ПРОБЛЕМЫ РИСК-МЕНЕДЖМЕНТА В УСЛОВИЯХ БЫСТРОГО РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Т. А. Бронская

Белорусский государственный университет, г. Минск
bronska@tut.by;
науч. рук. – С. В. Лукин, д-р экон. наук, проф.

В статье автором прослеживается актуализация проблем риск – менеджмента на предприятиях. Проанализированы новые риски, возникающие в связи с быстрым развитием информационных технологий и ответственности компаний за последствия кибер атак.

Ключевые слова: типы рисков; виртуальное пространство; информационные технологии; кибер риски; кибер атаки.

В последние годы в Республике Беларусь быстрыми темпами продвигается использование в деятельности компаний мобильных технологий, аналитики информации из виртуального пространства, использование облачных технологий, социальных медиа, искусственного интеллекта, интернет вещей. Использование информационных технологий необходимо для устойчивого развития предприятий в стратегии и инновациях, привлечении и удержании клиентов, операционной деятельности, технологии производства, ведении финансового и бухгалтерского учета, управлении персоналом. Однако деятельность в цифровом пространстве сопряжена с новыми рисками и угрозами.

Устойчивое и сбалансированное развитие белорусских компаний зависит от качественных изменений в своевременном определении и внедрении новых рисков в систему риск – менеджмента.

1. Эволюция риск – менеджмента

Область управления рисками возникла в связи с необходимостью обеспечения устойчивого развития предприятия и преодоления последствий наводнений, пожаров, краж, травм сотрудников, нарушений правил бухгалтерского учета, колебания курса валют. Постепенно управление рисками превратилось в необходимую часть планирования деятельности компании. Поскольку данная функция увеличивалась с каждым годом все больше и больше в результате, для широкомасштабного охвата всех систем компании, была создано управление рисками на предприятии или риск-менеджмент.

2. Типы рисков и управление рисками

Общие типы рисков включают автомобильные аварии, травмы сотрудников, пожары, кражи, наводнения, экологические проблемы. Кроме того существуют риски, связанные с характером деятельности ком-

паний. Выделяет пять категорий рисков: 1)бизнес-риски, связанные с конкретной отраслью; 2)рыночные риски, связанные с колебанием цен, процентными ставками и обменными курсами; 3)кредитные риски, связанные с платежеспособностью клиентов; 4)операционные риски, связанные с внутренними сбоями, такими как нарушение работы оборудования или ошибок персонала; 5)правовые риски, связанные с невыполнением обязательств по заключенным договорам [1].

Текущие тенденции развития активного использования информационных технологий связаны с критическими угрозами для деятельности компании, такими как кибер риски [2]. К ним относятся вредоносные коды, фишинг, атаки нулевого дня, мошенничество, кибер атаки с целью нанесения вреда организации, кибер атаки с целью похищения финансовых данных, кибер атаки с целью похищения интеллектуальной собственности.

Любой риск может привести к различным потерям и нарушить экономическую устойчивость компании или ее конкурентоспособность. Возникновение новых рисков требует модернизации системы риск – менеджмента. В различных уровнях защиты компании необходимо учитывать современные уязвимости, связанные с халатностью персонала, с использованием несанкционированного доступа, мобильных устройств, облачных вычислений, социальных сетей. Деятельность предприятия в информационно-цифровом пространстве сопряжена с угрозой непредвиденных последствий и уязвимостей посредством злоумышленных действий, направленных на неавторизованное раскрытие, изменение или разрушение цифровых активов.

3. Проблемы риск – менеджмента

По мере расширения спектра возникающих рисков и для успешного управления ими, риск – менеджменту необходимо составить сценарий возникновения и преодоления угрозы, правильно классифицировать и оценить потенциальные потери, выбрать и применить метод управления риском. Важным подходом, включающим управление финансовыми, технологическими, экологическими и информационными рисками, является управление риском предприятия в целом, что позволяет создать единую для всех подразделений культуру ведения бизнеса [3]. Опасность кибер – рисков для экономической устойчивости компании состоит в том, что очень сложно рассчитать временной промежуток и объем распространения угрозы. Например, в случае утечки персональных данных, согласно новому закону Евросоюза «General Data Privacy Regulations» («Общие правила конфиденциальности данных») от 25 мая 2018 года, предприятие обязано уведомить как надзорный орган, так и владельцев этих данных. В зависимости от количества скомпрометированных записей будет размер стоимости уведомлений и соответственно

размер убытков. В случае единого центра управления рисками существует возможность разработки эффективных превентивных стандартов – корпоративной культуры, обязательной для всей компании в целом. Главной задачей риск – менеджмента является баланс в максимальном применении и использовании современных информационных технологий для успешного развития компании и мер по предотвращению кибер – рисков. Это очень сложная проблема. Каждая компания стремиться не только сохранить достигнутые результаты, но и постоянно внедрять новые технологии для развития бизнеса, привлечения новых клиентов, что связано с возникновением нового риска.

В целях принятия и выполнения управленческих решений, ориентированных на минимизацию потерь в результате возникающих негативных событий, риск – менеджменту необходимо прогнозировать риски, регулярно проводить мониторинг рисков, классифицировать их, использовать методику по оценке и анализу рисков и их предотвращения.

Развитие информационных технологий способствует применению эффективных и разнообразных моделей развития инцидентов как ранее изученных, так и возникающих в настоящее время в виртуальном пространстве и приводящих к финансовым, репутационным потерям. Идентификация и оценка рисков предоставляет возможность конкретизировать факторы, выполнение которых позволит построить стратегические сценарии для экономически устойчивого конкурентоспособного функционирования компании.

Библиографические ссылки

1. Основы страхования. URL: http://www.grandars.ru/college/strahovanie/strahovye–riski.htm (дата обращения 10.03.2018).
2. URL: http://podzontom.net/strahovanie/info–3/kiber–riski.html (дата обращения 10.03.2018).
3. Риск-менеджмент в страховой компании – тренды и перспективы Ладыгина Е. В. URL: http://www.insur–info.ru/interviews/1194/ (дата обращения 26.02.2018).