Полис необязательного страхования

Яков ШПУНТ

В последние годы инцидентов, связанных со сбоями в работе информационных систем, становится все больше, а ущерб от злонамеренного вмешательства, человеческой ошибки или аварии, как материальный, так и репутационный, все более ощутим. Ответом на данную проблему стало появление услуги страхования такого рода рисков. Более того, все чаще слышны предложения сделать этот тип страхования обязательным.

Компания практически любого сектора экономики использует собственную или арендованную ИТ-инфраструктуру, различные сервисы и системы. Соответственно, обеспечение их работоспособности становится как никогда актуальным. В перечне европейских бизнес-рисков киберугрозы занимают одно из первых мест – сразу после тех, которые связаны с ростом международной напряженности. Кроме того, в развитых странах ужесточается законодательство, регламентирующее защиту данных и обеспечение работоспособности критически важной инфраструктуры.

Однако многие представители бизнеса до сих пор не подозревают, что ущерб от инцидентов, связанных с нарушением канонической триады «конфиденциальность – целостность – доступность», можно застраховать. И такие услуги страховые компании в России и мире предлагают уже довольно давно. Например, в США подобные риски страхуют с начала 2000-х годов, в Европе и России – с начала 2010-х. Более того, все чаще появляются предложения сделать такое страхование обязательным. В России эти призывы стали звучать громче с начала работы над законом о защите критически важной информационной инфраструктуры (187-ФЗ).

Рынок страхования киберрисков России (2016-2025)

Источник: Mains Group

Предложение и спрос

В нашей стране услуги по страхованию киберрисков оказывают минимум пять компаний. Однако до недавнего времени целевой аудиторией таких программ были представительства международных компаний. Но ситуация меняется. Начальник отдела страхования финансовых институтов СПАО «Ингосстрах» Антон Казиев говорит о повышении спроса на программы страхования от киберрисков со стороны российских компаний. «Это обусловлено как цифровой трансформацией компаний из различных отраслей, так и появлением угроз, способных за короткий срок парализовать деятельность компании, как произошло во время массовых эпидемий зловредов Petya и WannaCry», – говорит он. Антон Казиев отметил, что наибольший интерес к подобным услугам проявляют финансовые и ИТ-организации.

Директор по страхованию ответственности директоров, должностных лиц и компаний департамента страхования финансовых линий и корпоративной ответственности АО СК «Альянс» Вадим Михневич согласен с тем, что новости о масштабных кибератаках или эпидемиях опасных вредоносных программ повышают интерес к страхованию таких рисков.

Отмечает запрос на страхование киберрисков в России и технический директор Check Point Software Technologies Никита Дуров. «При этом большинство компаний до сих пор полагается на устаревшие методы защиты, которые на 10-15 лет отстают от сегодняшних угроз», – подчеркивает он.

Однако заместитель генерального директора ООО «Мэйнс страховые брокеры и консультанты» (Mains Insurance Brokers & Consultants) Павел Озеров не разделяет общего мнения. По его наблюдениям, несмотря на однозначную тенденцию и серьезные потери от инцидентов, многие российские компании не торопятся страховаться от киберрисков и остаются совершенно незащищенными. И это притом что такая страховка сопоставима по стоимости с КАСКО на иномарку. Тем не менее, по оценкам Mains Insurance Brokers & Consultants, к 2025 году на рынке страхования киберрисков в России страховые премии достигнут 1 млрд рублей.

Руководитель аналитического центра Zecurion Analytics ЗАО «СекьюрИТ» Владимир Ульянов согласен с тем, что спрос на услуги подобного рода пока слабый: «Компании не понимают, зачем это нужно. Многие еще не доросли до страхования киберрисков. Есть сегменты рынка, где интерес выше: например, банки или компании из области

Фото: «Ингосстрах»

Антон Казиев, начальник отдела страхования финансовых институтов СПАО «Ингосстрах»: **«Повышение спроса на программы страхования от киберрисков со стороны российских компаний обусловлено цифровой трансформацией бизнеса представителей различных отраслей и появлением новых угроз, способных за короткий срок парализовать деятельность компании»**

Фото: «Альянс»

Вадим Михневич, директор по страхованию ответственности директоров, должностных лиц и компаний департамента страхования финансовых линий и корпоративной ответственности АО СК «Альянс»: **«Лишь в некоторых штатах США регуляторы и надзорные органы публично рекомендуют финансовым институтам оформлять страхование киберрисков»**

онлайн-торговли, где критична непрерывность бизнеса. Но даже среди них интерес точечный».

По мнению руководителя лаборатории компьютерной криминалистики ООО «Группа информационной безопасности» (Group-IB) Валерия Баулина, запрос на услуги по страхованию киберрисков крайне низок из-за того, что у российских компаний нет понимания киберугроз и опыта по проведению подобного типа страхования. «В России рынок киберстрахования пока находится в зачаточном состоянии. Рост начнется только в 2019 году, но он будет стремительным», – прогнозирует он.

Однако некоторые компании уже сейчас страхуют риски и рекомендуют сделать это своим партнерам. Управляющий партнер ООО «МТ Финанс» (RUVDS) Никита Цаплин рассказал, что его компания застраховала свою ответственность на случай нарушения конфиденциальных данных клиентов, а также предлагает всем юридическим лицам приобрести расширенный полис на случай кражи данных, потери связи и возникновения других ситуаций, которые наносят существенный ущерб клиенту. Он добавил, что данная мера стала дополнительной гарантией безопасности облачных сервисов, которые предлагает RUVDS.

Об ускорении и торможении

Как полагает Антон Казиев, динамика развития рынка киберстрахования будет позитивной. Основные драйверы его роста – появление новых вирусов и постоянное расширение арсенала киберпреступников, в результате чего в зоне риска оказываются даже компании с надежной киберзащитой. Среди таких угроз представитель «Ингосстраха» выделяет увеличение атак на криптовалюты и инфраструктурные киберугрозы (атаки на интерфейсы, банкоматы, POS-терминалы, облачные сервисы). Никита Дуров добавляет к этому списку человеческий фактор: «Люди по-прежнему уязвимы перед манипулятивными технологиями, использование которых позволяет злоумышленникам добиваться целей, обходя лучшие технические системы защиты».

Основной сложностью для развития данного рынка являются вопросы законодательного регулирования. Так, с 25 мая 2018 года вступает в силу разработанный в Европе Общий регламент по защите данных (General Data Protection Regulation, GDPR). Этот норматив затронет и российские компании, сотрудничающие со странами – участницами Евросоюза, в связи с чем потребуется модификация некоторых отечественных законов или принятие дополнительных положений для урегулирования различных аспектов.

По мнению Владимира Ульянова, наиболее действенный драйвер рынка – это страх. «Компании, серьезно пострадавшие от утечек информации или других инцидентов в сфере ИБ, не только активно внедряют системы защиты, но и готовы дополнительно страховаться. Такие факторы, как использование чужого опыта или соблюдение требований законодательства, работают значительно хуже. Что касается факторов торможения, то это, как правило, сопротивление специалистов по информационной безопасности, а также позиция лиц, отвечающих за распределение бюджетов. Первые опасаются за свое место, рассуждая примерно так: «Зачем буду нужен я, если информационные риски застрахуют?». Вторые не понимают, зачем внедряли дорогостоящие средства защиты. При этом все забывают, что страховка не является панацеей и не всегда компенсирует потери. В свою очередь технические средства серьезно снижают вероятность наступления страхового случая, а страховка для защищенных компаний обойдется заметно дешевле», – говорит глава Zecurion Analytics.

Валерий Баулин также уверен, что инциденты раскачивают страховой рынок, но, к сожалению, многие «начинают лечиться, когда уже болит». Так, эпидемии вирусов-шифровальщиков прошлого года способствовали существенному росту спроса на услуги страхования киберрисков по всему миру.

Павел Озеров полагает, что такой вид страхования будет неизбежно включаться во многие привычные массовые продукты. «Этому будет способствовать, в частности, распространение беспилотного автотранспорта и систем «умного» дома, которые приведут к трансформации программ автомобильного и жилищного страхования. Так, при переходе к беспилотному транспорту ответственность человека как минимум серьезно размывается», – говорит представитель Mains.

Вместе с тем рынок страхования от нарушения непрерывности процессов уже переживает серьезную трансформацию. «Перегревы и пожары на сложных индустриальных агрегатах, крушения самолетов в связи со сбоем бортового компьютера, отмены тысячи рейсов по причине поломки системы регистрации пассажиров – вот лишь несколько примеров ущерба от кибератак. И все больше компаний уже ведут диалог о страховании на такой случай. Мы видим это в своей ежедневной работе страхового брокера», – добавил Павел Озеров.

68

Фото: СТАНДАРТ

Никита Дуров, технический директор Check Point Software Technologies: **«Запрос на страхование киберрисков в России есть, но при этом большинство компаний до сих пор полагается на методы защиты, которые на 10-15 лет отстают от сегодняшних угроз»**

Фото: Mains

Павел Озеров, заместитель генерального директора ООО «Мэйнс страховые брокеры и консультанты»: **«Страхование киберрисков будет включаться во многие массовые продукты. Этому будет способствовать распространение беспилотного автотранспорта и систем «умного» дома, которое приведет к трансформации программ автомобильного и жилищного страхования»**

Фото: Zecurion

Владимир Ульянов, руководитель аналитического центра Zecurion Analytics ЗАО «СекьюрИТ»: **«Обязательное страхование киберрисков не будет эффективным. Результатов удастся добиться тогда, когда компании будут замотивированы лучше защищать информацию, данные клиентов и партнеров»**

Директор управления рисками ЗАО «Делойт и Туш СНГ» (Deloitte) Денис Липов считает, что услуга страхования киберрисков будет становиться популярнее по мере разработки законодательных требований в области кибербезопасности, либо по мере введения существенных штрафных санкций, связанных с нарушением таких требований.

Немного практики

В целом, как напоминает Павел Озеров, процедура заключения договора страхования киберрисков проходит в три этапа: оценка риска, исполнение рекомендаций и заключение договора страхования.

«И страхователю, и страховщику стоит оценить уровень рисков – например, провести аудит кибербезопасности, поскольку размер страховой премии зависит от киберрисков, присущих отрасли и конкретной организации», – говорит Денис Липов.

По мнению Валерия Баулина, процесс получения такого полиса несложный, но есть принципиальный пункт – проведение предстрахового аудита, цель которого – установить, защищен или, наоборот, уязвим клиент в текущий момент времени. «И это вполне естественно: чем выше риски, тем дороже должен стоить полис. Страховка является дополнительной гарантией для покупателей комплекса TDS от Group-IB, который предотвращает заражения и эксплуатацию уязвимостей в корпоративных сетях. Страховка позволяет справиться с последствиями инцидента, если атака киберпреступников на компанию будет успешной», – отмечает представитель Group-IB.

Никита Дуров напоминает, что нужно определить, к каким последствиям может привести кибератака, будь то порча имущества организации, остановка производства, подрыв доверия клиентов или даже промышленная катастрофа. Он подчеркнул, что важно понять, какие финансовые и репутационные потери последуют за этим, какие средства понадобятся для возвращения доверия клиентов, восстановления бизнеса, обновления взломанных систем и т. д.

Вадим Михневич полагает, что страховое соглашение зависит от величины и сложности ИТ-инфраструктуры потенциального клиента. «Иногда котировку можно выпустить в течение одного дня без проведения аудита, или можно ограничиться дополнительными вопросами клиенту. Промежуточным этапом между аудитом и обычными вопросами может быть тестирование на проникновение. Полноценный ИТ-аудит требуется в основном крупным промышленным объектам или банкам, где риск от перерывов деятельности высок», – рассказал специалист СК «Альянс».

Антон Казиев предупреждает, что проведение полного аудита может стоить дороже самого полиса, но полученная информация помогает страхователю четко понимать уязвимые места и вовремя их закрыть. С другой стороны, как предупреждает Владимир Ульянов, размер страховой премии в случае проведения полноценного аудита будет заметно ниже, чем тогда, когда компания ограничилась анкетированием.

Никита Цаплин делится практическим опытом RUVDS: «Если говорить о договоре общего страхования Cyber Edge, то с момента знакомства с менеджером страховой компании до заключения договора прошло 17 дней. За это время мы несколько раз встречались с представителями страховщика, которые подробно и обстоятельно описывали свой продукт. Процесс мог занять значительно меньше времени, однако

Топ-10 бизнес-рисков в России

(% от опрошенных компаний)

Место	Категория бизнес-рисков	2017 / 2016
1	**Изменения в правовом поле** (смена правительства, экономические санкции, протекционизм и т. д.)	▼**52%** / 54%
2	**Макроэкономическое развитие** (программы жесткой экономии, рост цен на товары, дефляция, инфляция)	▼**37%** / 39%
3	**Перерыв в бизнес-деятельности** (включая перерывы в цепочке поставок)	▲**33%** / 21%
4	**Развитие рынков** (нестабильность, повышенная конкуренция, новые игроки, поглощения и слияния, стагнация и колебания рынка)	▼**26%** / 50%
5	**Пожар, взрыв**	▼**22%** / 25%
6	**Человеческие ошибки**	▲**19%** / 7%
7	**Политические риски** (война, терроризм и т. д.)	▲**19%** / 14%
8	**Кража, мошенничество, коррупция**	▼**19%** / 39%
9	**Природные катастрофы** (шторм, наводнение, землетрясение и т. д.)	▲**11%** / 7%
10	**Киберинциденты** (киберпреступность, поломка ИТ-системы, кража данных и т. д.)	▼**7%** / 11%

Источник: Allianz

Фото: Group-IB

Валерий Баулин, руководитель лаборатории компьютерной криминалистики ООО «Группа информационной безопасности»:
«Принципиальный момент при получении полиса киберстрахования – проведение аудита, цель которого – установить, защищен или уязвим клиент в текущий момент времени»

Фото: Deloitte

Денис Липов, директор управления рисками ЗАО «Делойт и Туш СНГ»:
«Услуга страхования киберрисков будет становиться популярнее по мере разработки законодательных требований в области кибербезопасности, либо по мере введения существенных штрафных санкций, связанных с нарушением таких требований»

мы хотели выяснить все досконально, поскольку в России RUVDS первым из провайдеров оформлял такую страховку. Аудита не понадобилось – было достаточно ответить на вопросы анкеты. На момент покупки страхового полиса компания уже прошла проверку по нормативам ФСТЭК, и защищенность RUVDS в области киберрисков мы оценивали довольно высоко. Вместе с тем мы понимали, что развитие технологий и инструментов, используемых злоумышленниками, не стоит на месте, что все учесть в работе невозможно, и поэтому наличие страхового полиса добавляет уверенности в защищенности. Было несколько нюансов, на которые нам указали в страховой компании, и мы их сразу учли».

Топ-10 бизнес-рисков в Европе
(% от опрошенных компаний)

Место	Категория бизнес-рисков	2017 / 2016
1	**Перерыв в бизнес-деятельности** (включая перерывы в цепочке поставок)	▼35% / 53%
2	**Киберинциденты** (киберпреступность, поломка ИТ-системы, кража данных и т. д.)	▼32% / 40%
3	**Развитие рынков** (нестабильность, повышенная конкуренция, новые игроки, поглощения и слияния, стагнация и колебания рынка)	▼32% / 52%
4	**Изменения в правовом поле** (смена правительства, экономические санкции, протекционизм и т. д.)	▼28% / 39%
5	**Макроэкономическое развитие** (программы жесткой экономии, рост цен на товары, дефляция, инфляция)	▼23% / 31%
6	**Природные катастрофы** (шторм, наводнение, землетрясение и т. д.)	▼21% / 31%
7	**Политические риски** (война, терроризм и т. д.)	▼16% / 17%
8	**Пожар, взрыв**	▼15% / 22%
9	**Потеря репутации/ценности бренда**	▼12% / 29%
10	**Новые технологии** (повышенная взаимозависимость, нанотехнологии, искусственный интеллект, 3D-принтеры, дроны и т. д.)	▼12% / 19%

Источник: Allianz

Осознанный выбор

Антон Казиев напоминает, что в программе «Цифровая экономика РФ» указано, что с 2022 года страхование киберрисков станет обязательным условием для представителей банковской сферы, операторов аэропортов и вокзалов, а также для предприятий металлургической, машиностроительной, авиапромышленной и судостроительной отраслей.

Тем не менее пока, как отметил Вадим Михневич, страхование киберрисков не является обязательным ни в одной стране. Лишь в некоторых штатах США регуляторы и надзорные органы публично рекомендуют финансовым институтам оформлять такой вид страхования.

Денис Липов убежден, что страхование киберрисков постепенно начинать привлекать внимание регуляторов – например, оно может стать обязательным требованием для деятельности финансовых организаций за рубежом. «Прежде чем страхование киберрисков станет широко распространенным, должны быть выработаны механизмы определения уровня риска для страховщиков и драйверы со стороны регуляторов или участников рынка – например, требования по страхованию киберрисков в отношении контрагентов», – говорит представитель Deloitte.

По мнению Владимира Ульянова, обязательное страхование киберрисков не будет эффективным. «Результатов удастся добиться тогда, когда компании будут замотивированы лучше защищать информацию, данные клиентов и партнеров. С точки зрения эффективности, полезнее было бы ввести ответственность за утечку информации, а также обязательное уведомление потенциальных жертв, если речь идет об утечке персональных или иных чувствительных данных», – убежден руководитель Zecurion Analytics.

Валерий Баулин, наоборот, считает, что страхование киберрисков должно быть обязательным – по крайней мере для финансовых учреждений, транспортных компаний, промышленности, стратегических объектов ТЭК. Он связывает эту необходимость с быстрым ростом разного рода атак на ИТ-инфраструктуру: его темпы составляют 20% в год.

По мнению Павла Озерова, такой вид страхования изначально должен быть осознанным, и клиенту следует оформлять его не ради галочки, а верно оценивая свои риски. «Очень легко купить страховое покрытие «от всего», но, к сожалению, зачастую непредвиденные события могут быть исключены из такого покрытия. Не стоит забывать и о том, что стоимость страховой защиты в разы меньше размера убытка. Так, крупные компании в среднем тратят около 11 млн рублей на ликвидацию последствий одного инцидента информационной безопасности, средние и малые – 1,6 млн рублей. И это без учета прямого убытка. В то же время стоимость полиса на 1 млн рублей лимита в среднем составляет 7-10 тыс. рублей», – приводит данные представитель Mains.