БАНКИ ПОСПЕШАТ РАСКОШЕЛИТЬСЯ НА ПРОСТУЮ, ЭФФЕКТИВНУЮ И НЕ СЛИШКОМ ДОРОГУЮ СТРАХОВКУ IT-РИСКОВ

Александр ВЕЛИГУРА, председатель Комитета по информационной безопасности Ассоциации российских банков, кандидат физико-математических наук

БЕЗ ЛИШНИХ ПРЕМУДРОСТЕЙ

Ущерб банковского сообщества США от компьютерных преступлений измеряется $100 млрд ежегодно, в Европе аналогичный показатель составляет $30 млрд, «рекордным» считается компьютерное ограбление банка в Германии на $1 млрд

Страхование рисков российских банков в сфере информационной безопасности – предмет на удивление парадоксальный. Давно созрело всеобщее понимание, что подобные услуги нужны и выгодны всем – и банкам, и клиентам, и, разумеется, страховым компаниям. Тем не менее, этот вид страховых услуг в нашей стране пока прозябает в зачаточном состоянии. Что поможет сдвинуть дело с мёртвой точки?

ГРОЗНЫЙ СОБЛАЗН

По мере развития компьютерных и коммуникативных технологий информационные риски превращаются в непременный пункт договоров корпоративного страхования. Всё чаще крупные компании, наученные чужим и собственным горьким опытом, стараются подстраховаться от сбоев в работе высокотехнологичного оборудования. Страхование рисков, связанных с технологическими неполадками либо вызванных действиями злоумышленников, помогает свести к минимуму собственные потери и убытки от возмещения ущерба контрагентам и клиентам.

Очевидно, что банки находятся в «группе повышенного риска» не столько в плане возможности техногенных аварий, сколько как объект, соблазнительный для IT-криминалитета. Получив несанкционированный доступ к корпоративным информационным ресурсам других видов бизнеса, придётся ещё думать, как конвертировать их в деньги. Зато взлом информационной защиты банка, в отличие от любой другой компании, позволяет похитить чужие «живые» деньги – «товар товаров», порой весьма немалые. Соблазн для злоумышленников сильнейший!

Исходя из этого, страхование от электронных и компьютерных преступлений в кредитно-финансовой сфере представляется крайне актуальной темой. Широко известны следующие красноречивые цифры: ущерб банковского сообщества США от компьютерных преступлений измеряется $100 млрд. ежегодно. В Европе аналогичный показатель составляет $30 млрд, «рекордным» считается компьютерное ограбление банка в Германии на $1 млрд. В Великобритании средний размер хищений при проникновении в банковские компьютерные сети оценивается $500 000.

Поэтому за рубежом – в США и Европе – страхование информационных рисков является необходимым дополнением к генеральному полису страхования банков – BBB (Bankers Blanket Bond). Существуют два вида специализированных полисов: Computer Crime – от преступлений в компьютерной сфере, и Haker Insurance – соответственно, от хакеров.

ЦЕНА ПОКОЯ

У различных предложений – свои нюансы. Ведущие компании – члены лондонского страхового объединения Ллойда – разработали перечень из нескольких пунктов, которые подробно описывают каждый вид риска. Версия, предлагаемая американской компанией AIG, лидирующей на мировом рынке информационного страхования, лаконична: единственный параграф сулит покрытие убытков от несанкционированного доступа мошенников к компьютерной системе страхователя или к системе, к которой он подключен.

Собственные версии полисов предлагают и две крупных монополии – страховые компании Chubb и Zurich North America. Линейки страховых продуктов и тарифы разнообразны: например, для банков, использующих для информационной защиты продукцию определённых вендоров и разработчиков программного обеспечения, предлагаются существенные скидки.

Непременные участники рынка – специализированные консалтинговые и аудиторские фирмы. Они изучают риски, действующие в банках системы информационной защиты, и математически точно рассчитывают условия страхования. Услуги по проверке системы информационной безопасности страхователя стоят от $4 500 до $50 000.

Как правило, лимит ответственности страховщиков составляет $5–10 млн, для крупнейших банков – до $100 млн, а с учётом повышенной страховой премии – и до $200–300 млн. Страховые взносы составляют от 2 до 8% суммы покрытия. Устойчивость системы этого вида страхования обеспечивается широко развитой практикой перестраховки – страхование рисков самих страховых компаний.

Хотя полис страхования от компьютерных преступлений не является обязательным ни в США, ни в странах ЕС, трудно найти банк, который бы был не застрахован от таких рисков. Для зарубежного банкирского сообщества такое страхование – как для приличных людей привычка мыть руки перед едой. Не помоешь – за стол, конечно, пустят, но смотреть будут косо. Страхование рисков в сфере информационной защиты банков за рубежом – хорошо отработанный, повсеместно применяемый механизм, а также солидный и устойчиво развивающийся сектор рынка страховых услуг.

В США и Европе необходимым дополнением к генеральному полису страхования банков – BBB (Bankers Blanket Bond) – являются два вида специализированных полисов: Computer Crime – от преступлений в компьютерной сфере, и Haker Insurance – от хакеров

В России страхование IT-рисков банков буксует, в частности, оттого, что банки, опасаясь ущерба имиджу и массового оттока клиентов, предельно неохотно «выносят сор из избы»: предпочитают напрямую возместить ущерб потерпевшему, даже в небесспорных случаях

НЕОТРАЗИМЫЕ ЦЫПЛЯТА

Поскольку банковская система России создавалась с учётом мировой практики и действующих стандартов, то и у нас были попытки перенять лучший опыт. Были зафиксированы два всплеска деятельного интереса к тематике страхования информационных рисков кредитно-финансовых учреждений: в конце 1990-х и в середине 2000-х годов. Если не считать цепочки афер с фальшивым авизо, первыми громкими преступлениями в сфере информационной защиты банков стали хищения в 1991 году $125 500 у Внеш-экономбанка и в 1996 году $320 000 в «Автобанке».

В 1997 году была выдана первая лицензия Министерства финансов РФ на комплексное страхование финансовых институтов от преступлений и ответственности. Всероссийский научно-исследовательский институт проблем вычислительной техники и информатизации (ВНИИПВТИ) разработал предложения по развитию законодательной базы, подготовке методической документации, сбору статистических данных, расчету базовых тарифов и определению условий страхования.

В середине 2000-х годов на рынке уже присутствовали предложения ряда страховщиков для банков, в том числе в области информационной безопасности. Но не чувствовалось серьёзной заинтересованности самих страховых компаний в развитии и продвижении этого специфического продукта. Более того, хотя, как известно, начало особенно трудно, не прилагалось особых усилий для его адаптации к нашим реалиям.

Автору довелось лично посетить офис одной из крупных и серьёзных страховых компаний, чтобы ознакомиться с условиями страхования информационных рисков кредитно-финансовых учреждений. Увы! Хотя такой продукт был заявлен, сотрудники профильного отдела не нашли времени для продуктивного общения. Они сослались на «горячую пору» и «нехватку времени» – большую занятость текущими договорами.

Оказывается, страхование рисков информационной защиты банков для них было лишь одним из направлений работы, причём далеко не главным. В то время, по-видимому, из-за жаркого лета случилось массовое вылупливание цыплят. Страховщики оказались по уши погруженными в работу по договорам с птицефабриками, а на банки просто не осталось времени.

СТЕСНЯЯСЬ НАГОТЫ

Справедливости ради стоит отметить: полным страхованием либо теми или иными его видами пользуются крупные банки вроде Альфа-Банка, Внешторгбанка и Газпромбанка. Однако и по объёмам, и по значимости куда как более заметна программа страхования лиц, которой охвачены все банки, принимающие вклады физических лиц. Только это, во-первых, программа государственная, а не собственно банковская; во вторых – чрезвычайная антикризисная мера; в-третьих – защищает не столько банки, сколько интересы вкладчиков.

Почему же страхование информационных рисков банков не демонстрирует внятных и заметных успехов? Существуют некоторые препятствия. Возьмём хотя бы требование максимальной прозрачности, без которой ни для каких рисков нельзя сформулировать эффективные, приемлемые и привлекательные условия страхования. Для сравнения, при страховании автомобиля тариф устанавливается в зависимости от его стоимости, наличия и типа сигнализации, места хранения – в гараже, хранения на охраняемой стоянке или на улице, а также возраста, водительского стажа, дополнительно – с учётом статистики угонов.

Разработать подобные методики взаимно понятных и бесспорных критериев оценки информационных рисков банков непросто. Автомобилей – миллионы, разновидностей и марок не так много. Банков, напротив – всего-навсего сотни, и каждый из них очень индивидуален. Большинство банков весьма ревниво относятся к возможности полного аудита их систем информационной безопасности. Кое-кто, возможно, побаивается показаться в роли «голого короля»?

Далее, основа для оценки рисков – полная и подробная статистика случаев, которые могут квалифицироваться как страховые. Случаи IT-ограблений банков, похоже, одни из самых скрытых видов преступлений. Где можно найти

официальную статистику и в какой степени ей можно доверять? Опасаясь ущерба имиджу и массового оттока клиентов, банки предельно неохотно «выносят сор из избы», предпочитая напрямую возместить ущерб потерпевшему, даже в небесспорных случаях.

> ***В сфере информационной безопасности банков необходим следующий недорогой, доступный, эффективный страховой продукт: страхуемый риск – типичный и частый, ущерб – прямой и легко подсчитываемый, признаки страхового случая – простые и однозначные***

ПРОСТОТА ИЗНАЧАЛЬНА

Барьер между банками и страховыми компаниями должен быть разрушен с обеих сторон. Информационная безопасность, многократно более важная для банков в сравнении с реальным сектором экономики, может оказаться прорывным направлением. Начать, по моему убеждению, было бы можно не с глобальных законодательных инициатив. Равно не стоит ждать чудесного решения этого вопроса, как и всех прочих, сразу после образования отраслевых СРО – саморегулируемых организаций.

Просто в сфере информационной безопасности банков нужно попробовать сформировать простой, понятный и эффективный страховой продукт. Не замахиваться на страхование всего и сразу, но сосредоточиться на наиболее востребованных видах банковских услуг. Скажем, на использовании кредитных и дебетовых пластиковых карточек или некоторых видах дистанционного банковского обслуживания. Для начала ограничиться немногими рисками, зато характерными для самых частых и болезненных типов инцидентов.

Крайне необходим убедительный пример недорогого, доступного, эффективного страхового продукта в сфере информационной безопасности банков. Наподобие медицинской страховки выезжающих за рубеж, которой раньше пользовались единицы, теперь – все. Параметры этого предложения таковы: страхуемый риск – типичный и частый, ущерб – прямой и легко подсчитываемый, признаки страхового случая – простые и однозначные.

Интересно, что в постсоветском пространстве уже есть примеры попыток сформировать страховое предложение с указанными параметрами. Увы, пока не в России, а на Украине. Пару месяцев назад OTP Bank, украинская «дочка» одноимённого венгерского банка, совместно с французской страховой компанией Cardif предложили новый для держателей платежных карт VISA и MasterCard новый сервис. Программа «Дополнительная защита» предусматривает для клиентов страхование ряда типичных информационных рисков, связанных с использованием эмитированных банком карт.

* * *

На аналогичном российском примере, ставшем массовой практикой, страховщики смогут убедиться: страхование банков от высокотехнологичных преступлений в нашей стране становится не менее выгодным видом бизнеса, чем за рубежом. Банки в свою очередь увидят: наличие «IT-страховки» – яркий плюс их имиджу. Страховой полис по информационным рискам может стать не менее эффективным средством привлечения клиентов, чем сейчас, – значок участия в государственной системе страхования вкладов.

Публикацию подготовила Александра Лосева