Национальная Банковская Премия 2021
Проект Страхового Брокера GrECo International
Страхование кибер-рисков

Актуальность проекта

В последние годы существенно возросла значимость кибер-рисков. В прессе регулярно появляются новости, связанные с кибер-атаками на крупнейшие российские банки и компании.

Данные, представленные на Всемирном Экономическом Форуме (World Economic Forum) в Докладе о глобальных рисках за 2021 год (The Global Risks Report) свидетельствуют о высоком риске кибератак, нацеленных на инфраструктуру и кражу данных или денежных средств. Данный риск входит в Топ-10 рисков по вероятности наступления, занимая 9 место в рейтинге и в Топ-10 рисков по степени воздействия, занимая 10 место.[1]

В своих действиях кибер-преступники в большинстве случаев руководствуются меркантильными интересами. Таким образом, целью хакеров являются денежные средства и данные, которые впоследствии могут быть проданы на черном рынке. Чем чувствительнее и уникальнее данные, тем больший интерес они представляет для злоумышленников. Соответственно среди компаний кибер-атакам подвергаются чаще те предприятия, которые оборачивают большие суммы и обладают большим массивом уникальной информации. В первую очередь к таким компаниям относятся финансовые институты. Именно бизнесу банков присущ оборот крупных сумм и хранение конфиденциальной информации, в том числе персональных данных. Более того, с развитием технологий объем и чувствительность хранимых данных только возрастают. Так к таким данным, которые представляют интерес для кибер-преступникам относятся:

- персональные данные (ФИО, паспортные данные, данные банковских карт, номер телефонов, адреса почты и т.п.);
- данные, связанные со сбором big data (потребительские привычки, регулярные платежи и т.п.);
- биометрические данные.

Отдельно стоит отметить биометрию, которую в отличие от любой другой информации субъект данных не сможет изменить в случае их компрометации.

Хакерская атака может оказать существенное влияние на работу банка и причинить крупные убытки, в том числе (но не ограничиваясь):

- кража хакерами денежных средств со счетов банка
- компрометация данных как (как данных третьих лиц, так и собственных данных банка)
- остановка деятельности банка в связи с кибер-инцидентом (например, все данные системы, в том числе резервные копии, зашифрованы)
- претензии третьих лиц в связи с кибер-инцидентом и компрометацией данных
- расследования со стороны регулятора(ов) в связи с кибер-инцидентом и компрометацией данных
- собственные расходы на восстановление систем и работы банка

Представляемый нами проект предлагает страховое решение для банков и иных компаний для минимизации рисков и возможных потерь, связанных с кибер-инцидентами.

Описание проекта

Договор страхования кибер-рисков предлагает комплексное страховое решение на случай кибер-инцидента. Объем покрытия договора страхования предлагает не только возмещение связанных с кибер-инцидентом потерь, но и панель консультантов, которые будут работать над восстановлением работы банка.

[1] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf The Global Risks Report, стр.12

На схеме ниже представлен объем покрытия по договору страхования кибер-рисков.

Договор страхования покрывает целиком всю Группу страхователя. Таким образом, если кибер-атака затронет одну или несколько компаний, договор страхования покроет убытки и расходы на консультантов всех обществ.

Практика показывает, что важной частью покрытия являются расходы на консультантов и кризисный менеджмент. Правильная и своевременная координация действий консультантов, как правило позволяют оперативно преодолеть кризисный период и восстановить работу банка до штатного уровня.