УДК: 368.19 **Экономические науки**

Коломасова Регина Александровна, *студентка экономического факультета ФГБОУ ВО «Национальный исследовательский Мордовский государственный университет, им. Н.П. Огарёва», г.* Саранск

МИРОВЫЕ ТЕНДЕНЦИИ СТРАХОВАНИЯ ИНФОРМАЦИОННЫХ РИСКОВ И ПРОБЛЕМЫ ЕГО ВНЕДРЕНИЯ В РОССИЙСКУЮ ПРАКТИКУ

Аннотация: В статье рассматриваются основные тенденции мирового рынка кибер-страхования, подчеркивается актуальность проблемы защиты от риска информационных преступлений. Раскрываются основные виды кибер-рисков и соответствующие им способы страховой защиты. Проводится анализ объективных ограничений адаптации исследуемого вида страхования к российским условиям; вносятся предложения по их минимизации и ликвидации.

Ключевые слова: кибер-преступность, кибер-риски, кибер-страхование, цифровые технологии, информационная безопасность.

Annotation: The article discusses the main trends of the global cyber insurance market, emphasizes the urgency of the problem of protecting against the risk of information crimes. The main types of cyber risks and the corresponding methods of insurance protection are disclosed. An analysis of the objective limitations of the adaptation of the studied type of insurance to Russian conditions is carried out; proposals are made for their minimization and liquidation.

Keywords: cybercrime, cyber risks, cyber insurance, digital technologies, information security.

Технический прогресс не стоит на месте, а применение различного рода интернет- и компьютерных технологий все плотнее входит в нашу жизнь. Такой процесс значительно упрощает проведение конкретных операций, что естественным образом экономит как временные, так и финансовые ресурсы.

Торговля ценными бумагами и криптовалютой, электронные расчеты и ведение бизнеса – все это и многое другое в период цифровых технологий становится возможным осуществлять через компьютерные гаджеты и сеть Интеренет.

Вместе с технологиями неизбежно возникают и новые виды преступлений, в частности киберпреступность, которая в том числе и в нашей стране набирает все большие обороты [4] (рисунок 1).

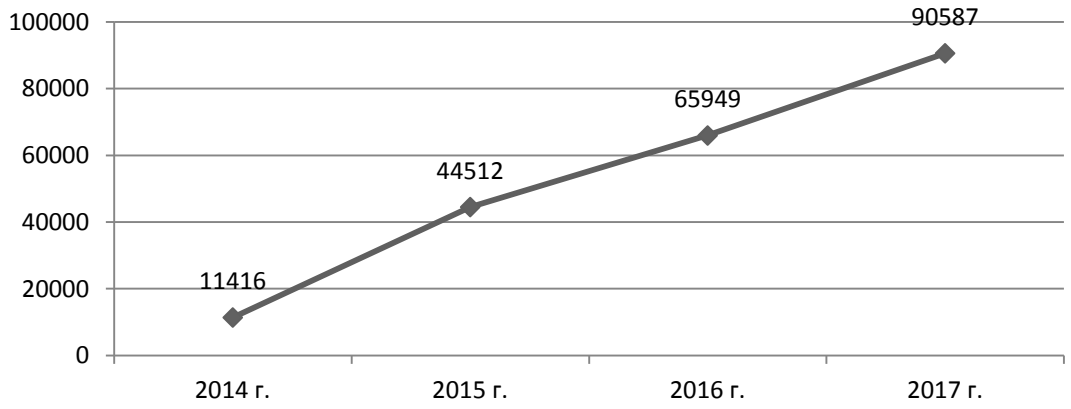

Рисунок 1. Статистика числа преступлений в сфере информационно-телекоммуникационных технологий.

Кроме того, за первое полугодие 2018 года правоохранительными органами РФ зарегистрировано 107980 преступлений, совершенных киберпреступниками. Ущерб от этих преступлений составил около 400 млрд. рублей, что на 44% больше аналогичного показателя прошлого года.

Кибер-риски вдвойне опасны тем, что они не подвластны осознанию на первый взгляд, и последствия атак на цифровые данные или системы могут проявиться лишь по прошествии определенного периода времени.

Одним из возможных методов защиты от такого вида преступлений выступает кибер-страхование, которое позволяет предприятиям вернуться функционированию, сохранить стабильность и платежеспособность, а также снизить потери в результате возникновения кибер-угроз.

Сегодня в мировой практике выделены следующие кибер-риски, которые частично или полностью могут быть застрахованы:

– риск присвоения и использования конфиденциальной информации сотрудниками компании;

– 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 обнародования служебной, коммерческой, государственной тайны;

– риск проникновения на сервер с целью распространения вируса и модификации информации или уничтожения документов и устройств их хранения;

– виртуальное вымогательство – запрос денежных средств у страхователя в обмен на обещание прекратить кибер-атаку;

– перебои и перерыв в работе сервера;

– риск утери материального носителя, содержащего конфиденциальную информацию.

Кроме того, в некоторых странах страховщики предлагают такие дополнительные услуги, как:

- возмещение расходов на расследование кибер-преступления;

- антикризисный пиар с целью восстановления репутации;

- затраты на защиту в суде и восстановление работы ИТ-систем [3, с. 77].

Основными мировыми компаниями, оказывающими услуги по страхованию от кибер-рисков являются: Lloyd’s of London, Zurich North America, AIG, Chubb. Следует отметить, что на последние две приходится 29,3% рынка и в общей сложности 544,992 тыс. долларов [8].

Базирующийся в Цюрихе Chubb выделяется тем, что это самый популярный в мире и крупнейший коммерческий поставщик страхования. В нем работают 31 000 человек во всем мире, Chubb обладает 167 миллиардами долларов активов и 36 миллиардами долларов валовых премий по состоянию на начало 2018 г. Компания предоставляет несколько различных продуктов кибер-страхования. Во-первых, продукт управления рисками предприятия (ERM) для крупных организаций; DigiTech ERM, который предлагает расширенную защиту с учетом потребностей технологических компаний, консультантов и разработчиков программного обеспечения. Integrity+ обеспечивает разрешение претензий клиентов, поставщиков и третьих лиц. ForeFront Portfolio 3.0 предназначен для частных компаний и включает в себя страхование от преступлений, похищений данных и вымогательств, а также несколько других видов страхования, в дополнение к кибер-страхованию. Наконец, chubb's Cyber Protection product охватывает частных лиц.

Типы покрытия: зависит от продукта, но может включать в себя страхование ответственности перед третьей стороной покрытия, потерю средств платежных карт, прерывания деловой активности, цифровое восстановление данных, телефонные мошенничества, вымогательства по сети, компьютерное мошенничество, мошенничество при переводе средств и многое другое.

Ограничения: для большинства классов риска минимальная сумма составляет 10 млн. долларов; максимальная – 100 млн долларов.

Способ получения услуг: агенты и брокеры.

Также известная как AIG, American International Group была основана в 1919 году в Шанхае и открыла свой первый офис в США в 1926 году. Сегодня, она осуществляет деятельность более чем в 80 странах мира, а штаб-квартира компании находится в Нью-Йорке. AIG предлагает страховые продукты как для частных лиц, так и для предприятий, а ее коммерческие направления включают в себя кибер-страхование, страхование от несчастных случаев и болезней, фронтинговые услуги, управленческую ответственность, политический риск,

профессиональную ответственность, собственность, поручительство, гарантию и другие виды страхования. В 2017 году годовая выручка страховщика составила 49,52 млрд. долларов, а общие активы - 498,3 млрд. долларов. Компания имеет почти 50 000 работников.

Базовый продукт, CyberEdge, покрывает финансовые расходы, связанные с нарушениями и управлением событиями по восстановлению данных, финансовыми расходами для третьих лиц, прерывание деятельности и кибер-вымогательство. CyberEdge Plus добавляет покрытие за физический ущерб, вызванный кибератаками, а CyberEdge PC – избыточное покрытие плюс услуги кибербезопасности, предоставляемые через партнерство с IBM.

Типы покрытия: нарушение кибер-конфиденциальности, вымогательство, прерывание деятельности бизнеса.

Ограничения: до 100 млн. долларов.

Как приобрести: заявка онлайн [7].

До недавнего времени в России рассматриваемого рынка практически не было, вернее, он был достаточно узким, а страхование, главным образом, осуществлялось указанными выше компаниями (преимущественно AIG). При чем, American International Group в РФ предоставляет все виды своих продуктов.

Кроме того компания AIG совместно Group-IB TDS (ведущая международная компания по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий) предлагает российским страхователям дополнительные услуги для разработки комплексной программы управления кибер-рисками.

Стандартный пакет включает:

1) Убытки в связи с нарушениями данных. В покрытие входит:

- убытки в результате возникновения требований против Страхователя за нарушение данных и корпоративной информации третьих лиц (коммерческие тайны, профессиональная информация, бюджеты, перечни клиентов и др.);

- убытки в результате возникновения требований против Страхователя за нарушения безопасности компьютерной системы (заражение вирусами, уничтожение, модификация или удаление информации, физическая кража или утеря аппаратного обеспечения и др.).

2) Административное расследование в отношении данных. В покрытие входят расходы Страхователя на юридическую помощь в связи с расследованием в результате нарушения законодательства или иных нормативно-правовых актов в связи с обработкой данных или корпоративной информации, за которое которые Страхователь несет гражданскую ответственность, в размере, не превышающем расходы на защиту.

3) Расходы на реагирование при нарушении данных. В покрытие входит:

- расходы на реагирование и упреждающую программно-техническую экспертизу;
- расходы на восстановление репутации страхователя и его работников;
- расходы на уведомление субъектов данных;
- расходы на мониторинг;
- расходы на восстановление электронных данных и программ.

При этом лимит составляет от 10 млн. рублей до 30 млн. рублей. Франшиза равна 1 млн. рублей, а период страхования 1 году [6].

Вернемся к отечественному рынку страхования кибер-рисков. Российские организации до настоящего момента не вполне понимали, стоит ли им тратиться на страхование от кибер-рисков и реально ли приобрести такой вид услуг как отдельный продукт. Однако, учитывая сложившуюся в нашей стране ситуацию относительно роста числа данного вида преступлений, а также суммы хищений, российским предпринимателям стало предельно ясно, что кибер-риски – основная угроза двадцать первого века; от этого можно и нужно страховаться.

Сегодня кибер-страхованием в России занимаются лишь 6-7 страховщиков, в числе которых «Ингосстрах» и компания «Страховой брокер Сбербанка», являющаяся дочерней структурой Сбербанка.

В настоящее время в "Ингосстрахе", застраховано от таких рисков порядка 15 клиентов, не считая финансовые институты.

Если посмотреть на динамику по компании «Сбербанк страхование», объем премий по киберстрахованию за II квартал 2018 года относительно I квартала вырос почти на 9%. Средняя премия по этому виду страхования в России составляет 2,5–5% от страховой суммы. Учитывая вероятность возникновения этого риска, инвестиции в такую защиту оправданны [5].

Кроме того, в октябре 2018 г. Group-IB, международная компания, специализирующаяся на предотвращении кибератак, и «АльфаСтрахование», одна из крупнейших российских страховых компаний, объявили о начале сотрудничества и запуске нового продукта АльфаCyber, позволяющего минимизировать последствия кибератак, а также обеспечить клиентам оперативную структурированную защиту от финансовых потерь и репутационного ущерба.

Почему же перечень отечественных компаний, оказывающих услуги по страхованию кибер-рисков настолько узок? Постараемся разобраться в объективных ограничениях адаптации таких страховых продуктов в России.

Во-первых, в нашей стране исследуемый рынок достаточно сильно отстает от зарубежного опыта. Акционеры считают данный сегмент слишком рисковым и, кроме того, не видят перспектив его развития в период общего экономического спада. На помощь российским страховщикам в данном случае может прийти фронтинг. Обычно такая схема производится в случае, к примеру, если компании необходимо обеспечить страховым покрытием своего клиента, выходящего на иностранный рынок. Применительно к кибер-страхованию в рамках данного механизма российским страховым компаниям можно порекомендовать удерживать минимальную долю риска у себя, а оставшуюся передавать иностранному партнеру.

Отечественный страховщик в данном случае осуществляет финансовые меры, гарантирующие управление заявляемыми прет ензиями и платежами, а зарубежный уже выполняет оценку риска и предоставляет условия страхования. Таким образом, клиенту предлагается уже проверенный и надежный страховой продукт.

Препятствиями на пути страхования кибер-рисков в нашей стране можно назвать и отсутствие опыта страховщиков в данном вопросе, а, соответственно, и их некоторую некомпетентность. При консультациях часто возникают недопонимания, которые связаны с тем, что потенциальный страхователь привлекает специалиста, ответственного за IT-технологии и безопасность, применяемая терминология которого зачастую непонятна страховщику, а значит последний не может предложить качественный и наиболее подходящий продукт той или иной системе; в свою очередь IT-специалисты не смогут оценить преимуществ конкретного вида страхования кибер-рисков относительно их повседневных задач. Соответственно не о каких преимуществах не может идти и речи, что неминуемо приведет к убыткам бизнеса и невозможности получения возмещения при возникновении страхового случая.

В настоящее время в нашей стране отсутствуют собственный подход к оценке кибер-рисков и отдельные страховые тарифы кибер-страхования, для этого практикуется обычная методика для рисковых видов страхования, что тормозит развитие данного сегмента в нашей стране.

Отечественные страховщики оценивают риски клиентов с помощью косвенных характеристик, к примеру, таких как: способы управления рисками, методы хранения данных, внедрение систем информационной безопасности, число занятых сотрудников в IT-сфере и т.п. Остается только ждать, что в перспективе сформируются более детальные методики, отвечающие на прямой вопрос по оценке кибер-рисков [2, с. 138].

Однако при разработке таких методик у российских страховых компаний возникает риск столкновения с проблемами оптимизации расходов.

Страховщикам придется рассмотреть данный вопрос с позиции применения передовых аналитических разработок. Это может быть андеррайтинг, блокчейн и т.д. Для сокращения издержек, получения конкретных положительных результатов и совершенствования рынка страхования кибер-рисков также необходимо совершенствовать виртуальное обслуживание и цифровое распределение.

Следующими ограничениями можно назвать отсутствие законодательной базы по кибер-страхованию и практики выплат. Маловероятно и то, что в России при столкновении с потерей данных пострадавший захочет разбираться с проблемой в судебном порядке. Доказать понесенный ущерб ему будет достаточно сложно, поскольку даже если это и возможно в теории, то судебная практика по таким вопросам отсутствует. Ярким примером может служить не так давно возникшая ситуация по поводу раскрытия персональных данных клиентов ВТБ и Сбербанка посредством поисковика Яндекс. Никакой информации о том, что за этим инцидентом стоят судебные разбирательства со стороны пострадавших не последовало. Наверняка за рубежом аналогичная ситуация вызвала бы огромный ажиотаж, и все необходимые меры со стороны регулятора были бы обеспечены в короткий срок.

Что касается законодательства в этой области (а точнее его совершенствования), то в рамках программы «Цифровая экономика» ко II кварталу 2020 г. в планах разработать индустриальные стандарты и другие нормативные документы для услуг по киберстрахованию; по разделу «Информационная безопасность» к 2024 г. предусмотрена разработка механизмов государственного содействия росту рынка услуг по страхованию информационных рисков [1].

Кроме того федеральный проект «Информационная безопасность» предполагает проработку возможности введения налоговых льгот при страховании кибер-рисков, в том числе отнесение страховых премий по ним на себестоимость при бухучете. Осенью 2021 года ведомствам и экспертам предстоит внести в правительство доклад на эту тему.

Еще одной проблемой является и то, большинство компаний заблуждается, будучи уверенными в том, что все принадлежащее им имущество и так находится под страховой защитой, не подозревая о том, что в 90% случаев в разделе «Исключения» указываются именно кибер-риски. Как правило, при таких обстоятельствах пристальное внимание сосредотачивается опять-таки на государственном регулировании данной сферы, на мерах которые должны существовать, но по каким-то причинам не регулируются законодательно. Безусловно, это имеет место быть, но, в первую очередь, ответственность в данном случае ложится на самих страхователей. Все дело в киберграмотности и заинтересованности в ее повышении. Как уже отмечалось выше, нашу жизнь нельзя представить без информационных технологий, которые осваиваются с раннего возраста. Однако сегодня ни ребенок, ни взрослый человек не осознают всех опасностей, с которыми они могут столкнуться в мире цифровой экономики. Недостаточно осваивать эти навыки, обучаясь по смежному профилю, необходимо уже с раннего возраста, к примеру, с уроков информатики или же элективных курсов (что активно практикуется за рубежом) прививать детям знания в области кибер-рисков и их недопущения и минимизации. Надо сказать, что первые шаги в этом направлении уже сделаны. Так зампред комитета Госдумы по образованию и науке Борис Чернышов в октябре прошедшего года предложил ввести в школах уроки кибер-безопасности в рамках курса информатики.

Таким образом, анализируя ситуацию кибер-страхования в России следует заключить, что оно находится лишь на начальной стадии своего развития, но в настоящее время вызывает все больший интерес как со стороны страховых компаний, так и со стороны потенциальных страхователей. Основные проблемы страхования кибер-рисков в нашей стране – это несовершенство законодательной базы, отсутствие понимания страхователями сути данных страховых продуктов, а также недооценка кибер-рисков, некомпетентность страховщиков и отсутствие передовых аналитических разработок и собственных подходов к разработке тарифов.

Библиографический список:

1. Программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р [Электронный ресурс]. – Режим доступа: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf .

2. Касьянова М.А. Экономические последствия киберпреступлений и страхования киберрисков // Современное состояние и перспективы развития рынка страхования. Воронеж: АМиСта. 2017. С. 137-143.

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

4. Основные статистические данные о деятельности органов прокуратуры Российской Федерации. Официальный сайт [Электронный ресурс]. – Режим доступа: http://genproc.gov.ru/stat/data/ .

5. Сбербанк Страхование. Официальный сайт [Электронный ресурс]. – Режим доступа: https://sberbankins.ru.

6. American International Group. Официальный сайт [Электронный ресурс]. – Режим доступа: https://www.aig.ru/business/products/cyber-edge#pr_cr_cr_inpagetitle_356503280 .

7. eSecurity Planet. Official site [Electronic resource]. – Access mode: https://www.esecurityplanet.com/products/top-cyber-insurance-vendors.html.

8. Insurance Information Institute. Official site [Electronic resource]. – Access mode: https://www.iii.org/table-archive/218710.