Российские страховщики имеют некоторый опыт страхования киберрисков — в добровольном порядке их страхуют крупные компании, столкнувшиеся со значительными убытками из-за пережитых хакерских атак. Впервые страхование таких угроз включено в федеральную программу, однако оно не будет поддержано бюджетными средствами — киберстрахование будет добровольным, а не обязательным, как предполагалось ранее. В качестве стимула в рамках федерального проекта «Информационная безопасность» обсуждается вариант предоставления налоговых льгот страхователям, страхующим добровольно риски киберугроз. Судя по опросам страховщиков, к широкому внедрению страхования таких рисков в РФ не готовы ни страхователи, ни сами СК, которые сомневаются в готовности Минфина пойти на налоговое стимулирование по таким договорам.

Эксперты подготовят доклад о перспективах киберстрахования

Поручение подготовить предложения по страхованию киберрисков включено в план по реализации национального проекта «Информационная безопасность» (документ имеется в распоряжении «Интерфакса»). Поручение дано Всероссийскому союзу страховщиков (ВСС), фонду «Сколково», Минфину, ЦБ РФ и Минкомсвязи. Они должны разработать предложения в период с 2019 года по 2021 год и осенью 2021 года внести в правительство доклад на эту тему.

Согласно документу им в том числе предстоит изучить «возможности введения налоговых льгот при страховании информационных систем», а точнее — возможность отнесения на себестоимость расходов страхователей по заключению договоров добровольного страхования киберрисков.

Как показал опрос «Интерфакса» участников страхового рынка, пока к масштабному страхованию от киберугроз сектор не готов. Кроме того, по их мнению, предложение о предоставлении налоговых льгот вряд ли с легкостью поддержит Минфин РФ.

«Законодательное предоставление налоговых послаблений страхователям при заключении добровольных договоров страхования представляется весьма сомнительным», — заявил «Интерфаксу» один из экспертов страхового рынка. По его словам, «до сих пор такая практика упорно отвергалась Минфином».

«По законодательству отнесение расходов на приобретение страховой защиты допускалось только в обязательных видах страхования ответственности и в рамках специальных законов. Подобные налоговые льготы означают недополучение государством части доходов, вряд ли такую практику удастся распространить на новые виды страхования, тем более добровольные. Кроме того, сами страховщики в России только начали обсуждать возможность разработки продуктов по киберстрахованию, редкие компании предлагают такую защиту клиентам, хотя актуальность темы в РФ действительно нарастает. Сложности разработки подобных услуг связаны с определением природы рисков и зоной их действия, с требованиями по проведению предварительного аудита информсистем страхователей, с ценой таких проверок. Убытки от киберрисков могут оказаться весьма чувствительными, опыт их

урегулирования, впрочем, как и опыт ценообразования, в РФ пока невелик», — пояснил эксперт.

ВСС И РНПК готовы подключиться к программе

Вместе с тем глава ВСС Игорь Юргенс сообщил «Интерфаксу», что союз готов работать над предложениями по страхованию от киберугроз. Он признал, что «сегодня объём рынка страхования киберрисков в РФ незначителен». «В зависимости от наличия тех или иных стимулирующих мер он может потенциально достигать десятков миллиардов рублей. ВСС поддерживает развитие новых перспективных видов страхования и готов участвовать в разработке мер поддержки нового направления страхования», — добавил он.

В свою очередь, глава «Российской национальной перестраховочной компании» (РНПК) Николай Галушин заявил «Интерфаксу», что его компания готова принимать в перестрахование риски киберзащиты. Вместе с тем он отметил: «Сейчас это направление в страховании развито достаточно широко только в США. Это неслучайно — там действуют два законодательных требования к участникам рынка: во-первых, они должны извещать специальные власти обо всех кибератаках; во-вторых, законом вводится персональная ответственность менеджмента за последствия кибератак. Бизнес предпочел не сохранять на себе такую ответственность, решил ее страховать, делается это добровольно. В российском законодательстве по информационной безопасности не установлена какая-либо персональная ответственность менеджеров компаний за ущерб третьим лицам, причиненный в результате кибератак».

По словам Н.Галушина, в России пока ни субъекты экономики, ни страховщики в целом не проявляют повышенного интереса к развитию этого направления страхования. «Разработать продукт по страхованию киберрисков можно, этим уже занимаются некоторые страховые компании. В мире, как показывает практика, страхуется оборудование от повреждений в результате атак, перерывы в производстве и потеря прибыли в связи с последствиями вирусных атак. То есть «железо», потеря продукта и ущерб от перерывов в производстве (неполученная прибыль и расходы на устранение последствий атак). Кроме того, целью атаки может быть кража персональных данных клиентов, что связано с репутационными и другими рисками для организации. Такая ответственность также может страховаться. Эти три направления киберзащиты для страховщиков очевидны», — добавил он.

Глава РНПК считает, что проведением аудита информсистемы клиента перед заключением договора могут заниматься специальные компании, которые уже создаются в РФ, в том числе у Сбербанка есть компания «Бизон».

Ранее и.о. главы СК «Сбербанк страхование» Дмитрий Попов подтвердил «Интерфаксу» намерение страховщика разработать специальную программу по защите от киберугроз.

Почти 30 млрд рублей из бюджета на информбезопасность

Согласно плану мероприятий в рамках проекта «Информационная безопасность» и плану достижения установленных показателей и индикаторов, в период с 2017 год по 2024 год произойдет «увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза».

При этом общий объем бюджетных расходов для финансирования плана мероприятий в рамках проекта «Информационная безопасность» за период до 2021 года составит

29,701 млрд рублей. В том числе на эти цели в 2018 году предусмотрено выделение бюджетных средств и средств внебюджетных фондов в размере 365 млн рублей, в 2019 году — уже 8,475 млрд рублей, в 2020 году — 10,519 млрд рублей, в 2021 году — 10,342 млрд рублей.

В списке исполнителей федерального проекта «Информационная безопасность» — Минкомсвязи, Минпромторг, Минэкономразвития, Минфин, ЦБ РФ, ФСТЭК, ФСБ, Роспатент, МИД, Минобороны, МВД, Роскомнадзор, Росстандарт и другие ведомства. Также к исполнению плана привлечены фонд «Сколково», отдельные банки, объединения банков и страховщиков, платежные системы.

В перечне ключевых инициатив нацпроекта, согласно документу, — «создание спецресурса для взаимодействия граждан и правоохранительных органов (до 31 декабря 2020 года), создание информационной системы «Интернет» (до 31 декабря 2021 года), развитие подходов по повышению грамотности бизнеса и представителей федеральных государственных органов власти в области информационной безопасности на базе Академии кибербезопасности (до 31 декабря 2021 года). Также планируется «создание системы автоматизированного обмена информацией о кибербезопасности об актуальных киберугрозах». Кроме того, проектом предусмотрено «создание центра мониторинга и управления Сетью связи общего пользования», «обеспечение преференций и приоритетов для отечественного ПО и оборудования при госзакупках, закупках компаний с госучастием, а также при предоставлении различных форм господдержки», разработка «национальной системы фильтрации интернет-трафика при использовании информационных ресурсов детьми» (она, согласно плану мероприятий, будет создана до конца 2020 года).

Проект «Информационная безопасность» также направлен на развитие отечественной криптографии, «в том числе в значимых платежных системах». Предполагается, что 100% россиян до конца 2021 года получат «возможность использования электронной подписи в соответствии с действующим законодательством», отмечается в документе.

Финмаркет, 17.08.2018