страхования дополнительные риски защиты от кибератак, которые сегодня отказываются в числе исключений, считает Н.Карпова.

Он подчеркнула, что до недавнего времени киберстрахование воспринималось как полная экзотика даже страховыми компаниями. Они только пытаются определить подходы к новому виду защиты, западные разработки на эту тему, к сожалению, прямо применить невозможно с учетом особенностей российского законодательства, сказала представитель РНПК.

Пока рабочая группа по страхованию киберрисков определила несколько ключевых подходов к будущему виду страхования.

"Необходимо, с одной стороны, упростить процедуру оценки риска, создать простые

понятные продукты, начать формировать статистику по киберстрахованию на рынке РФ", — пояснила Н.Карпова, добавив, что первопроходцем в создании простых "коробочных" продуктов по киберстрахованию оказалась компания "Сбербанк страхование", которая планирует внедрить три линейки полисов, начав с работы с предприятиями малого бизнеса. По ее словам, первая самая простая линейка полисов уже продается, в разработке сложные полисы по защите от киберрисков и промежуточные, покрытие по ним минимальное, они не требуют проведения дорогостоящего аудита безопасности предприятий (согласно оценке экспертов в страховании киберрисков, стоимость аудита безопасности в РФ начинается от 1 млн рублей — ИФ).

При этом Н.Карпова уточнила, что полисы страхуют риски перерыва в производстве, связанные с ущербом от кибератак.

"В принципе регулирование убытков по этому виду страхования, как мы полагаем, может быть только на ауторсинге. В настоящее время в России работают три компании, способные провести оценку убытков, такая работа оплачивается страховой компанией. Пока для нас остается не вполне ясной оценка ситуации, при которой страховщик может привлечь экспертов для вынесения решения о причинах события. В случае, если таковое не будет признано страховым, на кого должны лечь расходы по оплате подобной экспертизы?", — сказала представитель РНПК.

Со своей стороны, компания готова создать небольшую емкость для перестрахования подобных рисков. "Это необходимо для того, чтобы начать получать опыт практической работы с ними", — добавила зампред правления компании.

Такую же цель получения нового опыта, скорее всего, преследует "Сбербанк страхование", начав тестировать соответствующие программы.

Н.Карпова убеждена, что у страхования от киберугроз большое будущее. Так, в 2016 году сборы по этому виду бизнеса в Европе составили $2,5 млрд. Этот показатель, как предполагают западные эксперты, может увеличиться до $7,5 млрд к 2020 году.

Она отметила, что информация об убытках от кибератак неохотно публикуется даже западными партнерами. Достаточно широко известен пример информационной атаки на атомную электростанцию в Бушере, которая вывела из строя 1,3 тыс. центрифуг в установках по обогащению урана. Вирусом было заражено 30 тыс. объектов, что привело к переносу запуска АЭС "Бушер".

Также в практике анализа возможных ущербов от вирусных атак зафиксировано проникновение в систему медицинского учреждения с целью перехвата управления электрокардиостимуляторами и дефибрилляторами. Атака на реанимационный комплекс учреждения создает угрозу человеческим жизням, а не только имущественным комплексам.

В ходе дискуссии по поводу обязательного и вмененного вида страхования участники встречи говорили о необходимости обязательного характера страхования подобных рисков для таких поставок, как госуслуги, оборонные предприятия, другие критически важные объекты экономики.

Вместе с тем, представитель компании AIG сказала, что в подходах к организации нового вида бизнеса потребуется определиться с приоритетами и ориентироваться на индивидуальные потребности разных групп клиентов.

"Надо понять, какую защиту критически важно получить страхователю — защиту от перерывов в производстве при кибератаках, защиту от потери информации или защиту

от потери самих информационных систем", — сказала она. Кроме того, как показало обсуждение, западные варианты страхования киберрисков в основном ориентированы на страхование ответственности за утрату или передачу персональных данных, что пока считается не слишком актуальным для России. По оценке аналитиков, объем убытков от кибератак в Европе к 2019 году может достигнуть $2 трлн.

Источник: Финмаркет, 21.11.2017