

Кудиши Алексей Семенович

студент

ФГОБУ ВО «Финансовый университет
при Правительстве Российской Федерации»
г. Москва

СТРАХОВАНИЕ БАНКОВСКИХ РИСКОВ В ОБЛАСТИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Аннотация: в статье проанализированы основные компьютерные угрозы, которым подвержены банки и способы переноса ущерба с помощью страхования данных рисков. Проведен сравнительный анализ страховых продуктов данного сегмента на Западе и в России. Выработаны рекомендации относительно данного страхования в России.

Ключевые слова: банки, страхование, страховые продукты, банковские риски, компьютерные риски, компьютерные преступления, облачные технологии.

Вступление

С развитием информационных технологий и диджитализации банков происходит и переход мошенничества в компьютерную сферу. Все больше банков подвергаются компьютерным и хакерским атакам, целью которых является присвоение денег банков. Риски компьютерных преступлений для банков лежат не только в несовершенстве информационных систем, но и в недобросовестном поведении сотрудников.

Даже самым крупным и, казалось бы, надежным банковским системам хакеры наносят крупный ущерб. Международная банковская система SWIFT, к которой подключены порядка 11 тыс. банков и финансовых организаций по всему миру, с начала 2016 года уже не раз подвергалась более или менее успешным атакам. К примеру, в феврале 2016 года хакеры вывели со счетов Центробанка Бангладеша \$81 миллион.

Основная часть

Потребности неизменно рождают спрос. И в отношении страхования криминальных рисков банков он возник около ста лет назад, когда в Ллойде был разработан первый полис страхования банка от ограблений и нечестности сотрудников.

На Западе уже давно признают огромное влияние кибер-преступлений на банковские институты. Там широко распространено различное страхование компьютерных рисков: от комплексного страхования операционных и кибер-рисков, до, например, полиса страхования банка от электронных и компьютерных преступлений. Как свидетельствует статистика, убытки от компьютерных преступлений ощутимо выше, чем при «традиционном» подходе. Достаточно лишь сказать, что ежедневный объем платежей, осуществляемых банками во всем мире по системам электронного перевода денежных средств, составляет миллиарды долларов.

В России страхование банковских рисков от компьютерных преступлений пока не получило широкого распространения. Несмотря на это, данный сегмент бизнеса имеет все шансы на развитие: с ростом числа хакерских атак на счета клиентов банки станут предлагать страховки электронных рисков.

Экономический урон банкам от киберпреступлений в 2015 году по данным открытых источников составил от 0,1% до 0,25% ВВП. В России за информационной безопасностью в банковской сфере следит Центральный Банк России. Он разработал рекомендации по организации управления рисками, возникающими при осуществлении кредитными организациями операций с применением систем интернет-банкинга. С этого момента многие банки озабочились своей информационной безопасностью и способами минимизацией рисков. Одним из таких способов является перенос ущерба с помощью страхования рисков компьютерного мошенничества.

В последние годы были некоторые идеи в области страхования киберрисков, но они, как правило, заканчивались комплексным полисом. А это очень дорого и для этого необходимо проводить комплексную проверку всего банка. Да

и речь в этом случае идет только о рисках самого банка, а не только о рисках клиентов и пользователей кредитных карт.

Полис BBB – это базовый продукт комплексного страхования банковских институтов, предоставляющий защиту банка от хищений и мошенничества, а также страхующий профессиональную ответственность сотрудников банк. Данный продукт достаточно редко встречается на российском страховом рынке, не более чем о 5% охвате.

Более широкое распространение получило страхование от потери доходов, возникающих из-за сбоев в Сети или атак хакеров, от кражи информации через Интернет и т. п. При этом страхуется хищение денежных средств со счетов физических и юридических лиц при работе через систему дистанционного банковского обслуживания (ДБО). Этот продукт более массовый и ориентирован на риски, связанные с корпоративными и розничными клиентами банков.

Страховой полис, защищающий от последствий утечки конфиденциальной и платежной информации третьим лицам, появился в США около 15 лет назад. Компания AIG занимается страхованием кибер-рисков на американском рынке с 1999 года. На сегодняшний день насчитывается уже более миллиона клиентов, обслуживающихся по данной программе, ежегодно собирается порядка \$90 млн премии, а годовая сумма выплат составляет около \$30 млн, что наглядно демонстрирует обоюдную выгоду данного вида страхования как для банков, так и для страхователя.

Заключение

В ближайшем будущем рынок страхования банковских рисков будет расти, можно ожидать появление аналогов западных полисов от российских страховщиков. Если учитывать то, что стандартная премия за риск составляет 10% от потерь, то продажа страхования от банковских рисков, связанных с компьютерными преступлениями может стать новым источником роста страховых премий для страховых компаний, при очевидной пользе для банков – перенос рисков на страховые компании один из способов минимизации ущерба от них, если учесть,

что обновление всех информационных систем может оказаться в среднесрочной перспективе намного дороже покупки данного страхового продукта для банка.

В России уже сегодня реальной необходимостью стало страхование эмитентов пластиковых карт от рисков подделки, утери или же противоправного использования пластиковой карты третьими лицами. Особенностью России является большой удельный вес потерь от использования поддельных карт – 60% от всех мошеннических операций (в среднем по миру эта цифра составляет 26%) (Характерно, что около 35% установленных мошеннических операций с картами было совершено непосредственно в банках. По оценкам экспертов, реальная доля таких преступлений может быть еще выше, поскольку некоторые банки предпочитают не информировать соответствующие органы о своих проблемах по обслуживанию пластиковых карт).

Отдельно выделяется розничное страхование кредитных карт от мошеннических действий. В качестве защиты от рисков, связанных с мошенническими действиями с использованием пластиковых карт, банк может выпустить и застраховать всю эмиссию карт. Страхователем в представленном случае выступает сам банк, который обязан компенсировать своим клиентам похищенные денежные средства.

Список литературы

1. Конституция Р.Ф. от 12 декабря 1993 г. // Российская газета. – 1993. – Т. 25.
2. Федеральный закон «О Центральном банке Российской Федерации (Банке России)» от 10.07.2002 – №86-ФЗ // (последняя редакция).
3. Федеральный закон «О банках и банковской деятельности» от 02.12.1990 №395–1-ФЗ // (последняя редакция).
4. Дайховский А. Как защититься от рисков при работе с ДБО // Аналитический банковский журнал. – 2014. – Т. 217. – №04.
5. Дубровина Д.С. Страхование банковских рисков / Д.С. Дубровина, Е.В. Бенько. – 2016.

6. Лебедева Н.Ю. Страхование банковских рисков в России / Н.Ю. Лебедева, Ю.А. Демидова // Теоретические и прикладные аспекты современной науки. – 2015. – С. 95.
7. Ревенков П.В. Безопасность электронного банкинга: услуга и обязанность банка / П.В. Ревенков, А.А. Бердюгин // Финансы и кредит. – 2015. – №8 (632).
8. Шепелин Г.И. Особенности электронного страхования с использованием «облачных технологий» // Ученые записки Российской академии предпринимательства. – 2015. – С. 286–296.
9. Adeleke I. Cyber risk exposure and prospects for cyber insurance / I. Adeleke, A. Ibiwoye, F. Olowokudejo // International Journal of Management and Business Research. – 2012. – Т. 1. – №4. – С. 221–230.
10. Shackelford S. J. Should your firm invest in cyber risk insurance? // Business Horizons. – 2012. – Т. 55. – №4. – С. 349–356.