Вензель Виктория Владимировна
преподаватель
Красноярский филиал ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Красноярск, Красноярский край

СТРАХОВАНИЕ КИБЕРРИСКОВ: АКТУАЛЬНЫЕ ТРЕНДЫ И ПРОБЛЕМЫ

Аннотация*: в статье представлены основные проблемы и объективные причины необходимости в киберстраховании. На современном этапе очень часто организации сталкиваются с взломами своих информационных систем, которые содержат конфиденциальную информацию. Что влечет за собой недоверие сотрудников, клиентов и, конечно же, партнеров, не говоря уже и о других отрицательных последствиях.*

Ключевые слова*: мошенничество, риски, страхование, мошеннические атаки, последствия.*

Все чаще граждане и организации сталкиваются с мошенниками. При чем с каждым годом истории для совершения мошеннических операций становятся все более изощренными. Уже за 2024 год по данным Министерства Внутренних Дел РФ было зафиксировано 765,4 тысяч киберпреступлений, и это составляет 40% от всех противоправных деяний. Чуть больше 80% от этого количества составляют мошенничества с использованием интернета. При чем большая часть похищенных средств являются кредитные деньги [2].

По регионам также представлена характеристика по количеству преступлений. Так, в первую пятерку входят Мордовия, Марий Эл, Татарстан, Югра и Чувашия. Меньше всего киберпреступлений совершено в Дагестане, Чувашии и Туве. В 2023 году в лидерах по количеству таких преступных атак также находился Татарстан и Марий Эл. Наименьшее количество атак в 2023 году пришлось на те же регионы, что и в 2024 году [2].

С 2015 года в России начало развиваться такой способ защиты от мошенников, как киберстрахование. С тех пор потихоньку развивался. С увеличением кибератак стали и увеличиваться договоры на данный вид страхования. В 2023 году у страховых компаний, осуществляющих такой вид страхования, возросли страховые взносы почти на 80%, что говорит и об увеличении кибератак, причем, влекущих за собой большие потери сумм и информации. Проблема на территории России однозначно есть.

Аферы становятся все более продуманными, особенно на современном этапе, когда при помощи нейросетей и искусственного интеллекта можно позвонить по видеосвязи и представиться нужным человеком, сформировать шум работающих сотрудников на фоне и фон офиса компании.

Чтобы остановить рост киберпреступлений государством вводятся определенные нормы на рынок финансовых услуг [2]. Например, с 01 марта 2025 года начнет действовать возможность установления самозапрета на оформление кредитов и займов в банках и других микрофинансовых организациях.

Кроме того, разработан и уже принят Госдумой закон о защите от мошенников, который вводит «период охлаждения» при получении кредитов и займов.

И, конечно же, в ответ на это развивается и еще один сегмент страхового рынка – киберстрахование.

Актуальными трендами в страховании киберисков на данный момент являются [1].

1. Рост спроса на полисы киберстрахования.

В связи с увеличение кибератак руководители организаций осознают всю необходимость и важность защиты от таких рисков, влекущих большие убытки.

2. Расширение покрытия.

Страховыми компаниями проводится постоянное улучшение качества предоставляемых услуг. И киберстрахование не исключение. Страховщики, трезво оценивая объемы последствий кибератак, начали расширять перечень услуг, входящих в полисы такого рода. Так, например, включая не только ком-

пенсацию финансовых потерь, но и расходы на восстановление систем безопасности, на расследование инцидентов, на юридические услуги и даже восстановление имиджа за счет новой PR-программы.

3. Интеграция с искусственным интеллектом и большими данными.

Тут стоить отметить значение ИИ в данном виде страхования, как способ персонализировать услуги. На современном этапе персонализация товаров и услуг – это ключ к потребителям. И как раз ИИ помогает разрабатывать полис киберстрахования персонализированные решения и оценивать риски.

4. Киберстрахование как часть корпоративных стратегий.

У каждой организации есть риски, и каждая организация разрабатывает стратегию управления рисками. И полисы киберстрахования являются частью такой стратегии. Системы безопасности не бывают идеальными и полис снижает возможные убытки.

На каждом этапе сопровождения договора страхования, начиная от предложения условий и заканчивая ведением клиента и урегулированием страхового случая, возникают различного рода проблемы.

Рис. 1. Проблемы в страховании киберрисков

Самой главной проблемой является сложность в точной оценке риска вероятности наступления атаки, ведь как было сказано ранее, аферы с каждым разом становятся продуманнее, появляются новые виды атак. Помимо прочего организации не всегда знают сами какие у них есть уязвимые места, что тоже затрудняет оценку данного типа рисков.

К сожалению, на нашем финансовом рынке пока нет единых стандартов по определению рисков, по конкретным условиям киберстрахования. И данная проблема проявляется в сложности выбора страхового продукта клиентом, ведь у каждой страховой компании разные условия и предложения.

Следующей вытекающей проблемой является отсутствие законодательного регулирования такого страхования. В России, как и зарубежных странах, не разработаны отдельные нормативные акты по киберзащите организаций, по определению ответственных за атаки, опять же и по структуре договора и условий страхования, процедуры киберстрахования. Это создает определенные сложности страховщикам при определении объема ответственности и компенсации ущерба.

Помимо прочего такие полисы доступны не всем организациям. Стоимость достаточно высока, она складывается из неопределенности наступления атаки, из ее непредсказуемости. Именно поэтому такой полис могут позволить себе далеко не все организации.

И, конечно же, урегулирование страховых случаев. Данный этап очень осложняется необходимостью проведения тщательного расследования произошедшего, установление причин и последствий, а также оценки размера ущерба. В результате чего могут возникнуть претензии у клиентов. В таком случае с ними нужно работать и их нужно урегулировать. Данная проблема заключается в длительности такого процесса, что сказывается на имидже организаций.

Таким образом, выделив тренды и проблемы в киберстраховании, стоит отметить необходимость проработки данного вопроса всеми участниками данного процесса. Начиная от государства в части законодательного регулирования вида страхования, продолжая страховыми компаниями в части качественной разработки продукта и заканчивая самими организациями в части анализа своих систем безопасности и уязвимых мест. Работая над данными вопросами, общими усилиями возможно поднять страхование киберрисков на новый уровень, тем самым развить российский финансовый рынок.

Список литературы

1. Степанова М.Н. Обзор мировых тенденций развития киберстрахования / М.Н. Степанова, М.С. Канупа // Экономика. Информатика. – 2023. – №1 (50). – С. 122–132 [Электронный ресурс]. – Режим доступа: https://clck.ru/3GfFP4 (дата обращения: 14.02.2025).

2. Центральный Банк Российской Федерации [Электронный ресурс]. – Режим доступа: https://cbr.ru/ (дата обращения: 14.02.2025).