Защита сети

ТЕКСТ
Данис Юмабаев

В 2017 году каждая третья компания в России хотя бы раз подвергалась кибератаке. Проблему потерь бизнеса от хакеров пытается решить правительственная программа «Цифровая экономика» — документ предлагает введение в стране обязательного киберстрахования.

ФОТО: REUTERS

В июне в России была зафиксирована глобальная попытка вымогательства с использованием вируса-шифровальщика Petya. Тогда нефтяная компания «Роснефть» сообщила, что на ее серверы осуществлена хакерская атака. Вирус Petya блокировал компьютеры своих жертв, а за возобновление работы операционной системы требовал выкуп в размере $300 в биткоинах — так описывают поведение вируса в Group-IB — компании, специализирующейся на предотвращении и расследовании киберпреступлений и мошенничеств с использованием высоких технологий.

Такого рода киберинциденты могут обернуться для компании потерей клиентов и выручки, например из-за отказа кассового оборудования на автозаправках, рассказывает вице-президент международного страхового брокера «Марш», директор по развитию направления киберрисков Армен Гюлумян. По его словам, ущерб «Роснефти» от вируса-шифровальщика мог составить от десятков тысяч долларов до $2–3 млн. «Помимо этого некорректная работа систем может привести к искам от третьих лиц, требующих возмещения убытков. Например, из-за несвоевременной поставки товаров при отказе складской системы или системы обработки платежей», — говорит Армен Гюлумян.

В этом году каждая третья компания (36%) в стране хотя бы раз подвергалась DDoS-атаке, в 2016 году таких атак было вдвое меньше — всего 17%, следует из результатов исследования «Лаборатории Касперского». Под ударом хакеров может оказаться компания любого размера. Исследование показало, что среди микропредприятий от DDoS-атак пострадали 37%, среди компаний среднего и малого бизнеса — 31%, среди больших корпораций — 39%. У каждого пятого пострадавшего произошло значительное снижение производительности, а у 8% случился сбой транзакций и процессов. Одна DDoS-атака может стоить малому бизнесу более $123 тыс., не считая потерянных клиентов и партнеров. Россия, по данным исследования, заняла шестое место в мире по количеству DDoS-атак. В «Лаборатории Касперского» выяснили, что в финансовой сфере банки чаще других учреждений сталкиваются с DDoS-атаками: в 2016 году подобные инциденты зафиксировал каждый четвертый из них (26%). Для финансовых организаций в целом этот показатель достиг 22%. Средний ущерб от DDoS-атаки для банков составил $1,172 млн, в то время как для предприятий других сфер — $952 тыс.

Решить проблему потерь бизнеса от кибератак может правительственная программа «Цифровая экономика». В ее рамках обсуждается введение к 2020 году обязательного страхования киберрисков для предприятий отдельных отраслей экономики: например, финансовой и банковской, металлургии, машиностроения, судостроения, авиастроения, аэропортов, вокзалов и др. Проработать этот вопрос должны будут Минфин, Центробанк, Минкомсвязь, Федеральная служба по техническому и экспортному контролю и ФСБ.

ФОТО: REUTERS

Впрочем, в Минфине не уверены, что такой страховой продукт будет популярным, и устанавливать обязательную форму здесь не планируют, поспешил успокоить журналистов замминистра финансов Алексей Моисеев. Страховщикам, в свою очередь, не нравится идея обязательного страхования. В этом случае государство будет устанавливать тарифы. Страховое лобби настаивает на вмененной форме киберстрахования, которая заключается в том, что государство обязывает предприятия купить такой полис, а условия договора и тарифы устанавливает рынок. Такая форма сейчас практикуется у нотариусов, оценщиков, коллекторов, которые обязаны страховать свою гражданскую ответственность.

Киберриски на добровольной основе

Рынок киберстрахования в России делится на два сегмента: страхование от электронных краж и комплексное страхование киберрисков, говорит глава отдела страхования финансовых рисков AIG в России Владимир Кремер. В первом случае в 2016 году в России страховщики собрали премий примерно на $7 млн, во втором — около $100–150 тыс. «Эти сегменты по итогам 2017 года вырастут примерно на 5 и 15% соответственно», — прогнозирует эксперт. При этом мировой рынок страхования киберрисков уже составляет порядка $2,5 млрд, более 70% из которых приходятся на США.

Больший объем мирового рынка объясняется тем, что западные страховщики покрывают риски, которые не могут быть застрахованы в России из-за особенностей законодательства. «Разница — в страховании убытков, связанных с разглашением конфиденциальной информации: на Западе законодательство предусматривает штрафы за утечку данных. У нас такого нет, соответственно, и застраховаться от таких штрафов нельзя», — говорит начальник отдела страхования финансовых институтов компании «Ингосстрах» Антон Казиев. В России по нормам Гражданского кодекса не может покрываться страхованием и сумма выкупа, которую требуют хакеры, добавляет Армен Гюлумян. При этом в большинстве других стран сумма выкупа не запрещена к страхованию.

В нашей стране в рамках полиса по защите от киберрисков страхуют в основном убыток от перерыва в производстве, денежные средства на счетах, а также затраты на восстановление информации. На Западе включают еще и затраты, которые должна произвести компания при утечке персональных данных. «Существующие сейчас на российском рынке киберпродукты во многом базируются на переработке европейского или американского продукта. Они больше направлены на страхование гражданской ответственности от претензий, которые предъявляются со стороны регулирующих органов, клиентов», — отмечает заместитель генерального директора — директор по рискам компании «Сбербанк страхование» Владимир Новиков.

Для российского рынка отдельный полис страхования от киберрисков — большая редкость, тогда как за рубежом подобные полисы становятся все более популярными. «Обычно киберриски у нас вписывают в комплексные полисы, такие, например, как BBB (Bankers Blanket Bond — страхование банков от преступлений)», — говорит председатель наблюдательного совета Российского антитеррористического страхового пула Александр Гульченко. По таким полисам покрывается только прямой ущерб: расходы на восстановление данных или убытки от их потери, кража денег или акций со счетов клиентов.

Интересуются у нас страховой защитой от киберрисков интернет-магазины, разработчики программного обеспечения, компании из телекоммуникационного и финансового сегментов, производственные и индустриальные компании. «В основном всех интересует риск перерыва в деятельности из-за ИТ-инцидента», — утверждает замглавы департамента страхования финансовых линий компании «Альянс» Вадим Михневич. Развитие телемедицины в России подстегнет спрос на этот продукт со стороны медицинских учреждений, уверены страховщики. По данным Александра Гульченко, на медицинские учреждения в мире обрушивается на 340% больше кибератак, чем на компании других секторов. «Наши медицинские компании в среднем хуже защищены, так как используют старое оборудование, но при этом там хранятся ценные сведения: имена, даты рождения, номера страховок, диагнозы, платежная информация. С помощью этого хакеры могут подделывать документы для покупки и перепродажи лекарств, для обращений по мнимому страховому случаю», — говорит он.

На стоимость страховки влияет сфера бизнеса клиента, защищенность ИТ-инфраструктуры, уровень внутреннего риск-менеджмента, объясняет Вадим Михневич. «Для компаний из финансовой сферы, например банков, премия будет выше, чем для остальных сегментов, так как банки хранят большой объем персональных данных и риск перерыва в деятельности сразу может перерасти в крупный убыток», — говорит он. В целом стоимость полиса комплексного страхования киберрисков варьируется от $5 тыс. до 12 тыс. для маленьких фирм и от $50 тыс. до 100 тыс. для

ПРОДОЛЖЕНИЕ →

⟶ ПРОДОЛЖЕНИЕ

крупных промышленных компаний с лимитом покрытия до $3 млн, уточняет Владимир Кремер. С крупными корпорациями, для которых полис страхования будет дороже, страховщики практикуют индивидуальные договоры. «И стоимость полиса тут может начинаться от 1 млн руб., а сумма страхового покрытия — от 25 млн руб.», — рассказывает Владимир Новиков.

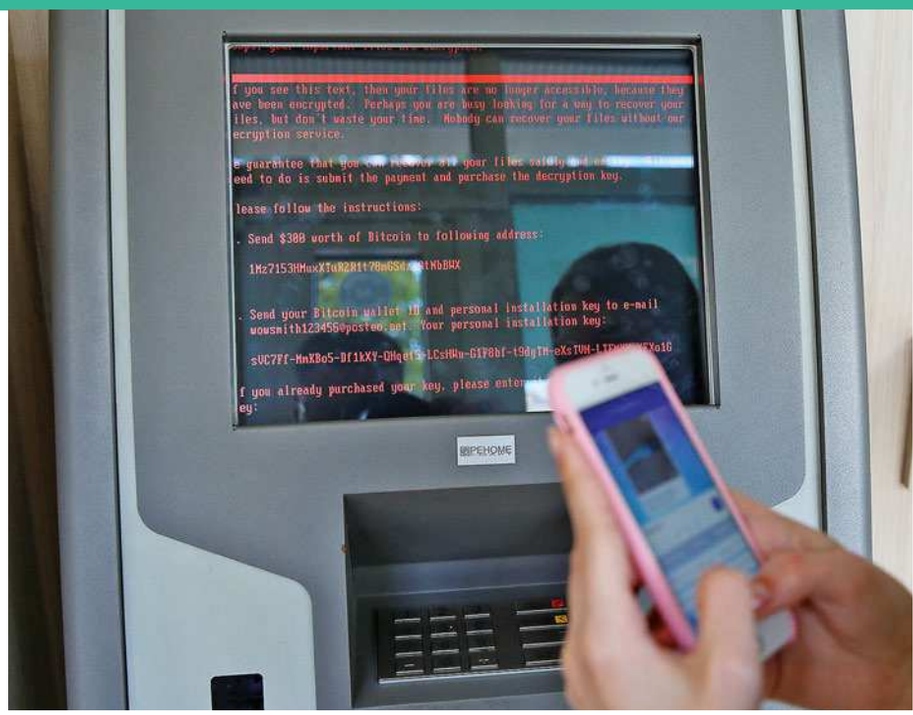
Оценка убытка по киберриску дается страховщикам непросто, так как на данный момент накоплено недостаточно практического опыта, для того чтобы говорить о существовании стандартизированной процедуры, говорит Владимир Новиков. Поэтому страховщики прибегают к экспертной оценке внешних ИТ-специалистов. «Их услуги стоят недешево», — утверждает глава управления страхования финансовых рисков «АльфаСтрахование» Андрей Макаренцев. Затраты сопоставимы со стоимостью услуг юристов: рабочий день одного эксперта обходится в сумму более $1500, уточняет Вадим Михневич.

По словам Андрея Макаренцева, оценка ущерба проходит в несколько этапов: от анкетирования до опроса специалистов о нюансах работоспособности систем клиента. «Усложнить процедуру, на наш взгляд, может некачественная информационная система клиента. Если она плохо настроена, то эксперту будет сложнее понять из протоколов, как именно происходил процесс взаимодействия системы с вредоносными файлами», — поясняет Владимир Новиков.

Случаи выплат по полисам страхования от киберрисков на нашем рынке неизвестны. Как говорит Армен Гюлумян, «несмотря на большое количество разных инцидентов, скорее всего, они не идентифицируются как киберинциденты, а объясняются сбоем в работе оборудования, коротким замыканием и т.д.».

Приводить примеры крупных выплат на Западе страховщики не хотят — опасаются, что пострадавших тогда удастся идентифицировать, а подобная информация для бизнеса нежелательна. Тем не менее Александр Гульченко в качестве примера одной из крупнейших выплат ($44 млн) приводит ситуацию с хищением персональных данных 70 млн клиентов сети Target — это третья по величине торговая сеть США.

Российским компаниям, которые планируют приобретать страховые полиси от киберрисков, эксперты



Весной этого года вирус, без какого-либо физического контакта заставляющий банкомат выдать все самые крупные купюры, пришел и в Россию

рекомендуют в тексте договора обращать внимание на то, от чего он их будет защищать. «Мы проводим анализ и видим, что далеко не всегда полис должным образом отвечает на угрозы для бизнеса», — предупреждает Армен Гюлумян. Страховщики опасаются, что на рынке могут появиться дешевые полисы, которые будут создавать иллюзию защиты от киберугроз, но из-за большого количества исключений полис фактически работать не будет. «В частности, я бы рекомендовал обратить пристальное внимание на полис, в котором говорится о страховании гражданской ответственности перед третьими лицами. Это создает иллюзию киберстрахования, но по факту таковым не является», — объясняет Владимир Новиков. Сейчас основная тяжесть убытков, например в случае кражи или раскрытия персональных данных, связана не с третьими лицами, а с восстановлением инфраструктуры и поддержанием работоспособности компании, добавляет эксперт.

Страховщики верят, что в среднесрочной перспективе рынок киберстрахования в России ожидает стабильный рост. «По сравнению с 2016 годом стало намного больше запросов по покупке полиса, так как интерес к этому продукту подстегнули вирусы WannaCry, Petya, а также атаки на российские банки в декабре прошлого года», — отмечает Вадим Михневич. Пока же рынок киберстрахования в России только формируется. «На сегодня вряд ли существует более двух десятков договоров», — говорит Владимир Новиков.

РБК+ «СТРАХОВАНИЕ» (18+)

СБЕРБАНК СТРАХОВАНИЕ

Тематическое приложение к журналу «РБК» является неотъемлемой частью журнала **«РБК» №12/2017**
Распространяется в составе журнала
Материалы подготовлены редакцией партнерских проектов РБК+
Партнеры: ООО СК «Сбербанк страхование», ООО СК «Сбербанк страхование жизни».
Реклама

Учредитель: **ООО «БизнесПресс»**
Издатель: **ООО «БизнесПресс»**
Директор ИД РБК: **Ирина Митрофанова**
Главный редактор партнерских проектов РБК+: **Наталья Кулакова**
Шеф-редактор печатной версии РБК+: **Юрий Львов**
Редактор РБК+ «Страхование»: **Вера Гордина**

Выпускающий редактор: **Андрей Уткин**
Дизайнер: **Дмитрий Иванов**
Фоторедактор: **Алена Кондюрина**
Корректоры: **Татьяна Поленова, Маргарита Тарасенко**
Главный редактор журнала «РБК»: **Валерий Владимирович Игуменов**
Арт-директор проектов РБК: **Дмитрий Девишвили**

Рекламная служба: (495) 363-11-11, доб. 1342
Коммерческий директор издательства РБК: **Анна Брук**
Директор по продажам РБК+: **Евгения Карлина**
Директор по производству: **Надежда Фомина**

Адрес редакции: 117393, Москва, ул. Профсоюзная, 78, стр. 1