Всероссийский союз страховщиков (ВСС) разработал и направил в Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России) проект методики оценки ущерба, возникающего в результате кибератак на информационные системы и сети хозяйствующих субъектов. В указанной методике для целей добровольного страхования киберрисков даны основополагающие определения объекта страхования и страхового случая. Документом также определены основные подходы к толкованию и определению состава возмещаемых расходов и убытков, связанных с компьютерными атаками.

Так, объектом страхования имущества являются имущественные интересы страхователя, связанные с риском повреждения, гибели или утраты имущества. Они включают в себя электронные данные, компьютерные программы, а также финансовые активы в электронной форме, которые могут пострадать в результате компьютерной атаки. Объектом страхования гражданской ответственности являются имущественные интересы страхователя, связанные с его обязанностью возместить вред, причиненный жизни, здоровью третьих лиц, ущерб имуществу третьих лиц, а также убытки третьих лиц за нарушение конфиденциальности, включая разглашение персональных данных.

При этом имущественные интересы страхователя, связанные с риском возникновения у него непредвиденных расходов, которые он понес или должен будет понести в связи с наступлением страхового случая по страхованию имущества и/или страхованию гражданской ответственности, и/или страхованию убытков от перерыва в хозяйственной деятельности являются объектами страхования финансовых рисков.

Также выделяются объекты страхования предпринимательского риска – это имущественные интересы страхователя, связанные с риском возникновения убытков от перерыва в его хозяйственной деятельности из-за недоступности либо значительного снижения производительности, нарушений в работе его информационных систем.

Важно отметить, что киберстрахование является добровольным видом, и размер премии, лимиты ответственности, а также состав убытков и расходов, возмещаемых по конкретному договору страхования от кибератак, будет зависеть от условий этого договора. В методике описаны основные подходы к толкованию и определению состава возмещаемых расходов и убытков, используемых страховщиками при определении суммы страхового возмещения по договорам страхования рисков, связанных с компьютерными

атаками. А также обозначены общие положения заключения договора и исключения, являющиеся основанием для отказав выплате возмещения.

«Страхование критической инфраструктуры от кибератак, защита имущественных, финансовых и предпринимательских рисков нашли поддержку со стороны страховщиков и профильных ведомств. Защита от киберрисков становится неотъемлемой частью программы безопасности любой компании, разрабатываемая методика поможет стандартизировать условия страхования», – отметил президент ВСС Евгений Уфимцев.

Он пояснил, что разработка этого важного документа была реализована во исполнении пунктов Стратегии развития отрасли связи Российской Федерации на период до 2035 года. Кроме того, методика была доработана в соответствии с выданным поручением по итогам майского совещания 2026 года, организованного Минцифры России. Тогда в совещании приняли участие представители Минэкономразвития России, Минфина России, Банка России, Роскомнадзора, ВСС, а также страховых компаний. По результатам встречи ВСС было предложено доработать проект, включив в него положения по установлению факта, причин и обстоятельств кибератак. Союз выполнил эту задачу в установленные сроки.

В настоящее время проект методики находится на рассмотрении в Минцифры РФ при участии Минэкономразвития России, Минфина РФ, Банка России, Роскомнадзора и других профильных ведомств.

Википедия страхования, 22.06.2026 г.