УДК 363:005(475)

М.А. Зайцева, Н.С. Ананенко
Белорусский государственный экономический университет

СТРАХОВАНИЕ КИБЕРРИСКОВ И ЕГО РАЗВИТИЕ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Развитие экономики страны предполагает широкое внедрение информационных технологий. Информационные технологии в экономике охватывает три ключевых компонента: соответствующая инфраструктура (информационные системы, информационно-телекоммуникационные сети и т.д.), электронное предпринимательство (предпринимательская деятельность с помощью компьютерных сетей) и электронная коммерция. Вместе с технологиями неизбежно возникают и новые виды преступлений в данной сфере. В последнее время особенно остро стоит вопрос обеспечения защиты от компьютерного мошенничества, ежегодные убытки от которого в США, например, составили до 100 млрд долл. США, а в Европе – до 30 млрд долл. США. В международной практике разработаны и внедрены в практическую деятельность специальные стандарты информационной безопасности – PCI DSS. Однако опыт свидетельствует, что полностью исключить соответствующие риски невозможно. В этой связи особую актуальность приобретает поиск соответствующих способов защиты от данных рисков, одним из которых является страхование киберрисков.

Основным толчком к развитию страхования киберрисков стала «проблема 2000», когда смена цифр в компьютерных сетях с одного на другое тысячелетие создала значительные затруднения в работе информационных баз данных. Крупнейшие международные корпорации обратились к страховщикам за получением соответствующего страхового покрытия. Однако страховые компании смогли предложить клиентам лишь отдельные полисы страхования имущества и ответственности. В дальнейшем страховщики стали уделять более существенное внимание разработке страховых продуктов по защите от рисков, связанных с утечкой данных. Основным видом страхования в данной сфере стало страхование ответственности за причинение вреда третьим лицам, а также потерь страхователя, вызванных утечкой данных. В дальнейшем предлагаемые программы усложнялись и совершенствовались.

Как правило, на практике информационные риски объединяются в укрупненные группы:

- ответственность страхователя перед клиентами, агентами, партнерами за потерю данных;

• имущественные риски, связанные с поломкой дорогостоящего оборудования и остановкой его работы;

• финансовые потери, связанные с проведением аудита, использованием услуг аутсорсеров и т. д.

Основными причинами утечки информации в настоящее время являются: хакерские атаки, воздействие человеческого фактора и сбои в системе данных.

В дополнение к имущественным рискам, связанным с киберпреступностью (хакинг жестких дисков или материальный ущерб, вызванный повреждением компьютеров, подключенных к одной сети) также растут риски, затрагивающие виртуальные (облачные) хранилища.

Страхование киберрисков позволяет покрывать убытки, связанные с утечкой информации или повреждением данных.

Основные группы рисков в данной сфере следующие:

- умышленные действия сотрудников;
- воздействие человеческого фактора;
- наличие внешних угроз;
- аутсорсинг;
- развитие социальных сетей.

Умышленная кража информации сотрудниками предполагает преднамеренную утечку данных в результате их противоправных действий, а также преднамеренное уничтожение имущества организации.

Воздействие человеческого фактора – отправка недостоверных данных другим лицам, потеря переносных устройств и др.

Внешние угрозы включают хакерство, внедрение вирусов в программное обеспечение и др.

Аутсорсинг затрагивает риски, связанные с хранением информации, в том числе в виртуальных хранилищах.

Развитие социальных сетей предполагает появление таких рисков как блокировка соответствующих страниц, искажение данных о бизнесе и др.

Как свидетельствует практика, сфера страхования киберрисков пока еще не изучена досконально, несмотря на то, что потребность в ее развитии существует уже более 20 лет. Сдерживают данное развитие следующие факторы:

1. Ограниченность спастической информации для проведения расчетов страховых тарифов по данным видам страхования с учетом всех факторов риска. В отличие от традиционных видов страхования, где оценка риска и расчёт страхового тарифа осуществляется на основе данных страховой статистики с помощью актуарных расчётов, при страховании киберрисков затруднено использование классических подходов к расчету необходимых составляющих страхового тарифа: ограничен

объем статистической информации, что не позволяет применять соответствующие математические законы распределения к рядам данных. Активное развитие информационных технологий сопровождается увеличением числа факторов риска, усилением их кумуляции друг с другом, что значительно увеличивает риск возникновения ошибок при расчетах.

2. **Недостаточное развитие** предстраховой экспертизы в данной сфере. На этапе заключения договора страхования информационных рисков, имеющихся данных о деятельности субъектов хозяйствования недостаточно для объективной оценки состояния их информационной безопасности. Кроме того, потенциальные страхователи могут скрывать результаты тестов кибербезопасности или не предоставлять информацию о состоянии информационной безопасности внутри организации. Привлечение узкоспециализированных специалистов (сюрвейеров и андеррайтеров) не всегда возможно в силу специфики банковской сферы, имеющимся требованиям к конфиденциальности информации о системах безопасности организации, не разглашении особенностей их построения.

3. Включение недостаточно изученных видов рисков в страховой портфель страховщика способно нарушить его сбалансированность и финансовую устойчивость компании в целом. Следствием недостоверного расчета страховых тарифов, завоевания маркетинговых преимуществ на страховом рынке по данным видам страхования является увеличение технического риска страховщика: превышение убытков над объемом сформированных страховых резервов. Для обеспечения финансовой устойчивости страховых операций при страховании информационных рисков страховщику целесообразно учитывать специфику деятельности его клиента. Например, в финансовой и особенно в банковской сфере кибератаки совершаются в основном с целью хищения денежных средств клиентов или с целью кражи информации. В этой связи особую значимость приобретает и необходимость разработки соответствующей программы перестраховочной защиты для данных видов рисков.

4. Особенно сложным является механизм урегулирования убытков в данной сфере, поскольку возможный ущерб включает в себя не только прямые финансовые потери при наступлении страхового случая, но и косвенные убытки в результате причинения ущерба репутации компании, потери клиентов и др.

Все выше названные проблемы сдерживают разработку и внедрение в практику страхования комплексного страхового продукта, позволяющего обеспечить защитой киберриски страхователя.

В зарубежной практике страхование информационных рисков за последние годы получило определенное развитие. Лидерами в сфере страхования киберрисков являются: AIG, Chubb. На их долю приходится практически одна третья часть рынка страхования.

Самый популярный страховщик, базирующийся в Цюрихе, – Chubb – предоставляет несколько различных продуктов киберстрахования: страхование информационных рисков для крупных организаций; их расширенная защита с учетом потребностей технологических компаний, консультантов и разработчиков программного обеспечения; страхование от преступлений, хищения данных и вымогательств, а также несколько других видов страхования, в дополнение к киберстрахованию, др.

В отличие от зарубежной практики в Республике Беларусь данный сегмент страхового рынка практически не развит. Страховщики страны предлагают клиентам лишь традиционные виды страховой защиты: имущества, ответственности перед третьими лицами и др.

Вместе с тем дальнейшее развитие субъектов хозяйствования невозможно без расширения комплексной страховой защиты от всевозможных рисков (в т.ч. информационных). Целесообразно поэтапно внедрять страхование киберрисков в их деятельности. Первоначально следует осуществить ряд мероприятий:

– использовать программное обеспечение высокого уровня безопасности, включая компьютеры и мобильные устройства;

– регулярно обновлять компьютерные системы и соответствующее оборудование к ним;

– осуществлять комплекс предупредительных мероприятий в данной сфере (сканирование информации для предотвращения и уничтожения входящих угроз по мере их возникновения и др.).

Эти и ряд других мероприятий будут способствовать внедрению страхования киберрисков в деятельность субъектов хозяйствования, что позволит обеспечить их комплексную страховую защиту и в целом расширит их деятельность в стране.

УДК 339.168:330.342.23(510+476)

С.Г. Заливако, Т.Г. Кучиц
Научно-исследовательский экономический институт
Министерства экономики Республики Беларусь

ОБ УПРОЩЕНИИ ТОРГОВЛИ МЕЖДУ КИТАЙСКО-БЕЛОРУССКИМ ИНДУСТРИАЛЬНЫМ ПАРКОМ «ВЕЛИКИЙ КАМЕНЬ» И КНР

Дальнейшему развитию Китайско-Белорусского индустриального парка (КБИП) «Великий камень» как высокотехнологичного и экспортоориентированного международного кластера будет способствовать открытие для его резидентов крупных внешних рынков.