

Страхование рисков информационной безопасности

написано Александр Астахов | 14 июня, 2023

По прогнозам ряда экспертов российский рынок кибер-страхования к 2025 году достигнет 1 млрд. рублей. Под кибер-страхованием понимается страхование от убытков, связанных с реализацией кибер-угроз в отношении застрахованного. Другими словами, речь идет о страховании кибер-рисков, а точнее остаточных кибер-рисков, а еще точнее остаточных информационных рисков или рисков ИБ (терминология никак не устоится).

Предпосылки страхования кибер-рисков

Тема страхования рисков ИБ мусолится с начала нынешнего века. На памяти автора за последние лет 10-15 неоднократно делались попытки запуска подобного бизнеса страховыми компаниями совместно с ИБ-интеграторами, но дальше 1-2 страховых договоров дело не шло по понятным причинам, главным образом, из-за сложности объективной количественной оценки риска ИБ. Страхователи используют статистические методы оценки, а оценка рисков ИБ в основном носит экспертный характер.

Кроме этого, в России законодательство в части определения ответственности за нарушения и преступления в сфере ИБ (кибер-преступления) развито слабо, а исполняется еще слабее. Сумма штрафов варьируется от 1 до 50 тыс. рублей. Т.е. компании не испытывают достаточного «регулятивного» давления для движения в сторону страхования кибер-рисков.

В то же время потребность в страховании кибер-рисков начинает обществом осознаваться, по мере осознания эфемерности и неэффективности большинства реализуемых компаниями мер по защите информации и по мере экспоненциального возрастания соответствующих рисков. Поскольку большинство компаний не только не в состоянии защититься от кибер-угроз, но и хотя бы

осознать эти кибер-угрозы, то единственным выходом становится страхование своей ответственности и возможных убытков.

Ситуация должна измениться уже в ближайшие годы. В рамках программы «Цифровая экономика» государство реализует меры, направленные на формирование цивилизованного рынка кибер-страхования в России. Одной из таких мер может стать обязательная покупка полиса страхования кибер-рисков.

В настоящее время объем страховых премий в России на данном рынке не превышает 10 млн рублей. Однако согласно оценкам Mains Insurance Brokers & Consultants, уже в 2019 году начнется экспоненциальный рост рынка, а в 2025 году его объем достигнет 1 млрд рублей. В подразделениях риск-менеджмента корпоративных клиентов наблюдается активность, связанная с подготовкой стратегии сокращения ущерба от киберрисков через инструменты страхования.

Механизм страхования кибер-рисков

Процедура страхования кибер-рисков значительно сложнее и дороже любой другой процедуры страхования и это еще одна причина отсутствия данного рынка в России. Компании, желающей застраховать свои кибер-риски, надо пройти следующие стадии.

Предварительная стадия:

- Предварительное анкетирование (проводится страховой компанией или страховым брокером)
- Выбор экспертной организации для проведения предварительного аудита (из числа организаций, аккредитованных страховой компанией)
- Предварительный аудит и оценка рисков ИБ (проводится экспертной организацией)
- Реализация мер по уменьшению рисков, внедрение СЗИ и процессов ИБ (проводится интегратором, лицензиатом ФСТЭК/ФСБ)
- Пост-аудит и оценка остаточных рисков ИБ (проводится той

же экспертной организацией-аудитором)

Заключение договора страхования:

- Определение областей страхования
- Определение размеров страхового покрытия
- Определение размеров страховых взносов
- Формирования комплексного договора (учитывающего специфику конкретного клиента)

Страховое покрытие может включать в себя:

- Расходы страхователя на защиту в суде
- Расходы на восстановление репутации
- Расходы на управление кризисными ситуациями
- Расходы на восстановление данных
- Расходы на кибер-вымогателей
- Ущерб, причиненный третьим лицам
- Убытки от прерывания производственного процесса

Урегулирование инцидента и получение страховых выплат:

- Обнаружение инцидента ИБ и реагирование на него (от скорости реагирования, как правило, зависит размер ущерба и соответствующие страховые выплаты)
- Расследование инцидента ИБ (определение того, является ли данный инцидент страховым случаем, оценка ущерба). Расследование проводится специализированной экспертной организацией, аккредитованной страховой компанией.
- Получение страхового возмещения

Нужен мега-интегратор ИБ?

Если посмотреть на описанную выше процедуру страхования кибер-рисков, то можно заметить, что услуга по страхованию там даже

не основная, т.к. помимо страховой компании в ней задействованы еще не менее трех экспертных организаций: «аудитор», «интегратор» и «следователь». Т.е. страхование кибер-риска – это часть набора сервисов ИБ, которые необходимы любой организации для того, чтобы обеспечить адекватную защиту своих активов в так называемом «цифровом мире». Собрать эту всю мозаику воедино (брокера, страховщика, аудитора, интегратора, следователя и т.п.) и предложить клиентам интегрированный набор сервисов ИБ может только некий глобальный провайдер ИБ-сервисов (мега-интегратор), т.к. страховщикам эта задача вряд ли по силам. Мега-интегратор ИБ не должен сам оказывать никаких услуг по обеспечению ИБ из перечисленного выше набора. Его задача – управление взаимодействием между поставщиками и потребителями сервисов ИБ, включая страхование, а также аккредитация и контроль участников процесса.

Выводы

Такая вот сложная и дорогая процедура страхования кибер-рисков получается. Но что же тут поделаешь, когда стоимость кибер-инцидентов может составлять миллиарды долларов, как при взломе хакерами сети Sony PlayStation, и совокупный годовой доход только российских хакеров стремится к той же величине. Эффективных же способов минимизации кибер-рисков либо не существует, либо они недоступны большинству компаний, в связи с чем, они тратят значительные средства на защиту информации, не получая реальной защиты и оставаясь лицом к лицу со своими кибер-рисками.

Первоисточник

А написан этот материал был по следам роскошного бизнес-завтрака, организованного страховым брокером Mains Insurance Brokers & Consultants, на котором были анонсированы материалы исследования рынка страхования кибер-рисков в России.

<http://iso27000.ru/novosti-i-sobytiya/rynok-kiber-strahovaniya>

[-k-2025-godu-dostignet-1-mlrd-rublei](#)