Сергей Цикалюк на ПМЭФ: важно сформировать перечень требований к компаниям по информационной безопасности

За последнее время российский бизнес столкнулся с беспрецедентным количеством кибератак. Подобные происшествия заставляют предпринимателей пересмотреть стратегию информбезопасности – оценить уровень профессионализма подрядчиков и партнеров, собственные инвестиции в IT-архитектуру, алгоритмы действия для минимизации финансового и репутационного ущерба по итогам хакерских атак. Об этом рассказал Сергей Цикалюк, председатель Совета директоров Страхового Дома ВСК, в рамках сессии «Стресс-тест в реальном времени: как не потерять миллиарды при кибератаке», состоявшейся на полях ПМЭФ-2026.

Страховой Дом ВСК выступил партнером сессии «Стресс-тест в реальном времени: как не потерять миллиарды при кибератаке», которая состоялась 4 июня в рамках деловой программы форума ПМЭФ-2026. В дискуссии, посвященной теме кибербезопасности отечественных предприятий, приняли участие Станислав Кузнецов, заместитель Председателя Правления ПАО Сбербанк, Виталий Лютиков, первый заместитель директора Федеральной службы по техническому и экспортному контролю (ФСТЭК России). Модератором сессии выступил Дмитрий Самарцев, директор группы компаний BI.ZONE – партнера ВСК.

В ходе выступления Сергей Цикалюк поделился опытом восстановления компании после кибератаки. На фоне таких инцидентов бизнес перестраивает собственную стратегию информационной безопасности. По мнению Сергея Цикалюка, крупным компаниям не стоит экономить на оптимизации IT-архитектуры и усилении контура кибербезопасности, т.к. впоследствии, в случае кибератаки, это поможет быстрее восстановить внутренние процессы и значительно сократить убытки от простоя.

Кроме того, важным инструментом повышения киберустойчивости бизнеса является страхование киберрисков. Комплексные сервисно-страховые продукты не только создают «подушку безопасности» в виде компенсации ущерба, но и помогают оперативно реагировать на инцидент и сформировать пул партнеров для минимизации последствий кибератаки.

«Сегодня практически никто не верит, что есть организации, которые невозможно взломать. Каждая пятая российская компания скомпрометирована и не знает об этом.

Мы сталкиваемся с огромным количеством инцидентов, когда киберпреступники находятся в инфраструктуре более полугода, иногда годы, — отмечает Дмитрий Самарцев, директор группы компаний BI.ZONE. — Ситуацию усугубляет то, что технологии искусственного интеллекта вошли в арсенал злоумышленников. Теперь атаки стали более доступными и масштабируемыми. За 2025 год количество целевых атак, совершенных с применением ИИ, выросло на 93%, а с начала 2026 го — еще в 3 раза. Чтобы успешно их отражать, необходимо внедрять ИИ в средства защиты и процессы кибербезопасности».

В ВСК базовые направления работы были восстановлены в течение 3 недель – были выстроены коммуникации с регулятором, клиентами и партнерами по теме инцидента, приглашены консультанты по кибербезопасности, восстановлена ИТ-инфраструктура. В аналогичной ситуации компаниями не стоит пытаться все решить самостоятельно — в сегменте информбезопасности сегодня работает множество профессионалов, которые помогут правильно реагировать на требования преступников и избежать повторных эпизодов цифрового шантажа.

«Наша компания на собственном опыте оценила важность вопросов кибербезопасности. По итогам киберинцидента мы сделали для себя три ключевых вывода. Прежде всего, чтобы минимизировать последствия кибератаки – а в современном мире речь идет именно об этом, а не о том, чтобы гарантировано избежать подобных ЧП, — важно формировать пул партнеров. Наличие даже большого штата IT-специалистов внутри компании не так эффективно, т.к. цифровой ландшафт слишком быстро меняется. IT-подразделения компании должны тесно взаимодействовать с внешними консультантами и экспертами. Второе – это открытость и прозрачность бизнеса. Наша компания уже больше 30 лет на рынке, мы ведем открытую коммуникацию с профессиональным сообществом, и для нас было ценно видеть поддержку игроков рынка, предлагающих нам свою зачастую безвозмездную помощь. И третье – важно сформировать перечень требований к компаниям по информационной безопасности», — отметил Сергей Цикалюк, председатель Совета директоров Страхового Дома ВСК.

Википедия страхования, 08.06.2026 г.