Секция 4

ЦИФРОВАЯ ЭКОНОМИКА И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 368.07:007

А.В. Афанасенко[1], И.Н. Емельянчик[2]
[1]Минский государственный лингвистический университет
[2] Научно-исследовательский экономический институт
Министерства экономики Республики Беларусь

УПРАВЛЕНИЕ КИБЕРРИСКАМИ И ИХ СТРАХОВАНИЕ

В современном мире, где организации коммерческой сферы, в том числе все правительственные структуры – организовывают сбор, хранение и обработку информации, наблюдается рост инцидентов в области информационной безопасности которые имеют широкое распространение и приобретают угрожающий характер.

Информационная безопасность является одним из ключевых слагаемых успешного бизнеса вне зависимости от его масштаба и сферы деятельности. В этой связи основной задачей информационной безопасности является сбалансированная защита конфиденциальности, целостности и доступности данных.

Составляющими элементами информационной безопасности являются компьютерная безопасность и кибербезопасность.

Компьютерная безопасность – раздел информационной безопасности, характеризующий невозможность возникновения ущерба компьютера, превышающего величину приемлемого ущерба для него от всех выявленных и изученных источников его отказов в определённых условиях работы и на заданном интервале времени.

Кибербезопасность – раздел информационной безопасности, в рамках которого изучают процессы формирования, функционирования и эволюции киберобъектов, для выявления источников киберопасности, образующихся при этом, определение их характеристик, а также их классификацию и формирование нормативных документов, выполнение которых должно гарантировать защиту киберобъектов от всех выявленных и изученных источников киберопасности.

На основании этого дадим определение киберрискам. Под киберрисками понимаются возможные взломы, перебои и другие нарушения

в работе компьютерных и информационных систем и сетей, при наступлении которых могут возникнуть определенные последствия.

Среди основных последствий киберрисков выделяют – потери прибыли, снижение стоимости фирмы, дополнительные затраты на расследование и восстановления данных, ущерб имиджу фирмы.

Составляющими процесса управления киберрисков фирмы являются процедуры своевременного выявления рисков, их оценка и последующая обработка.

Стоит отметить, что любая хорошо продуманная методология оценки киберрисков предусматривает такие шаги, как:

- выявление угроз, направленных на рассматриваемые активы;
- определение последствий от реализации угроз;
- выявление уязвимостей;
- выявление существующих контролей;
- определение вероятности реализации угроз.

Как видим, шаги методики оценки киберрисков определяются, исходя из предложенного определения понятия киберрисков.

Шаг 1. Определение критериев оценки.

Один из подходов, позволяющий определить критерии для оценки последствий киберрисков, заключается в том, чтобы оттолкнуться от целей, которые мы ставим перед разработкой методики оценки киберрисков. Что в дальнейшем позволит минимизировать финансовые потери, сохранить или даже улучшить имидж организации.

Шаг 2. Идентификация рисков.

На данном этапе необходимо идентифицировать угрозы и, соответственно, риски, а также проводиться анализ, кто или что может выступить в качестве источника киберриска.

Шаг 3. Оценка рисков.

Производиться оценка вероятности и последствий угрозы и соответственно определения значение киберриска.

Шаг 4. Ранжирование рисков.

После проведенной оценки киберрисков мы сразу можем их ранжировать по значениям, и определять, какому риску уделить внимание в первую очередь, а какому – в последнюю.

Число кибератак на компании с каждым днем растет. В 2013–2018 годах из-за этого инвесторы потеряли 52 млрд долларов. В 2018 году только вирусы WannaCry, Petya и NotPetya парализовали работу миллионов компьютеров в 99 странах мира [3].

Несмотря на то что киберриски вполне реальные, многие компании еще не нашли оптимального средства борьбы с ними. Результаты глобального опроса руководителей крупных корпораций, проведенного

KPMG в 2018 году, показывают, что многие респонденты относятся к кибератакам на свой бизнес как к неизбежности, а 68% руководителей американских компаний назвали это лишь вопросом времени. При этом 51% руководителей компаний из разных стран отметили, что они хорошо подготовлены к кибератакам [2].

С тех пор как деньги приобрели безналичную форму, возможность их хищения существенно увеличилась, так как взломать пароль намного проще, чем каменные стены подземных хранилищ.

Сейчас компании пытаются определить и оценить уровень уязвимости своих систем и принимать меры реагирования на постоянно растущие цифровые угрозы и целенаправленные кибератаки. Это серьезная проблема, с которой корпорациям могут помочь справиться страховые компании.

Страхование киберрисков – относительно новое направление на рынке страхования, обладающее колоссальным потенциалом развития. Популярность киберстрахования в мире растет вместе с киберрисками. PWC предсказывает, что к 2020 году объем ежегодно собираемых страховых премий в этой сфере достигнет 7,5 млрд долларов США.

Страхование киберрисков – страховой продукт, который защищает клиента от последствий DDoS-атак, вирусных заражений внутренней сети и других киберугроз.

Практика страхования киберрисков нарабатывается постепенно, страховые компании, как и их клиенты, учатся выявлять и страховать риски методом проб и ошибок.

На сегодняшний день лидером киберстрахования по праву считаются США с их мощной IT-инфраструктурой, где были отмечены первые в мире серьезные киберугрозы для бизнеса и где действует жесткое законодательство по защите персональных электронных данных.

Страхование киберрисков бывает двух типов: для первого лица и для третьей стороны. Большинство страховщиков предлагают полисы, которые сочетают в себе функции обоих, но не всегда.

Полис для первого лица – это то, что требуется большинству предприятий. Он защищает от потерь, понесенных страхователем, и может включать в себя компенсацию в следующих случаях:

- поврежденные или утраченные цифровые активы, например, данные и программное обеспечение;
- утраченные возможности для бизнеса или увеличение операционных расходов из-за простоя компьютерных систем;
- кибер-вымогательство, когда хакер требует выкуп в обмен на похищенные данные;
- похищение денег хакером со счета.

Полисы третьих лиц предназначены для сторонних компаний, которые управляют программным обеспечением, локальной сетью или системой хранения данных (интернет-провайдеры, модераторы соцсетей). Этим предприятиям страховщики обычно покрывают расходы, которые связаны со следующими событиями:

- нарушение конфиденциальности данных о сотрудниках;
- утрата информации о клиентах;
- уведомление клиента после нарушения безопасности;

борьба с нарушениями интеллектуальной собственности.

Полисы кибербезопасности не покрывают ущерб от потери репутации и падения продаж. Этот вид страхования настолько новый, что страховщики не всегда могут легко и точно оценить риск. Поэтому они исключают из полиса те элементы, которые трудно определить.

Если говорить о белорусском сегменте интернет-пространства, динамика роста киберпреступности сегодня весьма неутешительная. По предварительным прогнозам, в будущем эта тенденция не пойдет на спад в связи с тем, что все преступные явления, которые происходят в Интернете, давно коммерциализированы. Как показывает опыт. Уровень компьютерной преступности в любой стране прямо пропорционален росту технического прогресса.

Развитие рынка киберстрахования в Республике Беларусь со временем может стать качественным средством обеспечения информационной безопасности и защиты от кибер-угроз. Однако на сегодняшний день в Беларуси нет страховых компаний, готовых предложить качественный системный продукт, направленный на защиту клиентов от киберпреступности.

Для широкого внедрения этого вида страхования отсутствует законодательная база и судебная практика. Недостаточно пока и страховых компаний, и специалистов, имеющих представление о структуре киберрисков.

Список использованных источников

1. Дорофеев А.В. Марков А.С., Менеджмент информационной безопасности: основные концепции // Вопросы кибербезопасности. 2014. № 1(2). С.67-73.

2. Скрундь Е., Страхование киберрисков: международная практика и возможность применения в Республике Беларусь // Страхование в Беларуси. 2019. № 5(198). С. 25–28.

3. Страхование кибербезопасности: как уберечь бизнес от хакеров [Электронный ресурс]. Режим доступа: http://www. 365-invest.com/strahovanie-kiberbezopasnosti-kak-uberech-biznes-ot-hakerov/. – Дата доступа: 18.11.2019.