Кузин М. В.
Московский инженерно-физический институт (государственный университет)

ПРОБЛЕМА ОЦЕНКИ РИСКОВ, СВЯЗАННЫХ С МОШЕННИЧЕСТВОМ, В ПЛАТЕЖНОЙ СИСТЕМЕ БАНКОВСКИХ КАРТ

Рынок банковских карт в мире и в России развивается достаточно интенсивно, при этом растут потери от проведения мошеннических операций. В статье рассматривается проблематика рисков, связанных с мошенничеством, в платежной системе банковских карт.

1. Банковские карты в мире и в России

Банковские карты являются видом платежных карт как *инструмент* безналичных расчетов, *предназначенный для совершения физическими лицами*, в том числе уполномоченными юридическими лицами (держатели), *операций с денежными средствами*, находящимися у эмитента, в соответствии с законодательством Российской Федерации и договором с эмитентом [1].

Шесть крупнейших мировых платежных систем (Visa International, MasterCard Worldwide, American Express, Diners Club, Discover, JCB) в 2006 году осуществили 71,18 млрд. транзакций, что превышает аналогичный показатель 2005 года на 14,3%. В 2007 году доля торговых транзакций составила 64,46 млрд., а оборот — $4,341 трлн. [2].

Платежная система (ПС) представляет собой ассоциацию банков, называемых банками-участниками этой платежной системы, подчиняющихся единым правилам, называемым правилами ПС. Указанные шесть ПС являются международными платежными системами (МПС). Банк, присоединяясь к ассоциации, тем самым подтверждает свою готовность следовать установленным правилам. Эти правила определяют технические, юридические, организационные и финансовые аспекты функционирования банка в системе безналичных расчетов.

По данным ЦБ РФ на 1 января 2008 года российские банки эмитировали 103 496 582 платежные карты. Это на 28,7 млн. карт, или на 38,4%, больше, чем на 1 января 2007 года [3].

Наиболее крупным эмиссионным центром остается Москва и Московская область. Банки этого региона эмитировали в 2007 году 48 591 272 карты, что составляет 46,9% всей эмиссии в стране. На втором месте находится Санкт-Петербург — 4 862 659 карты, третье место занимает Свердловская область — 3 235 026 карты. Таким образом, на долю указанных трех регионов приходится 54,8% всей эмиссии банковских карт, что свидетельствует о сильной неравномерности распределения эмиссии по регионам.

В 2007 году российские держатели банковских карт совершили на территории РФ и за рубежом 1 641,09 млн. транзакций, или на 35,7% больше, чем в 2006 году. Характер развития российского рынка относится к экстенсивному, поскольку темпы прироста эмиссии выше темпов прироста транзакций. Экстенсивный характер развития бизнеса является свидетельством его низкой эффективности: рост оборотов происходит за счет увеличения численности продуктов, а не за счет отдачи от их использования.

В 2007 году с помощью одной банковской карты совершалось в среднем 15,9 транзакций. В 2006 году этот показатель был равен 16,2, что свидетельствует о наличии тенденции снижения средней отдачи от одной эмитированной банковской карты для эмитента. Всего за 2007 год российские держатели банковских карт совершили транзакций на общую сумму 6 459,44 млрд. руб., или на 45,7% больше, чем в 2006 году. Средняя величина одной транзакции в 2007 году составила 3 936 руб., в 2006 году эта величина была равна 3 666 руб. С учетом высокого роста цен прирост оборота примерно соответствует приросту эмиссии. Подавляющее большинство транзакций относилось к получению наличных денежных средств, и лишь 656 962,4 млн. руб., или 10,17%, пришлись на платежные транзакции. Аналогичный показатель в 2006 году равнялся 9,03%. Таким образом, зарплатная модель бизнеса банковских карт остается доминирующей.

2. Проблемы обеспечения безопасности

Положением Банка России № 266-П определяется, что эмиссия банковских карт, эквайринг платежных карт, а также распространение платежных карт осуществляются кредитными организациями на основании внутрибанковских правил, разработанных кредитной организацией в соответствии с законодательством РФ, нормативными актами Банка России, и правилами участников расчетов, содержащими их права, обязанности и порядок проведения расчетов между ними. Внутрибанковские правила, помимо прочего, должны содержать систему управления рисками при осуществлении операций с использованием платежных карт, включая порядок оценки кредитного риска [1].

По определению банковская карта является инструментом для совершения безналичных операций со счетом клиента в банке-эмитенте. С точки зрения обеспечения безопасности данный инструмент:

· может быть скомпрометирован и использован злоумышленником для несанкционированного доступа к счету владельца инструмента;

· может быть использован ненадлежащим образом самим клиентом.

Федеральный закон № 184-ФЗ «О техническом регулировании» устанавливает определение риска [4]. ***Риск*** — *вероятность причинения вреда* жизни или здоровью граждан, *имуществу* физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений *с учетом тяжести этого вреда*. При этом *безопасность* продукции, процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации есть *состояние, при котором отсутствует недопустимый риск*, связанный с причинением вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений.

Банк как кредитная организация ставит основной целью своей деятельности извлечение прибыли [5]. Риски для банка связаны с причинением вреда имуществу, потому для достижения обозначенной цели следует учитывать существующие риски.

3. Требования к менеджменту риска

По определению стандарта ГОСТ Р 51897-2002 «Менеджмент риска. Термины и определения» оценка риска — это общий процесс анализа риска и оценивания риска [6]. Анализ риска представляет собой систематическое использование информации для определения источников и количественной оценки риска, оценивание риска — процесс сравнения количественно оцененного риска с заданными критериями риска для определения значимости риска. Количественная оценка риска есть процесс присвоения значений вероятности и последствий риска. Управление риском — действия, осуществляемые для выполнения решений в рамках менеджмента риска.

К системам менеджмента информационной безопасности применимы требования ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» [7]. Система менеджмента информационной безопасности — часть общей системы менеджмента, основанная на использовании методов оценки бизнес рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности.

Письмо Банка России № 76-Т «Об организации управления операционным риском в кредитных организациях» содержит рекомендации по управлению операционным риском в кредитных организациях [8]. Операционный риск — риск возникновения убытков в результате несоответствия характеру и масштабам деятельности кредитной организации и (или) требованиям действующего законодательства внутренних порядков и процедур проведения банковских операций и других сделок, их нарушения служащими кредитной организации и (или) иными лицами (вследствие непреднамеренных или умышленных действий или бездействия), несоразмерности (недостаточности) функциональных возможностей (характеристик) применяемых кредитной организацией информационных,

технологических и других систем и (или) их отказов (нарушений функционирования), а также в результате воздействия внешних событий. Из данного определения следует, что риск информационной безопасности для банка может быть отнесён к операционному.

На основе приведенных терминов и определений можно сделать вывод, что в действующей нормативной базе РФ присутствует осознание проблематики рисков. Однако данные *нормативные документы не дают метрики оценки рисков*, что является серьезной проблемой. Следует отметить, что в настоящее время Стандарт Банка России СТО БР ИББС-1.2-2007 *определяет только качественную метрику оценки риска* [9]. При отсутствии обязательных требований к метрикам их оценки метрики могут быть выбраны самим банком.

Следует отметить, что существуют и количественные методики оценки рисков, в частности, методика Французской банковской комиссии. Однако такие методики не являются общедоступными.

4. Мошенничество с банковскими картами

Мошеннической операции дадим следующее определение. ***Мошенническая операция с точки зрения платежной системы*** — это операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем [10, 11].

Классификация видов мошенничества:

- утерянные и украденные карты (Lost and Stolen Cards);
- неполученные карты (Never-Received-Issue - NRI);
- поддельные карты(Counterfeit Cards);
- карта не присутствует (Card Not Present);
- несанкционированное использование персональных данных держателя карты и информации по счету (Card ID theft - Application Fraud, Account Take-over);
- другие виды мошенничества (miscellaneous).

Основными способами компрометации банковской карты (данных магнитной полосы, реквизитов, ПИН-кода) являются:

- скимминг — несанкционированное считывание и сохранение данных с магнитной полосы карты;
- фишинг — получение у держателя карты информации о реквизитах карты и/или ПИН-коде путем обмана (рассылка электронных писем, ссылки на мошеннические сайты и т. д.);
- установка специальных технических средств на терминальные устройства или поблизости от них с целью фиксирования вводимого держателем карты ПИН-кода;
- подглядывание реквизитов карты и/или ПИН-кода злоумышленником;
- ненадлежащие хранение и обработка информации по транзакциям в нарушении установленных правил МПС, стандарта PCI DSS (Payment Card Industry Data Security Standard);
- разглашение информации со стороны работников банка.

Следует обратить внимание на то, что в соответствии со статьей 159 Уголовного Кодекса Российской Федерации *мошенничество есть хищение* чужого имущества или приобретение права на чужое имущество *путем обмана или злоупотребления доверием* [12]. Если даже несанкционированная операция с использованием банковской карты является неуспешной, то с точки зрения УК можно говорить о покушении на мошенничество.

По данным исследования The Privacy Rights Clearinghouse в ноябре 2007 года среди десяти наиболее крупных взломов АС по числу похищенных уникальных единиц данных первые две позиции относятся к банковским картам [13]. В январе 2007 было похищено в результате атаки *45,7 млн. записей* в TJX Companies, относящихся к данным платежных карт или их реквизитам. Ранее аналогичные данные были скомпрометированы при взломе CardSystems в июне 2005 — *40 млн. записей*.

В 2006 году потери российских банков в ПС Visa составили $3 641 740, MasterCard — $1 658 830. Таким образом, объем мошенничества вырос почти на 57% по обеим указанным ПС, при

этом объем операций по банковским картам за тот же период вырос лишь на 45,7%. Увеличение объемов мошеннических операций опережает рост объемов операций по банковским картам в России.

За 2007 год мировые потери от мошенничества в ПС MasterCard составили $2 129 318 087, в ПС Visa – $ 3 455 622 938. По оценкам агентства Frost&Sullivan потери от мошенничества с банковскими картами к 2009 году могут достигнуть $15,5 млрд. Кроме того, по оценкам Visa, $100 прямых потерь в результате мошенничества влекут $200 дополнительных косвенных потерь (запросы документов, претензионная работа, расходы на сотрудников, программное обеспечение и др.) [11].

Следует отметить, что держатели карт часто пренебрегают правилами безопасного использования банковских карт. По данным исследования, проведенного банком Abbey National, 55% опрошенных держателей карт в Англии (22 млн. чел) в недавнем прошлом забывали свои ПИН-коды. Более 39% (16 млн.) признались, что хранят ПИН-коды записанными на бумаге [14]. Агентство НАФИ свидетельствует о том, что в России 11,8% держателей хранят ПИН-код вместе с картой, 19,8% когда-либо теряли карту [15].

Постоянный рост числа операций по банковским картам сопровождается также увеличением объемов мошеннических операций и возрастанием финансовых потерь (операционный риск). Это обуславливает необходимость применения комплексного подхода к обеспечению безопасности платежной системы банковских карт для защиты от мошенничества. Риски банка могут также быть связаны с техническими сбоями в платежной системе, но отсутствие статистики по таким инцидентам позволяет говорить о меньшей значимости проблемы доступности по сравнению с мошенничеством.

В рассматриваемой области оценка рисков может быть осуществлена количественно, поскольку мошенничество всегда связано с несанкционированными операциями по банковскому счету с использованием банковской карты как инструмента доступа к нему. При этом в настоящее время *общепринятой российской количественной методики оценки рисков в ПС банка, связанных с мошенничеством, не существует*.

Для противодействия мошенничеству недостаточно применить хорошее технологическое решение, необходимо соответствующим образом организовать и скоординировать работу МПС, банков, правоохранительных органов, повысить уровень осведомленности держателей карт о различных видах мошенничества. Банк со своей стороны должен руководствоваться следующими базовыми принципами:

- наличие политики обеспечения информационной безопасности и четко сформулированной стратегии в области управления рисками в ПС;
- наличие команды квалифицированных специалистов для расследования и пресечения мошенничества;
- применение современных технологических решений.

5. Обработка риска и мониторинг

Обработка риска включает в себя проведение мероприятий по его предотвращению, снижению, переносу или принятию.

1. *Соблюдение обязательных требований*. Необходимо руководствоваться обязательными требованиями и рекомендациями МПС, международных и российских стандартов, нормативных документов Банка России для обеспечения информационной безопасности ПС.

2. *Страхование рисков*. Все большее распространение получает в России практика переноса рисков ПС на страховые компании. Необходимо рассмотреть имеющиеся возможности по страхованию и использовать эту возможность совместно с другими принимаемыми мерами.

3. *Претензионная работа*. Качественное проведение претензионной работы позволит уменьшить суммы от мошенничества, относимые на убытки банка, клиентов или страховые компании.

4. *Мониторинг*. Своевременное выявление мошенничества и принятие адекватных и эффективных мер на основе системы мониторинга в ПС должно являться инструментом управления рисками в ПС.

Мошенничество с банковскими картами приводит к финансовым потерям и снижению доверия со стороны клиентов к данному банковскому продукту, поэтому важно осознать актуальность мер противодействия и разработать комплексный подход к решению проблемы для минимизации рисков. Раннее обнаружение мошенничества и принятие адекватных и эффективных мер являются необходимыми условиями обеспечения безопасности платежной системы банковских карт и должны проводиться в рамках мероприятий по управлению операционным риском в банке.

Мониторинг транзакций по банковским картам должен обеспечивать анализ всех авторизационных и клиринговых операций по банковским картам в платежной системе и принятие решений по подозрительным с точки зрения мошенничества операциям с целью уменьшения рисков.

Система мониторинга транзакций является инструментом уменьшения рисков, связанных с проведением мошеннических операций по банковским картам, и должна быть составной частью комплексного подхода к обеспечению безопасности платежной системы банковских карт банка.

Выбор той или иной системы мониторинга должен основываться на анализе существующих рисков. Система должна быть управляемой и эффективной с целью минимизирования финансовых потерь банка и держателей карт, недовольства клиентов и повышения доверия к банку.

6. Количественная оценка риска от мошенничества

Количественная оценка рисков основывается на следующих положениях.

1. Имеется БД совершенных мошеннических операций — как удачных, так и пресеченных, как с наличием ущерба, так и без такового.

2. Имеются данные по всем операциям со всеми банковскими картами банка.

3. По каждой карте банка имеются следующие данные: история всех операций; история движения средств по счету карты; история изменений статуса карты; параметры ограничения операций по карте (например, лимиты) и история их изменений; дополнительные признаки счета — VIP/(не VIP) клиент, зарплатная/(не зарплатная) карта.

4. Нет никаких специальных данных по уровню осведомленности держателя карты в вопросах информационной безопасности и соблюдения рекомендация по безопасному использованию карты.

5. Расчет рисков ведется с точки зрения возможности их уменьшения путем применения систем мониторинга транзакций.

При этом заданы следующие *исходные параметры*:

1) S_{adm} — годовой уровень допустимого риска по всем категориям мошенничества (руб.).

2) C_{sec} — годовая величина затрачиваемых средств на обеспечение безопасности в части борьбы с мошенничеством, в т. ч. страхование рисков, система мониторинга и реагирования.

Расчет риска по украденным картам ($SFRI_{tp\text{-}LS}$). В соответствии с договором между клиентом и банком ответственность по операциям по украденной/утерянной карте клиента лежит на нем до момента уведомления банка об утере/краже. Поэтому данный риск является не банковским, а клиентским.

Расчет риска по неполученным картам ($SFRI_{tp\text{-}NRI}$). Данный риск существует для банка в том случае, если технологически предусмотрена возможность получения клиентом карты иная, чем лично в руки. Безопасность получения карты держателем обеспечивается организационными и технологическими мерами (активация карты клиентом, отсутствие денежных средств на карте до момента активации), и не относится к компетенции систем мониторинга транзакций.

Расчет риска по поддельным картам ($SFRI_{tp\text{-}C}$). Риск по поддельным картам складывается из риска по поддельной карте без знания ПИН-кода и поддельной карте с известным злоумышленнику ПИН-кодом.

В случае компрометации карты без ПИН-кода злоумышленник попытается использовать поддельную карту в торгово-сервисном предприятии (ТСП). Если же злоумышленнику известен ПИН-код, то ему нет необходимости изготавливать поддельную карту для использования ТСП —

нужно изготовить поддельную карту для банкомата, в связи с чем нет необходимости подделывать внешний вид карты.

Расчет риска по операциям с отсутствием карты ($SFRI_{tp\text{-}CNP}$). Риск зависит от вероятности компрометации реквизитов карты, необходимых для совершения мошеннической операции без присутствия карты (номер карты, срок действия, CVC2/CVV2).

Расчет риска по несанкционированному использованию персональных данных держателя карты и информации по счету ($SFRI_{tp\text{-}IDF}$). Риск складывается из риска, связанного с использованием персональных данных держателя карты или информации по его счету для открытия нового счета, и риска, связанного с захватом уже открытого счета. Данный риск можно вывести за рамки деятельности системы мониторинга транзакций.

Расчет риска по другим видам мошенничества ($SFRI_{tp\text{-}M}$). Если возникают трудности в определении категории мошенничества из вышеперечисленных, ему выставляется данная категория. Поскольку статистика по мошенническим операциям ведется самим банком, категория мошенничества может быть присвоена любая из приведенных.

Исходя из вышеизложенного суммарный риск по эмиссии, уменьшение которого необходимо осуществлять через систему мониторинга, рассчитывается следующим образом:

$$S_{total} = \sum (SFRI_{tp-C}(i) + SFRI_{tp-CNP}(i))$$

При этом общий риск по эмиссии не должен превышать установленного порога с учетом затрачиваемых средств на обеспечение информационной безопасности:

$$S_{total} \le S_{adm}, C_{sec} = const$$

Требования к рискам по категориям:

$$\sum_i SFRI_{tp-C}(i) \le S_{adm\_C}$$

$$\sum_i SFRI_{tp-CNP}(i) \le S_{adm\_CNP}$$

7. Заключение

Подводя итог, можно сделать вывод об интенсивном развитии рынка банковских карт, а вместе с ним и росте объемов потерь от проведения мошеннических операций. Мошенничество с банковскими картами может быть отнесено к операционному риску. Несмотря на наличие осознания проблематики рисков в российской нормативной базе, нет общепринятой российской методики количественной оценки риска.

Отличительной особенностью обеспечения безопасности платежной системы банковских карт с точки зрения защиты от мошенничества является принципиальная возможность количественной оценки рисков — мошенничество всегда связано с несанкционированными операциями по банковскому счету с использованием банковской карты как инструмента доступа к нему.

СПИСОК ЛИТЕРАТУРЫ:

1. Положение ЦБ РФ № 266-П от 24 декабря 2004 г. (в ред. от 21 сентября 2006 г.). Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт // «Консультант Плюс» [Электронный ресурс]: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты. http://www.consultant.ru.

2. Bank Cards Worldwide. Мировая карточная статистика // Мир Карточек. 2008. № 3. С. 20.

3. *Смородинов О.* Карточный рынок в России в цифрах // Мир Карточек. 2008. № 4. С. 16.

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ (в ред. от 1 декабря 2007 г.). О техническом регулировании // «Консультант Плюс» [Электронный ресурс]: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты. http://www.consultant.ru.

5. Федеральный закон от 2 декабря 1990 г. № 395-1 (в ред. от 3 марта 2008 г.). О банках и банковской деятельности // «Консультант Плюс» [Электронный ресурс]: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты. http://www.consultant.ru.
6. ГОСТ Р 51897-2002. Менеджмент риска. Термины и определения. Введ. 2003-01-01 // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс]: национальные стандарты. http://www.gost.ru.
7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Введ. 2008-02-01 // Федеральное агентство по техническому регулированию и метрологии [Электронный ресурс]: национальные стандарты. http://www.gost.ru.
8. Письмо ЦБ РФ от 24 мая 2005 г. № 76-Т. Об организации управления операционным риском в кредитных организациях // «Консультант Плюс» [Электронный ресурс]: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты. http://www.consultant.ru.
9. Стандарт Банка России СТО БР ИББС-1.2-2007. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2006. Введ. 2006-01-01 // ABISS [Электронный ресурс]: стандарты и рекомендации по стандартизации. http://www.abiss.ru.
10. *Кузин М.* Современное состояние обеспечения безопасности банковских карт // Безопасность информационных технологий. 2006. № 3. С. 21.
11. *Кузин М.* Карты в руки. Мониторинг транзакций для обеспечения безопасности платежной системы банковских карт банка // Information Security. 2007. № 6–1. С. 60.
12. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 8 апреля 2008 г.) // «Консультант Плюс» [Электронный ресурс]: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты. http://www.consultant.ru.
13. Nefarious Numbers // Information Security. Dec. 2007/January 2008. С. 20.
14. Британцы страдают от «перегрузки ПИН-кодами» // ПЛАС. 2007. № 6. С. 87.
15. *Алексеев С.* Штурм денежной крепости // Кредит.ru [Электронный ресурс]: банковский кредит | потребительский кредит | ипотечный кредит | автокредит | лизинг | кредитные карты. http://www.credit.ru.