КИБЕРРИСКИ

В НОВОЙ РЕАЛЬНОСТИ

В прошлом году в связи с пандемией коронавируса произошел массовый переход многих компаний на удаленный режим работы. О том, какие риски в связи с этим возникли и как на них отреагировал рынок киберстрахования, рассказал Игорь Чичкан, руководитель отдела страхования финансовых рисков AIG в России.

Современные страховые технологии: Возникли ли в связи с пандемией новые риски и требования к обеспечению кибербезопасности в работе предприятий?

Игорь Чичкан: В целом, риски остались прежними, но вероятность их реализации значительно возросла. В основном они связаны с методом доступа и подключения к незащищенным сетям.

Работа через удаленный доступ, через настройки APN (Access Point Name), заставила многие компании обратить особое внимание на каналы, рабочие инструменты и системы безопасности. До пандемии в удаленном режиме работали 3-5 % сотрудников, теперь в некоторых компаниях — до 95 %.

Дистанционные каналы априори менее защищены. Злоумышленники с большей вероятностью и значительно проще могут получить доступ к домашним компьютерам сотрудников, а значит, и к корпоративным информационным системам. Дома или в публичных точках доступа wi-fi

иногда вообще не защищен, а это делает уязвимыми все подключенные устройства.

Если на домашнем или рабочем компьютере сотрудников стоит личная почта, любое письмо с вредоносным кодом способно подвергнуть риску корпоративную систему. Вероятность подобного сценария увеличилась в условиях дистанционной работы, как и количество атак, попыток доступа через e-mail и зараженные рассылки.

Другой тренд прошлого года — создание сайтов-клонов, особенно в социальной сфере: выплата пособий, выплаты на детей, госпрограммы поддержки туристической отрасли и т. д.

Кибератака может затронуть огромное количество предприятий одновременно в разных странах мира, разных масштабов — от небольших компаний в торговле и сфере услуг до промышленных гигантов. В таком случае к нам в агрегации попадают все индустрии, страны и категории компаний, и риск такой агрегации велик.

Игорь Чичкан

Руководитель отдела страхования финансовых рисков AIG в России

ССТ: Как в связи с этим изменился подход страховщиков и страхователей к страхованию киберрисков?

И. Ч.: Программы страхования киберрисков становятся менее доступными, поскольку риски растут. Готовность предприятий к самостоятельному противостоянию рискам снижается. Складывается ситуация, когда компании все больше интересует страхование киберрисков, но из-за зашкаливающего количества убытков и их масштабов оно становится не только дороже — в значительной степени снижаются и риск-аппетиты страховщиков. В силу целого ряда причин некоторым компаниям мы уже не можем предложить страхование киберрисков.

В 2020 году выросла активность кибервымогательства. Классический пример — когда компьютер заражен вредоносной программой, и вас просят перевести определенную сумму в долларах или биткоинах за ключ разблокировки. В Норвегии злоумышленники таким образом блокировали деятельность алюминиевого завода, а производитель электроники GARWIN заплатил около 10 млн долл. выкупа за разблокировку своих систем. В России пока ни один наш клиент не заявил о подобных убытках.

Тем не менее в связи с волной киберрисков, AIG, как и многие страховщики, глобально корректирует свою стратегию. У нас существенно снижаются емкости, с которыми мы работаем, и бизнес-аппетиты. Мы крайне осторожно подходим к страхованию любых убытков, связанных с кибервымогательством.

Рынок стал намного строже подходить к андеррайтингу. Мы просим клиента заполнить специальную анкету и указать используемые методы защиты и предупреждения киберугроз, внимательно изучаем их. Исходя из данных анкеты, мы понимаем, готовы ли страховать предприятие и, если да — будем полностью покрывать этот риск или частично. Предлагаем сострахование: 50 % риска клиент берет на себя, а 50 % передает страховщику. Бывают случаи, когда мы вынуждены отказывать в заключении договора страхования.

В мае 2018 года Европа перешла на обновленные правила обработки персональных данных, установленные Общим регламентом по защите данных — GDPR. Он имеет прямое действие во всех 28 странах ЕС и заменил рамочную Директиву о защите персональных данных 95/46/ЕС от 24 октября 1995 года.*

Важным нюансом GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных, поэтому российским компаниям следует внимательно отнестись к ним, если услуги ориентированы на европейский или международный рынок.

**Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR — General Data Protection Regulation.*

ССТ: От каких последствий кибератак предприятия страхуются прежде всего?

И. Ч.: Мы видим повышенный интерес к страхованию киберрисков со стороны финансовых институтов. Сейчас наши основные клиенты — это компании, у которых есть контракты с иностранными заказчиками. Большую долю в нашем портфеле занимают ИТ-компании — они лучше остальных понимают степень риска и пытаются подкрепить свою защиту нашим полисом.

ССТ: В финансовой сфере стало больше инцидентов с хищением баз данных. Ожидаете ли вы, что появятся крупные иски за утечку персональной информации клиентов?

И. Ч.: Пока нет изменений в законодательстве или процедурах, которые позволили бы более активно подавать такие требования, развития судебной практики ожидать не стоит. Но нужно разделять страхование киберрисков и мошенничество в интернете, которым занимаются физические лица. Безусловно, утечки данных из-за мошенников несут существенные репутационные и иногда финансовые риски для банков. Но физическим лицам предъявить претензии банку проблематично. Скорее, это вопрос к Росфинмониторингу, к регулятору, которые должны штрафовать финансовые организации.

В Европе с 2018 года действует стандарт General Data Protection Regulation. В Великобритании и континентальной Европе сам

Виктор Верещагин, *Президент Русского общества управления рисками (РусРиск), кандидат исторических наук*

Проблема кибербезопасности приобрела глобальный характер. Во всех опросах риск-менеджеров, которые проводились последние несколько лет в Европе и мире, киберриски попадают в первую тройку самых актуальных, их значимость постоянно растет. В полной мере это относится и к России.

Прежде всего, предприятия опасаются утечки коммерческих и персональных данных, а также вредоносного вмешательства в закрытые системы управления данными. Но разные сегменты бизнеса воспринимают и реагируют на

факт утраты данных является основанием для штрафов, которые могут достигать 5 % годовой выручки финансовой организации. Физическое лицо может подавать требования компании — оператору данных, основываясь на самом факте утраты, который уже считается основанием для возмещения ущерба. Но больше всего финансовые организации опасаются регуляторов, чьи требования гораздо серьезне.

ССТ: Страховать или не страховать киберриски — решение топ-менеджеров. Могут ли к ним быть предъявлены претензии со стороны акционеров, если предприятие понесет убытки из-за отсутствия договора страхования?

И. Ч.: Претензии, безусловно, могут возникнуть из-за отсутствия полиса. При наличии договора страхования убытки можно минимизировать, а если его нет — директора могут столкнуться с требованиями акционеров о недостаточном обеспечении страховой защиты предприятия.

Таких прецедентов в России не было, а в США после киберинцидента, когда компания понесла значительные убытки, акционеры предъявили требования к совету директоров. Они были связаны с тем, что совет директоров не приобрел защиту от киберрисков, решив сэкономить бюджет. Убытки во много раз превысили потенциальную страховую премию.

ССТ: Возможна ли в России ситуация, когда каждое предприятие будет иметь полис страхования киберрисков?

И. Ч.: Каждое — вряд ли, особенно когда не все предприятия покупают даже обязательные виды страхования.

Большинство руководителей предприятий в России не воспринимают страхование как инвестиции в безопасность. Расходы на антивирусные программы, ИТ-безопасность и специалистов тоже достаточно велики, но они материальны. Страхование воспринимают как гипотетическую договоренность, ее сложно потрогать. Так что сложно представить, какие должны быть предпосылки, чтобы большинство компаний страховали киберриски. Возможно, помогут определенные льготы, возможность отнесения на затраты расходы на страхование киберрисков.

Должно измениться отношение к страхованию в обществе в целом, культура риск-менеджмента. Надеюсь, что через некоторое время это произойдет.

киберугрозы по-разному. Более подготовлены к угрозам финансовый сектор и, прежде всего, банки. В реальном секторе экономики многие предприятия и компании не готовы в полной мере противостоять растущим киберугрозам из-за незнания и непонимания, как это нужно делать.

Несмотря на то, что о проблеме много пишут, ею активно занимаются ИТ и специализированные компании в области информационной безопасности, киберагрессоры действуют изощренно и часто оказываются на шаг впереди. Разработчики средств защиты зачастую предлагают новые инструменты по факту реализации угрозы, чтобы залатать пробоину.

Понимая серьезность угрозы, мы создаем в РусРиске рабочую группу по киберрискам с участием крупных ИТ-компаний, консалтеров и экспертов реального сектора. Мы планируем выработать серьезные комплексные меры, включая корректировку законодательной и нормативной базы, управленческие решения, возможно — страхование киберрисков. Мы также намерены пригласить к сотрудничеству коллег из ВСС, чтобы привлечь к работе и страховщиков.