На правах рукописи

Кузин Максим Витальевич

МЕТОДИКА ОЦЕНКИ РИСКОВ ЭМИТЕНТА В ПЛАТЁЖНОЙ СИСТЕМЕ БАНКОВСКИХ КАРТ С ИСПОЛЬЗОВАНИЕМ МОНИТОРИНГА ТРАНЗАКЦИЙ

Специальность: 05.13.19 – методы и системы защиты информации, информационная безопасность

Автореферат

диссертации на соискание учёной степени

кандидата технических наук

Автор:

Москва – 2009

Работа выполнена в Московском инженерно-физическом институте (государственном университете)

Научный руководитель: кандидат технических наук, доцент **Скородумов Борис Иванович**

Официальные оппоненты: доктор физико-математических наук, профессор **Крюковский Андрей Сергеевич**

кандидат технических наук **Сердюк Виктор Александрович**

Ведущая организация: **ФГОУ ВПО "Южный федеральный университет" Технологический институт**, г. Таганрог

Защита состоится 9 сентября 2009 г. в 15 часов 30 минут на заседании диссертационного совета ДМ 212.130.08 в Центре информационных технологий и систем органов исполнительной власти по адресу: 123557, Москва, Пресненский Вал, д. 19. Тел. для справок: +7 (495) 323-95-26, 324-84-98.

С диссертацией можно ознакомиться в библиотеке Московского инженерно-физического института (государственного университета).

Отзывы в двух экземплярах, заверенные печатью, просьба направлять по адресу: 115409, г. Москва, Каширское ш., д. 31, диссертационные советы МИФИ, тел. +7 (495) 323-95-26.

Автореферат разослан «____» июля 2009 г.

Учёный секретарь
диссертационного совета **Горбатов В.С.**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. В последние годы во всем мире активно развиваются платёжные системы на основе банковских карт (БК). Удобство совершения платежей с использованием БК и экономия при переходе от наличных денег к безналичным, возможность предоставлять держателям БК дополнительные сервисы – все это и многое другое обусловили стремительное развитие данного рынка. На 1 апреля 2009 года в РФ количество эмитированных БК по данным ЦБ составило 121,757 млн., что на 2,3% больше, чем в начале года, и почти в 8 раз больше, чем в начале 2003 года. Число платёжных карт в мире, выпущенных крупнейшими Международными платёжными системами (МПС), с 2005 по 2008 гг. возросло на 25% и превысило 3 млрд.

Как инструмент доступа к счёту клиента в банке-эмитенте БК может быть скомпрометирована и использована злоумышленником для несанкционированного доступа к этому счёту, т.е. проведения мошеннической операции. Общие мировые потери от мошенничества в 2007 году в МПС Visa International и MasterCard Worldwide составили более 5,58 млрд. долл. США. В РФ официально не публикуется общедоступная статистика по мошенничеству с БК в различных платёжных системах, а также статистика правоохранительных органов по соответствующим противоправным деяниям. Потери от мошенничества в российском сегменте названных МПС, вычисляемые на основе предоставляемых банками-участниками данных по определённым типам мошеннических операций, за 2007 г. превысил 9 млн. долл. США. Следует отметить, что прирост объёма мошеннических операций по указанным МПС за 2007 г. составил 66%, в то время как общий рост объёма операций по БК в РФ – всего 45,7%.

Мошенничество по БК клиентов приводит к рискам банка-эмитента, связанным с финансовыми потерями и ухудшением репутации. Поэтому банк-эмитент в своей платёжной системе банковских карт (ПСБК) должен выработать и применять специальную политику информационной безопас-

ности, реализовать мероприятия по управлению рисками, внедрять методы и средства выявления мошенничества и противодействия ему.

В соответствии с законодательной и нормативной базой РФ устанавливаются определения и требования к рискам в области информационной безопасности. Отечественные стандарты и нормативные документы ЦБ выдвигают общие требования к менеджменту рисков. Однако эти документы не дают метрики оценки рисков, что является серьезной проблемой при применении требований на практике. Следует отметить, что в настоящее время Стандарт Банка России СТО БР ИББС-1.2-2007 определяет только качественную оценку риска. При отсутствии обязательных требований к метрикам рисков банкам предлагается осуществлять их выбор самостоятельно.

Обозначенные проблемы отмечаются также Советом Безопасности РФ в основных направлениях научных исследований в области обеспечения информационной безопасности, к которым относятся:

- проблемы выявления и пресечения преступлений, совершённых с использованием информационно-телекоммуникационных систем;
- исследование проблем обеспечения информационной безопасности платёжных систем на базе интеллектуальных карт.

Одним из средств защиты ПСБК от мошенничества для банка-эмитента является система мониторинга транзакций (СМТ) по банковским картам. Под транзакцией понимается единичный факт использования БК для приобретения товаров или услуг, получения наличных денежных средств или информации по счету, следствием которого является дебетование или кредитование счета клиента. СМТ предназначена для выявления мошеннических транзакций и реагирования на них в ПСБК банка-эмитента с целью уменьшения рисков. В настоящее время отсутствуют общепринятая количественная методика оценки рисков банка-эмитента, связанных с мошенничеством, в ПСБК, и классификация СМТ, необходимая для их сравнения и обоснованного выбора банком-эмитентом.

Целью диссертационной работы является защита ПСБК банка-эмитента от мошенничества с использованием СМТ на основе разработанной методики количественной оценки рисков.

Для достижения поставленной цели в диссертационной работе решаются следующие задачи:

- исследование проблем информационной безопасности в ПСБК при проведении транзакций с использованием БК;
- формализация для банка-эмитента задачи обеспечения безопасности операций с использованием БК;
- разработка методики количественной оценки рисков в ПСБК банка-эмитента, связанных с мошенничеством;
- разработка, внедрение и эксплуатация СМТ в ПСБК банка-эмитента для выявления мошенничества и оперативного реагирования с целью уменьшения рисков.

Основными **методами исследований,** используемыми в работе, являются методы теории вероятности и математической статистики, теории множеств, объектно-ориентированного анализа. Разработка СМТ осуществлена на основе методов объектно-ориентированных проектирования и программирования.

Научная новизна работы заключается в следующем:

- показано, что мошенничество с БК относится к операционному риску, величина которого может быть оценена количественно на основе истории операций по карте;
- предложена ERD-диаграмма базы данных (БД) для регистрации всех мошеннических операций в ПСБК банка-эмитента;
- разработана методика количественной оценки рисков по категориям мошенничества на основе созданной БД мошеннических операций в ПСБК банка-эмитента.

Практическую ценность представляют разработанная, внедренная и эксплуатируемая СМТ в ПСБК банка-эмитента на основе созданной методики количественной оценки рисков, и предложенная классификация СМТ в ПСБК по ряду критериев.

На защиту выносятся следующие основные результаты работы:

1. Автором разработана классификация СМТ в ПСБК.
2. Разработанная автором методика количественной оценки рисков банка-эмитента в ПСБК позволяет принимать обоснованные решения для противодействия мошенничеству с БК.
3. Автором разработана и внедрена СМТ для выявления и противодействия мошенничеству в ПСБК, служащая для уменьшения рисков банка-эмитента, оцениваемых количественно на основе созданной методики.
4. Автором разработан учебный курс по данной тематике, позволивший внедрить в учебный процесс освещение подходов к противодействию мошенничеству с БК.

Достоверность полученных результатов основывается на формальных выводах и заключениях, практике эксплуатации разработанной СМТ в ПСБК банка Газпромбанк (Открытое Акционерное Общество).

Использование результатов исследования. Основные результаты исследования применены в разработанной и внедрённой автором СМТ, используемой в Процессинговом Центре ООО “Газкардсервис” ПСБК банка Газпромбанк (Открытое Акционерное Общество). Результаты диссертационной работы внедрены в учебный процесс на факультете "Информационная безопасность" Московского инженерно-физического института (государственного университета), в Институте Банковского Дела Ассоциации Российских Банков. Результаты работы представляют практическую ценность для обеспечения безопасности ПСБК для банков-эмитентов.

Публикации и апробация работы. По теме диссертации опубликовано 13 печатных работ, в том числе 5 научных статей (из них 3 статьи в журналах из Перечня ВАК), 7 тезисов докладов на конференциях и 1 глава в

коллективной монографии. Результаты работы докладывались на Межвузовской конференции «Инновационное предпринимательство и управление знаниями» (Москва, 2006 г.), Всероссийской научно-практической конференции «Проблемы защиты информации в системе высшей школы» (Москва, 2007 – 2008 гг.), научно-практической конференции «Информационная безопасность – Юг России» (Таганрог, 2007 г.), Международной научной конференции «Цивилизация знаний: инновационный переход к обществу высоких технологий» (Москва, 2008 г.), практической конференции «Безопасность пластиковых карт. Обнаружение и предотвращение мошенничества» (Москва, 2008 г.).

Структура и объём работы. Работа состоит из введения, пяти глав, заключения, списка литературы, включающего 206 наименований и 3 приложения. Текст диссертации изложен на 141 странице, включая 25 рисунков и 12 таблиц.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертации, выделяются и формулируются цели и задачи исследования, описывается структурно-логическая схема диссертационного исследования.

В первой главе - **“Анализ рисков эмитента в ПСБК”** - исследуются методы и пути решения поставленной научной задачи. Рассматриваются платёжные системы на основе БК, мошенничество с БК и связанные с ним риски банка-эмитента.

В соответствии с законодательством РФ БК является видом платёжных карт как инструмент безналичных расчётов, предназначенный для совершения физическими лицами, в том числе уполномоченными юридическими лицами, операций с денежными средствами, находящимися у банка-эмитента. Под риском в соответствии с Федеральным законом “О техническом регулировании” №184-ФЗ понимается вероятность причинения вреда имуществу с учётом тяжести этого вреда.

Как инструмент доступа к счёту БК может быть скомпрометирована и использована злоумышленником для несанкционированного доступа к этому счету, т.е. проведения мошеннической операции. Мошенничество в ПСБК определяется как операция с использованием БК или её реквизитов, не инициированная или не подтверждённая её держателем. В соответствии с общепринятой классификацией выделяются следующие виды мошенничества с БК: по утерянным или украденным картам, по неполученным картам, по поддельным картам, по операциям без присутствия карты, с использованием персональных данных держателя карты или информации по счёту, и иное.

Мировые потери от мошенничества в рамках крупнейших МПС Visa International и MasterCard Worldwide в 2007 году превысили 5,58 млрд. долл. США. По оценкам экспертов в 2009 году объём мошеннических операций в мире может составить 15,5 млрд. долл. США. В последнее время в мире происходят многочисленные хищения данных по БК, используемых при

проведении транзакций, что часто приводит к крупным потерям из-за последующих мошеннических операций, причём прямые потери вызывают вдвое большие косвенные затраты (например, ведение расследований и претензионной работы, внедрение методов и средств защиты).

В РФ рост объёмов публикуемых потерь от мошенничества опережает рост рынка БК. При этом статистика по мошенничеству с БК собирается платёжными системами на основе данных банков-участников, предоставляемых в рамках участия в программах по управлению рисками, и не включает все типы мошеннических операций, т.е. является неполной.

В соответствии с законодательной и нормативной базой РФ устанавливаются общие определения, требования к менеджменту риска в области информационной безопасности. Однако, проведённое автором исследование показывает, что отсутствует общепринятая, общедоступная методика количественной оценки рисков, поэтому банки вынуждены заниматься разработкой собственных методик.

Мошенничество с БК по определению относится к операционному риску. В работе показано, что этот риск может быть оценён количественно, поскольку мошенничество направлено на информационный актив (банковский счет), ценность которого имеет стоимостное выражение. Основным способом выявления мошенничества в ПСБК является применение СМТ. Автором делается вывод о том, что СМТ является инструментом уменьшения рисков, связанных с проведением мошеннических операций по БК, и должна быть составной частью комплексного подхода к обеспечению безопасности ПСБК банка-эмитента. СМТ осуществляет анализ всех транзакций с использованием БК в ПСБК и позволяет принимать решения по подозрительным на предмет мошенничества операциям для уменьшения рисков банка-эмитента.

В связи с этим ставится задача разработки методики количественной оценки рисков банка-эмитента в ПСБК и использования СМТ для уменьшения рисков банка-эмитента в соответствии с методикой.

Вторая глава – **“Задачи мониторинга транзакций в ПСБК”** – посвящена задачам мониторинга транзакций в ПСБК и обязательным требованиям к мониторингу со стороны МПС. В ней проводится анализ и сравнение наиболее известных коммерческих СМТ.

Показано, что СМТ в ПСБК является основным средством выявления мошенничества с БК. Учитывая увеличение объёма мошеннических операций, банки самостоятельно выбирают готовые СМТ, либо разрабатывают собственные. При этом отсутствует общая терминология в определении функций и характеристик таких систем, необходимая для их сравнения и выбора.

В диссертационной работе предлагается классификация СМТ в ПСБК по следующим критериям:

- скорость реагирования (реальное время, псевдо-реальное время, отложенный режим);
- тип принятия решения (автоматические, автоматизированные);
- информация, используемая при анализе (данные транзакции, история операций по карте и/или ТСП, модели поведения);
- используемый математический аппарат (простые логические проверки, статистические методы, системы с использованием интеллектуального анализа данных, системы с использованием искусственных нейронных сетей);
- тип анализируемых транзакций (эмиссионные, эквайринговые).

Анализ СМТ в ПСБК и применяемых подходов к построению таких систем позволяет сделать следующие выводы:

- доработка Фронтальной Системы (ФС) Процессингового Центра (ПЦ) банка в части интеграции с СМТ требует существенных затрат;
- системы на основе нейронных сетей в РФ в настоящее время являются экономически невыгодными - затраты на их приобретение, установку и сопровождение существенно превышают уровень потерь от мошенничества;

- рациональными являются системы реального или псевдо-реального времени, интегрируемые с ФС ПЦ и работающие на основе правил анализа транзакций.

В МПС Visa International и MasterCard Worldwide существуют обязательные требования к мониторингу транзакций, однако автором показано, что они являются общими и недостаточными в современных условиях. Эти требования формулируются в виде набора критериев, многие из которых включают пороговые значения сумм или количества операций. Пороговые значения, как правило, должны выставляться банком, а сами критерии должны применяться для систем, работающих в отложенном режиме. Указанных критериев недостаточно, поскольку в современных условиях необходимо выявлять мошенничество в ПСБК в реальном (или близком к реальному) времени, осуществлять гибкую настройку параметров мониторинга.

Несмотря на существование различных коммерческих СМТ, отсутствуют методики оценки рисков в ПСБК и основанные на них возможности настройки параметров СМТ.

На основе анализа обязательных критериев мониторинга транзакций в ПСБК и результатов практической части работы автором выделены некоторые характеристики транзакций, которые являются существенными для мониторинга:

- операции в разных странах в установленный интервал времени предлагается анализировать с учётом географического расстояния между городами;
- неуспешные операции по поддельным картам в случае своевременного выявления и противодействия им позволяют избежать потерь от последующих мошеннических операций;
- операции в банкоматах по зарплатным картам являются сложными для анализа, поскольку часто денежные средства длительное время накапливаются на счете БК, а затем получаются клиентом путём многочисленных

последовательных операций, что может быть ошибочно отнесено к мошенничеству;

- “дружественное мошенничество” сложно выявляется с помощью СМТ, поскольку совершается родственниками, знакомыми или коллегами по работе держателя карты и часто соответствует его поведению при пользовании БК.

В третьей главе – **“Формализация задачи количественной оценки риска”** – рассмотрены общие вопросы оценки рисков, в том числе количественной оценки рисков. Предложен подход к количественной оценке рисков, связанных с мошенничеством в ПСБК, по категориям мошенничества, а также схема представления данных для использования в расчётах рисков.

Один из возможных подходов к разработке методик оценки риска – накопление статистических данных об имевших место происшествиях. Риск определяется как вероятность причинения вреда с учетом тяжести этого вреда в стоимостном выражении. Тогда для некоторой БК риск будет равен

$$SFR = P_{мош} \cdot S_{сум},$$

где $P_{мош}$ - вероятность проведения мошеннической операции по БК,

$S_{сум}$ - величина доступных средств на счёте БК.

Для регистрации данных по всем мошенническим операциям в ПСБК автором предложена схема представления данных в таблицах БД мошеннических операций – как успешных, так и пресечённых, как с наличием ущерба, так и без такового. Разработанная автором ERD-диаграмма для построения БД мошеннических операций в ПСБК приведена на рис. 1. Следует отметить, что предлагаемый формат хранения позволяет фиксировать данные по мошенничеству для банка как по эмиссии, так и по эквайрингу.

На основе анализа особенностей проведения операций по БК в ПСБК автором выделен ряд необходимых условий осуществления мошеннической операции:

- данные БК должны быть скомпрометированы;

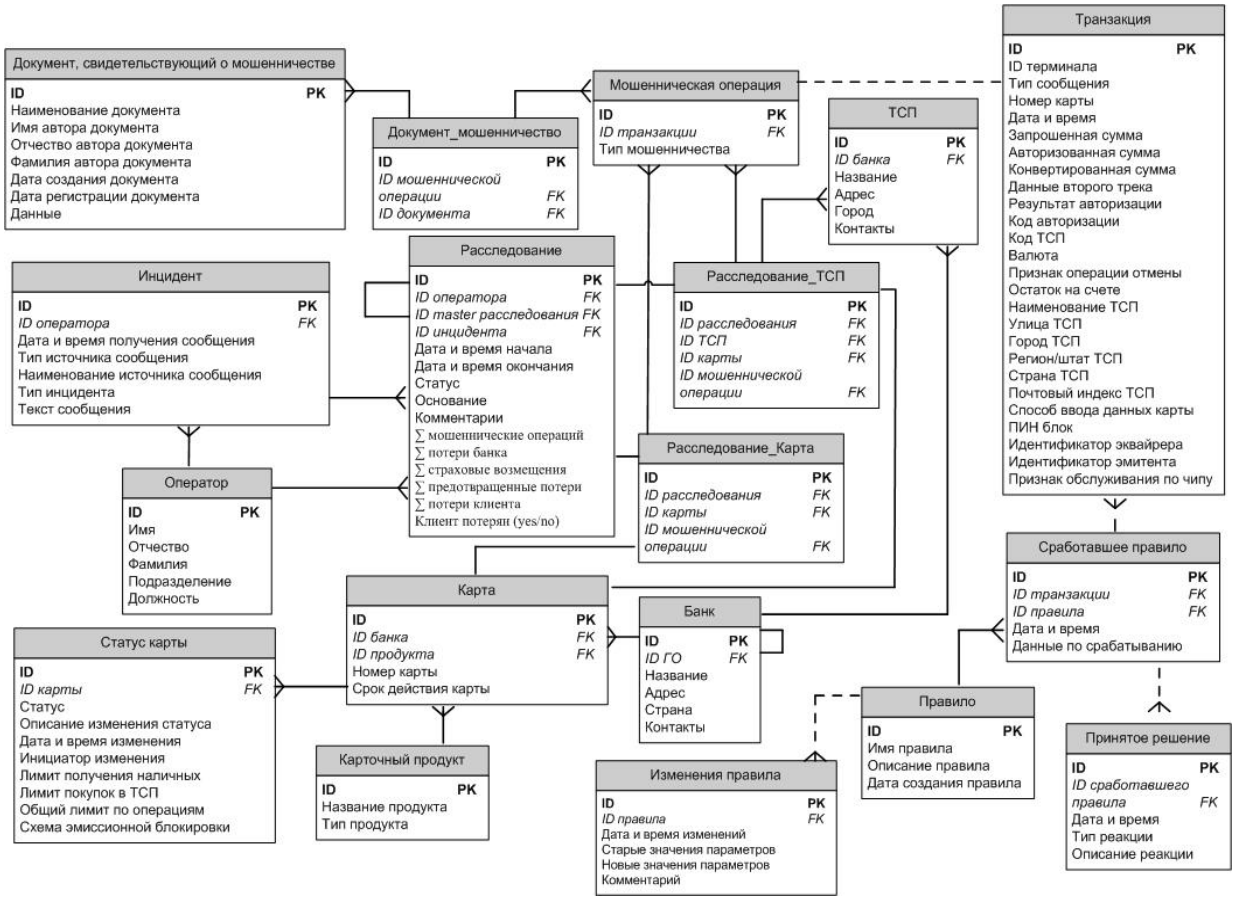

Рис. 1. ERD-диаграмма БД мошеннических операций

- скомпрометированные данные использованы для попытки проведения несанкционированной операции;
- попытка проведения несанкционированной операции была осуществлена;
- операция авторизована эмитентом.

В связи с этим вероятность проведения мошеннической операции по карте определяется следующим образом:

$$P_{мош} = P(кпр) \cdot P(исп \mid кпр) \cdot P(поп \mid кпр \cdot исп) \cdot (1 - P\ (обн)),$$

где $P(кпр)$ - вероятность компрометации данных карты, необходимых для проведения мошеннической операции,

$P(исп \mid кпр)$ - вероятность использования скомпрометированных данных для проведения операции,

$P(поп \mid кпр \cdot исп)$ - вероятность проведения несанкционированной операции (успех попытки проведения),

$P(обн)$ - вероятность обнаружения несанкционированной операции эмитентом.

Таким образом, количественная оценка рисков банка-эмитента, связанных с мошенничеством в ПСБК, осуществляется с использованием имеющихся данных по текущим остаткам на счетах БК банка-эмитента (или доступным кредитным лимитам в случае кредитных БК) и вероятностей компрометации данных БК и/или ПИН-кода для каждой БК в совершённых по ней клиентом операциях.

Четвертая глава – **“Методика количественной оценки рисков эмитента в ПСБК”** – посвящена разработке методики количественной оценки рисков.

Количественная оценка рисков опирается на данные, собираемые банком-эмитентом в своей ПСБК, для расчёта вероятности событий, связанных с мошенничеством. Исходные положения:

- имеется БД совершённых мошеннических операций, соответствующая ERD-диаграмме, приведённой в предыдущей главе;
- имеются данные по всем операциям со всеми БК в ПСБК банка-эмитента;
- по каждой БК имеются следующие данные: история всех операций, история движения средств по счёту карты, история изменений статуса карты, история и параметры изменения ограничений операций с картой, дополнительные признаки карты (зарплатная, относящаяся к VIP клиенту);
- нет никаких специальных данных по уровню осведомленности держателя карты в вопросах информационной безопасности, соблюдения рекомендаций по безопасному использованию карты;
- каждая совершенная клиентом операция по своей БК увеличивает риск проведения мошеннических операций в дальнейшем за счёт увеличения вероятности компрометации данных карты и/или ПИН-кода;

- вероятности обнаружения мошеннических операций СМТ для всех карт эмитента в ПСБК зависят только от типа мошенничества.

Заданы критерии риска для оценивания:

- $S_{год}^{под}$ - годовая величина в рублях допустимого риска по мошенничеству с поддельными картами;
- $S_{год}^{бпк}$ - годовая величина в рублях допустимого риска по мошенничеству без присутствия карты;
- $C_{год}^{мон}$ - годовая величина в рублях затрачиваемых средств на эксплуатацию СМТ.

Относительно применения СМТ для выявления мошенничества и принятия решений по подозрительным операциям рассчитываются значения следующих величин: риск мошенничества по поддельным картам и риск мошенничества по операциям без присутствия карты.

Риск мошенничества по поддельным БК:

$$SFR^{под} = P^{под\_крт}(кпр) \cdot P^{под\_крт}(исп \mid кпр) \cdot$$
$$\cdot P^{под\_крт}(пол \mid кпр \cdot исп) \cdot (1 - P^{под\_крт}(обн)) \cdot S_{сум}^{ТСП} +$$
$$+ P^{под\_ПИН}(кпр) \cdot P^{под\_ПИН}(исп \mid кпр) \cdot (1 - P^{под\_ПИН}(обн)) \cdot S_{сум}^{БКМ},$$

где $P^{под\_крт}(кпр)$ - вероятность компрометации данных магнитной полосы карты,

$P^{под\_крт}(исп \mid кпр)$ - вероятность использования поддельной карты для проведения оплаты в торгово-сервисном предприятии (ТСП),

$P^{под\_крт}(пол \mid кпр \cdot исп)$ - вероятность принятия к оплате поддельной карты,

$P^{под\_крт}(обн)$ - вероятность обнаружения несанкционированной операции эмитентом,

$S_{сум}^{ТСП}$ - доступные средства на счёте клиента для проведения операций в ТСП,

$P^{под\_ПИН}(кпр)$ - вероятность компрометации данных магнитной полосы карты и ПИН-кода,

$P^{под\_ПИН}(исп \mid кпр)$ - вероятность использования поддельной карты для проведения операции в банкомате,

$P^{под\_ПИН}(обн)$ - вероятность обнаружения несанкционированной операции эмитентом,

$S_{сум}^{БКМ}$ - доступные средства на счёте клиента для проведения операций в банкоматах.

Риск мошенничества по операциям без присутствия карты

$$SFR^{бпк} = P^{бпк}(кпр) \cdot P^{бпк}(исп \mid кпр) \cdot P^{бпк}(пол \mid кпр \cdot исп) \cdot (1 - P^{бпк}(обн)) \cdot S_{сум}^{бпк},$$

где $P^{бпк}(кпр)$ - вероятность компрометации данных для проведения мошеннических операций без присутствия карты,

$P^{бпк}(исп \mid кпр)$ - вероятность использования скомпрометированных данных для проведения мошеннических операций,

$P^{бпк}(пол \mid кпр \cdot исп)$ - вероятность принятия данных для проведения операции без присутствия карты,

$P^{бпк}(обн)$ - вероятность обнаружения несанкционированной операции эмитентом,

$S_{сум}^{бпк}$ - доступные средства на счёте клиента для проведения операций без присутствия карты.

Приемлемые результаты оценивания в соответствии с заданными критериями:

$$SFR_{год}^{под} \le S_{год}^{под},\ SFR_{год}^{бпк} \le S_{год}^{бпк},\ C_{год}^{мон} = const.$$

Значения вероятностей в указанных формулах вычисляются по стране и категории торгового предприятия. Так, для расчёта вероятности компрометации данных магнитной полосы карты *i* в некоторой стране за год в торговом предприятии определённой категории подсчитывается число операций, удовлетворяющих данному условию, в результате которых данные оказались скомпрометированы, и общее число операций, тогда:

$$P_{стр_c, мсс_m}(кпр)(\mathrm{i}) = \frac{W_{кпр}(стр_c, мсс_m)(i)}{W_{трз}(стр_c, мсс_m)(i)},$$

где $W_{кпр}(стр_c, мсс_m)(i)$ - число операций, связанных с компрометацией данных, по картам банка в стране $стр_c$ и категории торгового предприятия $мсс_m$ за год,

$W_{трз}(стр_c, мсс_m)(i)$ - общее число операций по картам банка в стране $стр_c$ и категории торгового предприятия $мсс_m$ за год.

Далее вероятность компрометации данных хотя бы в одной операции среди всех, проведенных держателем карты, вычисляется с использованием следующей формулы:

$$P(кпр) = 1 - \prod_{1}^{n}(1 - P_i(кпр)),$$

где $P_i(кпр)$ - вероятность компрометации данных в i-ой операции,

n – общее число операций.

Расчёт риска по поддельным картам производится как сумма рисков по всем картам банка. Расчёт риска по мошенническим операциям без присутствия карты осуществляется путем суммирования рисков по всем картам банка.

Оценивание рисков по заданным критериям позволяет установить требования к вероятностям выявления мошеннических операций с помощью СМТ - $P^{под\_крт}(обн)$, $P^{под\_ПИН}(обн)$, $P^{бпк}(обн)$.

Пятая глава – **“Разработка и эксплуатация СМТ”** – содержит описание разработанной автором, внедрённой и эксплуатируемой СМТ в ПСБК банка-эмитента для уменьшения рисков от мошенничества на основе разработанной методики.

Разработанная автором СМТ, имеющая промышленное наименование *FraMoS* (Fraud Monitoring System), является системой псевдо-реального времени, основанной на правилах с привлечением статистических профилей держателей карт для анализа эмиссионных операций и реагирования на подозрительные операции для уменьшения рисков, связанных с мошенничеством. Система осуществляет мониторинг транзакций и в части эквайринга.

СМТ FraMoS интегрирована с ФС ПЦ для анализа всех осуществляемых авторизационных транзакций в ПСБК банка и принятия адекватных оперативных решений по подозрительным операциям. Программной платформой FraMoS является Microsoft .NET Framework 2.0.

Основные функции и особенности FraMoS:

1. Анализируются транзакции по всем БК в ПСБК.
2. Имеются механизмы оповещения сотрудников отдела сопровождения о возникающих неисправностях, сбоях, приостановке работы отдельных модулей и компонент.
3. Анализ транзакций проводится по формализованным критериям, реализуемым в правилах анализа транзакций.
4. Анализ каждой отдельной транзакции выполняется в реальном времени и не превышает 50 мс.
5. Изменение параметров существующих, добавление новых правил анализа транзакций проводится без прерывания анализа транзакций.
6. По операциям с БК, признанным FraMoS подозрительными, автоматически могут устанавливаться ограничения, все действия протоколируются.
7. Осуществляется автоматическая рассылка почтовых уведомлений и сообщений сотрудникам банка и его филиалов, отвечающим за безопасность ПСБК, а также уполномоченным сотрудникам банков-партнёров.
8. Осуществляется автоматическая рассылка SMS-уведомлений держателям карт по подозрительным операциям определённых типов.
9. Оператору FraMoS предоставляется информация по подозрительной операции для проведения расследования.
10. Обеспечивается формирование отчётов по работе системы, в том числе и в автоматическом режиме.

FraMoS обеспечивает взаимодействие с филиалами банка и сторонними банками в части реагирования на подозрительные операции по БК. FraMoS состоит из серверной и клиентской частей. Серверная часть реализует

сбор данных о транзакциях, их анализ и реагирование на подозрительные транзакции, имеет консоль администратора для локального управления модулями и компонентами.

ФС ПЦ предоставляет серверной части FraMoS данные по транзакциям в ПСБК банка (рис. 2). Серверная часть FraMoS осуществляет разбор данных транзакции, проводит её анализ по заданным правилам, разработанным в соответствии с методикой, и реагирует в зависимости от настроек правила. Через Почтовый сервер осуществляется отправка автоматически формируемых почтовых сообщений о сработавших правилах анализа транзакций. Через SMS-сервер реализовано уведомление держателей БК о подозрительных операциях и устанавливаемых ограничениях.

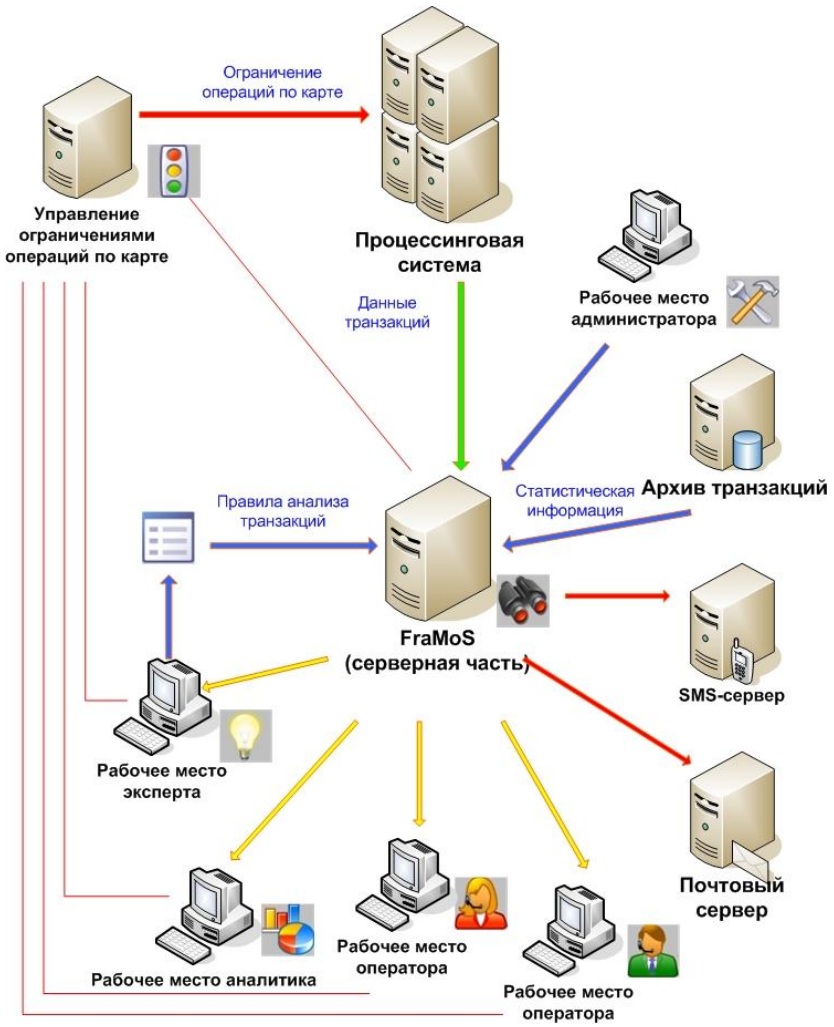

Рис. 2. Компоненты СМТ FraMoS

Рабочее место администратора предназначено для контроля работоспособности серверной части FraMoS и устранения возникающих проблем.

Рабочее место оператора, являющееся клиентской частью FraMoS, представляет собой прикладную программу с графическим интерфейсом, позволяющую принимать решения о подозрительных операциях и проводить расследования. Оператор получает информацию о срабатывании правила и на основе анализа истории операций по данной карте и статистических данных предпринимает действия по подозрительной операции. Аналитик со своего Рабочего места аналитика имеет возможность формировать отчёты о работе системы. Рабочее место эксперта предназначено для проведения работ по настройке правил анализа транзакций в соответствии с методикой.

Серверная часть FraMoS состоит из четырёх модулей, работающих независимо в отдельных доменах приложений .NET, связь между которыми обеспечивается Главным менеджером (рис. 3):

- Менеджер разбора транзакций осуществляет приём и разбор данных по транзакциям, формат которых соответствует ISO 8583, для последующего анализа;
- Менеджер анализа транзакций применяет заданные правила к данным транзакции с привлечением дополнительных данных и рассчитываемой статистики для выявления подозрительных операций;

Рис. 3. Модули серверной части CMT FraMoS

- Менеджер знаний обеспечивает расчёт статистических данных для анализа и загрузку вспомогательных данных;
- Менеджер реакции обеспечивает автоматическое и автоматизированное реагирование по подозрительным операциям.

СМТ FraMoS интегрирована с ФС ПЦ ООО “Газкардсервис” и используется в ПСБК банка Газпромбанк (Открытое Акционерное Общество). Система находится в промышленной эксплуатации с августа 2006 года.

В **заключении** приведены основные результаты диссертационной работы, рассмотрены пути дальнейшего развития темы исследования.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Основной результат работы заключается в разработке количественной методики оценки рисков банка-эмитента, связанных с мошенничеством, в ПСБК и использование методики в разработанной промышленной СМТ.

1. В рассматриваемой области оценка рисков может быть осуществлена количественно, поскольку мошенничество в ПСБК банка-эмитента всегда связано с несанкционированными операциями по банковскому счету с использованием БК как инструмента доступа к нему.
2. В работе предложена классификация СМТ для выявления подозрительных транзакций в ПСБК и противодействия им.
3. Разработана методика оценки рисков банка-эмитента в ПСБК, связанных с мошенничеством. Для количественной оценки риска использован аппарат теории вероятности и математической статистики.
4. Автором предложен формат хранения данных по мошенническим операциям для использования в расчётах и для подготовки аналитических отчётов.
5. Разработана и внедрена в промышленную эксплуатацию СМТ FraMoS в ПСБК, используемая для уменьшения рисков банка-эмитента в соответствии с методикой.

6. Разработан и внедрён в учебный процесс курс по основам обеспечения безопасности технологии банковских карт.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ:

1. **Кузин М. В. Проблема оценки рисков, связанных с мошенничеством, в платежной системе банковских карт / М.В. Кузин // Безопасность информационных технологий. – 2008. - №3. – С. 117-123. (Перечень ВАК)**

2. **Кузин М.В. Современное состояние обеспечения безопасности банковских карт / М.В. Кузин // Безопасность информационных технологий. – 2006. - №3. – С. 21-24. (Перечень ВАК)**

3. **Кузин М.В. Кассовый менеджер как средство обеспечения безопасности автоматизированной торговой системы / М.В. Кузин // Безопасность информационных технологий. - 2005. - №3. – С. 32-34. (Перечень ВАК)**

4. Кузин М.В. Платежные карты / М. В. Кузин // Бизнес-энциклопедия / под ред. А. С. Воронина. – М.: Маркет ДС, 2008. – 750 с.

5. Кузин М.В. Современные технологии борьбы с карточным мошенничеством. Мониторинг и предотвращение мошеннических операций. Технологические аспекты / М.В. Кузин // Практическая конференция. Безопасность пластиковых карт. Обнаружение и предотвращение мошенничества. 24-25 июня 2008, infor-media Russia.

6. Кузин М.В., Скородумов Б.И. Оценка рисков, связанных с мошенничеством, в платежной системе банковских карт / М.В. Кузин, Б.И. Скородумов // Цивилизация знаний: инновационный переход к обществу высоких технологий. Материалы Девятой Международной научной конференция. 25-26 апреля 2008г., в 2-х частях, Ч. 1. – М.: РОСНОУ. – С. 487-489.

7. Кузин М.В. Оценка рисков, связанных с мошенничеством, в платежной системе банковских карт / М.В. Кузин // Научная сессия МИФИ-2008. XV Всероссийская научная конференция. Проблемы информационной

безопасности в системе высшей школы. Сборник научных трудов. – М.: МИФИ, 2008. – С. 82-83.

8. Кузин М.В. Мониторинг транзакций для обеспечения безопасности платежной системы банковских карт банка / М.В. Кузин // Информационная безопасность-2007. Материалы IX Международной научно-практической конференции. 3–7 июля 2007г. Таганрог. Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – С. 197-201.

9. Кузин М.В. Проблемы обеспечения информационной безопасности платежных систем на основе банковских карт / М.В. Кузин // Научная сессия МИФИ-2007. XIV Всероссийская научная конференция. Проблемы информационной безопасности в системе высшей школы. Сборник научных трудов. – М.: МИФИ, 2007. – С. 82-83.

10. Кузин М.В. Карты в руки. Мониторинг транзакций для обеспечения безопасности платежной системы банковских карт банка / М.В. Кузин // Information Security. – 2007. - №6-1. – С. 60-61.

11. Кузин М.В. Современный рынок банковских карт в России / М.В. Кузин // Межвузовская конференция. Инновационное предпринимательство и управление знаниями. 28 ноября 2006г. Тезисы докладов. – М.: РИПО ИГУМО, 2006. - С. 94-95.

12. Кузин М.В., Скородумов Б.И. Информационная безопасность в розничной торговле / М.В. Кузин, Б.И. Скородумов // Information Security. – 2006. - № 3-4. – С. 12.

13. Кузин М.В. Кассовый менеджер для обеспечения информационной безопасности автоматизированной системы торгового предприятия / М.В. Кузин // Технологии Microsoft в теории и практике программирования. Всероссийская конференция студентов, аспирантов и молодых ученых. 2-3 марта 2006г. Тезисы докладов. – М.: МГТУ им. Н.Э. Баумана, 2006. – С. 80-82.