Роман Фролов из ВСК в рамках ЦИПР рассказал, как бизнесу снизить риск кибератак

Риск кибератаки в современных реалиях актуален для всех компаний, независимо от сферы деятельности и масштаба предприятия. Поэтому бизнесу важно инвестировать и развивать системы информационной безопасности, а также использовать механизм киберстрахования, позволяющий нивелировать финансовые потери на всех этапах инцидента. Об этом рассказал Роман Фролов, член Совета директоров Страхового Дома ВСК, в рамках своего выступления на конференции ЦИПР-2026.

Роман Фролов, член Совета директоров Страхового Дома ВСК, принял участие в партнерской сессии Инфосистемы Джет «Непрерывность бизнеса в эпоху цифрового терроризма» ежегодного форума по цифровой экономике и технологиям в России ЦИПР-2026. В рамках выступления эксперт рассказал об опыте ВСК по восстановлению IT -инфраструктуры и бизнес-процессов после кибератаки.

В среднем возобновление работы IT-систем у крупного бизнеса по итогам масштабной кибератаки может занимать недели и месяцы. На первом этапе восстанавливаются базовые сетевые и вычислительные мощности, системы хранения и доступа, далее прикладная инфраструктура, включая развёртывание сервисов, необходимых для работы приложений, а также пользовательские приложения и рабочие места. Последний шаг включает восстановление целостности данных, синхронизацию между системами, подключение внешних сервисов.

Наличие полиса киберстрахования позволяет нивелировать финансовые убытки, т.к. в покрытие включаются затраты на привлечение экспертов по форензике, пересборку IT-систем, расследование инцидента и пр. Возмещение убытков по данным рискам способствует скорейшему восстановлению нормальной деятельности компании.

На фоне беспрецедентного количества кибератак на российский бизнес экспертное сообщество – ВСС, Банк России – рассматривает введение вмененного страхования от киберрисков. По мнению Романа Фролова, это актуальная для рынка инициатива, однако она должна быть тщательно проработана. В первую очередь проект затронет финансовые организации – банки, страховые компании, а в дальнейшем может быть масштабировано и на другие отрасли.

В целом, при планировании мер для информационной безопасности бизнеса важно учитывать ряд факторов. Внедрение сплошного мониторинга по модели Zero Trust защищает бизнес от катастрофических убытков, лишая хакеров возможности использовать дешевые «некритичные» узлы как бесплатный плацдарм для скрытого проникновения к контроллеру домена. Без этой защиты злоумышленники могут месяцами незаметно находиться в вашей сети, готовя полную остановку бизнес-процессов, кражу конфиденциальных данных или шифрование всей инфраструктуры ради выкупа. Кроме того, не стоит экономить на пентестах, т.к. внешняя оценка безопасности покажет уязвимости, о которых штатные специалисты по ИБ могли не догадываться.

«Для бизнеса восстановление после кибератаки — это всегда своего рода марафон. В этот период важна постоянная и открытая коммуникация с клиентами, партнерами и сотрудниками. Снизить риски происшествий, сэкономить время и ресурсы для восстановления систем и существенно сократить издержки позволит наличие BCP (Business Continuity Plan). Не менее важны регулярные тренировки действий в условиях внезапного падения IT-инфраструктуры. Обязательным инструментом нивелирования киберрисков является и страхование. Полис покрывает расходы на всех этапах восстановления систем – от юридических рисков до привлечения подрядчиков и формирования форензик-отчетов», — отметил Роман Фролов, член Совета директоров, заместитель генерального директора Страхового Дома ВСК.

Википедия страхования, 21.05.2026 г.