Год после масштабной кибератаки: как ВСК восстановила работу и какие выводы легли в основу её подхода к киберустойчивости – об этом рассказал член Совета директоров Страхового Дома ВСК Роман Фролов на конференции Сбера «Страхование 2030: технологии будущего» в рамках сессии «Устойчивость нового времени».

Роман Фролов поделился опытом восстановления работоспособности ВСК после кибератаки. В результате инцидента, который длился меньше суток, была повреждена ИТ инфраструктура компании. Восстановление внутренних и внешних сервисов продающего контура заняло у компании примерно 3 недели.

На протяжении инцидента ВСК вела открытую коммуникацию со своими клиентами, регулятором, налоговой службой и правоохранительными органами. ВСК даже во время кибератаки не останавливала процессы урегулирования и продолжила принимать заявления от клиентов, они обрабатывались вручную.

По итогам киберинцидента ВСК увеличила инвестиции в информационную безопасность, стала проводить регулярные киберучения с участием руководства и оптимизировала инфраструктуру.

Отдельно Роман Фролов отметил, что корректнее говорить не о «киберзащите», а о «киберустойчивости» компаний. Киберустойчивость — это способность быстро восстановиться после кибератаки. Ключевыми элементами киберустойчивости становятся информационная безопасность, безопасное резервированное копирование, готовность команды IT и бизнеса, а также киберстрахование.

Этот опыт компания положила в основу собственного продукта: ВСК обновила программу по киберстрахованию на базе практики, которую прошла сама. Сегодня это, по сути, сервисно-страховой продукт: наличие полиса позволяет укрепить киберустойчивость бизнеса за счёт защиты от финансовых потерь и дополнительных сервисов — например, привлечения специалистов для расследования инцидентов, формирования команды и привлечения сторонних специалистов для восстановления повреждённой инфраструктуры.

«Киберстрахование – это инструмент, который позволяет компании не тратить свой оборотный капитал на ликвидацию атаки, а спокойно восстанавливаться за счет страховых средств. Сколько бы мы не инвестировали в кибербезопасность, это всего лишь снизит вероятность инцидента, но не гарантирует безопасность бизнеса. Преступники постоянно развивают инструменты и методики хакерских атак. Отсутствие страховой защиты в перспективе может обойтись компании в разы дороже расходов на оформление полиса», — отметил член Совета директоров Страхового Дома ВСК Роман Фролов.

Википедия страхования, 23.11.2026 г.