Начало страхованию киберрисков в России положили дочерние структуры международных страховщиков около 7 лет назад, однако реальный интерес к страхованию со стороны рынка появился не больше чем 2-3 года назад. При этом пока работать в этом сегменте отважились от силы пять крупных российских страховщиков.

В качестве страхования от киберрисков российские компании предлагают, как правило, расширение для действующего классического покрытия с триггером кибератаки или же реализуют отдельный полис, покрывающий различные ущербы от киберпреступлений для физических и юридических лиц.

Одним из самых популярных продуктов для физлиц, по данным страховщиков, является страхование средств на банковских картах. По данным ЦБ РФ, в прошлом году объем несанкционированных операций с платежными картами в России в вырос на 44% по сравнению с 2017 годом и составил 1,385 млрд рублей. Одно из самых частых хищений денег физлиц совершается через получение мошенниками несанкционированного прямого доступа к электронным средствам платежа владельцев карт.

Что касается страховых выплат, то страховые компании не раскрывают статистику, признавая, что пока никаких крупных инцидентов по данным договорам не возникало. Одной из причин является то, что, как правило, страхованием от подобных рисков интересуются клиенты, которые предприняли достаточные меры безопасности для предотвращения случаев наступления кибератак.

Первые шаги

СК «АльфаСтрахование» выпустила продукт страхования от киберопасностей в 2018 году. Как пояснили «Интерфаксу» в компании, базовый пакет полиса покрывает риски утраты, разглашения и искажения данных, программ, а также включает расследование и диагностику кибератаки. На стоимость страхования влияет род деятельности страхователя и результаты оценки рискозащищенности. Страховые суммы по полисам начинаются от 5 млн рублей и могут превышать 150 млн рублей. При этом в компании отметили, что в первую очередь страховкой интересуются компании IT-сектора и финансовые институты, также есть спрос со стороны добывающей, перерабатывающей, машиностроительной отраслей и медицинской сферы. За последний год компания заключила более 10 договоров страхования от киберрисков.

«У «АльфаСтрахования» на данный момент времени выплат по данному виду не было. Этот вид страхования — новый не только для нас, но и в целом в России. Мы уверены, что урегулирование первых страховых случаев повлечет за собой стремительный рост интереса и увеличение количества заключенных договоров», — сообщила агентству руководитель управления страхования финансовых рисков департамента страхования финансовых рисков и ответственности «АльфаСтрахования» Анастасия Селезнева.

Стремительного развития этого сегмента в ближайшие годы также ожидают специалисты «Сбербанк страхования». В 2017 году компания включила в пакет

страхования для малых предприятий риск перерыва в производстве в результате кибератак. За первый год действия программы такие полисы оформили около 3,5 тыс. клиентов, а за 6 месяцев 2019 года были застрахованы около 5 тыс. корпоративных клиентов от киберрисков. В конце 2018 года «Сбербанк страхование» предложило подобную страховку физлицам, включив риск киберугроз в продукт по страхованию банковских карт. За полгода действия программы такие полисы оформили около 2 млн клиентов. Помимо этого, около 3 млн клиентов застраховали свои смартфоны и планшеты.

Как сообщил агентству и.о. гендиректора «Сбербанк страхования» Дмитрий Попов, среди юрлиц интерес к этому виду страхования в основном проявляют ритейлеры и лесная промышленность. В частности, «Сбербанк страхование» застраховало от киберрисков информационные системы и ресурсы компании «Додо пицца». Программа предусматривает страхование убытков от перерыва в хозяйственной деятельности и от несанкционированного списания денег со счета клиента в результате киберинцидента, а также страхование гражданской ответственности за вред, который может быть причинен третьим лицам, в результате киберинцидента.

Официально программа продаж от киберпреступлений также была запущена в «Ингосстрахе», где первые договоры были заключены осенью 2017 года. В «СОГАЗе» продукт по страхованию от кибератак был запущен в начале прошлого года. Обладателям полисам покрывается ущерб от перерывов в деятельности, расходы на восстановление системы и дешифровку данных, а также расходы по минимизации последствий и расследованию причин кибератаки. В компании наблюдают растущий интерес к страхованию киберрисков со стороны финансовых институтов, предприятий энергетической отрасли, нефтегазового сектора, телекоммуникационных компаний и транспортных операторов.

В СК «Арсеналъ» продажи полисов страхования от компьютерных преступлений начались в 2013 году. В компании пояснили «Интерфаксу», что самым продаваемым стал продукт по страхованию рисков держателей банковских карт от противоправных действий третьих лиц с использованием реквизитов банковской карты. В планах страховщика — расширять функциональность продукта по банковским картам и запустить страхование в корпоративном секторе.

Отсутствие прецедентов

Опрошенные «Интерфаксом» эксперты единогласны в том, что сегмент страхования от киберрисков в нашей стране находится в зачаточном состоянии, и большинство компаний не имеют подобных продуктов.

Такой вид страхования, к примеру, отсутствует в «РЕСО-Гарантии» и «Росгосстрахе», так как в отличие от стран Запада в России данный сегмент страхования развит крайне слабо.

«Основная причина — в разнице законодательства, так как фактически отсутствует законодательная и судебная база по ответственности за неразглашение персональных данных, что влечет низкий интерес у российских компаний (в первую очередь финансовый сектор и сектор услуг) в страховании от подобных рисков», — пояснили агентству в «Росгосстрахе».

При этом в страховой компании видят небольшой рост интереса к страхованию от киберрисков у промышленных предприятий, где кибератаки могут привести к поломкам дорогостоящего производственного оборудования и существенным перерывам в

производстве.
«Однако здесь также существует естественное ограничение в доступных страховых емкостях. Российские страховые компании по отдельности не обладают существенными емкостями, чтобы самостоятельно на себе держать подобные риски по крупным предприятиям, а западные перестраховочные рынки на данном этапе практически не принимают подобные риски из РФ», — сообщили в компании.
Руководитель отдела страхования финансовых рисков дочерней компании AIG в России Владимир Кремер считает, что для развития данного сегмента необходимо ужесточение закона о защите персональных данных, который должен стать немного строже к нарушителям, а также должна появиться соответствующая судебная практика.
«В нашей действительности мы постоянно сталкиваемся с нарушениями — совсем недавно мы слышали о серьезной утечке данных сотрудников крупной российской компании, а базы данных наших с вами телефонов утекают постоянно. К сожалению, никто не слышал о том, что регулятор установил и хоть как-то покарал виновных в этом — лишил лицензии, заставил оплатить возмещение пострадавшим, присудил штраф в размере такого-то процента от оборота. Более четкое понимание того, что ответственность за данные — это не пустой звук, не только даст дополнительный толчок к развитию страхования киберрисков, но и поможет существенно сократить количество инцидентов, вследствие которых утекают базы данных и другая конфиденциальная информация», — пояснил Кремер.
В «АльфаСтраховании» сообщили, что многие компании, даже сталкиваясь с кибератаками, не знают, что такие риски могут быть покрыты страхованием.
Во Всероссийском союзе страховщиков (ВСС) существует рабочая группа по страхованию от кибер-рисков, в которую входят 16 страховщиков, среди которых «Сбербанк страхование», «РЕСО-Гарантия», «Ингосстрах», «СОГАЗ», САО «ВСК», «Группа Ренессанс страхование», «Российская национальная перестраховочная компания» (РНПК).
Вице-президент ВСС, руководитель рабочей группы по страхованию киберрисков при комитете по страхованию имущества и юридических лиц Светлана Гусар сообщила агентству, что пока группа занимается выработкой методологических подходов, сбором информации по киберрискам и ее анализом.
«Рабочая группа взаимодействует с Торгово-промышленной палатой РФ, основное препятствие в сборе информации связано с тем, что компании крайне неохотно делятся сведениями о том, как защищаются их IT системы. На заседаниях обсуждаются в том числе вопросы организации защиты платежных карт», — сказала Гусар агентству.
При этом ЦБ РФ регулярно публикует статистику в обзорах по несанкционированным списаниям с банковских карт, эмитированным в стране. В числе факторов, облегчающих совершение незаконных действий со стороны мошенников — использование облачных технологий, аутсорсинга в работе с данными, простота используемых клиентами паролей и другие причины. Внешними угрозами остаются хакерские атаки и кража данных. Кроме того, злоумышленники взламывают соцсети для получения дополнительных данных, которые помогают получить доступ к финансовым средствам пользователей.

Финмаркет, 4 сентября 2019 г.