Рынок киберстрахования может сделать рывок в развитии благодаря внедрению единых подходов к оценке риска на основе существующих «ГОСТов»

Об этом заявил директор по информационной безопасности Национальной страховой информационной системы (НСИС) Алексей Янов на форуме Клуба страховых конференций по теме ИБ.

Алексей Янов сформулировал позицию по созданию единой методологии оценки киберготовности. В основу легло предложение использовать адаптированный ГОСТ Р 57580.x, что вызвало оживленную дискуссию со стороны практиков.

Ключевая проблема, сдерживающая развитие рынка киберстрахования, — субъективизм. Разные страховщики используют собственные опросники, что размывает критерии риска и создает трудности при перестраховании. Как отметил Алексей Янов, «размытость» критериев — главный тормоз.

Участники дискуссии поддержали эту мысль, иронизируя по поводу «волшебных анкет», которые страховщики просят заполнять. Прозвучало мнение, что даже «сканирование», которое часто воспринимается как панацея, дает лишь «слепок на данный момент» и не отражает реальной картины: ложноположительные срабатывания пугают, а реальные угрозы могут остаться незамеченными.

В качестве практического инструмента предлагается взять за основу серию стандартов ГОСТ Р 57580.x, уже хорошо зарекомендовавшую себя в финансовом секторе и признанную Банком России. Для универсального применения во всех секторах экономики — от промышленности до МСП — стандарт может быть доработан: в этом случае из него уберут узкую банковскую специфику, превратив в базовый чек-лист кибергигиены. Ожидаемо, что крупные игроки с большими страховыми суммами будут проходить потоковую оценку через SIEM-систему и телеметрию, тогда как для малого бизнеса достаточно периодической самооценки.

Реализация методологии строится на принципе «черного ящика»: страховщик не получает доступа к конфиденциальным данным (настройкам, инцидентам), а видит

только интегральную динамическую оценку. Это решает проблему неразглашения и создает «базу нормального состояния»: эксперты смогут оперативно фиксировать факт взлома, отсекать мошенничество и урегулировать убытки на основе объективных данных, рассказал Алексей Янов.

Этот подход обещает прозрачное ценообразование и жесткую стимуляцию безопасности. Плохая оценка по ГОСТу автоматически означает высокий тариф или отказ в покрытии, подталкивая бизнес реально «подтягивать» защиту, отметил Алексей Янов.

Википедия страхования, 22.07.20726 г.