Аляев, Данила Александрович. Система комплексного управления риском мошенничества с использованием банковских карт : диссертация ... кандидата экономических наук : 08.00.10 / Аляев Данила Александрович; [Место защиты: Рос. ун-т кооп.].- Москва, 2011.- 205 с.: ил. РГБ ОД, 61 11-8/2107

**Содержание к диссертации**

Введение

**Глава 1. Теоретические основы использования банковских карт 13**

1.1 Сущность банковских карт, их виды и характеристика использования в современных условиях 13

1.2 Классификация видов мошенничества с использованием банковских карт 31

1.3 Зарубежный опыт выявления рисков мошенничества с использованием банковских карт 49

**Глава 2. Характеристика механизмов комплексного управления риском мошенничества с использованием банковских карт 59**

2.1 Анализ механизмов идентификации держателей, как составляющей безопасности проведения финансовых операций с банковскими картами 59

2.2 Оценка мер противодействия мошенничеству, осуществляемых самостоятельным подразделением безопасности банка 68

2.3 Управление риском мошенничества при эмиссии и эквайринге банковских карт 81

**Глава 3. Реализация инновационных решений в целях обеспечения безопасности приложений банковских карт 106**

3.1 Разработка автоматизированной системы управления авторизациоными лимитами в рамках обеспечения безопасности проведения финансовых операций с банковскими картами 106

3.2 Проектирование интерактивной системы раннего предупреждения мошенничества с использованием банковских карт (ifews) 118

3.3 Повышение безопасности финансовых операций с использованием банковских карт на основе CDA-аутентификации микропроцессорных приложений стандарта emv 144

3.4 Внедрение разработанных инновационных карточных технологий в области обеспечения безопасности проведения финансовых операций с использованием банковских платежных инструментов 158

Заключение 169

Список использованных источников 173

Приложения 186

**Введение к работе**

**Актуальность темы.**Рынок банковских услуг на базе карточных решений развивался по экстенсивному пути, причем по пути роста количественной его составляющей - инфраструктуры, обслуживающей исключительно финансовые операции по получению наличных денежных средств. Такой стратегический вектор формирования бизнеса был выбран в свете закономерной необходимости обеспечения потребностей держателей банковских карт, эмитированных в рамках повсеместно реализуемых проектов по выплате заработной платы, стипендий, пенсий и т.д. Современный рынок претерпел существенные изменения, и сейчас его можно охарактеризовать как стремительно развивающийся, ориентированный на поддержание жесткой конкурентной атмосферы между игроками. В этой связи все его участники, так или иначе, вовлечены в процесс становления современной банковской инфраструктуры, в которой пластиковые (банковские) карты играют немаловажную роль.

Действительно, банковские карты, являясь универсальным, многофункциональным и крайне востребованным розничным продуктом, сегодня составляют неотъемлемую часть широкого спектра предлагаемых финансовых услуг со стороны кредитных организаций. Постоянно расширяется инфраструктура приема и обслуживания банковских карт, развиваются маркетинговые и сервисные аспекты ведения бизнеса. В настоящее время значительная часть банков-эмитентов широко использует технологические возможности магнитных и микропроцессорных приложений банковских карт для внедрения совместных кобрендовых программ, а также предоставления конечному пользователю дополнительных сервис пакетов в рамках конкретных целевых проектов.

Наряду с внушительным перечнем достоинств, современные банковские карты имеют и определенные недостатки, среди которых наиболее существенным является их практическая уязвимость перед

несанкционированным воздействием со стороны третьих лиц с целью

организации незаконного доступа к счету держателя и последующего хищения денежных средств.

Проблема обеспечения безопасности проведения финансовых операций с использованием банковских карт и, в первую очередь - снижение риска мошенничества, по праву считается глобальной, поскольку в процесс ее решения вовлечены все участники мирового рынка платежных инструментов. Предупреждение мошенничества с использованием банковских карт также является весьма важным вопросом совершенствования системы безналичных взаиморасчетов ввиду того, что любое несанкционированное воздействие, как по отношению к платежному инструменту, так и к его реквизитам, потенциально может привести к рискам банка-эмитента, связанным с прямыми финансовыми потерями, ухудшением деловой репутации, недоверием к предоставляемым продуктам со стороны клиентов и общим ухудшением качества обслуживания.

Принимая во внимание стремительные темпы развития рынка банковских услуг решение проблемы обеспечения комплексности и эффективности предпринимаемых мер по контролю риска мошенничества в системе безналичных расчетов является ключевым аспектом формирования политики безопасности, как на уровне отдельной кредитной организации, так и в масштабе всей банковской системы.

**Степень разработанности проблемы.**В современной научной литературе и многочисленных трудах отечественных ученых проблематика совершенствования механизмов управления риском мошенничества с использованием банковских карт занимает определенное значение, однако глубина и степень разработанности данных исследований не удовлетворяют реалиям экономического мира с его постоянно меняющимися тенденциями. До настоящего момента остаются непроработанными вопросы взаимодействия участников рынка банковских карт в области организации унифицированных, комплексных стандартов информационной и транзакционной безопасности

платежных инструментов, не освещаются элементы возможного

совершенствования систем управления рисками кредитных организаций, возникающими в результате несанкционированного воздействия со стороны третьих лиц, недостаточно определены классификационные категории мошенничества и механизмы нивелирования его последствий. Разработанные Центральным банком Российской Федерации различного рода методики и рекомендации имеют узкую направленность и не в полной мере соответствуют предъявляемым требованиям Международных платежных систем (МПС) по снижению риска мошенничества с использованием банковских карт.

На результаты работы повлияли научные труды таких авторов, как Н.П. Белотелова, Б.Б. Воронин, В.А. Гамза, А.И. Гинсбург, И.М. Голдовский, И.А. Демчев, В.В. Дик, В.М. Казиев, И.А. Киселева, М.В. Кузин, В.А. Кузнецов, Д.А. Лаптырев, А.В. Печникова, Г.А. Поллак, А.В. Пухов, И.Б. Ткачук, А.В. Шамраев, А.В. Шапкин, А.С. Шапкин и др. Диссертант обратил внимание на труды зарубежных ученых, где заявленная проблематика разрабатывается давно и достаточно успешно. Автор в процессе исследования обращался к работам следующих экономистов: Грюнинг X., Брайович Братанович С, Диксон Д., Маршал В., Уотерман Д., Хейос-Рот Ф., Робсон М., Уллах Ф.

Актуальность исследуемой проблемы, а также ее практическая значимость и востребованность рассматриваемых вопросов определили выбор темы диссертации, цель и задачи работы.

**Цель и задачи исследования.**Целью диссертационного исследования является разработка системы комплексного управления риском мошенничества с использованием банковских карт, позволяющей снизить общий уровень финансовых рисков банка.

Для достижения поставленной цели были обозначены и решены следующие задачи:

изучить организацию и провести анализ рынка современных банковских карт, определить вектор его развития;

исследовать механизмы организации несанкционированного доступа к счету карты держателя со стороны третьих лиц для последующего совершения мошеннической операции;

проанализировать влияние риска мошенничества, возникающего на стадии эмиссии и эквайринга банковских карт, на деятельность кредитной организации в целом и обосновать необходимость разработки комплекса мер по нивелированию сопряженных с ним финансовых потерь;

разработать автоматизированную систему управления авторизационными лимитами в рамках обеспечения безопасности проведения финансовых операций с использованием банковских карт;

осуществить анализ и выявить потенциальные резервы снижения риска мошенничества, возникающего на этапе функционирования микропроцессорных приложений банковских карт, разработать и внедрить в эксплуатацию интерактивную систему раннего предупреждения мошенничества.

**Область исследования.**Содержание диссертации соответствует п. 9.17 «Совершенствование системы управления рисками российских банков» паспорта специальности ВАК 08.00.10 «Финансы, денежное обращение и кредит» паспорта научных специальностей ВАК Российской Федерации (экономические науки).

**Предметом исследования**являются современные механизмы контроля рисков кредитных организаций, возникающих в связи с осуществлением несанкционированных (мошеннических) операций с использованием банковских карт.

**Объект исследования**- экономическая система безналичных взаиморасчетов с использованием банковских карт.

**Теоретическую и методологическую основу исследования**составили работы отечественных и зарубежных экономистов, специалистов-практиков в области банковского дела и риск-менеджмента, материалы научно-

практических конференций, а также аналитические и тематические публикации по исследуемой проблеме.

Основными методами исследований, используемыми в работе, являются методы научного познания: наблюдение, сравнительный и логический анализ, комплексный и системный подход к изучению оцениваемых показателей, методы экспертных оценок и структурного анализа сложных процессов. За основу разработанной продукционной модели базы знаний интерактивной системы раннего предупреждения мошенничества взяты концептуальные положения вероятностной модели Байеса.

**Информационной базой исследования**послужили нормативно-правовые акты Российской Федерации, регулирующие банковскую деятельность. Кроме того, использовались официально опубликованные материалы и методические рекомендации ведущих Международных платежных систем MasterCard Worldwide и Visa International, Центрального Банка Российской Федерации, статистические данные ряда крупных российских и зарубежных банков по уровню мошенничества и разработанные ими стратегические меры его предупреждения, различные аналитические материалы, характеризующие реальное развитие технологий снижения риска мошенничества, технические документы процедур взаимодействия микропроцессорных приложений с сервером эмитента на стадии запроса авторизации.

**Научная новизна**исследования заключается в теоретическом и практическом обосновании необходимости совершенствования системы управления риском мошенничества в рамках разработки комплексного решения проблем эффективного использования банковских карт, как на уровне отдельной кредитной организации, так и в масштабе всей банковской системы Российской Федерации.

Научная новизна исследования подтверждается полученными результатами, выносимыми на защиту:

сформулировано содержание системы использования современных банковских карт, определен вектор развития рынка безналичных финансовых операций;

выявлена и обоснована практическая неэффективность существующей модели предоставления авторизации по банковским картам с точки зрения предупреждения мошенничества, которая заключается в отсутствии использования систем авторизационного лимитирования для каждого держателя;

предложена многофакторная модель идентификации держателей банковских карт, которая позволит обеспечить дополнительный уровень безопасности конфиденциальной информации;

разработана и апробирована интерактивная система раннего предупреждения мошенничества с использованием банковских карт, способствующая повышению уровня эффективного проведения финансовых операций;

предложена и доказана необходимость внедрения разработанной автором автоматизированной системы управления авторизационными лимитами и интерактивной системы раннего предупреждения риска мошенничества в основе единой концепции его комплексного предотвращения с использованием банковских карт;

проведена оценка количественных и качественных характеристик потенциальных резервов снижения риска мошенничества, возникающего на этапе функционирования микропроцессорных приложений банковских карт, доказана и обоснована эффективность использования механизма комбинированной аутентификации приложений банковских карт с целью защиты конфиденциальной информации держателя.

**Практическая значимость**результатов исследования состоит в том, что основные положения работы направлены на их широкое практическое применение при формировании внутренней политики безопасности кредитной

организации и вносят определенный вклад в теорию риск-менеджмента и предупреждения риска мошенничества с использованием современных банковских карт.

Основные идеи и практические выводы диссертации могут быть включены в программы профессиональной подготовки и повышения квалификации руководителей, риск-менеджеров и профильных специалистов кредитных организаций.

**Апробация и внедрение результатов исследования.**Основные результаты исследования применены в разработанной и внедренной интерактивной системе раннего предупреждения мошенничества по банковским картам, используемой в процессинговом центре RusCard ЗАО «Банк Русский Стандарт».

Результаты диссертационной работы докладывались и получили одобрительную оценку на следующих конференциях: Международная научная конференция молодых ученых - преподавателей и аспирантов «Новые идеи и потенциал молодых - кооперации России» (Москва, 2007г.); Международная научная конференция молодых ученых - преподавателей и аспирантов «Социально-экономические проблемы кооперативного сектора экономики» (Москва, 2008г.); III Международная научно-практическая конференция молодых ученых - преподавателей, сотрудников, аспирантов и соискателей «Социально-экономические проблемы кооперативного сектора экономики» (Москва, 2010г.).

Разработанные в диссертационной работе предложения и рекомендации были успешно применены в проектах по реализации и внедрению системы автоматизированного управления авторизационными лимитами, интерактивной системы раннего предупреждения мошенничества (IFEWS), а также в проекте по стратегическому перепрофилированию бизнеса ЗАО «Банк Русский Стандарт» на базе современных платежных инструментов (справка № Д5-125 от 29.07.2010).

**Публикации.**По теме диссертации опубликовано шесть научных работ, общим объемом 1,27 п.л. (авторских - 1,27 п.л.), из них 3 статьи в изданиях, рекомендованных ВАК.

**Структура и объем работы.**Диссертация изложена на 205 страницах машинописного текста, включая 17 рисунков, 9 таблиц и 16 формул. Состоит из введения, трех глав, заключения, списка использованных источников и приложений. Список использованных источников включает 156 наименований.

## Классификация видов мошенничества с использованием банковских карт

В зависимости от схемы взаиморасчетов, применяемой к карте, в используемой МПС классификации выделяют следующие типы карт: расчетная карта (charge card) — платежная карта, держателю которой каждый отчетный период выставляется единый счет для оплаты всей суммы расходов, осуществленных в течение этого периода. По расчетной карте эмитентом не устанавливается лимит расходования средств на счете. В течение отчетного периода держатель вправе допустить перерасход имеющихся средств на счете (овердрафт) при условии своевременной и полной уплаты задолженности в установленный срок. При нарушении режима уплаты задолженности эмитент имеет право взыскать с держателя процент (штраф) за пользование овердрафтом; кредитная карта (credit card) - платежная карта, дающая держателю право на возмездной основе осуществлять расходные операции за счет предоставленных эмитентом кредитных средств в рамках установленного кредитного лимита на условиях, оговоренных в двустороннем кредитном соглашении (зачастую, договоре-оферте). Каждый отчетный период держателю выставляется единый счет для оплаты суммы расходов, осуществленных в течение этого периода. Держатель не имеет возможности допускать перерасход кредитного лимита и вправе осуществлять уплату задолженности установленными эмитентом минимальными аннуитетными платежами. Различают кредитные карты с невозобновляемой (Non-revolving credit) и возобновляемой (Revolving credit) кредитной линией; дебетовая карта (debit card) - платежная карта, все операции по которой дебетуются со счета держателя карты. Дебетовая карта не несет никаких рисков со стороны эмитента, так как каждая операция по ней производится только с авторизационным запросом и обязательным получением кода авторизации. Различают дебетовые карты с прямым (непосредственным) дебетованием счета (Direct debit card) и с отсроченным платежом (Deferred debit card); предоплаченная карта (prepaid card) — платежная карта, дающая держателю право на осуществление расходных операций в пределах предварительно оплаченного лимита. Различают пополняемые (Reloadable card) и непополняемые (Disposable card) предоплаченные карты. Общими признаками предоплаченных карт являются: 1) наличие предварительно оплаченного лимита расходования денежных средств, 2) дебетование счета происходит в момент совершения расходной операции, 3) незначительная величина предоплаченного лимита расходования денежных средств. Предоплаченные карты подразделяются в зависимости от характера предоплаченного лимита денежных средств следующим образом: 1) карты - электронные кошельки (Electronic purse, Electronic cash), содержащие электронные денежные средства, 2) карты, предоплаченный лимит которых позволяет осуществлять приобретение услуг (транспортные, телекоммуникационные и др).

Внутри приведенной классификации можно и далее выделять разнообразные категории в зависимости от условий обслуживания карточного счета. Например, как уже было указано, кредитные карты можно разделить на карты с невозобновляемой и возобновляемой кредитной линией, а дебетовые - на депозитные и обычные. Но в рамках проводимого исследования мы остановимся на приведенном уровне классификации, однозначно полагая, что отличия в обслуживании банковских продуктов могут устанавливаться самими участниками, которые наделены со стороны МПС полномочиями реализовывать широкую модификацию своего продуктового ряда в зависимости от задач бизнеса. Остальные модификации банковских карт (микропроцессорные, магнитные, именные, неименные, локальные, международные и т.д.) с той или иной степенью допущения можно подвести под приведенную ранее классификацию, а специфические признаки будут расценены как некоторая особенность функционирования конкретного карточного продукта.

Проведем исследование современного состояния российского рынка финансовых инструментов на платформе банковских карт.

Согласно данным всероссийского опроса, проведенного в августе 2009г. Национальным Агентством Финансовых Исследований (НАФИ), среди различных групп населения страны наибольшее количество банковских карт приходилось на возрастные категории от 25 до 44 лет (65%) и от 18 до 24 лет (25%), при этом наблюдался потенциальный прирост потребления финансовых продуктов на платформе банковских карт со стороны группы респондентов до 25 лет. Наименьшая доля банковских карт была зафиксирована у возрастной группы старше 60 лет (2%). В целом, около 33% россиян имеют банковские карты, 55% - не имеют и не планируют этого делать в ближайшем будущем, и лишь 12% - не имеют, но планируют оформить банковскую карту [81].

Среди держателей банковских карт подавляющее большинство составляют держатели расчетных карт. Их доля в общем количестве эмитированных карт - 90,9%. При этом количество карт, полученных держателями по собственной инициативе, по-прежнему незначительно, подавляющее большинство банковских карт - это карты, выданные в рамках зарплатных проектов.

Важно отметить, что в зависимости от уровня дохода, цели использования банковских карт россиянами коррелируют следующим образом. Для всех групп характерна высокая доля респондентов, использующих банковские карты исключительно для получения заработной платы, что четко характеризует общероссийскую картину. Прочие цели использования карт, а также уровень лояльности к Cross-sale продуктам прямо пропорционален уровню дохода той или иной группы респондентов. В частности, чем выше доход, тем большая доля опрошенных подтверждает свое желание и потребность в использовании банковских карт не только для совершения операций по снятию наличных денежных средств, но и для разного рода безналичных операций, в том числе приобретение товаров/услуг в глобальной сети Интернет.

По данным НАФИ подавляющее большинство держателей банковских карт в России используют их для получения заработной платы (72% респондентов), 30% участников опроса - для совершения операций по обналичиванию денежных средств. Значительное количество респондентов привлекает возможность расплачиваться с помощью банковской карты за товары или услуги, а также использовать ее как средство хранения денежных средств (по 14% соответственно). Использование карты с целью получения кредита отметили лишь 9% респондентов [73].

## Оценка мер противодействия мошенничеству, осуществляемых самостоятельным подразделением безопасности банка

Таким образом, количественная оценка риска мошенничества осуществляется посредством использования имеющейся информации по текущему остатку денежных средств на счете банка-эмитента, а также вероятностных значений компрометации данных банковской карты и PIN.

В Западной Европе на рядового жителя приходится до 5 банковских карт, при этом в год каждым совершается в среднем около 40 безналичных финансовых операций при характерном значении коэффициента использования банковской карты 0,1 раз в сути. В рамках актуального уровня F/S в 7-10 Ър вероятность того, что очередная операция по банковской карте конкретного жителя Европы завершится мошенничеством, равна р = 0,001. В действительности же этот показатель гораздо ниже представленного, поскольку по скомпрометированной злоумышленником банковской карте осуществляется несколько операций за короткий промежуток времени (порядка 5-10 минут в зависимости от платежного баланса карты), номинальный размер которых, как правило, выше, чем авторизованных непосредственно держателем. Однако для наглядной иллюстрации оценки вероятности наступления мошенничества по банковской карте данный пример вполне уместен.

Очевидно, что за 10 лет пользования банковской картой рассматриваемый держатель совершит N = 400 безналичных финансовых операций, а вероятность наступления мошенничества по его платежному инструменту при сохранении актуального уровня F/S на прежней отметке составит порядка 0,33, и будет рассчитана следующим образом: где р — вероятность наступления мошенничества по банковской карте; п — количество безналичных финансовых операций по банковской карте.

Исходя из вышеуказанного с определенной долей уверенности можно констатировать, что примерно каждый третий житель Западной Европы, который пользуется банковскими картами в течение 10 лет, при актуальном уровне F/S пострадает от карточного мошенничества (кардинга).

Верно будет заметить, что большинство держателей банковских карт напрямую или опосредованно сталкивались с инцидентами мошенничества с использованием платежных инструментов, что естественным образом предопределяет их осторожное и недостаточно частое использование при осуществлении ежедневных финансовых расчетов. Именно поэтому безопасность проведения финансовых операций с использованием современных платежных инструментов является приоритетным вектором развития бизнеса банковских карт.

Кроме прямых финансовых потерь, вызванных несанкционированным действием со стороны третьих лиц, кредитные организации несут также косвенные издержки, связанные с потерей клиентов, ухудшением деловой репутации, содержанием подразделений безопасности, приобретением и настройкой программного обеспечения и т.д. В результате, совокупные годовые потери по организации комплекса мер предупреждения мошенничества с использованием банковских карт, а также нивелирования его последствий значительно превышают цифры в регулярно публикуемых МПС аналитических сводках. И это очевидно, ведь в настоящее время сбор статистических данных по противоправным деяниям в сфере банковских карт в России не ведется [74,91,63]. А практика показывает, что далеко не все национальные банки добросовестно сообщают МПС в SAFE (System to Avoid Fraud Effectively), FIS (Fraud information service), Fraud Advice и иных фрод-репортах о текущем уровне мошенничества, пытаясь таким образом минимизировать репутационные риски.

Мошенничество с использованием банковских карт в мире имеет следующие характерные особенности [45]: использование злоумышленниками современных аппаратных и программных устройств, благодаря их доступности и закономерному падению стоимости; высокий профессиональный уровень криминальных элементов; постоянный поиск возможностей реализации новых схем несанкционированного доступа к карточным счетам клиентов; интернациональный характер преступлений в области осуществления мошенничества с использованием банковских карт; абсолютная мобильность криминальных структур по отношению к обнаруженным несовершенствам в ПО и алгоритмам информационной защиты финансовых институтов; нацеленность на определенный спектр участников рыка; специализация криминальных структур на наиболее доступных и легко реализуемых типах несанкционированного воздействия на конфиденциальную информацию; склонность мошенничества к модификации в зависимости от доступности технологического и программного инструментария проведения транзакций по банковским картам (около 80% всего мошенничества приходится на онлайновые транзакции); рост числа СКР-мошенничества в глобальной сети Интернет; непредсказуемость атак со стороны криминальных структур; кредитные карты - основная цель криминальных элементов. Особое внимание уделяется кредитным картам премиального сегмента со средним платежным (кредитным лимитом) лимитом от 300 тыс. рублей. В качестве подтверждения приведенного ранее заключения в таблице 1 укажем соотношение международного уровня мошенничества в зависимости от категории банковского продукта.

## Управление риском мошенничества при эмиссии и эквайринге банковских карт

В связи с прогнозируемым к 2011г., МПС ростом среднемировой доли CNP-операций до уровня 60% от всего торгового оборота в секторе В2С, ожидается постепенное увеличение спроса со стороны клиентов на использование банковских карт исключительно для операций типа Е- Commerce. По этой причине держателю, который предполагает использовать банковскую карту только для оплаты товаров услуг в сети Интернет, и который осознанно принимает на себя определенную (в соответствии с заключенным договором банковского обслуживания) долю ответственности за возможные риски, значение показателя CardFrW может быть увеличено до желаемого предела.

Помимо корректировки весового показателя CardFrW, организовать надлежащее управление значением максимально возможной суммы CNP- операции возможно посредством альтерации критерия Mail Ceiling (верхний предел суммы операции Mail Order) на уровне фронтального интерфейса АБС банка. Однако регулярное изменение этого показателя по первому желанию клиента возможно лишь на базе тех АБС, которые располагают технологическими возможностями установления его для каждого держателя индивидуально, в противном случае данный механизм не будет эффективным. Вместе с тем, стоит признать, что инструменты частичного делегирования полномочий по управлению риском мошенничества непосредственно держателю платежного инструмента в значительной степени позволяют повысить безопасность проведения CNP-операций с использованием банковских карт.

Необходимо отметить, что ввиду физического отсутствия платежного инструмента в момент осуществления CNP-операции, со стороны эмитента могут возникать определенные трудности в случае заявления клиента об отказе в совершении последней по следующим причинам: при обнаружении мошеннической операции в редких случаях удается обнаружить точку компрометации банковской карты (СРР); при поддержке ТСП алгоритма безопасности 3D Secure распределение финансовой ответственности согласно регламенту Merchant only liability shift возлагается на банк-эмитент без возможности инициации цикла опротестования в МПС путем выставления «запроса на возврат операции» (Charge back, Representment). Отдел фрод-мониторинга должен обеспечивать непрерывность процедур эффективного мониторинга потенциально несанкционированных финансовых операций, в том числе и категории CNP, во избежание случаев заявления клиентов об отказе в их совершении. При выявлении отклонения «модели поведения» держателя от предустановленной схемы ответственный сотрудник обязан предпринять соответствующие превентивные меры для нивелирования потенциального риска мошенничества вплоть до блокирования банковской карты, которое должно осуществляться с единовременным информированием держателя во избежание репутационных рисков. С целью минимизации вероятности подбора номера банковской карты эффективным представляется механизм обязательного представления со стороны ТСП значения CW/CVC (CW2/CVC2) в конкретном поле авторизационного запроса при осуществлении CNP-операции. В настоящее время немногие эмитенты предлагают в качестве дополнительного инструмента обеспечения безопасности CNP-операций виртуальные предоплаченные банковские карты (Virtual card), которые входят в классификационную группу предоплаченных карт. На российском рынке банковских карт представлена пока единственная виртуальная предоплаченная карта Visa Virtual с невозобновляемой (non- revolving credit) кредитной линией МПС Visa International, реальная эмиссия которой не предусмотрена в пользу виртуального взаимодействия с клиентом посредством передачи последнему реквизитов платежного инструмента (номер карты (PAN), срок действия (Expiry date), CW/CVC (CW2/CVC2), достаточных для осуществления CNP-операций категорий МО/ТО и Е- Commerce. При этом номер виртуальной банковской карты присоединяется к уже существующей карте клиента для списания денежных средств в пользу формирования кредитной линии. Как правило, номер виртуальной банковской карты генерируется в случайном порядке и имеет отличный от реально существующих карт BIN. При выявлении факта отказа клиента в совершении финансовой операции с использованием банковской карты, ответственный сотрудник самостоятельного подразделения безопасности банка принимает следующие меры: выполняет блокирование банковской карты, по которой было зафиксировано осуществление спорной операции, с присвоением неактивного статуса (Decline); проводит первичный анализ потенциального инцидента осуществления несанкционированной операции с использованием банковской карты на предмет выявления точки компрометации (СРР), степени ответственности держателя и фродовых схем; при необходимости взаимодействует с держателем по вопросу предоставления дополнительных документов (их копий), подтверждающих/опровергающих непосредственное участие клиента в совершении спорной операции, как то: копия всех страниц заграничного паспорта держателя; справка с места работы о местонахождении держателя в момент осуществления спорной операции; копия посадочного талона на авиарейс (при наличии) и других транспортных документов; талон-заявление об инциденте осуществления несанкционированной операции с использованием банковской карты в правоохранительные органы по месту регистрации держателя.

## Проектирование интерактивной системы раннего предупреждения мошенничества с использованием банковских карт (ifews)

Проведенное исследование выявленных инцидентов осуществления несанкционированных операций с использованием банковских карт держателей показало, что актуальные механизмы управления риском мошенничества, которые в настоящее время применяются в большинстве финансовых институтов, имеют узконаправленный сиюминутный характер и не могут обеспечить должного уровня безопасности проводимых операций. Очевидно, что постоянный рост их (операций) числа будет сопровождаться увеличением объемов мошенничества и, соответственно, ростом финансовых и репутационных потерь. Данное обстоятельство однозначно обуславливает необходимость применения исключительно комплексного подхода в решении проблем безопасности как на уровне отдельного финансового института, так и в масштабе всей банковской системы.

Представляется, что для оказания должного противодействия мошенничеству недостаточно применять удачное технологическое решение, необходимо соответствующим образом наладить организационную и координационную работу МПС, банков-участников, правоохранительных органов, а также повысить общий уровень финансовой грамотности держателей и их осведомленности о различных видах мошенничества. Кредитная организация со своей стороны должна руководствоваться следующими принципами управления риском мошенничества: наличие политики обеспечения информационной безопасности и четко сформулированной стратегии в области риск-менеджмента; наличие команды высококвалифицированных специалистов для расследования и выявления мошеннических схем; наличие и активное использование современных технологических решений в области мониторинга авторизационных и клиринговых транзакций, а также управления расходными (авторизационными) лимитами; наличие четкой авторизационной и эмиссионной политики. Высокая степень латентности регистрируемых инцидентов мошенничества различных категорий, а также практическая невозможность их прогнозирования определяют потребность в разработке принципиально новых механизмов обеспечения безопасности финансовых операций с использованием банковских карт. Так, исследование существующего алгоритма предоставления авторизации показало, что каждый авторизационый запрос, формируемый банком-эквайером и направляемый через хост МПС эмитенту, верифицируется последним на предмет: корректности предоставленных в запросе реквизитов банковской карты, а также идентификаторов ТСП и держателя; актуального статуса банковской карты на внешнем интерфейсе АБС эмитента (активная или заблокированная); соответствия параметров операции политике безопасности эмитента, нормам МПС и законодательно-правовым актам Российской Федерации; наличия специальных критериев использования банковской карты (авторизационные лимиты, ограничения по географической локации, МСС); достаточности платежного баланса на счете клиента (ОТВ) для успешного проведения запрашиваемой операции. В случае успешной верификации по всем вышеперечисленным условиям, банк-эмитент отвечает на запрос банка-эквайера авторизационным ответом, разрешающим осуществление финансовой операции, то есть предоставляет авторизацию, как показано на рис. 9. Предоставление авторизации с направлением кода-ответа (Authorization number) Проверка достаточности платежного баланса на счете карты (OTB) Проверка весового показателя (TrxnFrW) и авторизационных лимитов Приостановление авторизации с направлением кода-ответа «01» (свяжитесь с эмитентом) Рис.9. Процедура предоставления авторизации на основе проверки реквизитов авторизационного запроса, направляемого в банк-эмитент Корректность реквизитов банковской карты проверяется по представленному в Приложении 4 алгоритму. Проведенное исследование механизма предоставления авторизации на уровне ТСП показало, что проверке подвергаются следующие реквизиты запроса: номер банковской карты (PAN) верифицируется на его наличие в стоп- листе, загружаемом в POS с оффлайновым режимом работы (Offline Capable POS) банком-эквайером, а также в перечне принимаемых к акцептованию BIN; срок действия банковской карты (Expiry date) сопоставляется с текущей датой осуществления финансовой операции. При возможности предоставления авторизации в оффлайновом режиме, а также неудовлетворительном результате проведенной ТСП верификации реквизитов, авторизационный запрос может быть отклонен уже на уровне POS- терминала без передачи его на хост банка-эмитента. Следует, однако, отметить, что в рамках проводимого исследования отдельное внимание будет обращено на механизмы предоставления авторизации со стороны эмитирующего института. В случае успешной верификации реквизитов запроса, а также после проведения должной идентификации полученных от ТСП данных, банк-эквайер направляет авторизационный запрос банку-эмитенту через хост обслуживающей платежной системы посредством стандартных SMS или DMS- сообщений. Далее, на уровне АБС банка-эмитента, в первую очередь, осуществляется проверка тех полей авторизационного запроса, которые содержат сведения о реквизитах банковской карты (PAN, Expiry date, Service code), идентификаторе держателя (Cardholder name), идентификаторе ТСП (Merchant name, Merchant ID, Terminal ID, РЕМ) и специальной информации, генерируемой эмитентом и используемой им для удаленной проверки подлинности платежного инструмента. Затем проверяется актуальный статус банковской карты и корректность введенных значений PIN или CW/CVC (CW2/CVC2) при их наличии.