УДК 334.722-028.27:339.137:368

А.К. Костенко
kostenko@gsu.by
Гомельский государственный университет имени Ф. Скорины, Беларусь

КИБЕРСТРАХОВАНИЕ И ЕГО РОЛЬ В ОБЕСПЕЧЕНИИ КОНКУРЕНТОСПОСОБНОСТИ СУБЪЕКТОВ МАЛОГО И СРЕДНЕГО ПРЕДПРИНИМАТЕЛЬСТВА

В статье рассмотрены проблемные вопросы, связанные с обеспечением информационной безопасности предпринимательских структур, занятых в сфере электронного бизнеса, и развитием рынка киберстрахования в Беларуси; обоснована роль киберстрахования как одного из ключевых конкурентных преимуществ в эпоху цифровизации, достигаемых за счет укрепления деловой репутации субъектов малого и среднего предпринимательства и повышения к ним доверия со стороны потребителей.

Активное развитие инфо-коммуникационных технологий в эпоху общества потребления предопределило главенствующую роль электронной коммерции при построении бизнес моделей субъектами хозяйствования. В отсутствие барьеров входа на рынок потребительских товаров, которые ранее могли устанавливать крупные торговые сети, предприятия и организации получили возможность активного продвижения своей продукции и бренда через сеть Интернет и операторов мобильной связи, формируя культуру потребления – вкусы, желания, ценности, нормы поведения, интересы. На смену сетевой торговле через супермаркеты и гипермолы пришла эра транспортно-логистических хабов и пунктов выдачи товаров интернет-магазинами.

Современные информационные системы в сочетании с технологиями сбора, хранения и мгновенной обработки большого объема информации активно используются интернет-комерсантами для изучения мотивов поведения потребителя, составления полного представления о его запросах и индивидуальных предпочтениях. Контекстная интернет-реклама глубоко проникает в сознание потребителя и формирует спрос на товары. На этом фоне субъекты малого и среднего предпринимательства (МСП), традиционно ограниченные в размерах стартового капитала, при выборе направлений будущей деятельности все чаще отдают предпочтение такой форме его приложения как Интернет-торговля. По данным Министерства антимонопольного регулирования (МАРТ) в Беларуси в 2018 году доля Интернет-торговли в розничном товарообороте страны превысила 3,4% или 1,53 млрд. рублей. По состоянию на 01.10.2019 в торговом реестре было зарегистрировано 21 815 интернет-магазинов, что на 3263 единицы больше, чем на соответствующую дату предыдущего года. Прирост составил 17,6%. При этом более 50% зарегистрированных в нашей стране интернет-магазинов принадлежит ИП, которым с 1 января 2018 года в качестве послабления разрешили применять упрощенную систему налогообложения. Для сравнения, в США на долю Интернет-торговли приходится около 9-13% всего розничного рынка, в Великобритании – 17%, в Китае – 18%, [1,2]

Через сайты интернет-магазинов и интернет-порталов покупатель сам приходит к продавцу, повсеместно оставляя информацию о себе через разнообразные формы регистрации, личные кабинеты, подписки и т.д. Вполне естественно, что и оплата за товары чаще всего производится в онлайн-режиме, посредством использования дистанционных каналов банковского обслуживания, соответствующих платежных инструментов и электронных платежных систем. При проведении электронных платежей за товары или услуги происходит обработка персональных данных плательщиков (номеров платежных карт, логинов и паролей, кодов доступа) посредством мобильных устройств, персональных компьютеров, серверов, Интернет-ресурсов, пользователи которых подвержены рискам кибератак.

Любой бизнес построен на доверии участвующих в нем партнеров. Утрата доверия покупателя ведет к банкротству продавца, а его укрепление позволяет получить важные конкурентные преимущества – репутацию, имидж, PR. Потеря или утечка персональных данных приводит к утрате доверия клиентов и наносит ущерб репутации компании, который трансформируется в прямые (штрафы, пени, неустойки) и косвенные (недополучение выручки, прибыли, дохода) финансовые потери.

Киберриски, возникающие при работе с информацией в информационных системах, являются самыми быстрорастущими рисками нашего времени. За считанные секунды личная информация клиента может быть украдена, и использована для получения кредитной линии, оформления ипотеки или кредитных карт. Именно поэтому вопросы обеспечения кибербезопасности сегодня стоят как никогда остро.

В управлении по раскрытию преступлений в сфере высоких технологий МВД РБ обеспокоены тем, что если в 2015 году в Беларуси было совершено 2440 преступлений в сфере высоких технологий, то в 2018 году таких преступлений было зарегистрировано уже 4741 или на 53% больше чем в 2017 году, а за четыре месяца 2019 года – более 2500. На фоне впечатляющей динамики роста таких преступлений уровень их раскрываемости составляет всего 53-55%. Меняется и структура киберпреступлений. Если в 2015 году 83,4% из них были связаны со статьей 212 УК РБ «Хищение путем использования компьютерной техники», то в 2018 году аналогичные преступления составили уже 75,5%. При этом участились факты несанкционированного доступа к компьютерной информации (18%), которых стало на 97% больше, чем в 2017 году, а также компьютерного саботажа (3,5%). [3]

Часто жертвы не подозревают, что их личности были скомпрометированы, пока несанкционированные транзакции не появятся в выписках по кредитным картам, уведомления о сборе средств не поступят по почте, а заявки на получение кредита не будут отклонены. В одно мгновение репутация финансовых институтов или конкретных предпринимательских структур может быть скомпрометирована. Восстановление своего доброго имени и доверия клиентов, как показывает практика, может быть долгим и дорогостоящим процессом.

Чтобы предотвратить несанкционированную утечку персональных данных клиентов с серверов предпринимательских структур, занятых в сфере электронного бизнеса, а также облегчить их финансовое бремя, в мировой практике активно используются специальные программы киберстрахования. Так, например, на территории России одной из таких программ является программа компании AIG, разработчика новаторского продукта CyberEdge, который в 2013 году был признан лучшим инновационным продуктом на страховом рынке стран Ближнего Востока и Северной Африки. Благодаря грамотно выстроенному аутсорсингу с ведущими мировыми брендами в сфере кибербезопасности, объектами страхового покрытия по данной программе выступают: ответственность, связанная с использованием персональных данных или корпоративной информации (покрытие убытков страхователя, включая расходы на защиту от заявленного или фактического нарушения персональных данных или корпоративной информации); расследования со стороны регулирующих органов (покрытие крупных издержек и расходов, связанных с их проведением); услуги антикризисного PR (покрытие расходов по инструктированию и реагированию в случае утечки данных, восстановлению личной репутации, а также сопутствующих расходов на уведомления и мониторинг); электронные данные (покрытие расходов, связанных с восстановлением, повторных сбором или воссозданием информации после утечки или несанкционированного использования данных). [4]

В Беларуси вопросыстрахования киберрисков находятся на начальной стадии проработки. 2019 год стал годом активных обсуждений и дискуссий по вопросам киберстрахования. В апреле 2019 года, в рамках конференции TIBO-2019, состоялся круглый стол «Кибербезопасность», на котором экспертом компании ООО «ЮГИС групп» был

представлен доклад «Перспективы рынка киберстрахования в Республики Беларусь». В ходе презентации были озвучены результаты анализа данных по страхованию киберрисков за 2016-2018 год, полученные из отчетов организаций, занимающихся исследованиями в области кибербезопасности (KMPG, Deloitte, SANS Institute, CIRI, ISO и др.). В качестве страховых случаев, описанных в отечественной страховой практике, названы: заражение ВПО, нарушение конфиденциальности, утрата информации, физическая утрата устройств, ошибки при эксплуатации системы. [5]

Виюле 2019 года по инициативе научно-технологической ассоциации «Конфедерация Цифрового Бизнеса» на площадке Расчетного Центра Нацбанка был организована встреча-дискуссия по вопросам развития киберстрахования в Беларуси с участием представителей банковского и страхового сектора, а также компаний из смежных секторов экономики.

К настоящему времени на отечественном рынке киберстрахования рабочими страховыми продуктами, являются: *страхование банковских платежных карточекот несанкционированного списания денег со счета*, в т.ч. посредством интернет-мошенничества; *страхование риска хищения ценностей касс и банкоматов* с использованием компьютерной техники; *страхование электронных устройств и носителей информации* с возможностью покрытия расходов по восстановлению информации. Данные услуги предоставляют, в частности, ЗАСО «Промтрансинвест», ЗАСО «Белнефтестрах», СБА ЗАСО «Купала», ЗАО «СК «ЭРГО», ЗАСО «Кентавр»,ЗАСО «Imkliva Insurance»,ЗАО «СК «Белросстрах», действуя как напрямую, так и через обслуживающие страхователей банки на основании договоров поручения. Названные страховые продукты обладают высоким потенциалом капитализации, и прежде всего, страхование банковских платежных карточек, эмиссия которых в Беларуси по состоянию на 01.07.2019 составила 15 297,4 тыс. ед., включая виртуальные платежные карты. Договор страхования может оформляться сразу на несколько платежных карточек на срок от 1 месяца до 5 лет. Базовый страховой тариф устанавливается в процентах от страховой суммы (в ЗАСО «Промтрансинвест» - 0,21%) или в рублях в виде фиксированной величины за год, квартал, месяц (в ЗАСО «Купала» – 10-15 рублей в год). Страховая сумма в среднем составляет около 5000 рублей по всем сопутствующим данному виду страхования рискам.

По мнению экспертов, развитию киберстрахования в нашей стране препятствуют отсутствие достаточного объема информации для определения условий и величины страхового возмещения, а также независимых организаций-оценщиков возникающего в результате реализации киберрисков ущерба, и действующих методик по оценке страховой стоимости информации. Кроме того, предстоит трансформация сознания страхователя, повышение его цифровой грамотности и киберкультуры для полноценного формирования данного сегмента отечественного страхового рынка. Пока же в адрес страхового сообщества поступает небольшое количество реальных запросов от субъектов хозяйствования, и практически отсутствуют обращения субъектов МСП.

Перманентное стремление организаторов и участников электронных платежей технически обезопасить себя от неправомерных действий со стороны киберпреступников заставляет последних предпринимать активные попытки обойти системы защиты информации, используемые сегодня в дистанционных каналах доступа, переключиться на менее защищенные объекты и информационные системы. Если раньше кибератакам подвергались в основном крупные компании, то сегодня просматривается четкий тренд повышенного внимания киберпреступников к информации простых граждан. Причина кроется, с одной стороны, в легком доступе к персональным данным физических лиц через повсеместно используемые ими мобильные устройства, слабой осведомленности и защищенности граждан от киберугроз. С другой стороны – бурным ростом ритейла в электронной коммерции. По данным МАРТ две трети населения Беларуси являются активными интернет-пользователями, а 44% белорусов на начало 2018 года совершали покупки в интернет-магазинах. [1]

С учетом повышенного внимания государства к развитию МСП, а также активной поддержки в стране курса на цифровизацию экономки киберстрахование может оказаться важным фактором обеспечения конкурентоспособности отечественных предпринимательских структур. В этой связи требуются системные исследования методологии определения стоимости объектов страхования, исходя из природы киберрисков, а также опыта применения лучших мировых практик урегулирования убытков. Необходима также прозрачная статистика по инцидентам в стране и доработка соответствующей нормативно-правовой базы для эффективного взаимодействия с компетентными органами в ходе подготовки и вынесения судебных решений.

Таким образом, защита персональных данных и конфиденциальной информации от посягательств в интернете – залог успешного ведения бизнеса в современных условиях. Страхование киберрисков жизненно необходимо компаниям, занятым ритейлом через интернет-магазины и обслуживанием баз данных клиентов-физических лиц в процессе оказания широкого спектра услуг – профессиональных (в т.ч. юридических и бухгалтерских), финансовых, бизнес-услуг. Как правило, это компактные бизнес-структуры с небольшим запасом «финансовой прочности», репутационные потери которых могут оказаться невосполнимыми в случае реализации реальной киберугрозы. Кроме того, в развитии рынка киберстрахования должны быть заинтересованы и сами страховщики, активно осваивающие электронные продажи через удаленные каналы доступа, что автоматически увеличивает для них вероятность потерь от киберрисков.

Литература

1. Итоги 2018-го ритейл-года в Беларуси. Часть 3: онлайн-ритейл. – Режим доступа: https://belretail.by/article/itogi-go-riteyl-goda-v-belarusi-chast-onlayn-riteyl. – Дата доступа: 01.10.2019.
2. Торговый реестр Республики Беларусь: просмотр сведений в Торговом реестре Респ. Беларусь – Режимы доступа: офиц. сайт Министерства антимонопольного регулирования Респ. Беларусь https://mart.gov.by/sites/mart/home.html / Единый портал электронных услуг https://portal.gov.by/PortalGovBy. – Дата доступа: 01.10.2019.
3. Правоохранительные органы отмечают значительный рост киберпреступности в стране: Национальный правовой Интернет-портал РБ. – Режим доступа: http://www.pravo.by/novosti/novosti-pravo- by/2019/april/34341.– Дата доступа: 01.10.2019.
4. Страхование киберрисков – Страхование от компании AIG в России. – Режим доступа:https://www.aig.ru/business/products/cyber-edge – Дата доступа: 01.10.2019.
5. Дни ТИБО – 2019 в НЦЭУ: Круглый стол на тему: «Кибербезопасность». - Режим доступа:https://itexperts.by/news/doklad-g-memetova-na-tibo-2019-perspektivy-rynka-kiberstrahovanija-v-respubliki- belarus. – Дата доступа: 01.10.2019.