

Получение крупных штрафов за утечку конфиденциальной информации и персональных данных может мотивировать руководство предприятий делать выбор в пользу страхования киберрисков. Такое мнение высказал заместитель руководителя управления страхования кредитных, финансовых и предпринимательских рисков страховой компании «Согласие» Виталий Ус.

«Для развития киберстрахования в России требуются драйверы, стимулирующие интерес, – отметил он. – В США, например, драйвером является перспектива выплат крупных штрафов организациями за утечку конфиденциальной информации и персональных данных. В нашей стране редкость, когда организация несет убытки из-за того, что в результате кибератак пострадали клиенты».

По его словам, страховщики могут помочь предприятиям и организациям в борьбе с растущей киберугрозой. «Если судить по числу запросов от подразделений банков по работе с корпоративными клиентами, у организаций есть понимание необходимости страховых услуг, но классического формирования потребности в киберстраховании пока не произошло», – заявил Виталий Ус.

При этом отдельные пользователи и сервисы не могут противостоять кибератакам, направленным на вымогательство, хищение денежных средств со счетов, нанесение материального ущерба бизнес-процессам, объектам инфраструктуры, промышленности и т.д., полагает он.

В первом полугодии 2021 года эксперты «Согласия» отметили возросший спрос на киберстрахование со стороны эмитентов банковских карт. «Клиентов интересуют программы страхования для держателей банковских карт с покрытием рисков в результате фишинга, несанкционированных транзакций, использования поддельных банковских сайтов, сайтов торговых организаций и маркетплейсов, несанкционированных транзакций с реквизитами банковских карт и банковских счетов, полученными мошенническим путем, с использованием социальной инженерии, телефонных коммуникаций. Согласно действующему законодательству РФ,

страхованием не могут покрываться убытки, понесенные в виде выплаты выкупа кибервымогателям», – рассказал заместитель руководителя управления страхования кредитных, финансовых и предпринимательских рисков «Согласия».

Кроме того, запросы на страхование от киберрисков поступают от предприятий малого бизнеса и индивидуальных предпринимателей. Этим организациям «Согласие» предлагает:

1. Страхование от мошеннических действий в дистанционном банковском обслуживании (ДБО).

2. Страхование на случай внедрения вредоносного программного обеспечения в компьютерную систему страхователя (подтвержденных материалами уголовного дела, возбужденного по статье УК РФ ст. 159 часть 6 «Мошенничество в сфере компьютерной информации»; ст. 273 «Создание и распространение или использование компьютерных программ»), исключая операции ДБО.

Для частных клиентов стоимость страхования не превышает нескольких тысяч рублей в год, для малого бизнеса и ИП – может составлять десятки тысяч рублей. Страховые суммы соответственно от 30 тыс. руб. до 500 тыс. руб. и от 300 тыс. до 500 тыс. руб. Стоимость киберстрахования для среднего и крупного бизнеса может исчисляться сотнями тысяч и даже миллионами рублей в год.

По договору страховой защитой обеспечены материальные ценности, а также убытки, которые могут возникнуть в результате нанесения ущерба объектам инфраструктуры, технологическому оборудованию, бизнес-процессам организации. Программное обеспечение в данном случае может рассматриваться как нематериальный актив, имеющий свою стоимость.