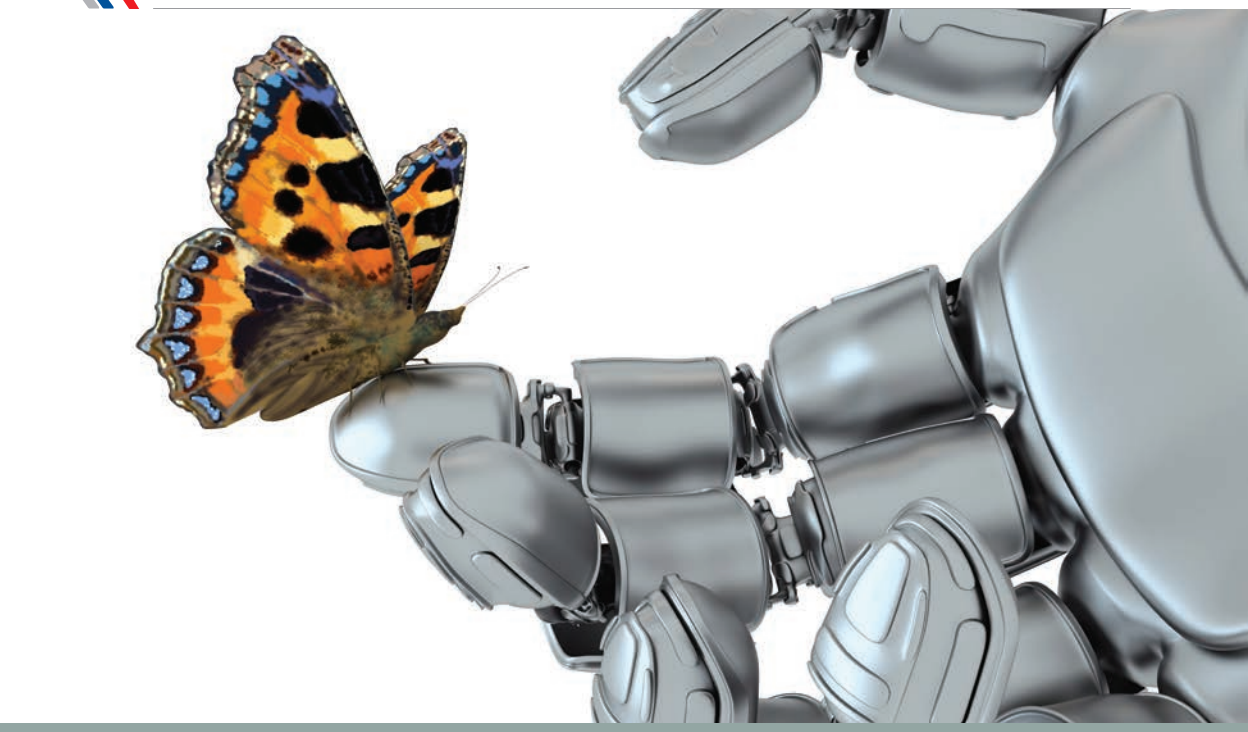

КИБЕРРИСКИ — ЧТО ЭТО?

Несмотря на то, что страхование киберрисков существует на рынке уже достаточно давно, потенциал этого вида страхования до сих пор не раскрыт. Пока многие компании не готовы нести расходы на страхование, надеясь на собственную систему информационной безопасности. Но одно не исключает другого, считает Вадим Михневич, руководитель отдела страхования финансовых рисков AIG в России. По его мнению, страхование киберрисков лишь усиливает защиту компании дополнительными мерами информационной и финансовой поддержки.

Современные страховые технологии: Цифровизация — это не только благо, но и риски. Какие они и как их можно застраховать?

Вадим Михневич: Сейчас в новостях часто можно встретить информацию об утечках персональных данных, которые уже стали новой «валютой» для мошенников. Юридические лица и государственные учреждения хранят огромное количество самых разных личных данных о гражданах. Получение несанкционированного доступа к персональным данным не только позволяет манипулировать физическими лицами, но и может стать точкой входа в периметр безопасности даже самых защищенных корпоративных сетей.

По риску хищения данных может быть застрахована как утечка данных, так и случайное раскрытие информации. В результате утечки данных также может произойти перерыв в деятельности компании, а это может привести к наиболее существенному ущербу. Представьте, например, убытки крупного банка, деятельность которого блокирована из-за взлома IT-системы на несколько часов. А если на несколько дней?!

Вадим Михневич

Руководитель отдела страхования финансовых рисков AIG в России

ССТ: Как злоумышленникам чаще всего удается обходить защиту IT-систем компаний?

В. М.: Один из вариантов — ситуация, когда с помощью социальной инженерии удается взламывать компьютерные системы предприятий и проникать во внутренний периметр компании. Второй вариант — фишинг: работникам предприятия направляется письмо, например, под видом сообщения от «начальника», только от подставного лица. Такое письмо побуждает человека открыть вредоносную ссылку, и это становится причиной утечки данных, которая приведет к взлому IT-системы компании.

Может быть также реализован сценарий, когда атака на предприятие идет от внешних лиц. Но ключевую информацию они в любом случае получают от работника компании. Это может быть и сговор, поэтому говорить о чисто внешнем или чисто внутреннем воздействии сложно. Однако полис страхования киберриска больше направлен на покрытие ущерба от внешнего воздействия, когда есть злоумышленники, которые пытаются получить доступ к внутренним системам компании.

ССТ: Если допущена возможность взлома базы или кражи данных, пострадавшее физическое лицо может подать иск на компанию, допустившую утечку. Можно ли страховать риски претензий к предприятию за неправильно организованную работу по хранению данных?

В. М.: Так как все больше сервисов и услуг переходят в цифровой формат, то неизбежен и рост мошенничества с персональными данными. Чтобы реагировать на новые преступные схемы и активность злоумышленников, уже сформированы законодательные инициативы и требования к хранению данных. В Национальной программе «Цифровая экономика» защита персональных данных является одним из приоритетов. Еще одним подтверждением актуальности этой проблемы является рост спроса на специалистов по кибербезопас-

> В Национальной программе «Цифровая экономика» защита персональных данных является одним из приоритетов. Еще одним подтверждением актуальности этой проблемы является рост спроса на специалистов по кибербезопасности: число вакансий по этому профилю для некоторых областей экономики за последний период выросло в 2,5 раза.

ности: число вакансий по этому профилю для некоторых областей экономики за последний период выросло в 2,5 раза.

Ответственность за утечку персональных данных тоже уже есть в действующем законодательстве. Пострадавший, действительно, может предъявить иск, но сумма возмещения обычно не превышает возмещений по моральному ущербу. Программа «Цифровая экономика» включает несколько инициатив и рабочих групп, нацеленных на ужесточение ответственности за сохранность персональных данных, поэтому, возможно, в будущем мы приблизимся к европейскому или американскому варианту, где персональные данные имеют очень большую ценность.

Многие компании не готовы выделять расходы на страхование, надеясь закрыть вопрос кибербезопасности только за счет собственных IT- специалистов. Однако страхование киберрисков как раз предназначено для закрытия непредвиденных сценариев IT-безопасности или неизвестных новых киберугроз.

ССТ: Но пока различия в подходах существуют?

В. М.: Если говорить о различиях, то, в первую очередь, это невозможность страховать в России штрафы за случаи несанкционированного раскрытия персональных данных. В то же время, расходы в связи с расследованием регулятора покрываются договором страхования — таким образом, договор страхования реагирует как на ущерб пострадавших от утечки (ответственность перед третьими лицами за раскрытие информации), так и на расходы компании-страхователя (расходы на защиту, расходы в связи с расследованием).

Если инцидент приведет к тому, что будет нарушена информационная безопасность страхователя, произойдет остановка или замедление процессов под управлением IT, то это тоже может быть застраховано по полису страхования киберрисков как «перерыв в деятельности». В этой части возмещение будет рассчитано как совокупность расходов на расследование инцидента и возмещение финансовых потерь страхователя, которые были вызваны киберинцидентом и недоступностью рабочих процессов.

ССТ: В России от кибермошенничества особенно сильно страдает банковский сектор. Есть ли специальные страховые продукты, защищающие банки от претензий со стороны клиентов за утечку данных?

В. М.: Полис страхования киберрисков не привязан к какой-либо отдельной индустрии, поэтому может использоваться и в банковском секторе. За рубежом многие банки уже приобрели себе такое страховое покрытие.

Повторюсь, в полисе страхования киберрисков есть несколько основных покрытий. Одно из них покрывает ущерб в случае утечки персональных данных практически по любой причине: раскрытие информации, хакерские атаки, утечка данных во время обновления системы. Под информацией мы понимаем утечку паспортных данных, данных кредитных карт и т. д. В связи с этим третьи лица — клиенты банка могут подать иски на банк. Полисом покрываются как расходы на юристов, так и само тело претензии, то есть возмещение претензий по поданным искам.

Основное покрытие страхования киберрисков в финансово-кредитной организации, как и на любом другом предприятии, всегда связано с перерывом в деятельности: банк не может обрабатывать запросы клиентов, не может осуществлять денежные транзакции и т. д., а в результате теряет деньги от простоя своих IT-систем.

При этом для банков существуют и отдельные страховые продукты, напри-

Основное покрытие страхования киберрисков в финансово-кредитной организации, как и на любом другом предприятии, всегда связано с перерывом в деятельности: банк не может обрабатывать запросы клиентов, не может осуществлять денежные транзакции, а в результате теряет деньги от простоя своих IT-систем.

мер, комплексное страхование банковских рисков (BBB), но в них нет покрытия ущерба по персональным данным — фокус направлен больше на покрытие ущерба от внутреннего мошенничества работников и мошенничество с деньгами: хищение денежных средств, подставные кредиты и т. д. Персональные данные в этих случаях мошенникам не очень интересны. Клиент может даже не знать, что с его счетом что-то произошло, но за вред от таких действий банк несет ответственность. Кроме того, BBB не включает в себя страхование перерыва в деятельности.

ССТ: Кто и насколько активно покупает полисы страхования от киберрисков?

В. М.: Банки в России страхование от киберрисков активно не покупают — пока они пытаются справляться с этой проблемой своими силами. Со стороны IT-компаний мы видим гораздо больший спрос. Будучи тесно связаны с кибербезопасностью и разработкой программного обеспечения, они как раз понимают, зачем нужно страхование киберрисков.

В России очень часто страхование киберрисков связано с приобретением лицензий или сертификата на работу в крупном проекте, где требуется сразу несколько видов страхования: киберкисков, профессиональной ответственности и часто — гражданской ответственности.

ССТ: Каковы перспективы страхования киберрисков в России?

В. М.: Мы уже несколько лет видим ежегодный рост как с точки зрения запросов и интереса рынка, так и в размере собранной премии. Потенциал этого вида страхования до сих пор не раскрыт, так как с точки зрения объема российского рынка количество застрахованных клиентов остается крайне небольшим — менее 1 % от рынка.

Причин тому несколько: многие компании не готовы выделять расходы на страхование, надеясь закрыть вопрос кибербезопасности только за счет собственных IT- специалистов. Однако страхование киберрисков как раз предназначено для закрытия непредвиденных сценариев IT-безопасности или неизвестных новых киберугроз. То есть страхование никак не подменяет функцию IT-безопасности, но лишь усиливает защиту компании дополнительными мерами информационной и финансовой поддержки.