УДК 658.15

ПРИМЕНЕНИЕ КИБЕРСТРАХОВАНИЯ В СОВРЕМЕННЫХ УСЛОВИЯХ РАЗВИТИЯ ЭКОНОМИКИ

Конюкова О.Л.

к.э.н., доцент,

Сибирский государственный университет путей сообщения,

Новосибирск, Россия

Рагозин Н.А.

магистрант,

Сибирский государственный университет путей сообщения,

Новосибирск, Россия

Аннотация

В данной статье рассматривается актуальная на сегодняшний день проблема - киберпреступность. Статья посвящена относительно новому виду страхования в России – киберстрахованию, которое является одним из способов защиты от возросших кибератак в современном мире. Также в статье раскрываются основные виды киберрисков, с которыми могут столкнуться практически все компании в мире.

Ключевые слова: страхование киберрисков, киберстрахование, киберпреступность, киберпреступления, кибербезопасность, киберриск, кибератака, хакерская атака.

APPLICATION OF CYBER INSURANCE IN MODERN CONDITIONS ECONOMIC DEVELOPMENT

Konyukova O.L.

PhD, Associate Professor,

Siberian State Transport University,
Novosibirsk, Russia

Ragozin N.A.
master's degree student,
Siberian State Transport University,
Novosibirsk, Russia

Annotation
This article discusses the current issue – cyber crime. The article is devoted to a relatively new type of insurance in Russia - cyber insurance, which is one of the ways to protect against increased cyber attacks in the modern world. The article also reveals the main types of cyber risks that almost all companies in the world may face.
Keywords: cyber risk insurance, cyber insurance, cyber crime, cyber security, cyber risk, cyber attack, hacker attack.

В связи с тем, что сегодня в быстром темпе происходит развитие технологий обработки и хранения информации, проблема киберпреступности набирает обороты с каждым днем, тем самым, являясь одной из актуальных проблем XXI века и серьезной угрозой для бизнеса во всех странах, да и для государств в целом. Цифровизация экономики становится необходимостью эффективного функционирования.

Под цифровизацией необходимо понимать использование и внедрение новых цифровых технологий, основной целью которых будет являться повышение эффективности и результативности деятельности государственных органов. Это может быть как изменение отдельных процессов, так и что-то большее. Эпоха цифровизации, охватывающая всё большие отрасли, в пер-

спективе затронет все сферы экономии и многие существующие компании [4].

Киберпреступность – это преступления, совершаемые в сфере информационных технологий, иначе говоря, в виртуальном пространстве, к которым можно отнести: распространение вредоносных программ, взлом паролей от социальных сетей и электронной почты, кражу номеров банковских карт и других банковских реквизитов и, как результат, списание со счетов денежных средств, фишинг, распространение противоправной информации через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем и другие виды интернет-мошенничества [3].

Так, согласно докладу о глобальных рисках Всемирного экономического форума 2019 года, кибератаки занимают 5-е место среди всех глобальных рисков. Аналитики считают, что такую глобальную проблему, как киберпреступность, по своей значимости можно приравнять к мировым экологическим проблемам [5].

В официальном ежегодном отчете о киберпреступности за 2019 год говорится о том, что атаки хакеров во всём мире происходят каждые 14 секунд. По данным международных экспертов в сфере кибербезопасности, за 2019 год во всемирную сеть утекло более 14 млрд. конфиденциальных данных. Также они опубликовали информацию о том, что число утечек информации во всем мире в 2019 году по сравнению с прошлым 2018 годом выросло на 10%, а в России – более чем на 40% [5].

При этом, с ростом киберпреступности растёт и причиняемый ущерб. Так, согласно аналитикам, потери мировой экономики в 2019 году от этой угрозы достигли 3 трлн. долларов [5].

По данным МВД России, доля киберпреступлений в общем объеме преступлений в России выросло с 11,2 % по итогам 2019 года до 19,9 % за первый квартал 2020 года, а количество киберпреступлений выросло на 83,9 % по сравнению с первым кварталом прошлого года [5].

Таким образом, полностью защититься от хакерской атаки невозможно, однако, можно переложить данные киберриски на страховщика. И одним из возможных способов защиты от киберпреступности, а также негативных последствий и убытков от нее может выступать киберстрахование.

Киберстрахованием (страхованием киберрисков) называется страховой продукт по защите киберрисков компаний, бизнес которых прямым или косвенным способом связан с обработкой и хранением данных. И на сегодняшний день практически все компании малого, среднего и крупного бизнеса в мире могут в любой момент быть подвержены кибератакам. Компании могут подвергнуться риску хищения какой-либо важной и конфиденциальной информации (например, кража ноу-хау), персональных данных сотрудников и клиентов или иной ценной коммерческой информации, которая может повлиять на котировки ценных бумаг компании [1].

Объектом киберстрахования являются имущественные интересы, связанные с риском получения финансовых убытков и ущерба в целом в связи с нарушениями конфиденциальности данных, интернет-мошенничеством, хакерскими атаками и др. [1].

Страхование киберрисков впервые появилось в США в 1999 году. В России данный вид страхования предлагается только с октября 2012 года.

В пятерке самых атакуемых отраслей по-прежнему остаются госучреждения, промышленность, здравоохранение, финансы и образование. Наибольший интерес хакеры проявляют к финансовому сектору, а именно к банкам, инвестиционным компаниям, участникам РЦБ, электронным платежным системам и самим страховым компаниям.

Крупнейшими российскими страховыми компаниями и иностранными страховыми компаниями, которые предлагают страховую защиту от киберрисков в России, являются: Ингосстрах, СОГАЗ, АльфаСтрахование, Allianz и AIG. Также данный вид страхования предлагает Страховой брокер Сбербанка.

В настоящее время страховые организации во всем мире предлагают полисы страхования, которые обеспечивают защиту от следующих киберрисков:

1. Риск хищения и использования чужой конфиденциальной информации, в том числе персоналом компании.

2. Риск получения информации о номерах банковских карт или счетов клиентов, персонала или компании в целом.

3. Риск хищения денежных средств с банковских счетов, а также ценных бумаг.

4. Риск разглашения конфиденциальной информации компании по вине сотрудников.

5. Риск приостановления деятельности компании вследствие нарушения работы компьютерной сети или сайта компании.

6. Риск получения убытков и ущерба компанией в результате размещения на сайтах страховой компании ложной информации.

7. Риск утери носителя ценной информации [2].

В стоимость полиса киберстрахования, как правило, должны входить следующие услуги:

- привлечение высококвалифицированных специалистов в области расследований киберпреступлений, интернет-мошенничества и хакерских атак;

- привлечение опытных специалистов по восстановлению репутации и бренда компании (антикризисный PR);

- привлечение юристов, специализирующихся в сфере информационных технологий;

- привлечение экспертов по восстановлению данных [2].

Стоит отметить, что рост спроса на киберстрахование происходит тогда, когда в какой-нибудь стране случается масштабная хакерская атака, о которой потом говорят и пишут СМИ.

Таким образом, рынок киберстрахования в России на данный момент находится на этапе формирования. Страхование киберрисков на сегодняшний день является достаточно эффективным механизмом для минимизации финансовых потерь, связанных с утечкой конфиденциальной информации компании. И несмотря на то, что рынок киберстрахования в последние годы в мире развивается довольно быстро, популярность киберстрахования в России все еще не столь велика, и можно сказать, что многие компании даже скептически относятся к такому новому виду страхования, как страхование киберрисков. На наш взгляд, данный вид страхования будет набирать популярность в России именно тогда, когда компании начнут осознавать серьезность потерь вследствие киберпреступлений.

Библиографический список:

1. Иванов И.К. Киберстрахование: как обеспечить информационную безопасность бизнесу // Большой портал для малого бизнеса - 2016, №16, С. 13-24.

2. Мамаева Л.Н. Ларионов В.И. Киберстрахование как способ обеспечения информационной безопасности // Экономическая безопасность и качество - 2018. №1 (30). С. 76-79.

3. Номоконов В.А. Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра - 2017. №24. С. 45-55.

4. Роль цифровизации в государственном управлении Конюкова О.Л., Летунов С.А. Global and Regional Research. 2019. Т. 1. № 1. С. 74-79.

5. Утечки данных 2019: статистика, тенденции кибербезопасности и меры по снижению рисков взлома [Электронный ресурс]. – Режим доступа – URL: https://vc.ru/services/103616 utechki dannyh 2019 statistika tendencii kiberbezopasnosti-i-mery-po-snizheniyu-riskov-vzloma (Дата обращения 29.04.2020).

Оригинальность 94%