Стоимость страховки

Вопрос «адекватности» стоимости страховки является извечным на страховом рынке, и не юристам его комментировать по существу.

Мы лишь приведем известную нам сухую статистику:

- на российском страховом рынке страховой тариф (отношение страховой премии к страховой сумме) по договорам страхования киберрисков до атаки на ИТ-инфраструктуру ПАО «Аэрофлот» составлял от 1% до 1,5%, со средним значением около 1,2%. Таким образом, договор с покрытием в 1 млрд. рублей обошелся бы российскому страхователю в среднем в 12 млн. рублей. Возможно, из-за текущего всплеска внимания к данному страховому продукту страховой тариф по нему может несколько подрасти;
- согласно данным RED Security SOC, общее количество кибератак на российские компании с января по июнь 2025 г. превысило 63 тыс. Это на 27% больше, чем за аналогичный период 2024 г.

Емкость страхового рынка

Исходя из имеющейся у нас информации, без особых сложностей на российском страховом рынке можно «собрать» страховую сумму по договору страхования киберрисков в размере до 2 млрд. рублей (чуть сложнее – до 3 млрд. рублей). Страховую сумму более 3 млрд. руб. без поддержки РНПК будет собрать уже затруднительно.

Объем страхового покрытия и сложность договора

Используемые на российском страховом рынке формы договоров страхования киберрисков являются достаточно объемными и сложными по своей структуре и терминологии. Это обусловлено, прежде всего, большим числом страховых покрытий, предоставляемых по таким договорам, а также спецификой страхуемых рисков.

Уйти от объемности и определенной сложности договоров страхования киберрисков не получится, но обеспечить их работоспособность и эффективную защиту интересов застрахованных лиц при правильной доработке условий договоров страхования вполне возможно. Исходя из нашей практики, страховщики готовы принимать правки (и вполне объемные) к договорам страхования, особенно, если они юридически обоснованы.

На настоящий момент российские страховщики предлагают широкое по объему страховое покрытие по договорам страхования киберрисков, не уступающее покрытию, предлагаемому за рубежом.

Так предоставляемые по российским договорам страхования киберрисков страховые покрытия можно обобщенно разделить на пять основных групп:

1. страхование имущества – покрываются риски утраты (гибели), недостачи или повреждения в результате киберинцидента имущества застрахованного лица (включая хищение денежных средств и акций в электронной форме);

2. страхование перерыва в деятельности – покрываются риски неполучения (недополучения) из-за киберинцидента застрахованным лицом ожидаемых доходов;

3. страхование ущерба деловой репутации – покрываются риски недополучения застрахованным лицом прибыли в результате сокращения объемов продаж товаров (работ, услуг) из-за оттока клиентов в связи с обнародованием информации о киберинциденте;

4. страхование гражданской ответственности – покрываются риски привлечения застрахованного лица к гражданской ответственности (суммы такой ответственности) перед третьими лицами, которая может возникнуть из-за киберинцидента в результате причинения вреда жизни, здоровью или имуществу третьих лиц (включая компенсацию морального вреда); а также

5. страхование расходов – покрываются риски несения застрахованным лицом различных расходов, связанных с киберинцидентом (например, расходов на юридическую защиту компании от привлечения к гражданской или административной ответственности, расходов на консультантов по связям с общественностью, расходов на уведомление пострадавших о нарушении конфиденциальности их данных, расходов на диагностику информационной системы, так называемых «расходов на форензик», расходов на сохранение клиентов, и пр. расходов). Перечень таких возможных расходов является очень широким и может быть адаптирован под потребности конкретного застрахованного лица.

Таким образом, на российском страховом рынке можно приобрести широкое и (при правильной доработке) эффективно работающее страховое покрытие киберрисков, адаптированное под потребности соответствующего застрахованного лица.

Необходимость раскрытия большого объема информации

Учитывая особую чувствительность российских компаний к предоставлению третьим лицам информации об ИТ-инфраструктуре и информационной безопасности, российские страховщики зачастую готовы заключать договоры страхования киберрисков без проведения IT-аудита и ограничиваются получением от страхователя ответов на вопросы специального (развернутого) вопросника.

Страхование административных штрафов

После ужесточения ответственности за нарушения законодательства о персональных данных на страховом рынке появилась позиция (поддержанная некоторыми страховщиками), что в определенных случаях административные штрафы, наложенные на компанию за нарушение законодательства о персональных данных, могут быть застрахованы в пользу самой компании по договору страхования киберрисков.

Насколько нам известно, Всероссийский союз страховщиков не поддержал данную позицию.

Данная позиция является очень смелой и, возможно, отражающей потребности некоторых операторов персональных данных, но не соответствующей текущему общепринятому толкованию российского законодательства, а именно п. 1 ст. 928 ГК РФ (запрещающего страхование противоправных интересов).

В тоже время по договору страхования киберрисков можно застраховать расходы на юридическую защиту компании от привлечения к административной ответственности.

В наших дальнейших постах мы более подробно остановимся на различных актуальных вопросах страхования киберрисков в России.