Киберриски перестали быть проблемой IT-департамента, став стратегической угрозой для предпринимателей. В фокусе преступников – крупный бизнес с оборотом от миллиарда рублей, т.к. основной целью кибератак является требование выкупа. При этом, небольшие компании также находятся в зоне риска – мошенники постоянно модернизируют свои инструменты, используют ИИ, тестируя свои технологии. И в новых реалиях стандартного контура кибербезопасности для бизнеса теперь недостаточно, на первый план должна выходить киберустойчивость – способность компании продолжать функционировать, даже находясь под постоянным цифровым давлением. Об этом рассказала Анна Рыбина, генеральный директор Страхового Дома ВСК, в рамках своего выступления на конференции «ВСС-2026: Культурный код страхования».

Анна Рыбина, генеральный директор Страхового Дома ВСК, приняла участие в пленарной дискуссии «Рост страхования: ищем драйверы». По мнению эксперта, российский рынок киберстрахования на данный момент находится на этапе становления. За 2023-2024г его совокупные объемы составляли порядка 2-3 млрд рублей, а в 2025 г. экспертно выросли до 3,5-4 млрд. рублей. Количество заключенных договоров киберстрахования увеличилось на 20-30%, а общий объем сборов в сегменте через пару лет может превысить 10 млрд рублей, а ежегодные темпы роста составить в среднем 20%.

По оценкам Анны Рыбиной, современные продукты по киберстрахованию подразумевают экосистемный подход. Так, страховщики совместно с партнерами по кибербезопасности занимаются превентивным аудитом рисков на основе реальных IT-сканирований, принимают участие в Incident Response (реагировании на инцидент). Кроме того, помимо покрытия убытков при наступлении страхового события, страховая компания может оказать юридическую поддержку при утечках персональных данных клиентов компании.

С каждым годом число киберпреступлений, без учета DDoS-атак, динамично растет – если в 2024 году было зафиксировано около 30 тыс. таких инцидентов, то в 2025 году их число выросло до 100 тыс. В таких реалиях игрокам рынка важно формировать перестраховочные емкости, в том числе на базе РНПК.

«Несмотря на невысокие в данный момент объемы рынка киберстрахования, этот сектор в ближайшие годы будет расти, прежде всего на фоне роста громких киберинцидентов,

ужесточения ответственности за утечки персональных данных, а также финансовых потерь бизнеса из-за кибератак. Средний ущерб от простоя после киберинцидента составляет 6–8 млн рублей в сутки, а для крупных игроков он в совокупности исчисляется сотнями миллионов. Поэтому бизнес, в зависимости от масштабов и выручки, заинтересован как в комплексных экосистемных программах страхования киберрисков, так и в коробочных продуктах с ограниченным покрытием», — отметила Анна Рыбина, генеральный директор Страхового Дома ВСК.

Википедия страхования, 28.05.2026 г.