эффективное функционирование российских предприятий, а также рост российской экономики в целом.

1. Дударева А.Б. Мониторинг факторов, влияющих на повышение уровня рентабельности // Вестник сельского развития и социальной политики. – 2018. - №1 (17). – С. 26-29 (дата обращения: 19.10.2020).
2. Бурлака Е. В. Анализ рентабельности деятельности предприятия // Молодой ученый. — 2017. — №12. — С. 243-245 (дата обращения: 19.10.2020).
3. Саргсян А.С. Анализ рентабельности и факторов ее изменения // Студенческий форум: электрон. научн. журн. – 2017. - № 3(3). С. 48- 50 (дата обращения: 19.10.2020).

Рахматуллина Р.Р., Байгузина Л.З.

Современная система страхования – киберстрахование

*ФГБОУ ВПО БГПУ им.М.Акмиллы
(Россия, Уфа)*

doi: 10.18411/lj-11-2020-148

idsp: ljjournal-11-2020-148

Аннотация

В статье рассматривается, проблема возможных методов защиты от кибер-атак и негативных последствий от них. Одним из способов может выступать рынок кибер-страхования. Авторы отмечают, что центральной задачей киберстрахования остается защита от крупномасштабных хакерских атак, проводится анализ рынка кибер-страхования.

Ключевые слова: Киберстрахование, кибер-атаки, киберопасности, защита

В странах с развитой рыночной экономикой страхование является стратегическим сектором экономики, так как оно обеспечивает социально-экономическую стабильность в обществе путем возмещения собственникам ущерба при гибели или повреждении их имущества. Страхование позволяет юридическим и физическим лицам возмещать ущерб, причиненный случайными неблагоприятными событиями, предоставляет гражданам возможность получения страхового обеспечения при дожитии до определенного возраста, наступлении временной нетрудоспособности, инвалидности. Таким образом, страхование обеспечивает непрерывность всех видов общественно-полезной деятельности, а также поддержание уровня жизни, доходов людей при наступлении определенных событий - страховых случаев.

На фоне стремительного развития цифровых технологий и усложнения IT-инфраструктуры компаний замечен и значительный рост числа киберпреступлений. По данным МВД, в 2018 году их стало на 92% больше, чем в 2017. Неудивительно, что вопросы защиты от рисков потери данных, простоя, хакерских атак или утечки конфиденциальной информации становятся более актуальными, а страхование киберрисков выглядит разумным способом минимизации ущерба.

Компании захотели знать, какие гарантии защиты обрабатываемых данных предоставляет сервис-провайдер, и как предлагается минимизировать ущерб в том случае, если атаку остановить не удалось.

Что предлагают страховые компании.

Договор может быть заключён от всех или от некоторых видов киберопасности. При желании клиент может выбрать один из стандартных страховых пакетов или составить индивидуальный, учитывая особенности бизнеса и индивидуальные потребности. Базовые пакеты полиса покрывают риски утраты и искажения данных (включая вирусы-шифровальщики), программного обеспечения, разглашения персональных данных и включает расследование и диагностику кибератак.

Также в полисе можно предусмотреть защиту от рисков: утраты информации; хищения интеллектуальной собственности; неправомерного использования вычислительных ресурсов; вымогательства; хищения денежных средств; нарушения конфиденциальности и разглашение персональных данных; причинения вреда имуществу, жизни и здоровью третьих лиц; ущерба деловой репутации; утрате, гибели или повреждению готовой продукции, сырья, материалов; перерыва в деятельности.

Стоимость страхования зависит от набора рисков, страховой суммы и франшизы, а также рода деятельности страхователя и результатов оценки рискозащищенности.

Государственное регулирование.

Пока что каких-либо стандартов в области киберстрахования нет, а законодательство слабо развито в части определения ответственности за нарушения и преступления в сфере информационной безопасности.

Но в ближайшее время ситуация должна измениться. В национальном проекте «Цифровая экономика Российской Федерации» предусмотрен ряд мер, направленных на популяризацию добровольного страхования рисков информационной безопасности и повышение киберкультуры. Также в проект включено предложение о проработке возможности использования налоговых льгот при страховании киберрисков.

Что сдерживает мировые продажи страховок от киберрисков

Рисунок 1 - Алгоритм страхования киберрисков

Как выглядит процедура киберстрахования? Чтобы ответить на этот вопрос, возьмём информационную систему с уже созданной системой защиты данных. Это может быть система хранения персональных данных, госсистема с аттестатом на соответствие требованиям информационной безопасности или другая информационная система со средствами защиты, выбранных по принципу разумности и соразмерности затрат.

В этом случае компании нужно будет пройти следующие этапы:

- Выбор страховой компании, предлагающей комплексную услугу по страхованию киберрисков;
- Выбор экспертной организации для проведения аудита ИБ (из числа организаций, аккредитованных страховой компанией);
- Аудит и оценка рисков ИБ (проводится экспертной организацией);

- Определение страховых случаев;
- Определение размера страхового покрытия и страховых взносов;
- Формирование договора на комплексную услугу киберстрахования.

Если у компании система защиты ещё не создана или не соответствует требованиям законодательства РФ по защите, то предварительным этапом станет создание системы защиты либо размещение информационной системы у сервис-провайдера с заключением договора на хранение конфиденциальной информации.

Виды страховых рисков

В мировой практике существует несколько рисков, которые частично или полностью могут получить страховую защиту:

- Риск присвоения и использования конфиденциальной информации сотрудниками компании и ее использования;
- Риск получения хакером информации о номерах кредитных карт или счетов клиентов компании;
- Риск хищения денежных средств со счетов в банке или ценных бумаг со счета в депозитарии;
- Риск хищения данных кредитных карт и средств с них;
- Риск утраты или разглашения информации из-за ошибки сотрудника;
- Риск утери материального носителя, содержащего конфиденциальную информацию.

Что оценивают страховщики при работе с глобальными киберрисками

ИСТОЧНИКИ: HANNOVER RESEARCH/MARKET INSIGHT CENTRE; DELOITTE UNIVERSITY PRESS

Рисунок 2 - Страховое покрытие.

Практически во всех страховых случаях наиболее сложным вопросом является вопрос достоверной оценки стоимости утраченной информации.

Кроме того, при оценке информации как нематериального актива и получения страхового возмещения не исключены проблемы с нашим налоговым законодательством, которое не преминет обозначить всю сумму страхового возмещения как прибыль и обложить ее налогом. Этот вопрос на уровне разъяснений Минфина ещё не отрегулирован.

Выводы

Несмотря на достаточно молодой рынок страхования киберуслуг, уже имеются сложные комплексные решения. Ожидается, что и облачные провайдеры в скором времени будут предоставлять услуги по страхованию своей ответственности.

1. Байгузина Л.З. Развитие инновационных банковских продуктов на современном этапе // Рецензируемый научный журнал «Тенденции развития науки и образования». Июнь 2020 г. №62, Часть 8 Изд. НИЦ «Л-Журнал», 2020. – 104 с. - С. 19-23 DOI 10.18411/lj-06-2020-p8
2. Бардовский, В.П. Экономика / В.П. Бардовский. - М.: Изд-во Форум. - Инфра-М. - 2016. - 672 с.
3. Буфетова, А.Н. Основы экономики. Учебное пособие для абитуриентов ЭФ НГУ / А.Н. Буфетова, Л.С. Веселая - Новосибирск. - 2016.
4. Ермасов, С. В. Страхование в 2 ч. Часть 1. : учебник для академического бакалавриата / С. В. Ермасов, Н. Б. Ермасова. — 6-е изд., перераб. и доп. — М. : Издательство Юрайт, 2019. — 475 с.
5. Марохонько, О.И. Организация самостоятельной работы студентов. – М.: Эксмо-Пресс, 2016. – 304 с.
6. Турчаева, И. Н. Страхование в апк : учебник и практикум для бакалавриата и специалитета / И. Н. Турчаева. — М. : Издательство Юрайт, 2019. — 229 с.

Сагидуллина А.В.

Поддержка малого и среднего бизнеса в рамках профессионального образования

*ФГБОУ ВПО БГПУ им.М.Акмиллы
(Россия, Уфа)*

doi: 10.18411/lj-11-2020-149

idsp: ljjournal-11-2020-149

*Научный руководитель
Байгузина Л.З.*

Аннотация

Актуальность. Проблема формирования эффективной поддержки малого и среднего бизнеса в рамках профессионального образования персонала становится краеугольным камнем современного бизнеса в условиях рыночных отношений. Для современных предпринимателей постоянное повышение профессиональных знаний и компетенций особенно важно в российских условиях, когда экономика и технологии постоянно развиваются.

Цель статьи - выявить факторы и проблемы, а также рассмотреть поддержку малого и среднего бизнеса в рамках профессионального образования.

Для исследования и анализа вопросов, посвященных поддержке малого и среднего бизнеса в рамках профессионального образования, использовались специальные методы научного исследования, например, такие, как: диалектический, статистический, формально-логический, сравнительно-правовой, системно-структурный и др.

Только комплексный подход к организации поддержки субъектов малого и среднего предпринимательства будет способствовать их дальнейшему развитию. На современном этапе развития общества, экономики и образования, меры государственной поддержки по вопросам повышения профессионального образования становится необходимым компонентом развития бизнеса.

Ключевые слова: Малый бизнес, малое и среднее предпринимательство, образование, профессиональные компетенции, учебные заведения, государство, поддержка, субсидии, инновации.

Abstract

The problem of forming effective support for small and medium-sized businesses within the framework of professional education of personnel is becoming the cornerstone of modern business in the conditions of market relations. For modern entrepreneurs, the constant