

банк

Риск, подстерегающий в сети

страхование

Российские банки пока не испытывают потребности страховать риски интернет-банкинга. Они объясняют это тем, что риски по сравнению со страховой премией, которую надо заплатить за страховку, не так уж велики. Страховщики же утверждают, что банки просто боятся раскрывать случаи мошенничества в этой сфере. В отсутствие спроса и предложение развито очень слабо. Но варианты застраховать риски интернет-банкинга все же есть.

Мошенничество в интернете — один из самых быстроразвивающихся видов обмана во всем мире, и в России в том числе. По данным исследовательской компании Datamonitor, в 2003 году мировой экономический ущерб от хакерских атак — явных и скрытых, а также от последствий распространения вирусов и червей превысил \$132 млрд, в то время как в 2002 году этот ущерб составил \$48,5 млрд. По прогнозам специалистов, в 2004 году ущерб, нанесенный через интернет, может достигнуть 155,5 млрд. Более 30% этих потерь приходится на операции интернет-банкинга.

Потери от хакерских атак в России не оценены. По словам директора Центра исследования компьютерной преступности Владимира Голубева, в России рост числа правонарушений в сфере компьютерной информации идет не менее быстрыми темпами, чем процесс компьютеризации. «За последний год количество зарегистрированных причинений ущерба путем обмана или злоупотребления доверием, совершенных с использованием компьютерной информации, в России удвоилось. Но надо иметь в виду, что мировая практика такова, что только 12% из общего числа киберпреступлений становятся известными общественности и доходят до правоохранительных органов. В России этот процент и того меньше», — говорит Владимир Голубев.

Полис от хакера

Впрочем, от мошенников в интернете можно застраховаться. По словам страховщиков, если у банка появится желание застраховать риски интернет-банкинга, то их можно включить в комплексное страхование от-

ветственности банков — полис BVB (Bankers Blanket Bond). «Основной риск, который покрывает BVB, — мошенничество сотрудников, в том числе с использованием интернет-технологий. Это ключевой риск, и на него приходится самая большая часть убытка. Также этот полис покрывает противоправные действия третьих лиц в отношении банка или его клиентов. В первую очередь это компьютерные преступления, мошеннический перевод денег по электронным инструкциям. Этот риск как раз один из основных и в интернет-банкинге», — подчеркивает начальник управления страхования финансовых институтов компании «Ингосстрах» Олег Кудрявцев.

Полисы страхования BVB есть в России у нескольких десятков банков. Наиболее полное покрытие приобретают Внешторгбанк, Московский международный банк, Газпромбанк, Альфа-банк, Внешэкономбанк. Возможно оформить полисы BVB у российских банков появилась еще в середине 90-х годов. Однако договоров по покупке таких полисов было заключено считанное количество, несмотря на то что были задействованы серьезные механизмы перестрахования, а сами договоры были абсолютно лишены налета «схемности».

Глава брокерской компании «АФМ страховые консультанты и брокеры» Владимир Бирюков утверждает, что российские страховые компании предлагают включать риски интернет-банкинга в полис BVB от нехватки спроса. «На Западе риски интернет-банкинга покрываются совершенно отдельным полисом, который называется cyber или hacker insurance. Этот вид

страхования покрывает все, что связано с интернет-приложениями. У нас же происходит подмена, и интернет-преступления страхуются в рамках BVB. Суть подмены в том, что основной риск, который покрывает BVB, — это мошенничество сотрудников, то есть преступления изнутри. А при интернет-банкинге наиболее опасно именно внешнее вторжение. У нас был случай, когда один из российских банков хотел приобрести полис cyber insurance, но никто не взялся за такое страхование. Наши страховые компании испытывают большое недоверие и сомнение. Если и берутся за такое страхование, то предлагают усеченные лимиты, например страхуют только трансакции до \$100. Как правило, страхователям такие услуги не подходят», — рассказывает Владимир Бирюков.

Впрочем, Олег Кудрявцев утверждает, что полисы hacker и cyber insurance на Западе покрывают в первую очередь специфические риски интернета, например всю связанную с интернетом ответственность: нарушения законодательства в области интеллектуальной собственности или рекламы. «И лишь во вторую очередь покрываются риски компьютерных преступлений и DDOS-атак, когда злоумышленники ломают систему, крадут деньги или пытаются «повесить» сервер, забрасывая его большим количеством ложных сообщений, с которыми сервер не справляется. К банковским процессам это имеет весьма опосредованное отношение», — считает Олег Кудрявцев.

По его словам, и сами банки предпочитают включать риски интернет-банкинга в полис BVB, а не покупать от-

дельный. «Если у вас уже есть BVB, то включить в него дополнительный риск гораздо проще и дешевле, чем покупать новый продукт», — говорит Олег Кудрявцев. Теоретически покрытие риска компьютерных преступлений можно купить отдельно от BVB, но часто происходит наоборот — его покупают «в довесок» к основному полису.

Цена безопасности

По словам начальника отдела страхования финансовых рисков компании «Прогресс-Гарант» Павла Круглякова, комплексная защита — довольно дорогой продукт и обходится банку в \$0,3–1,5 млн. «Приобретению полиса предшествует достаточно дорогая процедура оценки и анализа систем безопасности и рискозащищенности банка. Эти затраты, как правило, включаются в страховую премию. По результатам проверки банку представляют комплекс мер по устранению выявленных недостатков и подбирают оптимальные условия страхования и объемы покрытия. Лимиты ответственности по российским банкам колеблются в пределах от \$5 млн до \$25 млн и выбираются, исходя из анализа деятельности банка и его предпочтений», — отмечает Павел Кругляков.

Впрочем, есть и третий вариант страхования рисков интернет-банкинга. Как рассказал руководитель управления по реализации специальных проектов группы «АльфаСтрахование» Андрей Рассветаев, основной продукт, покрывающий риски интернет-банкинга, — это страхование банков от электронных и компьютерных преступлений (Computer Crime Insurance). «Этим видом страхования возмещаются не

только убытки, причиненные банку, но и вред, причиненный третьим лицам, в том числе клиентам банка. Этот полис может покрыть ущерб, причиненный в результате электронных переводов денежных средств, когда во время пере-сылки электронных данных в них несанкционированно были внесены изменения. Также может быть застраховано причинение убытков вследствие несанкционированного входа как непосредственно в компьютерную систему банка, так и через системы сервисных и процессинговых компаний — партнеров банка. Еще можно застраховать ущерб, нанесенный вирусами, порчу электронных данных в системах банка и сервисной компании», — рассказывает Андрей Рассветаев. — Computer Crime — это лишь небольшая часть программы страхования банков, которая включает также полис комплексного страхования банков (BVB), страхование ответственности финансовых институтов, а также еще целый ряд страховых продуктов. Далеко не каждый российский банк может похвастаться наличием стандартного имущественного полиса, а уж полисы BVB и Computer Crime имеют вообще единицы».

Край непуганых банкиров

По мнению страховщиков, низкий спрос на страхование компьютерных и интернет-рисков объясняется тем, что услуга не развита в достаточной мере — не было, например, ни одного громкого случая мошенничества в этой сфере. Кроме того, банки не готовы платить значительные страховые премии, не видя реальной угрозы. «Допустим, преступнику удалось добраться до чужого интернет-счета и снять с него определенную сумму. Если это стало известно службе безопасности банка, то есть вероятность, что банкиры, заботясь о репутации своей кредитной организации, просто пополнят «недостачу» на вкладе этого гражданина. Одновременно начнется расследование. Но банку не очень выгодно, чтобы общественность узнала о том, что его система интернет-банкинга

взломали. Это может отпугнуть клиентов, как имеющих, так и потенциальных. В России это особенно актуально. Интернет-банкинг, как и другие интернет-услуги, только развивается. Любая негативная информация становится дополнительным препятствием на пути его развития», — говорит директор по страхованию «Межрегионального страхового соглашения» Борис Шмигирилов.

По мнению Андрея Рассветаева из «АльфаСтрахования», российские банки в своей массе предпочитают нести подобные риски самостоятельно, потому что стремятся сэкономить на страховых премиях (десять тысяч долларов в год), считая риск незначительным. Кроме того, они не желают знакомить страховщика с информацией о своей процессинговой системе и финансовых операциях из опасения утечки информации к конкурентам, а также выявления низкой защищенности своих систем.

По словам Павла Круглякова из компании «Прогресс-Гарант», страхование таких рисков в России осложнено еще несовершенством законодательной базы. «Сложно не застраховать банк от такого рода рисков, а обосновать факт наступления страхового случая в соответствии с действующим законодательством. А это необходимо страховщику, чтобы иметь возможность произвести выплату страхового возмещения», — объясняет он. Кроме того, услуги интернет-банкинга в России начали предоставляться банками для широкого круга потребителей лишь пару лет назад. На сегодня объем таких операций у российских банков еще очень мал, соответственно, достаточно редки случаи мошенничества.

Впрочем, по прогнозам страховщиков, лет через пять большинство российских банков будут иметь полис BVB. А те банки, которые активно займутся развитием дистанционного обслуживания, обязательно будут покупать «в довесок» полис страхования рисков интернет-банкинга: мировой опыт показывает, что рост мошенничества в этой сфере выльдится просто угрожающе.

ВАРВАРА ИНОЗЕМЦЕВА

прямая речь

Вы риски интернет-банкинга страхуете?

Владимир Смирнов, Заместитель председателя правления АКБ «Союз»:

— Наша система интернет-банкинга имеет необходимые степени защиты для безопасного проведения операций по счетам клиентов. Банк гарантирует сохранение полной конфиденциальности и неразглашение информации о счетах клиентов. Для обеспечения безопасности системы в ней применены технологии, обеспечивающие шифрование передаваемой информации и электронную подпись платежных документов. Средства шифрования и электронной подписи имеют сертификат ФАПСИ. Так что дополнительно страховать риски при работе в системе нет необходимости.

Валерий Кардашов, Директор центра развития розничных продуктов и маркетинга ОАО «Импэксбанк»:

— На мой взгляд, страхование рисков систем интернет-банкинга необходимо. Но на сегодняшний день застрахованы единичные такие системы. Причина этого, как мне кажется, в отсутствии достаточной законодательной базы и нарабатанной практики. В частности, не всегда очевидно, как определить и подтвердить наступление страхового случая.

Елена Корнева, Аналитик АКБ «Автобанк-НИКойл»:

— Мы риски интернет-банкинга не страхуем. Программное обес-

печение систем «Интернет-сервис-банк» для физических и «Банк-клиент» для юридических лиц надежно защищено от мошенничества. Эти системы сертифицированы ФСБ, что является хорошей гарантией конфиденциальности электронной подписи и документооборота. Мы первыми среди российских банков, еще в 1998 году, предложили частным клиентам банковские услуги по интернету. За это время не было ни одного случая несанкционированного доступа к клиентским счетам.

Дмитрий Самошников, Специалист отдела систем доставки банка «Первое ОВК» (группа «Росбанк»):

— Банк не занимается страхованием рисков по интернет-банкингу. Считаем, что на данном этапе в этом нет необходимости.

Виталий Воробьев, Заместитель директора департамента розничного бизнеса Банка Москвы:

— Операции интернет-банкинга мы не страхуем. Страхуют, как правило, то, что болит. В данном случае системы абсолютно безопасны. Мы используем либо систему разовых паролей, подобрав которые невозможно, либо систему ключа в виде дискеты. Не зная, как ею пользоваться, получить доступ к счету невозможно. Поэтому страховать тут нечего. Я за свою практику ни разу не встречал случаев мошенничества в интернет-банкинге.

Какие риски интернет-банкинга страхуют

- Несанкционированный ввод информации непосредственно в компьютерную сеть финансовой организации или злоумышленное изменение финансовой информации с целью перечисления средств со счетов данной финансовой организации;
- признание финансовой организации ответственной за убытки клиента вследствие несанкционированного ввода или изменения информации в системе организации, когда выполнялось корреспондентское обслуживание клиента;
- злоумышленное уничтожение или хищение электронных данных или информации в момент хранения в компьютерной системе финансовой организации или в момент передачи по компьютерным сетям;
- действие компьютерного вируса, ставшее причиной уничтожения электронных данных и/или ошибочного перечисления средств финансовой организацией.

NISSAN PRIMERA ВНУТРЕННЕЕ ПРЕОБРАЖЕНИЕ

Nissan Primera – от \$ 22 200

- Новый интерьер
- Цветная камера заднего вида
- Круиз-контроль и управление магнитолой на руле
- Система Fine-vision

ПРЕВОСХОДЯ_окидания

SHIFT_expectations

ОФИЦИАЛЬНЫЕ ДИЛЕРЫ В РОССИИ. Москва: АВТО-KEY (095) 737-5400; АВТОПЛАНЕТА (095) 105-5510; АВТОЦЕНТР НА ТАГАНКЕ (095) 797-6060; АВТОЦЕНТР НАХИМСКО-ВСК (095) 129-2907; АВТОЦЕНТР НИССАН НА ВОЛКОВСКОЙ (095) 786-2503; АВТОЦЕНТР ОБОД (095) 787-5533; BENSER (095) 788-2050; ГРУППА NATU TWOX (095) 784-6410; MAJOR AUTO (095) 730-0073; НИССАН В КРЫЛАТКОМ (095) 506-9737; АВТОЦЕНТР КУСНЕВО (095) 333-4033; ОЧАКОВО МОТОРС (095) 238-8889; ЭЛЬБА (095) 210-8330; ЮНИОН МОТОРС (095) 813-2525; Санкт-Петербург: АВТОДИМ РОССИАН (812) 325-5585; АВТО-ПРОДВИС (812) 102-4282; АУДИО АВТО (812) 320-1847; Екатеринбург: АВТОСАН (3432) 12-8615; ЛУКОЙЛ МОТОРС (3432) 10-0100; Казань: АМО (8432) 65-0065; Краснодар: МОТОРС (8612) 23-9450; Нижний Новгород: НИКОПРОД (8312) 75-9911; Пермь: УРАЛПАТОМПОРТ (3422) 65-7386; Петрозаводск: НИССАН-СТК (8142) 79-7010; Ростов-на-Дону: ОРЕИТА (8632) 32-7815; Самара: САМАРСКИЕ АВТОМОБИЛИ (8482) 57-1690; Уфа: КАПИЛА (3472) 25-4915.

www.nissan.ru

ЖИЗНЬ ИДЕТ сама по себе

пока БАНК незаметно РАБОТАЕТ ДЛЯ ВАС

РосЕвроБанк

ВЗАИМНЫЙ УСПЕХ

Тел.: (095) 938-3131
www.rosevrobank.ru