В ПОЛЕ ЗАЩИТЫ ОТ КИБЕРРИСКОВ

КИБЕРСТРАХОВАНИЕ В РОССИИ ПОКА ОСТАЕТСЯ СЛАБО РАСПРОСТРАНЕННЫМ, КОНСТАТИРУЮТ ОПРОШЕННЫЕ GUIDE АНАЛИТИКИ И ИГРОКИ РЫНКА. СРЕДИ ОПАСЕНИЙ ОТНОСИТЕЛЬНО ДАННОГО ПРОДУКТА БИЗНЕС НАЗЫВАЕТ ВЫСОКУЮ СТОИМОСТЬ ПОЛИСОВ, НЕПРОЗРАЧНЫЕ УСЛОВИЯ ДОГОВОРОВ, ТРУДНОСТИ В ДОКАЗЫВАНИИ ИНЦИДЕНТА И ПОЛУЧЕНИИ СТРАХОВЫХ ПРЕМИЙ. ОДНАКО С РОСТОМ ЧИСЛА УГРОЗ ИНТЕРЕС К СЕГМЕНТУ БУДЕТ РАСТИ, УВЕРЕНЫ ЭКСПЕРТЫ. ТАКЖЕ В БЛИЖАЙШИЕ ГОДЫ СТРАХОВЩИКИ НАЧНУТ ПРЕДЛАГАТЬ БОЛЕЕ ГИБКИЕ И ДОСТУПНЫЕ РЕШЕНИЯ, АДАПТИРОВАННЫЕ ПОД БИЗНЕС РАЗНОГО УРОВНЯ. АЛЛА МИХЕЕНКО



ОЛЕГ ХАРСЕЕВ

РОСТ ЧИСЛА АТАК И УСИЛЕНИЕ РЕГУЛЯТОРНЫХ НОРМ ПОДТОЛКНУТ БОЛЬШЕ КОМПАНИЙ К ИСПОЛЬЗОВАНИЮ ИБ-СТРАХОВАНИЯ КАК ЧАСТИ СТРАТЕГИИ ЗАЩИТЫ

По данным страхового брокера Mainsgroup, представившего исследование рынка страхования киберрисков в начале марта 2025 года, данный сегмент еще недостаточно развит: всего 8 из 15 страховщиков России предоставляют услугу по киберстрахованию, а количество договоров насчитывает около полутора тысяч — от мелких «коробочных» решений до стандартных полисов с полноценным покрытием.

Согласно открытым данным, услуги по страхованию киберрисков предоставляют АО «Альфастрахование», СПАО «Ингосстрах», АО «Согаз», «СберСтрахование», «Зетта Страхование» и др. Опрос Mainsgroup показал низкую активность бизнеса в таком гаранте безопасности. Всего 12,5% опрошенных (в исследовании участвовало 37 представителей страховых компаний, страховых брокеров и страхователей) застраховали киберриски.

«Это услуга не сильно популярна в России,— констатирует руководитель группы защиты инфраструктурных IT-решений компании «Газинформсервис» Сергей Полунин.— Да, первые предложения появились уже в 2017 году на волне атак шифровальщиков WannaCry и Petya, но с тех пор спрос на эту услугу если и рос, то крайне слабо. В основном отношение организаций не то чтобы было скептическим, но бюджет на это точно мало у кого был предусмотрен».

По словам эксперта, сейчас эта услуга востребована в IT и финансовом секторе, остальные все же полагаются на технические способы защиты и не пытаются переносить риски таким способом.

«В России 13–14% компаний имеют киберстраховку»,— приводит свою статистику директор Центра мониторинга и противодействия кибератакам IZ:SOC компании «Информзащита» Александр Матвеев. Одним из факторов низкой популярности, по мнению спикера, является страх компаний сообщать о случившемся инциденте ИБ из-за репутационных потерь. «Другой фактор состоит в том, что страховка не может защитить от инцидента, не всегда покрывает потери, не позволяет решить задачу минимизации последствий. Поэтому популярность услуги остается низкой»,— рассуждает он.

Эксперты отмечают, что с учетом роста кибератак логично, что запрос на данную услугу будет увеличиваться. Вопрос только в том, насколько сильно.

В «СберСтраховании» посчитали, что за три квартала прошлого года услугу по страхованию киберрисков оформили более 100 юрлиц, что в два раза больше в сравнении год к году. А сумма вложений компаний составила 4 млрд рублей, что в три раза больше, чем за аналогичный период прошлого года. Всего за семь лет «СберСтрахование» обеспечило страховую защиту от киберрисков более чем 9 тыс. компаний. Программы киберстрахования помогают бизнесу справиться с последствиями действий злоумышленников в киберпространстве, уверены в «СберСтраховании». Предприятиям МСБ достаточно страховой суммы от 10 до 50 млн рублей, чтобы защититься от основных рисков. А для холдингов и крупного бизнеса составляются индивидуальные андеррайтинги.

ДОПОЛНИТЕЛЬНЫЙ СТИМУЛ К 2025 году ожидается, что главным трендом в киберстраховании станет интеграция с ожесточающимися нормативными требованиями, обращает внимание директор Ideco Дмитрий Хомутов. «Рост числа атак и усиление регуляторных норм подтолкнут больше компаний к использованию ИБ-страхования как части стратегии защиты»,— думает эксперт.

Данную тенденцию выделяет и Дмитрий Калинин, руководитель департамента по работе с уязвимостями и инцидентами ИБ компании «Бастион». «С увеличением числа и сложности кибератак растет и интерес к киберстрахованию. На этом фоне страховые компании расширяют спектр услуг, в том числе завлекая потенциальных клиентов применением AI-технологий в своих решениях. Все больше руководителей задумываются об информационной безопасности, изучают инструменты управления киберрисками, среди которых встречают киберстрахование. Кроме того, усиление регуляторного контроля и введение новых требований к защите данных стимулируют компании обращаться к страховщикам»,— делится эксперт.

УГРОЗЫ БУДУТ РАСТИ По прогнозам экспертов, 2025 год станет годом эскалации киберугроз: количество атак продолжит расти, а хакерские группировки расширят свою деятельность, выбирая в качестве целей не только госструктуры, но и частный бизнес. Согласно аналитическому отчету о реагировании на инциденты в 2024 году от команды «Лаборатории Касперского» (GERT, отчет опубликован 20 марта 2025 года), в минувшем году большинство запросов поступило от промпредприятий, тогда как госучреждения подвергались атакам реже, чем в 2023-м. «Мы также зафиксировали рост числа инцидентов, связанных с транспортной отраслью: количество запросов на услуги реагирования удвоилось по сравнению с 2023 годом»,— отмечают в «Лаборатории Касперского».

Среди популярных киберинцидентов 2024 года там называют атаки с использованием шифровальщиков (их число за 2024 год увеличилось на 8,3 п. п. по сравнению с 2023 годом и составило 41,6% от общего числа инцидентов). По оценкам экспертов, тренд сохранится и в следующем году шифровальщики останутся главной угрозой для организаций по всему миру. Также сохраняется тенденция утечек данных, являющейся второй по частоте причиной запросов на реагирование на инциденты, составляя 16,9% от всех случаев.

«Киберстрахование становится необходимым инструментом для компаний всех отраслей в условиях растущего числа кибератак»,— считает господин Хомутов. Он напомнил, что в 2023 году общий объем страховых премий в сфере киберстрахования в России увеличился на 20%, достигнув примерно 900 млн рублей. В целом, по мнению эксперта, страховки помогают минимизировать финансовые потери, сохранить репутацию, обеспечить соответствие нормативным требованиям и восстановить бизнес с минимальными затратами.

ОПАСЕНИЯ БИЗНЕСА Среди основных причин неиспользования услуг по киберстрахованию игроки рынка отмечают высокую стоимость полисов. «Основная проблема тут в том, что подобное страхование стоит немалых денег: компании-страховщики сами перестраховываются и завышают цены на услуги, так как оценить все риски очень и очень сложно, особенно когда появляется столько решений, позволяющим злоумышленникам взламывать системы быстрее и дешевле. Кроме того, есть и сложности с возмещением потерь, так как требуется сначала проводить дорогостоящие расследования»,— говорит бэкенд-разработчик Филипп Щербанич.

Компании также сомневаются в страховом покрытии и недостаточно информированы о политике и практике поставщиков таких услуг. «Условия страхования не всегда прозрачны»,— обращает внимание гендиректор компании «Фрикейк» Виталий Панов.

«Я считаю, что проблема заключается в том, что источник ущерба трудно доказать. А посчитать выплату еще труднее. Высока вероятность отказа, так что понятнее пустить страховую премию на реальные защитные меры»,— указывает технический директор IT Task Антон Антропов.

Заместитель генерального директора ГК «Гарда» Рустэм Хайретдинов поясняет: «До сих пор нет независимого арбитража и практики экспертизы при расследовании инцидентов. Непонятно, как доказывать вину (страховая компания заинтересована обвинить клиента в нарушении правил страховки и не платить при первой возможности) и потери (потерявший считает застрахованные потери огромными, страховая старается их занизить). Также нужны инструменты сбора данных, аналог авиационного „черного ящика“, к которому никто не имеет доступа и который вскрывается во время расследования инцидента,— и таким инструментам должны доверять все стороны и суд. Пока данных не будет накоплено достаточно и пока нет понятных инструментов и институтов принятия решения, никто не будет страховать ущерб, а лишь, как сегодня, стоимость средств защиты».

Валентин Поляков, владелец продукта «Антивирус» в компании PRO32, рассказал, что несколько лет назад компания пробовала запустить этот продукт, но инициатива не увенчалась успехом. «Даже если все условия соблюдены, есть вероятность, что страховая выплата может не покрыть тот ущерб, который был нанесен бизнесу в случае утери критически важных данных. Так бывает, например, если организация пострадала от нацеленной атаки при помощи вируса-шифратора»,— рассказывает господин Поляков.

При этом многие игроки рынка все же считают, что необходимо применять страховку наравне с другими мерами киберзащиты. «2025 год принесет новые вызовы в сфере кибербезопасности. Компании должны внедрять комплексные меры защиты, повышать осведомленность сотрудников и учитывать риски, связанные с новыми технологиями. Только так можно эффективно противостоять современным киберугрозам»,— агитирует бизнес-партнер компании «Компьютерные технологии» Павел Карасев. ■