Как не потерять бюджет на инновациях: СОГАЗ представил комплексное страхование киберрисков на форуме ЦИПР-2026

Промышленные предприятия, переходящие на отечественное ПО, столкнулись с новой реальностью: ошибки интеграции систем и кибератаки могут остановить производство и обернуться серьёзными финансовыми потерями. На конференции ЦИПР-2026 СОГАЗ представил решение — комплексное страхование киберрисков — и провёл дискуссию «От импортозамещения до нейросетей: как не потерять бюджет на инновациях» с участием представителей бизнеса, государства и ведущих ИТ— и ИБ-компаний.

Участники обсудили угрозы, связанные с использованием ИИ, масштабное импортозамещение в промышленности, влияние киберрисков на устойчивость бизнеса, государственные инициативы в сфере киберстрахования и механизмы фиксации и урегулирования убытков. Программа страхования СОГАЗа покрывает в том числе убытки из-за последствий промпт-инъекций и ошибок интеграции нового ПО в ходе импортозамещения. Эксперты компании также рассказали, какие шаги нужно предпринять в первые 72 часа после инцидента, чтобы получить страховую выплату.

Заместитель министра цифрового развития Александр Шойтов сообщил, что на государственном уровне разрабатывается методика оценки киберинцидентов и обсуждается концепция вменённого страхования для объектов критической инфраструктуры. «Киберстрахование необходимо для бесперебойности бизнеса. Можно провести аналогию с аварийными комиссарами на дорогах: когда происходит ДТП, есть понятная процедура — приехали, зафиксировали, запустили страховой процесс. В киберстраховании такая рамка тоже должна постепенно появиться», – сказал Александр Шойтов.

«Несмотря на кратный рост цифровых угроз лишь 10-12% российских компаний используют киберстрахование как элемент риск-менеджмента. Для сравнения, в западных странах показатель достигает 80%», — отметил Дмитрий Добродей, руководитель продукта «Киберстрахования» АО «СОГАЗ». В основном интерес проявляет крупный и средний бизнес, при этом страховая защита от киберинцидентов актуальна для компаний любых отраслей. По данным СОГАЗа спрос со стороны автопрома за последние семь лет вырос на 11%. Киберстрахование по-прежнему востребовано у производственных предприятий, агропромышленного комплекса и организаций здравоохранения. Растёт интерес к страховой защите и у средств массовой информации.

Промышленность подтвердила запрос на страховую защиту. Владимир Курицин, генеральный директор «ЗН Цифра», подчеркнул: «Восстановление может не привести ни к чему, если резервные копии уничтожены. Нужен план Б, план В и страхование остаточных рисков». Сергей Хомяков, директор департамента информационных технологий и цифрового развития ПАО «РусГидро» добавил, что простой из-за кибератаки – это сценарий, где страхование уже востребовано, хотя ключевой фокус компании остаётся на надёжности энергоснабжения.

Эксперты зафиксировали резкий рост цифровых угроз, в том числе связанных с повсеместным использованием искусственного интеллекта. Евгений Сидоров, директор по информационной безопасности Yandex Cloud, обратил внимание на новую поверхность атаки: «Промпт-инъекция может быть не так опасна сама по себе, как в сочетании с избыточными правами ИИ, в том числе к ценным базам знаний, отсутствием контроля действий. Нейросеть не различает вредоносный текст и системный запрос – просто выполняет инструкцию. Это создаёт новые векторы угроз, от которых бывает сложно защититься. Чтобы бизнес мог безопаснее интегрировать ИИ в процессы, мы составили руководство по снижению рисков при разработке и внедрении агентов на базе LLM AI SAFE».

Андрей Янкин, директор дирекции информационной безопасности «Инфосистемы Джет», привёл статистику, которая объясняет рост интереса к киберстрахованию: 22% атак в 2025 году были связаны с тем, что подрядчик становился входной точкой для атаки на заказчика. «В этой ситуации растёт роль страховых инструментов, которые помогают закрывать остаточный риск там, где полностью исключить инцидент невозможно», — отметил он.

Технический директор Positive Technologies по развитию отрасли Алексей Сидорюк резюмировал: «Если компания всё сделала для информационной безопасности, она всё равно не защищена на 100%. Страхование — это финансовый контур киберустойчивости, который должен включаться тогда, когда технологическая защита и реагирование уже работают».

Участники сессии сошлись во мнении, что страхование не заменяет информационную безопасность, но без него бизнес остаётся один на один с многомиллионными убытками. Эксперты также признали важность оперативных выплат и бесшовной модели, когда специалисты по информационной безопасности привлекаются к локализации угрозы без

тендеров и согласований, а их работу напрямую оплачивает страховая компания. В СОГАЗе подобные решения уже доступны для малого бизнеса, возможность их масштабирования для крупных предприятий активно прорабатывается.

В качестве практического инструмента СОГАЗ предложил участникам сессии чек-лист с порядком действий при киберинциденте. «В первые 72 часа после атаки компания должна уведомить страховщика, зафиксировать происшествие, все технические подробности атаки и последствия инцидента – это важно для финансового урегулирования», – пояснил Георгий Старостин, директор дирекции информационной безопасности АО «СОГАЗ». Основные шаги: незамедлительно локализовать угрозу и принять меры для остановки атаки; уведомить страховую компанию, а также надзорные органы — в случае утечки данных или атаки на объекты критической информационной инфраструктуры; инициировать расследование и восстановления систем, после чего передать всю собранную информацию и результаты анализа в страховую компанию.

Википедия страхования, 21.05.2026 г.