Содержание

Введение.....7
1 Проблема использования платежных систем для мошеннических схем….9
1.1 Актуальность проблемы и основной понятийный аппарат по вопросам противодействия мошенничеству в кредитно-финансовой сфере.....9
1.2 Законодательные требования и требования Банка России. Нормативные документы надзорных органов.....17
1.3 Способы и методы реализации мошеннических действий со счетами и банковскими картами.....20
1.4 Алгоритмы эксплуатации угроз и уязвимостей банковских систем. Социальная инженерия и обратная социальная инженерия.....29
2 Анализ технологий противодействия мошенничеству.....37
2.1 Практика мошенничества в системах ДБО, АБС. Средства выявления мошеннических действий, осуществленных со стороны Клиента/третьего лица/сотрудника Банка.....37
2.2 Принципы работы антифрод системы. Построение правил.....44
2.3 Анализ сомнительных операций на предмет наличия мошеннических действий со стороны клиента или сотрудника Банка.....54
3 Предложение по решению проблем обеспечения защиты в системах обработки больших данных в финансово-кредитных организациях.....66
3.1 Технологии структуризации данных для выявления утечек и уязвимостей.....66
3.2 Анализ имеющихся данных на аномалии путем их классификации…74
3.3 Конфигурирование механизмов защиты и мониторинга.....83
3.4 Предложения по технологии организации реагирования на инциденты 92
Заключение.....102
Список использованных источников.....104

Введение

Проблема повышения безопасности платежных операций становится все более актуальной вместе с развитием предоставления удаленных продаж и услуг. Привлечение новых пользователей в удалённые платежи позволяет мошенникам наращивать объемы получения преступного дохода. Рост числа операций требует поиска новых схем защиты, в том числе и технического характера.

Одной из таких современных систем защиты является система фрод-мониторинга, ориентированная на оценку финансовых транзакций в Интернете на предмет подозрительности с точки зрения мошенничества. Функционал системы предназначен на выработку рекомендаций по дальнейшему анализу и организации работы с подозрительными транзакциями.

Целью работы является исследование проблемы систем информационной безопасности на основе фрод-мониторинга.

Для достижения поставленной цели в работе предполагается решение целого комплекса задач:

- анализ проблемы использования платежных систем для мошеннических схем;
- изучение способов и методов реализации мошеннических действий со счетами и банковскими картами;
- анализ технологий противодействия мошенничеству;
- исследование принципов работы антифрод системы;
- выработка предложений по решению проблем обеспечения защиты в системах обработки больших данных в финансово-кредитных организациях.

Объектом исследования являются платежные операции и существующие схемы мошенничества при их проведении.

В качестве объекта исследования выступает организация безопасности платежных операций с использованием систем фрод-мониторинга.

Структура работы представлена тремя главами. Первая глава посвящена изучению проблемы использования платежных систем для мошеннических схем. В рамках первой главы рассматриваются также законодательные требования и требования Банка России к проведению и защите платежных операций и способы и методы реализации мошеннических действий со счетами и банковскими картами.

Вторая глава касается анализа технологий противодействия мошенничеству: отражены практики мошенничества с системами ДБО, АБС и средства выявления мошеннических действий.

Предложение по решению проблем обеспечения защиты в системах обработки больших данных в финансово-кредитных организациях представлены в рамках третьей главы.

-

1 Проблема использования платежных систем для мошеннических схем

1.1 Актуальность проблемы и основной понятийный аппарат по вопросам противодействия мошенничеству в кредитно-финансовой сфере

В настоящее время различного рода злоупотребления и правонарушения в банковской сфере относятся экспертами к значительным угрозам, оказывающим негативное влияние на экономические интересы любого общества. Интенсивное развитие и внедрение актуальных информационных технологий в мире повлекло за собой активизацию процессов формирования глобального информационного пространства, и, как неизбежный результат, привело к появлению новых вызовов и угроз [7].

Целесообразно остановиться на общем понятии платежной системы.

Платежная система является обязательным элементом кредитно-денежной системы, в состав которой входят заранее оговоренные процедуры, правила и механизмы перевода денежных средств с участием определенных организаций. Исходя из этого, ответственность за эффективное взаимодействие внутри платежной системы возлагается как на участников рынка, так и на официальных лиц, в частности, представителей центрального банка. Опираясь на опыт проведения рыночной реформы, можно утверждать, что платежная система, удовлетворяющая нужды частных и юридических лиц в сфере безопасного и эффективного перевода средств, представляет собой важный элемент инфраструктуры, которая необходима для перехода к рыночной экономике. Действительно, нельзя не отметить центральную роль хорошо отлаженной платежной системы в развитии межбанковского взаимодействия [13].

Существуют и другие определения. Так, специалистом ФРС США Б.Д. Саммерсом утверждается, что платежная система является обязательной

частью, в состав которой входит совокупность подсистем, состоящих из правил, соглашений, инфраструктуры, технологии механизма осуществления денежных переводов, методических указаний, регламентов. По его версии, платежная система – неотъемлемая часть кредитно-денежной системы.

В то же время, Поль Ван ден Берг описывает платежную систему в виде некоторой совокупности обязательств, которые принимают хозяйствующие субъекты. Реализация этих обязательств происходит в момент приобретения финансовых или материальных ресурсов, а также других ценностей.

Стандартный вид платежной системы представлен на Рисунок Error: Reference source not found.1.



Рисунок Error: Reference source not found.1 – Состав платежной системы

В любой платежной системе можно выделить следующие ключевые элементы:

- законодательная основа (нормативные акты, стандарты, правила, законы);
- механизм процедур консультационного характера;
- наблюдение, надзор;
- кооперация и внутрирыночное сотрудничество (соглашения, тарифы, регламенты, договоры).

Вообще говоря, развитие деятельности любой платежной системы зависит от совокупности факторов, среди которых ключевыми являются:

- относительно быстрое и повсеместное на современном этапе внедрение информационных технологий в функционирование платежных систем. Использование IT-технологий способствует повышению эффективности работы платежной системы, увеличению ее скорости работы и устойчивости;
- неуклонное возрастание роли центрального банка в деятельности платежных систем. С его стороны выполняется поведение оценки соответствия платежей системы стандартам международного образца, выдвигаются предложения, касающиеся внесения изменений в правила платежных систем, выполняется мониторинг деятельности уже существующих платежных систем;
- в настоящее время отмечается стремительное развитие предприятий финансовой сферы, в частности, в банковской отрасли постоянно появляются новые банковские продукты и услуги, наблюдается неуклонная глобализация финансовых рынков.

В связи с этим, центральным банком и другими органами, ответственными за регулирование платежных систем, должны обеспечиваться единые равные условия для функционирования между крупными банками, небанковскими кредитными предприятиями и некредитными предприятиями (общества с ограниченной ответственностью, акционерные общества). При этом должна быть учтена обширная база клиентов крупных банков, широкий спектр бизнес-моделей и доступ к информации.

Так как у крупных операторов платежных систем существует возможность использования значительной базы существующих клиентов для быстрого достижения глобального присутствия, является крайне важным своеврем5енность оценки регулятором рисков и последствий для глобальной финансовой системы.

Целесообразно рассмотрение некоторых значимых соображений, используемых в качестве основы для решения стабильности функционирования платежных систем. В данном случае среди них следует выделить

исключительно подмножество соображений, способствующих решению всего спектра приоритетов государственной политики.

Прежде всего, в платежных системах необходимо обеспечение общественного доверия, соответствие самым высоким стандартам с точки зрения нормативов и обеспечение необходимого всестороннего надзора и наблюдения. Это может быть начато, но не ограничено, соответствующими указаниями и постановлениями со стороны Банка России, также используются принципы инфраструктуры финансового рынка, которые закреплены комитетом по платежам и рыночным инфраструктурам (Банк международных расчетов). В данном случае речь идет о применении концепции фундаментального характера «тот же бизнес, те же риски, те же правила». Согласование нормативных подходов должно осуществляться на глобальном уровне, при этом должно быть обеспечено обнаружение любого пробела или несоответствия с последующим его устранением.

Платежными системами должна демонстрироваться надежная правовая основа во всех соответствующих юрисдикциях для организации должной защиты и гарантий для всех вовлеченных заинтересованных сторон и пользователей.

Кроме того, структура управления рисками должна быть разработана таким образом, чтобы были достигнуты операционная устойчивость и киберустойчивость. Также нельзя не учитывать риск ликвидности.

Наконец, необходимо обеспечение безопасности, осмотрительности, прозрачности управления активами, которые лежат в основе жизнедеятельности оператора платежной системы, а также их соответствие характеру обязательств. Это требуется для обеспечения широкой целостности рынка и уверенности пользователей платежных систем в безопасном проведении платежных операций.

К сожалению, в современных платежных системах недостаточна защита от организованной преступности, занимающейся отмыванием денежных

средств, которые получены незаконным путем, выводом капитала за рубеж, финансированием терроризма. Причиной этого является наличие огромного количества современных информационных технологий, финансовых инструментов, облегчающих данные операции, а также обезличенность денежных средств, которые находятся в обращении.

Каждый день во всем мире объем денежных средств, перечисляемых с помощью электронных систем, составляет около 2 триллионов долларов США. При этом наблюдается постоянная тенденция со стороны банков и других финансовых посредников к расширению своей деятельности в сети Интернет. Целью этого является значительное сокращение собственных административных затрат и получение возможности для своих клиентов повысить эффективность управления своими счетами. Помимо этого, жесткая конкуренция в данной сфере побуждает многие предприятия к проведению большей части своих бизнес-коммуникаций в сети Интернет, что в условиях недостаточного обеспечения защиты информации, увеличивает их уязвимость для злоумышленников.

Борьба с мошенничеством при использовании пластиковых карт является комплексным мероприятием, в которое должны быть вовлечены банки, платежные системы, правоохранительные органы.

Необходимым является совершенствование самих пластиковых карт, увеличение количества степеней ее защиты, в частности, с использованием микропроцессорных карт, чипов. В соответствии с данными, полученными на середину 2019 г., всего около 49% карт в Российской Федерации оборудовано микропроцессором.

Большая часть операций мошеннического характера становится возможной вследствие недостаточной надежности методов идентификации пользователей. Среди всех методов идентификации к наиболее надежным следует отнести сочетание логина и пароля. Вместе с тем, хакеры не считают подобный метод серьезной преградой, препятствующей совершению действий

мошеннического характера. Поэтому необходимым является разработка новых систем идентификации пользователей, например, систем идентификации пользователей с помощью карт доступа, специальных пластиковых карт с микрочипом. Эти карты вставляются в считывающее устройство специального типа с последующим вводом логина и пароля. При этом производится генерация микрочипом однократного кода, длина которого составляет 2048 бит. Этот код необходим для регистрации пользователя в сети, уничтожение данного кода происходит после выхода пользователя из сети.

Очевидно, что с помощью подобного метода можно предотвратить любые попытки злоумышленников, направленные на кражу пароля.

В последнее время получила широкое применение такая методика защиты, как биометрическая идентификация. При использовании такого способа осуществляется идентификация клиента в соответствии с отпечатками его пальцев или роговой оболочки глаза. Это приводит к практической невозможности доступа в систему злоумышленника, выполнившего похищение идентификатора, либо пароля. Вместе с тем, нельзя не учитывать достаточно высокую стоимость применения подобного метода, что, безусловно, накладывает дополнительные ограничения на степень его использования в практических разработках.

К наиболее уязвимым местам утечки информации могут быть традиционно отнесены точки подключения к сети Интернет и другим электронным сетям. Они чаще всего и являются теми «воротами», через которые в банковскую сеть стремятся внедриться хакеры. Для защиты банками, как правило, осуществляется установка межсетевых экранов (firewall), выполняющих фильтрацию сетевого трафика с целью недопущения несанкционированного проникновения, а также установка систем Content Security на серверы и рабочие станции. Эффективность определения операций мошеннического характера значительно возрастает благодаря проведению мониторинга всех транзакций.

Одна из задач банков заключается в обеспечении надежности систем защиты информации, регулярном осуществлении контроля за деятельностью собственных сотрудников, организации мониторинга (проверки) оборудования, средств защиты баз данных, программного обеспечения.

В ходе выявления, расследования и документального выявления эпизодов мошенничества с пластиковыми картами целесообразным является акцентирование внимания на совокупности признаков, анализ которых способствует определению возможных нарушений со стороны сотрудников банка. Среди этих признаков:

- отсутствие внятного и четкого разграничения функций сотрудников, в сферу ответственности которых входит оформление и выдача пластиковых карт, а также сотрудников, отвечающих за назначение персональных идентификационных номеров;
- отсутствие необходимого эффективного контроля за возвращенными почтовыми отправлениями (в случае рассылки пластиковых карт по почте);
- отсутствие эффективного мониторинга изменения имен и фактического адреса проживания клиентов банка;
- наличие систематических задержек, не вызванных объективной необходимостью, при выдаче клиентам банка пластиковых карт и персональных пин-кодов;
- отсутствие предельно допустимого лимита на размер снятия денежных средств через банкоматы в течение одних суток;
- наличие систематических сбоев в системе авторизации;
- отсутствие мониторинга и контроля за увеличением размера овердрафта по счету;
- отсутствие надлежащего контроля за неоформленными пластиковыми картами и пин-кодами.

Чтобы сократить число операций мошеннического характера с использованием пластиковых карт банковскому учреждению целесообразно принятие следующих мер:

- проведение комплексной проверки контрагентов при заключении договоров эквайринга;
- осуществление проверки кредитной истории держателя пластиковой карты;
- проведение всесторонней проверки подлинности документов и сведений, которые предоставляются контрагентом при выдаче пластиковой карты.

Следует учитывать наметившуюся во всем мире тенденцию объединения хакеров в группы, в частности, в международные, для централизованного совершения крупномасштабных мошеннических действий. Злоумышленниками с целью сокрытия собственной причастности к совершению преступлений используются различные методы, среди которых: похищенные реквизиты доступа в сеть Интернет, однократные выходы в сеть с присвоением различных IP-адресов, а также иные способы электронной конспирации [22].

В связи с этим для правоохранительных органов становится актуальным принятие мер, направленных на организацию обмена опытом, тесного сотрудничества при обнаружении и расследовании преступлений подобного характера. На базе МВД Российской Федерации должны быть созданы картотеки в соответствии с существующими признаками и механизмами подделки банковских пластиковых карт.

Очевидно, что появление новых технических возможностей приводит к изменению способов совершения преступлений. Вместе с тем, необходимые изменения в уголовного законодательстве, касающиеся преступлений в данной сфере, запаздывают. Например, осуществление сбора и хранения физическим лицом на персональном компьютере информации о действующих пластиковых картах (номерах, сроках действия, CVC, в том числе данных, получаемых с

магнитной полосы), в соответствии с законодательством Российской Федерации не относится к правонарушениям или преступлениям. Таким образом, уголовный кодекс России нуждается во внесении новых составов преступлений.

1.2 Законодательные требования и требования Банка России. Нормативные документы надзорных органов

Регламентация процессов осуществления платежей, которые касаются платежной системы Банка России, выполняется на основании основных документов по организации работы в платежной системе:

- Положение «О платежной системе Банка России» от 24 сентября 2020 г. N 732-П. [5];
- Положение «О требованиях к защите информации в платёжной системе Банка России» от 23.12.2020. N 747-П [6].

В рамках требований к защите информации в платежной системе Банка России определены основные ключевые аспекты защиты, которые связаны со строгой регламентацией процесса и ответственностью его участников.

При этом согласно положению «О платежной системе Банка России» от 24 сентября 2020 г. N 732-П. участниками процесса выступают:

- все кредитные организации, принимающие непосредственное участие в предоставлении услуг по переводу денежных средств в электронном виде;
- операционный центр, под операционным центром понимается организация, организующая в рамках платежной системы доступ к совершению операций по обмену с использованием средств электронных платежей, а также поддержку обмена с использованием сообщений;
- платежный клиринговый центр другой платежной системы (организация, занимающаяся определением и проверкой выполнения обязательств участников обмена в процессе сделки) в случае использования сервиса быстрых платежей;

- непосредственный оператор услуг, осуществляющий информационный обмен между участниками платежной операции, называемой обменом.

Дополнительно, требования к защите данных и обеспечению безопасности процесса обмена распространяются на:

- автоматизированные системы, участвующие в процессе обмена или обработки информации;
- программное обеспечение, выполняющее поддержку процесса обмена или его технического обеспечения;
- средства вычислительной техники, используемые в процессе обработки и передачи данных;
- телекоммуникационное оборудование, используемое в процессе обработки и передачи защищаемых данных.

Основные требования, предъявляемые к элементам описанной инфраструктуры, которая обеспечивает процесс обмена, заключаются в следующем:

- организация работы в выделенных (отдельных) сегментах сети, имеющих дополнительную защиту и поддерживающих политику разграничения доступа;
- элементы выделенного сегмента сети должны быть снабжены как минимум стандартным уровнем защиты, именуемым уровень 2 согласно ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций» [1].

Уровень защиты 1 определяется как усиленный, 2 – стандартный, 3 – минимальный. Обычно в финансовых организациях реализуются несколько контуров безопасности, в рамках которых устанавливаются разные уровни защиты [2].

Регламентированные Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах

персональных данных» [3] уровни защиты персональных данных распределяются по указанным уровням следующим образом:

- четвертый уровень обеспечивается минимальным уровнем защиты;
- третий и второй – стандартным уровнем;
- первый уровень – усиленным уровнем защиты.

В процессе предоставления услуг операционного характера и процессного клиринга необходимо обеспечивать в выделенных сегментах сети усиленный уровень защиты информации.

Участники процессов обмена и обеспечивающие их организации должны во внутренних документах определять порядок и состав применения организационных мер защиты, а также порядок применения технических средств.

Направления защиты информации, определенные ГОСТ Р 57580.1-2017:

- обеспечение защиты вычислительных сетей;
- обеспечение защиты при управлении доступом;
- контроль целостности и защищенности информационной инфраструктуры;
- защита от вредоносного кода;
- предотвращение утечек информации;
- управление инцидентами защиты;
- защиты среды виртуализации;
- защита информации при осуществлении удаленного логического доступа с использованием мобильных устройств.

Участники обмена должны сформировать в рамках внутренней документации следующие, регламентирующие работу с платежными операциями положения:

- о хранении , подготовке и передаче сообщений, сопровождающих платежные операции;

- о необходимом наборе технологических средств защиты, определяющих целостность, подлинность передаваемых электронных сообщений, включая определение криптографических средств защиты и принципов управления ключевой информацией;
- о регулировании деятельности направленной на непрерывность и восстановление деятельности при осуществлении переводов;
- об определении прав и обязанностей лиц, выполняющих сопровождение платежных операций и регламентации правил допущения специалистов к таким операциям;
- об определении прав и обязанностей лиц, выполняющих обеспечение защиты и восстановления в процессе платежных операций и регламентации правил допущения специалистов к таким операциям;
- об определении прав и обязанностей лиц, выполняющих хранение и формирование криптографических ключей и регламентации правил допущения специалистов к таким операциям [4].

1.3 Способы и методы реализации мошеннических действий со счетами и банковскими картами

В соответствии с информацией, предоставленной Computer Emergency Response Team (CERT), являющейся признанным международным авторитетом в сфере безопасности в сети Интернет, наиболее актуальные информационные технологии, средства компьютерной техники повсеместно применяются организованными преступными группировками, в частности, для легализации прибыли, полученной незаконным путем. По оценке аналитиков ОБСЕ сумма ежегодного ущерба для мировой экономики, причиной которого стало мошенничество, воровство и промышленный шпионаж в сети Интернет, составляет не менее 100 миллиардов долларов.

К наиболее активно развивающимся областям деятельности российских коммерческих банков можно смело отнести организацию безналичных расчетов населения с использованием пластиковых карточек. В соответствии с данными

Банка России, на 1 августа 2020 года число кредитных организаций, осуществляющих эмиссию пластиковых карт, составило 305, при этом количество эмитированных на территории Российской Федерации пластиковых карт составило 301,2 миллиона [8].

Очевидно, что рост количества пластиковых карт ведет к увеличению ущерба, связанного с мошенничеством с ними. Основываясь на аналитических материалах платежных систем VISA и MasterCard, ассоциация региональных банков оценивает ущерб от мошеннических операций с пластиковыми картами по итогам 2020 г. в сумму около 2 млрд. рублей, что составляет около 204% от аналогичных результатов предыдущего года. Эксперты постоянно говорят о постоянном росте ущерба от подобных махинаций.

Вместе с тем, точная статистика, отражающая число мошеннических операций с пластиковыми картами, до сих пор отсутствует. На это оказывает непосредственное влияние высокая латентность подобных преступлений. Кроме того, банки далеко не всегда стремятся к разглашению информации о мошеннических транзакциях или, тем более, о взломах без данных. Причина и тут очевидна – подобная информация негативно сказывается на деловой репутации банка. Согласно оценкам аналитиков, в поле зрения правоохранительных органов находится не более 16% всех совершаемых преступлений. Не вызывает сомнений факт, что сумма ущерба от мошеннических операций с пластиковыми картами растет неуклонно. Также следует отметить транснациональный характер подобных мошенничеств [11].

Практика правоохранительных органов свидетельствует о том, что к самому распространенному виду мошенничества с пластиковыми картами относится мошенничество, основанное на применении поддельных карт, и кража реквизитов действующих карт.

Злоумышленные действия, совершаемые с использованием пластиковых карт можно разделить на две группы: осуществляемые в системе банка и осуществляемые вне банка.

Первая группа преступлений включает в себя:

несанкционированная установка на карту кредитного лимита, что позволяет повысить авторизационный остаток на карточном счете с возможностью последующего снятия средств;

выпуск параллельной карты-двойника, преступный сговор с представителями торговых точек, несанкционированный выпуск новых пластиковых карт, несанкционированная установка в авторизационной системе специального статуса счета, дающего возможность в определенных пределах осуществлять снятие средств с карты [26].

Среди преступлений, совершаемых вне банка, следует выделить три большие категории, а именно:

преступления, осуществляемые с участием владельца пластиковой карты;

преступления, осуществляемые с применением украденных, поддельных карт или других данных идентификации;

преступления, заключающиеся в незаконном проникновении в хранилища данных, или во внедрении в различные специальные устройства [14].

Мошенничество владельца пластиковой карты может состоять в мошенничестве с долимитными суммами, а также с ложными заявлениями, касающимися утери или кражи карты.

В качестве примера можно упомянуть о случае, когда злоумышленником, на основании подложного общегражданского паспорта на чужое имя, в консульском отделе МИД России был получен подлинный заграничный паспорт на ту же фамилию. По предъявлению этого паспорта в филиале московского банка была получена дебетовая карта «Еврокард/Мастеркард» с первоначальным взносом 5000 долларов США. Далее, пребывая на территории Франции, и имея информацию об отсутствии средств на счете, который обеспечивает карту, злоумышленником были произведены оплаты этой картой

за услуги и товары, в том числе, получен напрокат автомобиль, который был угнан в Российскую Федерацию и продан там.

Злоумышленные действия, осуществляемые с помощью украденных, поддельных карт и данных идентификации, включают в себя:

- мошенничество с применением украденных карт;
- мошенничество с применением карт с частичной подделкой. Пример из практики: преступником были приобретены пластиковые карты четырех банковских структур «Золотая корона». После этого, с применением специального оборудования, была нарушена электронная защита пластиковых карт и, с применением специального программного обеспечения, внесены изменения в записанную на них информацию, что дало возможность неоднократного получения в банкоматах суммы, превышающей находящуюся на счете. В 2019 г. было раскрыто преступление, суть которого заключалась в использовании для получения наличных денег пластиковых карт. Группой лиц было зарегистрировано фиктивное предприятие для прикрытия преступной деятельности, связанной с обналичиванием денежных средств и уклонения от уплаты налогов. Сумма материального ущерба, который был причинен федеральному бюджету в виде неуплаченных налогов, оказалась более 197,5 млн. рублей. Проведенные оперативные мероприятия позволили изъять документы регистрационного и финансового характера, печати 32 фирм-однодневок, которые были частью схемы незаконной банковской деятельности, электронные ключи доступа к системе дистанционного управления счетами «Банк-Клиент», в том числе зарубежных предприятий, а также неучтенные наличные денежные средства в объеме более 3,6 млн. рублей, 38 кредитных банковских карт, оформление которых было выполнено на подставных физических лиц, заведенных для снятия наличных денежных средств;
- мошенничество торговой точки. Например, кассиром магазина в процессе продажи товара за наличные деньги, не осуществлялось оформление кассовых чеков покупателям. После окончания смены, выполнялся ввод в POS-

терминал данных пластиковых карт, предъявляемых держателями к оплате за товары в течение дня. При этом проставлялась сумма, заметно превышающая полученную от покупателей наличными. На слипах выполнялась подделка кассиром подписей держателей карт, за образец при этом брались чеки, хранившиеся в кассе;

- скиминг (копирование магнитной полосы). Для данного вида мошенничества необходимы устройства особого вида, осуществляющие считывание информации с магнитных полос карт. Скиммером выполняется считывание и запись информации на магнитной полосе. Другими словами, в руки злоумышленников попадают данные, являющиеся необходимыми для последующего изготовления поддельной карты и ее применения в собственных целях;

- вишинг (голосовой вишинг) – мошенничество, заключающееся в использовании технологии, дающей возможность выполнять сбор информации о реквизитах действующих карт в автоматическом режиме. При этом преступниками выполняется имитация звонка автоматического информатора, сообщающего о якобы проведении с картой владельца мошеннических действий и выдающего соответствующие инструкции. Суть этих инструкций – совершение звонка по указанному номеру. Принимающий звонки злоумышленник позиционирует себя, как сотрудник банка, и требует проведения сверки, в ходе которой и выясняет все необходимые данные;

- фишинг. Суть данного вида мошенничества – получение преступниками обманным путем реквизитов и пин-кода банковской карты. Наиболее часто осуществляется путем рассылки через сеть Интернет писем от имени банка или платежной системы. В этих письмах содержится просьба о подтверждении указанной конфиденциальной информации на сайте предприятия. В Российской Федерации увеличилось количество открытия веб-сайтов с предложениями различных финансовых услуг с применением банковских (платежных) карт международных платежных систем, в частности,

MasterCard и VISA. На этих страницах содержится предложение пользователям, касающееся заполнения электронных форм с указанием реквизитов и пин-кода банковских (платежных) карт. При передаче информации конфиденциального характера отсутствуют защищенные протоколы обмена информацией;

- мошенничество с применением номера счета. При взломе сети, преступники получают полный доступ к данным, касающихся номеров действительных пластиковых карт, сроков их действия и имен держателей (владельцев). Основываясь на этих данных, злоумышленники осуществляют перевод средств на счет виртуальной фирмы или магазина. После этого, используя предлог отказа от покупки, выполняется возврат электронных денег на счет злоумышленника, и, далее, легкое обналичивание денежных средств;
- «белый пластик». Данный способ заключается в эмбоссировании номеров действительных пластиковых карт на заготовках пластика, имеющих стандартный размер. Осуществляется копирование магнитной полосы с карты, например, с помощью, скимера. Для использования «белого пластика» мошенниками заключается сговор с кассирами торгового предприятия, чаще всего для операций с «белым пластиком» выполняется создание подставных фирм. В 2018 г. преступниками была получена информация, касающаяся уязвимого места компьютерной защиты компании PBS WorldPay (расположена в Атланте, является подразделением Royal Bank of Scotland), ориентированной на оформление платежей, в том числе, по дебетовым и кредитным картам. В качестве объекта взлома были выбраны дебетовые карты, привязанные к счетам, на которые выполнялось перечисление заработной платы работодателями сотрудникам. В течение четырех дней преступниками (гражданами Эстонии, Молдовы и России) выполнялся взлом компьютеров PBS и хищение из ее баз данных номеров дебетовых карт с их пин-кодами. После этого номера и коды похищенных 48 карт были сообщены подельникам, которые осуществили изготовление фальшивых карт и нанесение на них похищенных данных. Спустя короткий срок времени, сообщниками была

выполнена попытка снятия денег из банкоматов в Эстонии, в результате чего через несколько часов была похищена сумма в размере 293 тыс. долларов. Так как на счетах истинных держателей карт находились небольшие суммы, злоумышленники через компьютеры PBS выполнили повышение кредитного лимита, иногда до нескольких сотен тысяч долларов. В течение следующих суток из более чем 2000 банкоматов в 273 городах мира было снято около 10 млн. долларов. При этом у себя злоумышленники оставляли от 35% до 50% украденной суммы, остаток же отправлялся хакерам через фирмы WebMoney и Western Union;

- мошенничество с применением поддельных карт. Следует привести иллюстративный пример. Сотрудники Управления «К» МВД России в 2018 г. пресекли деятельность участников организованной преступной группы, занимавшейся на протяжении нескольких лет производством поддельных пластиковых карт и хищением денежных средств со счетов законных владельцев. Жертвами такого незаконного бизнеса стали как банки Российской Федерации, так и восемь крупных банков Германии, Франции, США, Бразилии. Каждый из участников преступной организации являлся пользователем сети Интернет и пользователем одного из сайтов, осуществлявшего продажу данных о реквизитах действующих карт (номерах действующих карт, сроках их действия, Card Verification Value (Card Validation Code, CVC)). Местоположением сайта являлись Кокосовые острова. Одним из участников осуществлялся доступ неправомерного характера к серверам процессинговых центров банковских предприятий и копирование информации, касающейся держателей пластиковых карт. После этого обеспечивалось поступление данных к организатору, который, с помощью термо-сублимационного принтера, выполнял изготовление пластиковых карт с магнитной полосой и логотипами банков. Далее, с помощью специального устройства «энкодера» производилась запись похищенной банковской информации на пластиковые карты. Применяя подобные подделки, члены организованной преступной

группы осуществляли в крупных торговых сетях покупки дорогостоящих товаров с последующей их реализацией. Весь доход собирался в «бюджете» преступной группы. В течение периода с февраля по апрель 2018 г. было выявлено 365 финансовых операций, которые были проведены злоумышленниками. Размер общего ущерба, нанесенного действиями злоумышленников, составил 127 миллионов рублей.

Преступления, использующие несанкционированное проникновение в хранилища данных или внедрение в различные устройства можно разделить на следующие группы:

- использование фальшивых банкоматов. Вставив карту и набрав пин-код пользователь обычно видит на дисплее фальшивого банкомата сообщение об отсутствии денег в банкомате или о неисправности банкомата. За это время мошенниками выполняется копирование данных с магнитной полосы карты и ее пин-кода
- взлом баз данных платежных систем и торговых точек. Так например, гражданином США с помощью хакерских атак с 2016 по 2018 годы было похищено данных 140 млн. карт путем взлома платежной системы Heartland Payment Systems, кроме того данных 3,7 млн. карт путем взлома данных супермаркетов Hannaford Brothers Co, а также данных трех торговых сетей. Совместно с другим злоумышленником хакером устанавливалось на взломанных компьютерах программное обеспечение, обеспечивающее им многоразовый доступ в систему. Атаки осуществлялись с серверов, расположенных в Калифорнии, Иллинойсе, Нью-Джерси, Голландии, Латвии, на Украине. На серверах находились вредоносные программы, а также украденные данные, касающиеся пластиковых карт и их держателей. В соответствии с предварительными данными, сумма ущерба превысила 420 млн. долларов. Также в 2019 г. был произведен арест гражданина Украины, который в течение трех лет (2014-2016 гг.) присвоил около 12 млн. долларов путем совершения мошеннических операций, связанных с продажей данных

похищенных кредитных и дебетовых карт, большей частью принадлежащих гражданам США;

- внедрение вредоносного программного обеспечения. Согласно информации Федерального бюро расследований США, осенью 2019 года на серверы, принадлежащие финансовой компании Citigroup, была осуществлена хакерская атака. Следователями было установлено, что похищение паролей клиентов банка выполнялось с помощью программы Black Energy, автором которой являлся российский хакер с ником Cr4sh. Продажа программного обеспечения, содержащего Black Energy, осуществлялась в сети Интернет по цене 700 долларов. В соответствии с данными Wall Street Journal, общий объем потерь клиентов Citibank может составлять десятки миллионов долларов. В частности, у совладельца компании Bridge Metal Industries, Роберта Бланчарда преступниками могло быть похищено и переведено на счета в Латвии и на Украине не менее одного миллиона долларов. Показателен еще один пример. В 2019 году сотрудники отдела «К» УВД по Курганской области пресекли деятельность организованной преступной группы, члены которой в течение двух лет занимались подделкой пластиковых карт и хищением денежных средств с банковских счетов. Для этого использовался неправомерный доступ к счету через сеть Интернет. Злоумышленники осуществляли с помощью вредоносных программ хищение ключей электронно-цифровой подписи для получения доступа к банковским счетам, а также данные пластиковых карт частных лиц. После этого выполнялась регистрация фиктивных предприятий и оформление расчетных карт для обналичивания украденных денежных средств. Размер ущерба, нанесенного злоумышленниками, оценивается 11 млн. рублей;

- применение в банкоматах так называемой «ливанской петли», то есть пластиковых конвертов, немного превышающих своими размерами стандартные пластиковые карты, закладываемые в банкоматы. Попытка снятия наличных средств в банкомате вызовет невозможность считывания устройством данных с магнитной полосы и невозможность извлечения карты

владельцем. В это время следует совет от злоумышленника, находящегося рядом, о необходимости ввода пин-кода. После его ввода карта все так же не извлекается и владелец покидает место для связи с сотрудниками банка. Далее злоумышленник производит извлечение карты, которая затем может быть использована для снятия наличных денег в банкомате, поскольку ее пин-код уже известен.

1.4 Алгоритмы эксплуатации угроз и уязвимостей банковских систем. Социальная инженерия и обратная социальная инженерия

Под термином «социальная инженерия» понимается методика получения злоумышленником требуемой информации или управления действиями человека без применения технических средств. Другими словами, социальная инженерия представляет собой использование исключительно методов воздействия на людей психологического характера, среди которых, убеждение, хитрость, внушение доверия. За основу в методах социальной инженерии всегда берется манипуляция такими базовыми основополагающими человеческими эмоциями, как жадность, страх, эмпатия. Главной задачей социального инженера можно считать «подбор ключа» к каждому конкретному человеку с последующей игрой на его эмоциях и чувствах таким образом, чтобы он не думал об осторожности и совершал требуемые злоумышленнику действия.

Итогом успешных атак с использованием методов социальной инженерии является предоставление жертвой (часто добровольно и без особых подозрений) важных данных (логинов и паролей учетных записей, реквизитов банковских карт), либо необходимых возможностей, связанных с получением доступа к целевой системе в обход ограничений безопасности.

В качестве типичного примера атаки социального инженера можно упомянуть о звонке или рассылке сообщений клиенту банка от лица сотрудника данного банка. Клиенту поступает сообщение о блокировке его карты и под

предлогом восстановления карты предлагается предоставление реквизитов и кодового слова.

Методы социальной инженерии используются следующими категориями:

- blackhat-хакеры: имеют мощную развитую техническую базу, продвинутые навыки социальной инженерии и взлома информационных систем. Данная категория, чаще всего, преследует исключительно собственные корыстные интересы;
- промышленные шпионы: осуществляют ведение незаконной деятельности, ориентированную на хищение информации конфиденциального характера, принадлежащей конкурентам заказчика;
- частные детективы: выполняют легальный поиск информации для заказчика;
- whitehat-хакеры (пентестеры): сотрудники предприятий, осуществляющих свою деятельность в области информационной безопасности, а также независимые исследователи. Деятельность этой категории направлена на тестирование информационной системы заказчика на наличие различных уязвимостей.

Атака социального инженера обычно включает в себя следующие этапы:

1. Сбор как можно более полной информации о целевом объекте.
2. Подготовка сценария действий и наиболее эффективных средств для атаки (вредоносные вложения, фишинговые ресурсы и т.п.).
3. Установка связей и получение доверия со стороны жертвы.
4. Достижение цели, для которой совершалась атака (получение требуемой информации).

Как уже было сказано, начало атаки заключается в сборе информации о целевом объекте (в данном случае, будет идти речь об атаке не на физическое, а на юридическое лицо). Для этого желательной будет следующая информация:

- перечень имен и занимаемых должностей сотрудников;
- организационная структура предприятия;

- применяемые на предприятии технические средства и установленное программно-аппаратное обеспечение;
- любые данные о конкурентах, партнерах и контрагентах предприятия;
- принятый на предприятии жаргон и терминология;
- архитектура корпоративной вычислительной сети предприятия;
- адреса электронной почты, внутренние телефонные номера, номера мобильных телефонов сотрудников предприятия.

Очевидно, что больший собранный злоумышленником объем информации повышает вероятность успеха. Для добычи первичной информации чаще всего используется разведка из открытых источников (OSINT – Open Source Intelligence). Адреса электронной почты и номера мобильных телефонов часто можно взять с сайта предприятия или из рекламных проспектов. Для получения необходимых сведений можно осуществить их покупку у информационных брокеров, которые представлены в даркнете, либо в сообществах криминального характера. К сожалению, сами сотрудники нередко предоставляют требуемую информацию, которая не относится к конфиденциальной, например в ходе телефонного разговора с атакующим, представляющимся коллегой из другого департамента, клиентом, подрядчиком предприятия.

После сбора информации социальным инженером осуществляется разработка сценария действий. При этом им заранее определяется:

- с кем будет производиться общение (сведения о конкретном человеке могут быть легко найдены, например, в социальных сетях);
- какие именно средства наиболее целесообразны для установки контакта (телефонный звонок, личный разговор, переписка по электронной почте);
- кем лучше всего представиться;
- какие темы должны быть затронуты в процессе общения;

- пути входа в доверие;
- получение какой информации или выполнение какого действия будет являться конечной целью общения.

В качестве жертвы атаки с применением социальной инженерии может быть выбран любой человек. К сожалению, универсальное средство защиты от них отсутствует. Вопрос состоит только в степени изощренности и достоверности схемы обмана, придуманной социальным инженером, для входа в доверие и побуждения своей жертвы к совершению требуемых и заранее спрогнозированных действий.

Целью атак социальных инженеров могут стать как обычные пользователи, так и сотрудники различных предприятий и банков. В первом случае ключевым мотивом злоумышленника почти всегда является корысть, во втором мотивов может быть несколько: получение доступа в корпоративную сеть с целью хищения данных, нарушение полноценного функционирования информационных систем, конкурентная разведка. Следует отметить, что даже наличие надежной защиты с помощью актуальных технических и аппаратных средств и изоляция от сети Интернет информационной системы не является гарантом отсутствия ее уязвимости к атакам такого рода. Причина этого заключается в действии «человеческого фактора».

Социальную инженерию можно рассматривать как один из этапов заранее спланированной компьютерной атаки. Действительно, для преступника более легким представляется начальный «взлом» человека и получение доступа к системе, либо убеждение жертвы в необходимости самостоятельного запуска на компьютере вредоносного файла, нежели поиск и эксплуатация технических уязвимостей.

В соответствии с информацией, предоставленной институтом InfoSec в 2020 г., следующие методы относятся к наиболее частым атакам социальной инженерии:

- фишинг (phishing). Атака подобного рода заключается в использовании злоумышленником сообщения, отправляемого по электронной почте, SMS, клиенте для обмена мгновенными сообщениями, в социальных сетях для получения конфиденциальной информации от жертвы или обманным путем вынудить ее перейти по ссылке, которая ведет на веб-сайт вредоносного характера. Цель фишинговых сообщений – привлечение внимания жертвы и призыв к действию путем возбуждения любопытства, просьб о помощи или вызова других эмоциональных спусковых механизмов. В них часто находят свое отражение логотипы, стили текста, изображения для подделки личности, путем создания впечатления, что источником сообщения является коллега по работе, банк жертвы или другой официальный канал. Кроме того, большая часть фишинговых сообщений спекулирует на факторе срочности, возбуждая в жертве впечатление, что промедление в передаче информации конфиденциального характера неизбежно приведет к негативным последствиям;
- атака китобоя (whaling attack). Данная атака представляет собой тип фишинговой атаки, ориентированной на определенных пользователей, имеющих привилегированный доступ к системам или доступ к конфиденциальной информации повышенной ценности. Например, целью атаки китобоя могут являться старшие руководители, состоятельные люди или сетевые администраторы. Сложность атаки китобоя выше, чем у обычной фишинговой атаки. Преступники осуществляют тщательную разработку для создания сообщения, которое принудит определенные цели дать ответ и выполнить требуемое действие. Письма подобного рода нередко маскируются под критически важные деловые письма, отправленные коллегой, ведущим менеджером, сотрудником, нуждающимися в срочном вмешательстве со стороны жертвы;
- атаки «приманка» и «услуга за услугу» (baiting and quid pro quo). В атаке «приманка» злоумышленниками предоставляется то, что жертва относит

к полезному. В этом качестве может выступать предполагаемое обновление программного обеспечения, являющееся, фактически, вредоносным файлом, зараженным USB-токеном с меткой, которая указывает, что в нем находится ценная информация, а также другие методы. Атака «услуга за услугу» (quid pro quo) аналогична атаке «приманка», но вместо обещания предоставления чего-либо полезного от злоумышленников поступает обещание выполнения действия, полезного для жертвы, но требующего от нее действия в обмен. Например, злоумышленником могут быть вызваны случайные внутренние телефонные номера на предприятии под видом перезвона по запросу службы технической поддержки. При ответе человека, у которого действительно существует проблема, делается вид оказания помощи, однако при этом жертва инструктируется к выполнению действий, ставящих под угрозу ее компьютер;

- предлог (pretexting). Атака «под предлогом» заключается в создании злоумышленником поддельной личности и использовании ее для манипуляции своими жертвами и предоставлении информации личного характера. Например, злоумышленник может представиться внешним поставщиком IT-услуг и сделать запрос данных учетной записи пользователя и паролей для помощи им в решении проблемы. Другой вариант – притвориться финансовым учреждением жертвы, чтобы запросить подтверждение номера их банковского счета, либо учетных данных веб-сайта жертв;
- водопой (watering hole). Данный вид атаки состоит из запуска или загрузки вредоносного кода со вполне легального и легитимного веб-сайта, посетителями которого являются цели атаки. Например, злоумышленниками может быть скомпрометирован сайт новостей финансовой индустрии, если у них есть информация, подтверждающая возможность его посещения людьми, работающими в сфере финансов и, таким образом, представляющими привлекательную цель. Взломанный сайт, чаще всего, осуществляет установку трояна-бэкдора, дающего преступнику возможность взлома и дистанционного управления устройством жертвы. Атаки «водопой» обычно используются

опытными злоумышленниками, которые обнаружили эксплойт нулевого дня. Может быть сделана пауза перед атакой в несколько месяцев для сохранения ценности найденного ими эксплойта. Иногда запуск атаки «водопой» осуществляется не против веб-сайта, а непосредственно против уязвимого программного обеспечения.

Среди других атак социальной инженерии (потенциально, ставящих под угрозу системы и конфиденциальные данные жертв):

- vishing – голосовой фишинг. Как следует из названия, аналогичен фишингу, однако для его осуществления требуется звонок жертве по телефону;
- кража при переадресации – выполняет перенаправление доставщика или посыльного в неправильное место, после чего занимает их место для овладения конфиденциальной посылкой;
- задняя дверь – злоумышленник проникает в охраняемый объект, двигаясь за кем-то, обладающим санкционированным доступом, после чего обращается к нему с просьбой «просто придержать дверь», чтобы он так же мог войти;
- медовая ловушка – злоумышленник изображает привлекательного человека и выполняет фальсификацию онлайн-отношений для получения информации конфиденциального характера от своей жертвы;
- scareware – осуществление отображения на устройстве пользователя уведомлений, которые дают им основания думать, что они заражены вредоносным программным обеспечением и требуют установки программного обеспечения (вредоносных программ злоумышленника) для лечения своей системы.

Кроме того существует, так называемая обратная социальная инженерия. Это методика, при которой жертва в результате действий злоумышленника вынуждена сама просить у него помощи. Такой метод характерен для преступников, которые представляются сотрудниками технической поддержки. Такая атака выполняется в несколько этапов. Например, сначала

злоумышленником осуществляется создание на компьютере жертвы обратимой неполадки. После этого каким-то образом отправляет сообщение пользователю о своей готовности решить подобные технические проблемы (осуществляет размещение объявления или собственных контактов рядом с рабочим местом пользователя или там, где он их точно увидит). Далее, пользователь сам обращается к злоумышленнику за помощью, а тот выполняет решение проблемы, попутно получая требуемый для своих целей доступ к компьютеру.

2 Анализ технологий противодействия мошенничеству

2.1 Практика мошенничества в системах ДБО, АБС. Средства выявления мошеннических действий, осуществленных со стороны Клиента/третьего лица/сотрудника Банка

Основная проблема корректной организации дистанционного банковского обслуживания состоит в серьезном росте процента операций. При этом около 80% клиентов банков используют электронные платежи для приобретения не менее четверти всех товаров и услуг. Расширение цифровых каналов породило специализированные онлайн-банки, которые осуществляют исключительно электронные платежи. В связи со стремительным развитием дистанционного облуживания банки вынуждены сокращать свои реальные отделения и сотрудников, что приводит к снижению уровня безопасности отслеживания операций.

Использование электронного платежа практически не оставляет банку времени на проверку самой транзакции и отправителя и получателя. Соответственно, стандартные признаки мошеннической транзакции, которую мог бы уловить сотрудник при наличии определённого времени и доступа к информации, могут быть реализованы без специальной подготовки. Электронные платежи также в значительной мере снижают вероятность возмещения, так как риски не отследить мошенническую транзакцию вырастают в разы: за несколько секунд средства со счета могут перейти через несколько счетов и осесть в оффшорных зонах, возврат средств из которых практически невозможен в связи с особенностями используемого законодательства в банковской сфере.

Относительно новым видом мошенничества стали так называемые операции без присутствия карты (Card Not Present transaction, CNP). Они

представляют собой тип транзакций по банковским платежным картам, при которых физическое присутствие держателя карты со своей картой во время и в месте осуществления оплаты не требуется. Наиболее характерной данная операция является при заказе и оплате товара через сеть Интернет, по факсу, телефону, почте (Mail Order/Telephone Order (MO/TO)). Очевидно, что подобные транзакции стали весьма привлекательными для злоумышленников.

Основной трудностью для продавца, принимающего заказ, в операциях без присутствия карты можно считать осуществление проверки, было ли разрешение со стороны держателя карты на проведение транзакции. Чаще всего, выполняется проверка номера карты (PAN), верификационного кода (например, для карт типа Visa – это CVV2), а также срока действия карты (expired).

При заявлении о факте мошенничества типа CNP на банк-эквайрер, выполняющий обслуживание счета продавца, на который выполняется поступление денежных средств от мошеннической операции, возлагается ответственность по возмещению средств. В то же время, ответственность за возврат при операциях с магнитной полосой возлагается на эмитента карты. Повышенный риск операций диктует необходимость некоторым эмитентам карт взимания увеличенной оплаты за осуществление CNP. В качестве защиты для эквайрера используется протокол 3-D Secure, дающий возможность осуществления дополнительных проверок держателя карты и переноса ответственности на банк-эмитент.

В соответствии с данными «Лаборатории Касперского» в русскоязычном сегменте сети Интернет наблюдается тенденция к повышению объемов так называемого scam (мошенничество с авторизованными платежами), а также онлайн-объявлений и рассылок мошеннического характера. Цель подобных операций проста – выманивание денежных средств пользователей. По итогам первого полугодия 2020 года аналитиками компании было обнаружено не менее 23 тысяч ресурсов подобного рода, что практически в четыре раза

больше по сравнению с аналогичным периодом прошлого года. Число попыток перехода пользователей на scam-страницы также возросло почти в два раза и составило 28 миллионов.

Фактически, scam является сообщениями, в которых злоумышленники предлагают пользователям достаточно крупное денежное вознаграждение в обмен на прохождение опроса или участие в определенной акции. Для получения денежных средств пользователю необходимо осуществить оплату «комиссии» или «закрепительного платежа». Чаще всего, эта сумма является незначительной, в настоящее время она составляет около 350 рублей. Однако, что естественно, никакие выплаты пользователю не поступают, а «комиссия» поступает на счет мошенников. Кроме того, пользователь, выполнивший ввод данных карты, получает дополнительный риск, связанный с сохранностью своей платежной информации.

Согласно данным исследования, можно утверждать о росте мошеннических ресурсов, на которых размещены предложения о выплате пользователям различных социальных выплат. С начала 2020 года «Лабораторией Касперского» было выявлено в 5 раз больше подобных страниц, чем за первое полугодие 2019 года. Мошенниками часто осуществляется имитация оповещения от несуществующих фондов на предмет финансовой помощи, пособий, страховых взносов, доплат, а также иных видов доплат.

Для предотвращения таких угроз специалистами «Лаборатории Касперского» предлагается помнить об основополагающих правилах безопасности, заключающихся в недопустимости перехода по подозрительным ссылкам в социальных сетях и почте, а также в скептическом и здравом отношении к сообщениям, касающимся крупного выигрыша или неожиданной выплаты.

Основными инструментами банка, позволяющими снизить риск мошеннических переводов, на данный момент являются установки лимитов и увеличение уровней идентификации транзакций.

Дополнительным методов для усиления безопасности является идентификация не только отправителя, но и получателя, а также необходимость предоставления не только счета на оплату, но и получаемой квитанции. Такое средство защиты связано с участившимися случаями, в которых мошенники представляются телекоммуникационными или другими компаниями, предоставляющими услуги, и предлагают оплатить счет. Проверка квитанций получателя снижает риск отправки средств по звеньям длинных транзакций.

Как показывает практика, в случае использования дистанционного банковского обслуживания, основную роль в борьбе с мошенническими действиями должны играть сами клиенты, которые и осуществляют переводы своих средств на счета сторонних организаций. При этом банки должны предоставлять клиентам полную информацию о возможных вариантах мошенничества и средствах защиты от него.

Получая данные о мошеннических действиях в сфере ДБО, банки используют следующие внешние каналы (Рисунок Error: Reference source not found.2):

- сообщения от клиентов (89%%);
- данные от третьих лиц (55%).

На стороне банка:

- отслеживание проводят специализированные автоматизированные системы (до 82%);
- осуществление внутреннего и внешнего аудита (58%);
- получение данных от информаторов (до 68%).

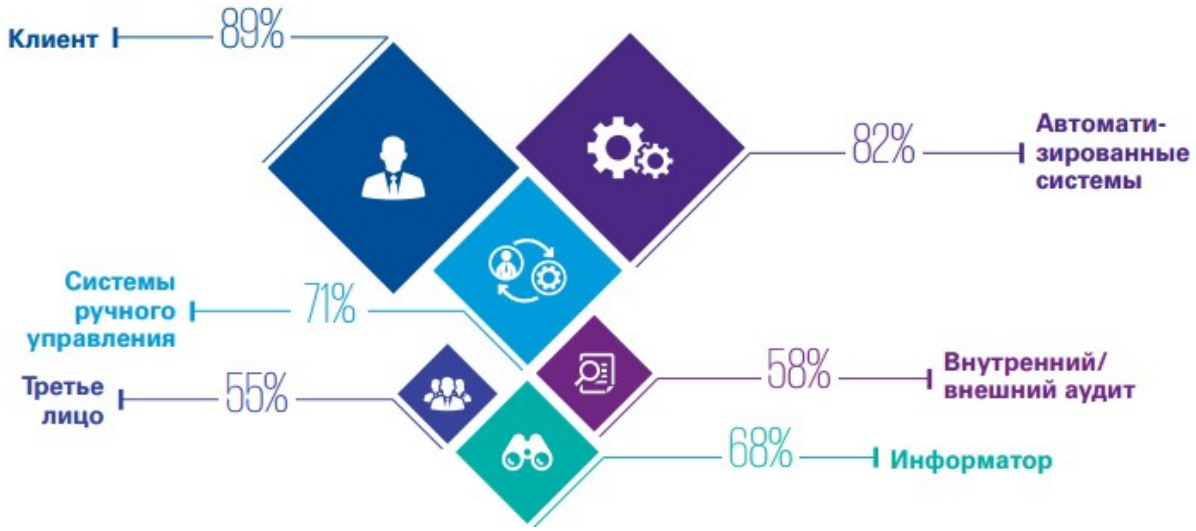


Рисунок Error: Reference source not found.2 – Распределение по источникам выявления мошеннических действий [24]

Также следует остановиться на особом виде мошенничества, связанном с использованием АБС (автоматизированная банковская система).

Злоумышленники в определенной мере переориентировались и пытаются убедить людей в существовании угрозы их накоплениям. Другими словами, вместо сценарий поступления сообщений типа «с вашего счета выполнен перевод денежных средств» осуществляется другой – сообщения «существует непосредственная угроза вашему депозиту». Вместе с тем, суть мошенничества осталась неизменной – необходим перевод денежных средств на безопасный, защищенный счет. С этой целью от человека требуется добровольная передача данных карты, кодов из SMS-сообщений и т.д. Такой интерес со стороны злоумышленников легко объясним – депозиты представляются гораздо более интересной мишенью, чем остаток денежных средств по обычному счету, поскольку появляется возможность одномоментного получения значительной суммы денежных средств. Данное смещение интереса может означать, что в массовом сегменте, в котором на величину дохода мошенника оказывало непосредственное влияние количество обзвонов жертв, намечается тенденция снижения величины прибыльности. При этом количество обзвонов неуклонно растет, однако их результативность очевидно снижается. Отсутствует существенное увеличение сумм похищенных денежных средств. Также

специалистами отмечается, что процент несанкционированных операций в общем объеме платежей снижается. Кроме того, отмечаются попытки злоумышленников совершать звонки несколько раз по одному и тому же номеру, да еще и в течение нескольких дней подряд. Это может свидетельствовать либо о наличии нескольких групп мошенников, либо об одной, но у которой наблюдается дефицит доходов. Фактически, процент удачных звонков (со стороны злоумышленников), увенчавшихся хищением денежных средств, уменьшается. На снижение эффективности массовых обзвонов несомненно оказало влияние и повышение информированности граждан о существовании обзвонщиков-мошенников, увеличение настороженности к звонкам с неизвестных номеров.

Как известно, для совершения звонков злоумышленникам необходима клиентская база. В последние годы рост утечек в финансовом секторе не наблюдается. Можно утверждать об относительной стабильности черного рынка нелегальной информации, касающейся персональных данных. Разговор о каких-то всплесках в данной отрасли является неуместным и не подкрепленным фактами. Продажа подобных утечек осуществляется в гораздо меньшем объеме, чем утверждается самими злоумышленниками. Интересен тот факт, что на этом черном рынке стало появляться большое количество мошенников, обманывающих других мошенников. Ими заявляется о существовании миллиона, например, записей из банка, тогда как в реальности они могут предложить, в лучшем случае, несколько тысяч подобных записей, при этом они получены не из банка, а в результате утечки из других организаций или представляют собой скомпилированную выборку из источников открытого типа, например, социальных сетей. На подобных рынках представлено большое количество материалов, выдаваемых за актуальные данные, тогда как в действительности они являются очень давними утечками, не представляющими особого интереса.

Безусловно, необходимо ужесточение правил защиты информации в различных организациях, однако даже это не является полным решением проблемы. Люди сами разглашают о себе, например, в социальных сетях, интернет-магазинах, фишинговых сайтах информацию, представляющую интерес для злоумышленников, и об этом необходимо помнить.

Кроме того, проблема утечек должна рассматриваться комплексно. Кража данных осуществляется в целях использования в противоправных действиях. Используя технологии социальной инженерии, обзвонщики побуждают людей к совершению поступков, приводящих к утечке денежных средств от законного владельца к злоумышленнику. Выполняя сравнение объемов утечек из банков с количеством людей, которым поступают звонки от злоумышленников, можно отметить диспропорцию: звонки мошенниками осуществляются гораздо большему количеству людей, чем число клиентов банков, данные которых были похищены. Это позволяет сделать вывод, что проблема утечек является характерной не только и даже не столько для банковских учреждений.

В отличие от ситуации, сложившейся со внешним мошенничеством, специалистами отмечается, что общая и средняя сумма потерь, а также число случаев внутреннего мошенничества в последние годы остается на одном и том же уровне. Вместе с тем, данное утверждение может неадекватно отражать реальную угрозу совершения операций мошеннического характера, которые осуществляются внутри банковских учреждений, так как практический опыт свидетельствует о том, что при совершении внешних действий мошеннического характера часто совершается с помощью сговора между злоумышленниками и сотрудниками банков, хорошо владеющими спецификой функционирования банковских систем, средств контроля и процессов (фактически, всех сфер, не попадающих в зону ответственности систем контроля, а также всеми недочетами в существующих средствах контроля) [18, 19].

С учетом возможности для сотрудников банковских организаций использования уязвимых мест средств контроля для хищения наиболее значимых активов банка, размер потенциального ущерба от внутреннего мошенничества может быть столь же значителен, как и от внешнего, если не более. В соответствии с реальным характером данной угрозы, в банковских организациях существует необходимость продолжения активного поиска возможностей, направленных на выявление случаев мошенничества со стороны собственных сотрудников.

2.2 Принципы работы антифрод системы. Построение правил

Как уже было сказано выше, роль сервисов дистанционного банковского обслуживания (ДБО) в сегменте продуктов, предлагаемых банками физическим и юридическим лицам, неуклонно растет. Объемы платежей, осуществляемых через ДБО, постоянно увеличиваются. Значительная часть стратегии развития банковского бизнеса неотъемлемо связана с повышением объема подобных сервисов, увеличением качества и скорости их функционирования. Такой подход способствует, очевидно, повышению степени лояльности клиентов банка, снижению расходов на операционную деятельность с одновременным повышением оперативности и удобства осуществления платежных операций. Вместе с тем, увеличивающиеся объемы удаленных банковских транзакций влекут за собой рост мошеннических действий в рамках сервисов дистанционного банковского обслуживания. Не является секретом, что в Российской Федерации доля операций мошеннического характера, выполняемых через каналы ДБО, занимает свое место в тройке видов операционного банковского мошенничества, начиная еще с 2010 года.

Специалистами отмечается возможность повышения значимости мошеннических операций в общем объеме платежей в несколько раз в течение одного года. Такие темпы роста, очевидно, свидетельствуют о невозможности снижения объемов мошенничества до приемлемого уровня только за счет усиления процедур, связанных с обеспечением целостности и

конфиденциальности данных, или внедрения передовых технологий, направленных на обеспечение аутентичности выполняемых операций.

На сегодняшний день большей частью банковских организаций уже выполнена оценка (положительная) эффективности применения технологий контроля, не зависящих от клиента. Другими словами, можно отметить нацеленность банков на использование таких инструментов для определения и предотвращения действий мошеннического характера, которые никак не зависят от соблюдений клиентом общих требований информационной безопасности.

В данном случае, речь идет о системах фрод-мониторинга (Fraud Monitoring) или Fraud Management System (FMS). В основе возможности подобных систем осуществлять идентификацию незаконных операций лежат методы формирования правил и политик, дающих возможность выполнять детектирование хищений [9].

С повышением степени развития и гибкости инструментов настройки и моделирования в системе потенциально увеличиваются возможности, связанные с определением мошенничества, предоставляемые ею. Помимо этого, системы подобного рода дают возможность определения не только совершаемых атак, но и предотвращения готовящихся краж путем всестороннего исследования процессов на клиентской стороне.

Практический опыт применения систем типа Fraud Monitoring или FMS свидетельствует, что внедрение систем данного типа повышает возможности банка, связанные с предотвращением существенного количества хищений денежных средств со счетов клиентов через сервисы дистанционного банковского обслуживания [20].

Общую схему функционирования практически любого механизма фрод-мониторинга можно описать следующим образом: в момент совершения оплаты с помощью банковской карты осуществляется сбор совокупности показателей определенного типа (у каждой из антифрод-систем они

различаются) – это и IP-адрес компьютера, и статистика оплат по данной карте и многое другое. Число фильтров может достигать сотни (например, система электронных платежей PayOnline насчитывает более ста двадцати фильтров). В системе содержится набор определенных правил, то есть лимитов фильтров безопасности. Каждым из фильтров осуществляется проверка пользователя, а именно его персональных и карточных данных [23, 25].

Основная цель подобной системы заключается в подтверждении того, что пользователь является реальным владельцем карты, осуществляющим определенную покупку на сайте. При определении активности подозрительного характера, то есть превышении какого-нибудь установленного параметра, происходит автоматическая блокировка фильтром возможности осуществления платежа по этой карте. Целесообразно пошаговое рассмотрение антифрод-системы [10].

Пользователем осуществляется оплата на сайте. Данные о платеже поступают в систему фрод-мониторинга. Фактически, в этот момент в антифрод присутствуют два пакета – информация о данном единичном платеже и профиль, присущий среднестатистическому плательщику этого интернет-магазина . Благодаря разработанным алгоритмам для системы фрод-мониторинга существует возможность оценки группы факторов, среди которых особого внимания заслуживают следующие:

- государство, с территории которого осуществляется данный платеж;
- размер (сумма) платежа;
- общее количество платежей, совершенных с данной карты;
- платежная история банковской карты;
- профиль среднестатистического плательщика магазина.

Далее осуществляется начальный (первичный) анализ транзакции с использованием вышеперечисленных и других факторов. Основываясь на результатах анализа, совершается присваивание транзакции «метки»,

характеризующей способ обработки данной транзакции. В настоящее время эти метки бывают трех типов. «Зеленая» метка предназначена для пометки транзакций, вероятность возникновения мошеннических операций при проведении которых низка. «Желтая» метка присваивается транзакциям, в которых вероятность появления операции мошеннического характера выше среднего, что, безусловно, требует дополнительного внимания при осуществлении платежа. Наконец, «красная» метка свидетельствует о том, что транзакция со значительной долей вероятности относится к мошенническим, и для ее проведения необходимым является документальное подтверждение аутентичности владельца карты [12].

Необходимо отметить, что дальнейшая судьба всех присвоенных меток сугубо индивидуальна. Графическая схема жизненного цикла транзакций всех трех типов представлена на Рисунок Error: Reference source not found.3. Далее, с использованием нескольких довольно простых примеров, будут рассмотрены транзакции всех трех типов и пояснен количественный и качественный состав проверок, определяемых транзакциям системой фрод мониторинга в соответствии с уровнем риска появления фрода.

Транзакции с присвоенной «зеленой» меткой наиболее просты. Например, оплата осуществляется плательщиком с территории Российской Федерации, картой, выпуск которой был произведен российским банком. Сумма платежа не выше, чем средний чек магазина.

Системой мониторинга данной транзакции присваивается «зеленая» метка. После этого выполняется отправка транзакции на проверку с помощью 3-D Secure. В случае, если отсутствует подписка данной карты на сервис одноразовых паролей, либо банком-эмитентом данный сервис еще не поддерживается, будет осуществлен обычный способ (напрямую) направления запроса на авторизацию этой транзакции в процессинговый центр банка-плательщика [15].

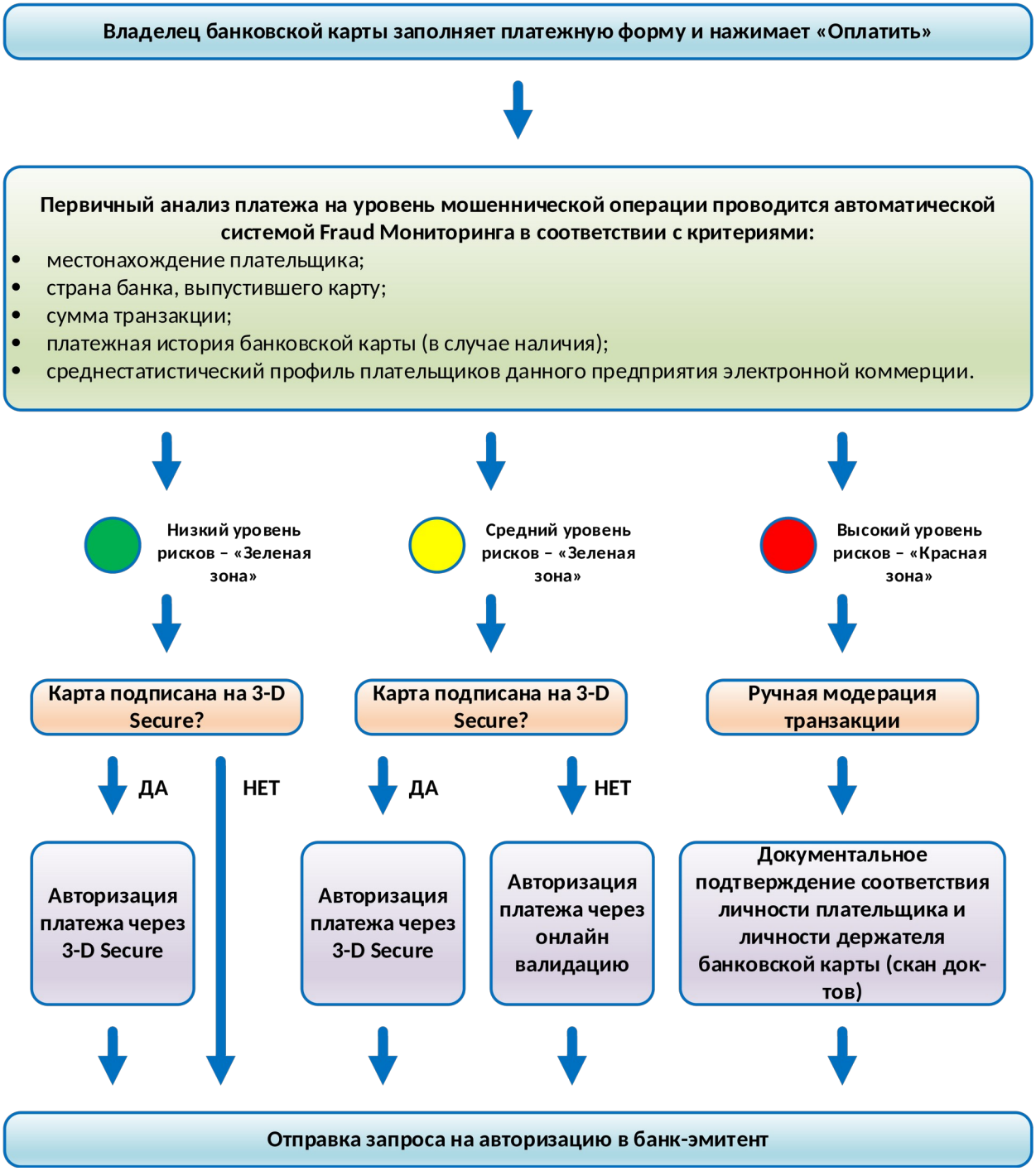


Рисунок Error: Reference source not found.3 – Жизненный цикл транзакций с различными типами риска возникновения мошеннической операции

Для среднего уровня риска появления фрода характерен другой путь проверки оплаты на допустимость. Присваивание метки «желтого» цвета выполняется транзакциям, имеющих средний и выше среднего уровень возникновения операций мошеннического характера. Например, в интернет-магазине, находящемся на территории Российской Федерации, выполняется

оплата покупки банковской картой, которая выпущена в России, однако сумма оплаты значительно превышает размер среднего чека магазина.

В этом случае выполняется пометка данной транзакции «желтой» меткой, после чего ее авторизация может потребовать дополнительных действий со стороны плательщика. Если у данной карты существует подпись на 3-D Secure, то для авторизации транзакции (как и для случая с «зеленой» меткой) будет использован одноразовый пароль. Однако, при недоступности данного способа для авторизации платежа клиентом, то будет осуществлено автоматическое перенаправление его банковской карты на онлайн-валидацию, либо ручную проверку.

«Красная» метка автоматически назначается системой фрод-мониторинга транзакциям, имеющим высокий уровень риска совершения операций мошеннического характера, Например, оплата в интернет-магазине, находящемся на территории Российской Федерации, осуществляется картой, выпуск которой был произведен в США, а физическое местоположение плательщика – Франция.

Если до этого момента оплата с помощью этой банковской карты не выполнялись, системой фрод-мониторинга данная транзакция будет помечена «красной» меткой с одновременным переводом ее в ручной режим авторизации из автоматического. Будет осуществлена отправка платежа специалистами департамента рисков на модерацию в ручном режиме. В этом случае, аутентификация владельца банковской карты будет нуждаться в документальном подтверждении, а именно, отсканированном изображении банковской карты и документа, который удостоверяет личность владельца. В случае поступления со стороны владельца корректных сканов документов будет осуществлен перевод операции из «красного» в «зеленый» цвет с последующим направлением на авторизацию в процессинговый центр банка. Если же операция признана сомнительной (не прошла ручную модерацию), то

она будет отклонена во избежание риска появления операций мошеннического характера.

Следовательно, можно говорить об автоматическом проведении анализа транзакций системой фрод-мониторинга сразу на трех уровнях: уровне единичной банковской карты, уровне профиля предприятия электронной коммерции, а также уровне общего потока транзакций, обработка которых выполняется IPSP. Необходимо отметить, что постоянно происходит совершенствование алгоритмов автоматического сбора, обработки и анализа данных о выполненных платежах. Это обстоятельство вместе с многоуровневым анализом транзакций дает возможность системе фрод-мониторинга осуществлять своевременное изменение, что ведет к повышению уровня безопасности выполнения оплат на сайтах клиентов, а также к снижению рисков, связанным со всеми видами фрода, характерными для электронной и интернет-коммерции.

Далее необходимо остановиться на факторах, способных вызвать подозрение у антифрод-системы. Ниже представлены наиболее ключевые параметры, которые, чаще всего, привлекут внимание системы на предмет осуществления операций мошеннического характера:

- оплата по одной карте выполняется с различных устройств, идентификация которых производится с помощью различных IP-адресов;
- обратный случай – с одного и того же устройства (один IP-адрес) осуществляются операции с использованием большого количества банковских карт;
- с одной карты выполняется несколько неудачных попыток оплаты (существует вероятность, что для пользователя прохождение процедуры подтверждения представляет значительные трудности);
- имя плательщика, которое указано на платежной форме, не совпадает с именем владельца карты;

- различные страны регистрации интернет-магазина, покупателя и банка-эмитента;
- выявлена ситуация регистрации одного и того же клиента под несколькими аккаунтами с применением различных адресов электронной почты, а также оплаты с одной карты.

Приведенная совокупность «подозрительных ситуаций» позволяет получить общее представление о логике функционирования системы. Для специалистов, задействованных в сферах риска и бизнес-аналитики, важным является учет всех нюансов, добавление (при необходимости) принципиально новых фильтров, направленных на защиту бизнеса интернет-предприятий от действий злоумышленников. Также следует сказать о том, что в соответствии с платежным сервис-провайдером может происходить изменение логики работы системы фрод-мониторинга, а также ее соответствующих параметров.

Кроме того, наблюдается различие настроек системы фрод-мониторинга в соответствии с типом бизнеса. При этом учету подлежит целая совокупность параметров, а именно:

- профиль плательщика (среднестатистический);
- уровень рисков в данном сегменте бизнеса;
- специфика реализуемых товаров и услуг (цифровой или физический их характер);
- сумма среднего чека.

В некоторых случаях бизнес является очень узкоспециализированным, что приводит к невозможности прохождения некоторыми платежами стандартных настроек антифрода без соответствующей индивидуальной настройки, хотя и не содержащих в себе мошеннических операций.

Например, следует отметить ограничения, связанные с географией, платежей в сфере онлайн-туризма: у клиента может возникнуть необходимость приобретение билета на самолет, находясь в командировке за границей, при этом подобный платеж будет заблокирован системой, поскольку он

осуществляется не из того государства, в котором был произведен выпуск карты плательщика.

В данном случае решение заключается в тонкой настройке фильтров: допустимо задание условий, в соответствии с которыми платеж будет признан легитимным даже в при невыполнении условия географии платежа. Очевидно, что внесение подобных изменений в систему допустимо только по результатам анализа вероятных рисков, при непосредственном участии специалистов, и по результатам согласования изменений с уполномоченным представителем конкретного интернет-магазина.

Ручной режим внесения изменений в работу системы сопряжен с риском значительных потерь – действительно, одобрив операции мошеннического характера, интернет-магазин принимает на себя обязательство возврата денежных средств на карту владельца даже при условии совершившейся фактической отгрузки мнимому покупателю. Кроме того на интернет-магазин могут быть наложены штрафные санкции в соответствии с объемами мошенничества, а в случае систематического повторения подобных ситуаций – приняты санкции особого характера от международных платежных систем (МПС).

На основании вышесказанного, достоинства системы мониторинга операций мошеннического характера заключаются в автоматическом предотвращении сомнительных транзакций, защите интернет-магазина от неизбежных последующих конфликтных ситуаций с платежными системами, банками и реальными держателями банковских карт. Помимо этого, важную роль играет минимизация финансовых и репутационных рисков. Репутационный уровень интернет-магазина сохраняется на высоком уровне, что способствует доверию со стороны пользователей подобному ресурсу и повышению их лояльности.

Вместе с тем, как и любой сервис, система фрод-мониторинга обладает и рядом существенных недостатков. Отклонение платежей, в перспективе, может

вызвать отток клиентов и, соответственно, уменьшение доходности. При недостаточно профессиональной настройке фильтров возможна ситуация блокирования ими важных для интернет-магазина (или другого подобного предприятия) транзакций, что точно не буде способствовать поддержанию лояльности покупателей на приемлемом уровне.

Выбирая платежного сервис-провайдера, следует обратить непосредственное внимание на уровень заявленной конверсии в успешные платежи: сервисы, декларирующие «100% успешных оплат», чаще всего, либо неадекватно оценивают свои функциональные возможности, либо подвергают клиентов значительному риску стать жертвой мошенников. Например, уровень конверсии в успешные платежи после «ручной» настройки (или у стандартных интернет-магазинов, имеющих стандартную клиентскую аудиторию) системы электронных платежей PayOnline находится в диапазоне 93,2-96%, что является весьма хорошим показателем для соответствующего рынка.

Еще один малоприятный, но ключевой момент, которого не получится избежать при разработке системы фрод-мониторинга на стороне интернет-магазина, связан с необходимостью защиты данных пользователей, как платежных, так и персональных. Существует необходимость прохождения сертификации соответствия требованиям стандарта PCI DSS, а также учета ограничений, связанных с хранением и обработкой данных, которые регулируются законом. Данное обстоятельство имеет отношение, по большей части, к тем, кто собирается осуществлять самостоятельную разработку антифрод-системы, следовательно все возможные риски и проблемы ложатся, в данном случае, на плечи разработчиков.

Безусловно, осуществление мониторинга операций мошеннического характера является необходимостью в современной реальности электронной коммерции. Для банковского учреждения сумма затрат, расходуемых на поддержку и развитие антифрод-системы, представляет более чем адекватную сумму, которая многократно окупится в процессе ее эксплуатации.

Также и для платежного сервис-провайдера система фрод-мониторинга относится к одному из наиболее важных сервисов, предоставляемых предприятиям-клиентам.

Однако, для предприятий, относящихся к малому и среднему бизнесу, разработка собственной антифрод-системы является заведомо убыточным и нецелесообразным проектом. С учетом постоянно повышающихся требований к подобным механизмам они более тонко обрабатывают полученную информацию с учетом статистики и поведенческих факторов. Для обеспечения эффективности работы системы и ее соответствия современным требованиям необходимым является наличие штата высококвалифицированных специалистов и существенных технических мощностей. Очевидно, что для большинства игроков сферы электронной коммерции такие постоянные затраты являются неприемлемыми, что приводит их к необходимости делегирования мониторинга операций мошеннического характера платежным сервис-провайдерам, специализация которых и ориентирована на анализ и обработку платежных операций. Например, для осуществления деятельности, связанной с мониторингом операций мошеннического характера, в PayOnline разработана собственная система Fraud Management System (FMS). В данной системе предусмотрена тонкая настройка безопасности в соответствии со 140 фильтрами.

2.3 Анализ сомнительных операций на предмет наличия мошеннических действий со стороны клиента или сотрудника Банка

Наиболее очевидным механизмом обеспечения безопасности финансовых операций в сервисах ДБО, в частности, в «онлайн-банке», является применение совокупности ограничений или лимитов на совершение операций, так называемой второй линии обороны, находящейся в составе комплекса фрод-мониторинговых решений:

- ограничение числа покупок по одной банковской карте или одним пользователем в течение заранее определенного периода времени;

- ограничение, накладываемое на число банковских карт, которые может использовать один пользователь в течение определенного периода времени;
- накопление истории покупок по банковским картам и конкретно пользователями (иногда используется терминология создания так называемых «черных» или «белых» списков);
- ограничение на количество пользователей, которые могут использовать одну и ту же банковскую карту;
- ограничение, накладываемое на максимальную сумму единоразовой покупки по одной карте или одним пользователем в течение заранее определенного периода времени.

Безусловно, обязательное требование к реализации вышеприведенных правил состоит в необходимости корректного распознавания пользователя в соответствии с различными параметрами и алгоритмами. В связи с этим, достоинство антифрод-сервиса определяется согласно его способности максимально быстро и эффективно осуществлять распознавание злоумышленника. Еще одна значимая функция фрод-мониторинга заключается в способности выполнения оценивания покупателя в процессе совершения электронного платежа, например, а интернет-магазине. Практически все фрод-мониторинговые системы, в первую очередь, стараются учитывать, насколько информация, указанная человеком о себе, соответствует действительности, и насколько набор параметров пользователя удовлетворяет стандартным шаблонам поведения добропорядочных пользователей [16].

На сегодняшний день растет проблема не просто мошенничества, а именно цифрового мошенничества. Это связано со стремительным погружением человечества в цифровые технологии. И ряд платежных сервисов, о которых ранее можно было прочесть только в произведениях писателей-фантастов, например, оплата покупок с помощью часов или перевод друг другу

денежных средств по фото, становятся неотъемлемой частью повседневной жизни [21].

Естественно, что актуальные технологии становятся привлекательными не только для новых клиентов, но и для всякого рода злоумышленников. Практически большинство людей хотя бы раз становился целью мошенников в дистанционных каналах, поэтому данная проблема может уже быть отнесена к наиболее массовым и социальным.

Центральный банк отмечает всю актуальность данной проблематики – осуществляется выпуск рекомендаций как для банковских организаций, так и для клиентов, готовятся соответствующие законопроекты, в одном из которых, как декларируется, будет явно прописано обязательство для кредитной организации обладать антифрод-механизмами для эффективного противодействия фродстерам, в противном случае на банк будут наложены обязательства, связанные с резервированием существенной суммы для компенсации возможных потерь. Однако большая часть банков и без этого законопроекта прониклась серьезностью вопроса, поскольку со стороны банков значительно возром интерес к различным антифрод-сервисам.

Безусловно, у банковских организаций возникает соблазн переложить ответственность на собственных партнеров (интернет-магазины, платежные системы). Однако у банков существует уверенность, что при таком подходе уровень рисков значительно возрастет и станет практически неконтролируемым, а на репутацию банка непосредственное влияние станет оказывать качество функционирования антифрод-сервисов сторонних предприятий. Очевидно, что серьезные предприятия, к которым конечно же относятся банки, не могут допустить такой ситуации и осуществляют внедрение собственных систем, ответственность за уровень риска возлагая на себя, а антифрод-сервисы партнеров играют в данном случае роль дополнительных факторов для обработки информации, связанной с возможным мошенничеством [17].

Кроме того, невозможность смещения ответственности в сторону партнеров объясняется еще и тем, что для этого необходимо обладать качественно выстроенной претензионной работы абсолютно со всеми контрагентами. Она должна быть абсолютно понятной для каждого из участников, наделять их определенным уровнем ответственности. Если в платежных системах подобный механизм давно уже отлажен и качественно функционирует, то в условиях постоянного появления новых платежных сервисов такой арбитраж установлен далеко не везде и не во всех случаях. Результатом этого является необходимость со стороны пользователя в случае появления у него определенных проблем, связанных с его платежом (операционная ошибка, мошенничество) обращения в банк. Именно со стороны банка, скорее всего, будут возмещаться потери клиента за счет собственных средств, а если подобная проблема примет массовый характер – будет просто выполнен отказ от такого сервиса.

Есть еще один аспект. Излишнее доверие партнерам в области мониторинга клиентских операций приводит, в определенной степени, к снижению уровня управляемости уровня клиентского сервиса. Подходы и технологии, применяемые злоумышленниками, постоянно совершенствуются, следовательно управление процессами определения операций мошеннического характера и формирования эффективных преград для злоумышленников относится к перманентным задачам для антифрод-офицеров. Если управление данным процессом выстроено без должного качества, то возможны проблемы у добросовестных клиентов и благая цель станет играть роль преграды для доступа к полюбившимся сервисам. Это окажет непосредственное негативное влияние на качество оказываемых услуг, на степени лояльности клиентов к банкам, на удовлетворенность банковскими сервисами. Очевидно, что при наличии возможности у клиентов смены собственного банка за очень короткий интервал времени, такая ситуация категорически недопустима.

Поэтому вопрос самостоятельного управления рисками мошенничества относится к наиболее ключевым аспектам бизнес-репутации банка, а разработка эффективной системы противодействия мошенничеству – к факторам, влияющим на успешное и стабильное развития бизнеса банка.

Так уж сложилось, что злоумышленники практически всегда находятся на шаг впереди даже наиболее современных и актуальных антифрод-механизмов. Это опережение, конечно же, необходимо устранять по возможности. Задача разработки антифрод-решений и состоит в сведении данного отставания до минимума и предоставления инструментария, предназначенного для оперативного реагирования на перманентно возникающие новые схемы мошенничества.

Только определенная вариативность может помочь организациям в эффективной борьбе со злоумышленниками в различных каналах. Для мошенников характерно следование по пути наименьшего сопротивления – например, с момента начала выпуска банками в соответствии с процессами EMV-миграции только карт с чипами сразуже проявилась тенденция перемещения скимингового фрод в государства, которым еще не подписано Соглашение о переносе ответственности (Liability Shift), а в других странах фрод мигрировал в онлайн-каналы. Следует учитывать, что при малейшем наличии у злоумышленников лазейки (как глобальной, так и на уровне локального банка) будет предпринята мгновенная попытка воспользоваться данной уязвимостью. Соответственно, задача антифрод-сервиса – своевременное определение подобной активности и максимально оперативное предотвращение без каких-либо потерь для бизнеса.

До последнего времени для большей части банков характерным было использование собственных самописных антифрод-систем, а для достижения уменьшения риска от целевых атак, новых мошеннических схем, массового фрода использовалось установка лимитов. Однако понятно, что такие мероприятия могут относительно минимизировать потери банка от

потенциальной атаки мошенников, но, как и любые ограничения, являются существенной помехой для полноценного развития бизнеса.

Поэтому на данный момент передовые компании полным ходом внедряют интеллектуальные системы мониторинга, которые дают возможность качественного определения «своего» и «чужого», а также содействуют развитию бизнеса.

Внедрение подобных систем позволяет решить сразу две банковских задачи. Первая задача – это обеспечение качества данных, вторая – увеличение конверсии переводов. Наличие качественных данных позволяет организовать не только корректную коммуникацию с клиентом, но и автоматизированные целевые маркетинговые кампании и персональные предложения. Кроме того, без них невозможна организация процесса эффективного взыскания задолженности, качественных процессов управления рисками.

Вообще говоря, разработка на основе антифрод системы совершенного понимания даст возможность банку составить обобщенный портрет клиента вплоть до отдельной персоны, выполнять оценку его не только вразрезе возможного фрода по отношению к его счетам, но и одновременно осуществлять качественное управление его ожиданиями.

К эффектам синергетического характера относится и увеличение конверсии переводов. Для достижения этого необходимо досконально понимать поведенческие реакции своих клиентов. Например, в случае типичной клиентской операции нецелесообразной является отсылка клиенту SMS для входа в систему дистанционного банковского обслуживания или для подтверждения транзакции в сети интернет. В соответствии с имеющейся практикой, только такие весьма простые действия приводят к повышению конверсии переводов от 25% до 45%, при этом затраты на SMS уменьшаются для крупного банка на миллионы рублей в год.

Следовательно, современную интеллектуальную антифрод-систему следует считать не только системой мониторинга, которая привычна для

сотрудников безопасности, занимающейся определением фрод в соответствии с зашитыми в систему шаблонами. Данный подход в современных условиях постоянно изменяющихся схем мошенничества стремительно теряет свою эффективность. Она должна являться совокупностью механизмов, способствующих, в первую очередь, понятию поведения каждого из клиентов во всех банковских каналах и мониторингу его в режиме реального времени с определением не только фрод, но и нужд клиента в отдельных услугах.

В кросс-канальной системе онлайн-мониторинга выполняется анализ не только параметров, характеризующих конкретный платеж, но и анализ информации нефинансового характера, например, данных по сессии клиента в системе дистанционного банковского обслуживания, а также данных по активности пользователя в других платежных каналах. Для иллюстрации типичен следующий пример: если за полтора часа до осуществления карточной операции в Индии системой было зафиксировано обращение клиента в отделение банка, то эта операция подлежит безусловному отклонению.

Такая возможность обеспечивается способностью в режиме реального времени выполнять оценку активности клиента в любом из предоставляемых банком каналов – терминал самообслуживания, мобильное приложение, колл-центр или банкомат. С повышением количества каналов, подключенных к мониторингу, увеличивается точность понимания профиля клиента, где, когда и в каком объеме им осуществляются платежи, сколькими контрагентами он обладает и каков характер взаимоотношений с ними, какими устройствами он пользуется и т.д.

После этого системой осуществляется анализ специфичных для конкретного пользователя параметров с последующим формированием заключения об уровне риска того или иного события. Для этого происходит одновременное использование как механизмов экспертного характера (бизнес-правил, черных и белых списков), так и механизмов, в основе которых лежит

машинное обучение, предназначенных для определения аномалий в действиях клиентов.

Такой подход дает возможность системам рассматривать транзакцию не только с позиции единичного клиента, но и проводить анализ поведения других клиентов. Например, предполагается, что со счета клиента была фиксация платежа в пользу, с начальной точки зрения, нового для него контрагента в нетипичное для клиента время из странного для него места. Вместе с тем системе данный получатель достаточно хорошо известен – это лояльный банку клиент, имеющий кредиты и депозиты, активно использующий другие банковские продукты, кроме того, в его пользу в течение длительного времени осуществляются платежи и другими пользователями, материальные претензии к нему отсутствуют. По этим соображениям анализируемый платеж не будет удостоен высокого уровня риска, невзирая на нетипичность самой операции для данного клиента.

Это является весьма важным, поскольку применение подобного всестороннего анализа дает возможность избежать прямого обращения к клиенту тогда, когда в этом отсутствует необходимость.

В основу современной антифрод-системы закладывается глубокая клиентская аналитика, предназначенная для генерации в автоматическом режиме правил и построения моделей определения мошенничества. Благодаря этому существенно сокращаются трудовые затраты на разработку новых алгоритмов и их тестирование, а также увеличивается точность за счет определения скрытых от человека закономерностей в очень больших объемах данных. К тому же существующие инструменты антифрод-системы способствуют оперативному получению требуемой информации при расследовании инцидентов и мгновенному реагированию на внедрение актуальных алгоритмов определения операций мошеннического характера, на этот процесс уходят считанные минуты.

Также следует упомянуть о возможности проведения всех изменений в системе пользователями самостоятельно, без участия вендора, что, конечно, же, обеспечивает наилучшую оперативность и гибкость процесса управления риском. Важность такого управления риском объясняется возможностью быстрой адаптации банка к постоянно изменчивым условиям, например, при внедрении новых продуктов или при появлении новых клиентских сегментов, например, в рамках пакетных предложений, оценка которых должна осуществляться автономно. Это позволяет одновременно выполнять эффективное противодействие мошеннической активности и достигать этих целей с наибольшей степенью незаметности для клиентов банка. Фактически, реализуется стремление на возможность разрешения клиенту наибольшего количества операций при сохранении уровня риска на приемлемом уровне.

Fнтифрод-сервисы обладают устоявшейся твердой репутацией в мире. Например, клиентами компании SAS являются такие крупные компании, как Wells Fargo, ICBC, Bank Of America, HSBC. Клиентская база банков, которые используют антифрод-решения от SAS, составляет 1 миллиард человек. Вместе с тем, на российском рынке данная компания прежде всего ассоциируется прежде всего с рисками или с клиентской аналитикой, но точно не с антифрод. На такую ситуацию влияет разница в подходах к решению проблемы фрода в Российской Федерации и в мире. Так, за рубежом принят подход просчета рисков на годы вперед, что требует определенных инвестиций сегодня в те отрасли бизнеса, которые могут причинить проблемы в будущем. Российские компании в основном исходят из текущей ситуации, поэтому внедряют соответствующий инструментарий по мере возникновения необходимости. Однако на сегодняшний день подобная необходимость очевидна – уровень мошенничества не только растет, его вариативность и изощренность делает невозможной борьбу с ним с помощью классических средств «наколеночных» систем. К тому же, как уже было сказано выше, регулятором постоянно ужесточаются правила путем введения новых стандартов и инициации

законопроектов, прямо предписывающих обязательность наличия антифрод-систем. Благодаря этому, в Российской Федерации серьезно обратили внимание на данную проблему мошенничества и количество внедренных различных антифрод-механизмов заметно увеличилось.

Одним из первых проектов кроссканальной системы стал проект в банке ВТБ24, где система не была написана с нуля, а осуществлено дополнение существующей антифрод-системы современной мощной аналитикой. По итогам, банку была присуждена награда от VISA за лучший сервис для работы с клиентами (наиболее высокий уровень одобрения операций клиентов при минимально низком уровне риска).

Вопрос противодействия мошенничеству является комплексным, он не имеет одного единственного решения, так как подразумевается как взаимодействие с клиентами, так и работа внутри банка. Так, должен быть налажен постоянный контакт с клиентами, направленный на повышение степени их осведомленности о рисках мошенничества. Для увеличения заинтересованности клиентов целесообразным является даже задействование определенных бонусных схем.

Кроме того, противодействие фроду требует реализации определенных процессов и внутри кредитного предприятия: от изучения разного рода документации на предмет определения процессов, уязвимых для мошенничества, до работы с антифрод-системой.

При этом, если банком принято решение о начале серьезной борьбы с мошенничеством и открытии проекта по внедрению антифрод-системы, должно быть понимание, что подобная система сходна с домашним питомцем, нуждается во внимании и уходе за собой, в противном случае ее содержание превратится в обузу, а эффект может быть прямо зеркален ожидаемому.

Приведенные аргументы свидетельствуют о необходимости создания в банке команды, в должностные обязанности которой будет входить работа с

этой системой. В состав команды должны быть включены администраторы, операторы и аналитики.

В задачи операторов входит проведение дополнительного анализа в тех случаях, когда система не в состоянии принять решение самостоятельно. Например, при приеме нового клиента на обслуживание банк не владеет практически никакой информацией о нем, а им уже начато совершение операций, обладающих высоким уровнем риска. Считается, что подобных сотрудников не должно быть более одного на каждые 2-3 миллиона клиентов. Это связано с направленностью разработки антифрод-системы на максимально самостоятельное принятие ею решений.

Количество администраторов тоже не должно превышать одного-двух человек. В их обязанности входит управление системой и мониторинг ее постоянной и бесперебойной работы.

Аналитики в команде необходимы для отслеживания актуальности применяемых антифрод-механизмов и своевременного внедрения новых и актуальных. В соответствии с практическим опытом, для таких аналитиков характерна универсальность, что дает возможность одновременного их использования в нескольких подразделениях в банке – например, на кредитных рисках, работа которых подразумевает аналитические исследования, на CRM и других внутренних службах, применяющих инструментарий подобного рода.

Следует уточнить, что в соответствии с решаемой проблемой в качестве заказчиков могут выступать различные подразделения. Например, решение проблем в сфере дистанционного банковского обслуживания или интернет-банкинга возлагается чаще всего на подразделения информационной безопасности, поэтому именно они и выступают в качестве заказчиков. В сфере карточного бизнеса привлекаются подразделения, занимающиеся развитием продукта как такового. В качестве заказчиков модуля антифрод платформы чаще можно видеть либо службы, обеспечивающие внутреннюю безопасность, либо службы, занимающиеся операционными рисками.

Однако при необходимости внедрения кросс-канальной системы определения мошеннических операций инициатива всегда должна исходить от высшего руководства кредитного предприятия. Другую ситуацию представить трудно, поскольку необходимо наличие человека, отвечающего не за определенное направление, а за весь банковский бизнес, либо его существенную часть, например, за корпоративный бизнес или розничный бизнес. В такой ситуации, как правило, осуществляется назначение фрод-менеджера, в задачи которого входит курирование процесса определения фрода с самого начала, то есть с момента старта этой инициативы.

Как уже упоминалось, после внедрения интеллектуальной антифрод-системы повышается качество управления процессами мошенничества и снижаются расходы на него. Другими словами, снижается количество уведомлений системы, что позволяет уменьшить количество сотрудников, ответственных за связь с клиентами. Кроме того, уменьшается и нагрузка на подразделения, работа которых ориентирована на обработку претензий клиентов, поскольку общее количество претензий сократится. Такими подразделениями являются фронт-офис, колл-центр, службы по работе с платежными системами, службы безопасности, подразделения качества клиентского обслуживания. Это коснется даже юридической службы, поскольку клиенты достаточно часто осуществляют обращения в суды для оспаривания списанных с их счетов денежных средств – а это все приводит не только к существенным расходам для предприятия, но и к репутационному риску, оценка уровня которого представляется весьма проблематичной.

Вместе с этим, интеллектуальная антифрод-система дает возможность накопления информации о своем клиенте, что приводит к разного рода синергетическому эффекту. Благодаря только увеличению конверсии клиентских платежей в сети интернет и экономии на очень дорогих сегодня SMS-уведомлениях, срок окупаемости затрат на внедрение подобной системы может снизиться и составить всего несколько месяцев.

3 Предложение по решению проблем обеспечения защиты в системах обработки больших данных в финансово-кредитных организациях

3.1 Технологии структуризации данных для выявления утечек и уязвимостей

При проведении онлайн-платежа при покупке товара или услуги через сеть Интернет полная цепочка имеет вид, представленный на Рисунок Error: Reference source not found.4.

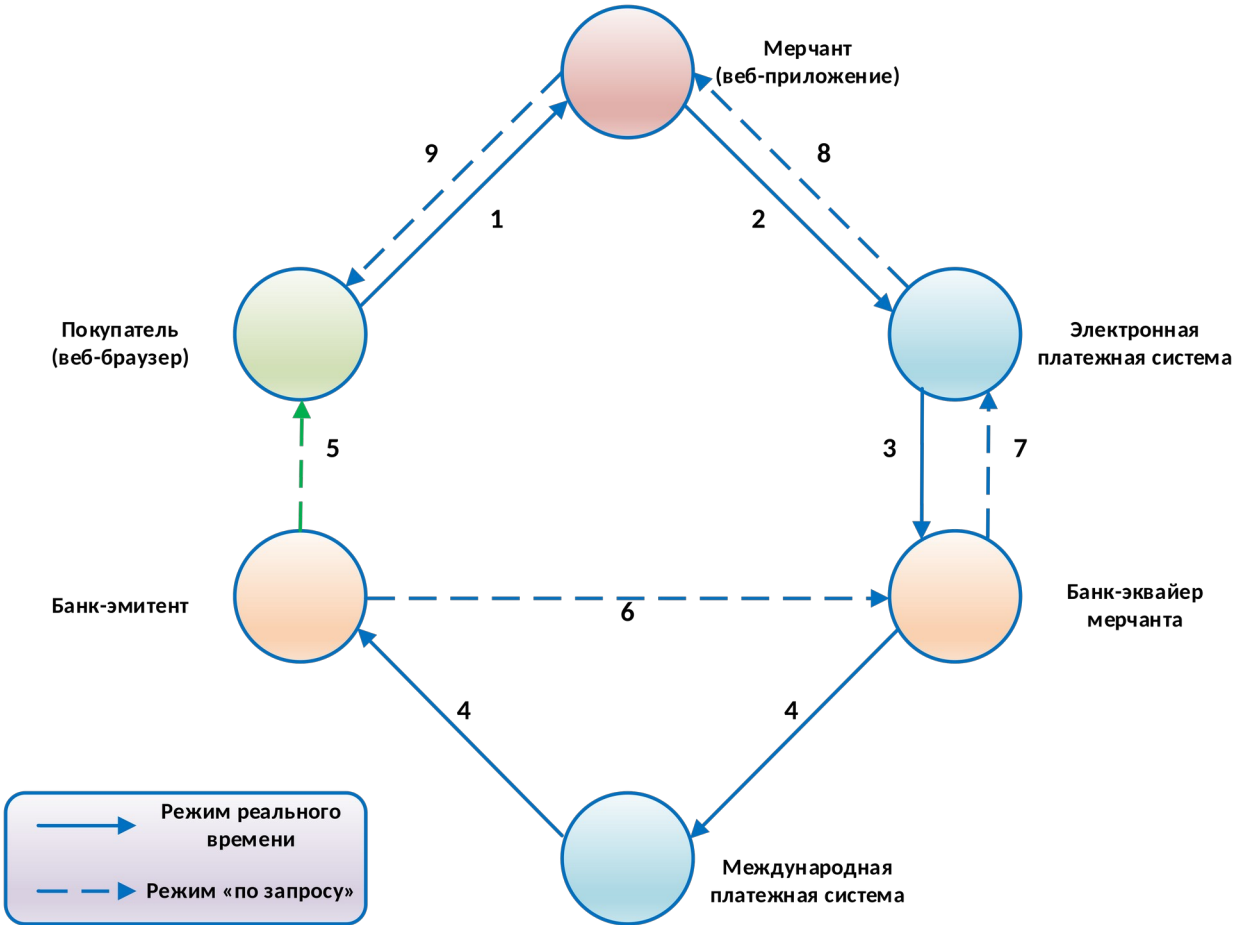


Рисунок Error: Reference source not found.4 – Жизненный цикл транзакций с различными типами риска

Необходимо пояснить некоторые детали приведенной схемы.

Под мерчантом понимается продавец товара или услуги. Это – веб-приложение, в котором для клиента доступна возможность оплаты выбранного товара или услуги.

Клиентом является покупатель, осуществляющий оплату товара или услуги на сайте мерчанта, используя при этом собственную банковскую карту (либо другой легальный способ).

Электронная платежная система (ПС) представляет собой сервис, который принимает к оплате электронные деньги, банковские карты через сеть Интернет. В качестве примеров платежных систем можно упомянуть о WebMoney, Яндекс.Деньги и т.п.

Банком-эквайром называется банк, осуществляющий предоставление услуг, связанных с обработкой платежей по банковским картам.

Международная платежная система (МПС) является системой расчетов между банками, зарегистрированных в различных государствах, использующих единые стандарты платежных средств. В качестве примеров международных платежных систем можно упомянуть о MasterCard, American Express, Visa.

Банком-эмитентом называется банк, осуществивший выпуск банковской карты, которая используется клиентом для оплаты товара или услуги.

На самом деле проблема транзакций мошеннического характера (фрод, от англ. fraud) касаеься каждого из участников представленной выше цепочки: от клиентов до банка, осуществившего выпуск карты для клиента (банк-эмитент). Всем участникам, кроме пожалуй держателей карт, операции мошеннического характера опасны существенными финансовыми издержками, а также значительными репутационными рисками. На сферу электронной коммерции в целом фрод оказывает вполне определенное негативное влияние, а именно: недополучение прибыли, возникновение недоверия со стороны пользователей, следствием чего является замедление широкого распространения электронных платежей.

Следовательно, можно утверждать, что наличие разработанной антифрод-системы (об этом уже говорилось выше) для каждого из серьезных участников проведения он-лайн платежа (все так же, за исключением покупателя) является безусловным требованием рынка. В то же время разработка полноценной антифрод-системы представляет собой обычно долгий, достаточно дорогой финансово и трудоемкий процесс, что часто останавливает руководителей профильных предприятий.

Целесообразно кратко остановиться на ключевых сложностях разработки антифрод-системы. Прежде всего, речь идет о финансовых сложностях (стоимости разработки, штрафных санкциях за фрод). Действительно, для даже весьма среднего банка затраты на разработку или приобретение анти-фрод системы в обшей структуре бизнеса представляются вполне неразорительными и оправданными, для платежной системы это вообще представляет собой неотъемлемую часть бизнеса, тогда как у мерчантов достаточно часто отсутствует финансовая возможность и/или понимание, какие шаги необходимо предпринять для разработки, внедрения и последующего технического сопровождения подобных систем.

Вместе с тем, и игнорирование фрода со стороны мерчанта не представляется возможным. В самом удачном случае произойдет недополучение денежных средств за платежи мошеннического характера мерчантом (даже в случае уже оказанной услуги), в самом крайнем же случае на мерчанта будут еще и возложены штрафные санкции. Размер этих санкций минимально может составлять около 100 рублей и может расти пропорционально в соответствии с объемом транзакций мошеннического характера. Также, если количество фрода достаточно велико, ведущие международные платежные системы (MasterCard, Visa) могут подвергнуть мерчанта весьма неприятным санкциям.

В качестве достаточно эффективного способа уменьшения затрат на стороне мерчанта можно говорить об осуществлении дополнительных проверок

для клиента с делегированием некоторой части или всех обязанностей проверки на фрод другому участнику цепочки оплаты. На данный момент наиболее востребованный способ – это 3-D Secure (фактически, представляет собой делегирование обязанностей, связанных с проверкой, банку-эмитенту).

3-D Secure (Three-Domain Secure) является защищенным протоколом, осуществляющим добавление дополнительного уровня безопасности для дебетовых и онлайн-кредитных карт. Реально его можно рассматривать в виде двухфакторной идентификации владельца карты. Целью разработки данной технологии являлось обеспечение безопасности оплаты товаров и услуг в сети Интернет. Изначально данный протокол был предложен платежной системой Visa, а затем, подвергшись определенным изменениям, был взят на вооружение и другими. У Visa данный протокол имеет название Verified by Visa (VbV), у MasterCard – Mastercard SecureCode (MCC), а у JCB International – J/Secure.

Данным протоколом осуществляется добавление дополнительного шага авторизации пользователя при оплате покупки в интернет-магазине. Первый этап подразумевает использование номера карты, срока ее действия, имени держателя карты и кода проверки ее подлинности (например, CVC2). На втором этапе с помощью протокола 3-D Secure сайт магазина отображает страницу банка-эмитента карты, на которой пользователь должен выполнить ввод дополнительного защитного кода. Он может быть получен клиентом банка посредством, например, SMS-сообщения на собственный мобильный телефон, с помощью карты разовых кодов или специализированного устройства. Кроме того, код может быть постоянным и установлен самим клиентом заранее. Вообще говоря, название метода Three-Domain Secure объясняется тем, что в онлайн-транзакции принимают участие три домена – домен мерчанта (торговой точки) или эквайрера, где осуществляется ввод данных платежной карты, домен платежной системы, выполняющей переадресацию платежа на страницу подтверждения разовым кодом или паролем, а также домен эмитента карты или

специализированного сервиса, где происходит формирование страницы подтверждения и проверка корректности введенных защитных кодов.

Следует отметить, что все передаваемые подтверждающие данные от клиента хранятся на платежном сервере банка-эмитента, при этом доступ со стороны интернет-магазина к ней отсутствует (у магазина существует возможность сохранения части информации, касающейся реквизитов платежной карты, однако в объеме, не превышающем предписанного в PCI DSS). Это способствует защите данных от хищения.

Далеко не у всех онлайн-магазинов и банков присутствует 3-D Secure. Данная технология не относится к обязательным и служит для защиты, в первую очередь, торговой точки и банка от операций мошеннического характера. Если существует возможность применения 3-D Secure, а сервис не задействован (например, карта клиента поддерживает данную технологию, а онлайн-магазин нет, либо наоборот), всей полнотой ответственности за осуществление несанкционированной транзакции наделяется сторона, на которой лежит вина за неиспользование 3-D Secure.

Однако нельзя забывать, что при добавлении шагов, принуждающих пользователя к дополнительным действиям, может наблюдаться стремительное снижение числа успешно завершенных транзакций. В соответствии с результатами исследования, проведенного некоторыми исследователями, включение 3-D Secure на территории Российской Федерации влечет за собой снижение количества успешных платежей в размере 20-27%.

Кроме того, при разработке антифрод-систем приходится преодолевать и сложности юридического характера. Действительно, процесс разработки неизбежно столкнется с такой ответственной сферой, как защита клиентских и платежных данных, а также с формальной частью данного вопроса – необходимостью сертификации по одному из уровней PCI DSS.

PCI DSS (Payment Card Industry Data Security Standard) является стандартом безопасности данных сферы платежных карт. По сути, представляет

собой совокупность требований, направленных на обеспечение безопасности хранения и передачи платежных данных. Разработка стандарта осуществлена Советом по стандартам безопасности индустрии платежных карт (Payment Card Industry Security Standards Council, PCI SSC), к учреждению которого приложили руку такие международные платежные системы, как MasterCard, JCB, Discover, American Express, Visa.

В данном стандарте содержится двенадцать требований:

- защита вычислительной сети;
- защита хранимой информации, касающейся держателей карт;
- антивирусная защита информационной инфраструктуры;
- управление доступом к информации, касающейся держателей карт;
- осуществление физической защиты информационной инфраструктуры;
- протоколирование действий и событий;
- выполнение контроля защищенности информационной инфраструктуры;
- управление информационной безопасностью;
- механизмы аутентификации;
- разработка информационных систем с последующей поддержкой;
- защита передаваемой информации, касающейся держателей карт;
- конфигурация компонентов информационной структуры.

Распространено глубоко ошибочное мнение, что сертификация PCI DSS является простой формальностью и существует возможность простой покупки сертификата. Это полное заблуждение. Для соответствия предприятия стандарту PCI DSS должен быть осуществлен комплексный подход к обеспечению информационной безопасности данных платежных карт.

Стандарт PCI DSS ориентирован на выполнение следующих аспектов:

- осуществление защиты информации о держателях карт;
- внедрение жестких мер контроля доступа;

- систематический мониторинг и тестирование сети;
- формирование политики информационной безопасности;
- управление уязвимостями;
- построение защищенной сети с последующим регулярным ее обслуживанием.

С более полной информацией по данному стандарту можно ознакомиться на сайте Official PCI Security Standards Council Site.

Также при разработке антифрод-сервиса следует не забывать о некоторых существующих законодательных ограничениях, касающихся хранения/обмена персональных и платежных клиентских данных. В Российской Федерации это закон «О персональных данных» (152-ФЗ).

Безусловно, разработчик сталкивается и с техническими сложностями. Действительно, в соответствующей классификации антифрод-система относится к business-critical системам, поскольку ситуация ее простоя повлечет за собой либо остановку бизнес-процесса, либо, если система функционирует некорректно, увеличение рисков потерь финансового характера для предприятия.

Именно этим и объясняются повышенные предъявляемые требования к безопасности хранения данных, надежности работы, возможностям, связанным с масштабированием системы.

В коллективе, ориентированном на разработку антифрод-системы, внимания заслуживают следующие роли и области ответственности этих ролей:

- эксперт в предметной области. В данном случае имеются в виду следующие предметные области: банковские системы, платежные системы, оплата через сеть Интернет, юридическая специфика функционирования подобных систем;
- разработчик. Для сотрудника, выполняющего данную роль, необходимо владение высокоуровневым языком программирования,

многопоточным и асинхронным программированием, а также наличие достаточно высокой математической подготовки;

- project manager. Занимается координацией разработки;
- data scientist. Сфера ответственности – исследование процессов, обработка данных с полноценным применением соответствующего математического аппарата;
- архитектор – осуществляет проектирование надежного высокодоступного (в идеале еще и масштабируемого и распределенного) приложения.

Как следует из вышесказанного, во всей цепочке осуществления онлайн-платежа наиболее сложное положение именно у мерчанта. Действительно, в отличие от покупателя, на мерчанта возлагается вся полнота ответственности за фрод и в случае нештатных ситуаций именно он будет терять свои денежные средства. В то же время, в отличие от банка, у мерчанта часто отсутствуют достаточные ресурсы, необходимые для эффективного предотвращения операций мошеннического характера.

Вместе с тем, мерчант обладает и рядом преимуществ. Именно у него есть уникальная информация о покупателе товара или услуги, которая в подавляющем числе случаев отсутствует у других участников онлайн-платежа (например, у международной платежной системы или банка-эмитента). Так можно утверждать с высокой степенью уверенности, что у ECN-площадок существует доступ к реальному имени плательщика; интернет-магазины, предлагающие услугу доставки, безусловно обладают информацией, касающейся реальной страны, города проживания плательщика и т.д.

Фамилия владельца учетной записи, его имя, количество ранее совершенных легитимных платежей через сайт мерчанта, время существования учетной записи, данные о браузере, используемом клиентом, информация о хосте, с которого поступил http-запрос – єто далеко не полній список информации, являющейся доступной мерчанту. Безусловно, такая информация

способствует повышению эффективности поиска транзакций мошеннического характера.

3.2 Анализ имеющихся данных на аномалии путем их классификации

Далее следует подробнее описать основные требования, к разрабатываемой антифрод-системе, влияние которых на программную архитектуру может считаться ключевым.

Как известно, требования делятся на функциональные и нефункциональные. Среди нефункциональных требований, прежде всего, следует остановиться на атрибутах качества.

Выбор атрибутов качества напрямую следует из типа проектируемой системы, а именно – business critical. Итак, выделяются следующие атрибуты:

- отказоустойчивость;
- надежность;
- значительная масштабируемость;
- распределенность.

Далее следует задать ограничения в соответствии с действующим законодательством. Законодательные ограничения, безусловно, относятся к важным факторам, оказывающим непосредственное влияние на программную архитектуру антифрод-системы. Так, в соответствии с требованиями стандарта PCI DSS недопустимым является хранение полного номера карты (PAN), а также кода безопасности (CVV). Допустимо хранение исключительно первых шести и последних четырех цифр карты. Помимо этого, не является запрещенной генерация внутреннего уникального идентификатора для карт, принадлежащих клиентам. Передача имени держателя карты и срока экспирации допустима только по защищенным каналам.

Фактически, на высоком уровне (около 81-го) сертификации стандарта PCI DSS допускается хранение PAN в зашифрованном виде.

Помимо требований, предъявляемых стандартом PCI DSS, не следует забывать об обязательности выполнения закона «О персональных данных» (152-ФЗ).

Юридическое толкование всего комплекса технико-бюрократических процедур (с вытекающими последующими нюансами), которые являются необходимыми только для хранения, обработки имени и фамилии клиента, представляется очень трудоемким и затратным процессом, процесс реализации данных инструкций ничуть не легче. Поэтому был сделан вывод о наиболее надежном методе соблюдения закона 152-ФЗ. Он заключается в непопадании под его действие.

Этим продиктовано обстоятельство, что в разрабатываемой антифрод-системе работа всех программных модулей будет осуществляться исключительно с деперсонализированными данными.

Собрав все ограничения, относящиеся к юридической сфере, можно добавить к проектируемой системе ряд следующих требований:

- запрет хранения PAN и CVV платежной карты в каком-либо виде;
- хранение других данных платежа производится только в защищенном виде;
- передача данных между мерчантом (программным клиентом) и антифрод-системой должна осуществляться исключительно по защищенным каналам;
- все операции должны производиться только с персонифицированными данными.

Теперь можно переходить к формулировке требований функционального характера.

Первыми будут сформированы требования, предъявляемые к API. Другими словами, необходимо рассмотрение требований к системе с позиции внешнего мира, то есть мерчантов (программных клиентов). Программными

клиентами осуществляется взаимодействие с антифрод-системой согласно следующим функциональным требованиям к API:

- реализация возможности предоставления клиенту API для передачи информации о платеже;
- предоставление клиенту API для модификации (корректировки) платежных данных;
- обязательное уведомление клиента о результатах предсказания, отнесен ли платеж к мошенническим.

Помимо этого, к API предъявляется некоторое количество требований нефункционального характера, среди которых ключевыми являются:

- предоставление общедоступного протокола взаимодействия с клиентом;
- ведение взаимодействия с клиентом исключительно через защищенные каналы связи.

Безусловно существует совокупность бизнес-требований, предъявляемых к проекту разработки антифрод-системы. Рассматривая внутреннюю логику антифрод-системы, можно выделить только одно значимое бизнес-требование, заключающееся в обязательности прогнозирования в соответствии с информацией о платеже, будет ли пропущена или блокирована транзакция. В ходе реализации данного требования будет предпринята попытка доказательства, что платеж будет отклонен. Целесообразно рассмотрение основных причин отказа в проведении транзакции. Среди них выделяются следующие: формирование данных было осуществлено некорректно, либо транзакция отнесена к мошенническим. Далее будут разобраны методы анализа каждой из указанных причин.

Первой проверяется корректность ввода платежных данных. Нельзя переносить ответственность за надлежащую проверку платежных данных на мерчанта. Невзирая на то, является ли данная ошибка ошибкой пользовательского ввода, либо была произведена попытка злонамеренных

действий, своевременное определение ошибок в реквизитах платежа на ранних этапах будет способствовать как экономии тактов процессора (CPU), так и предотвращению зашумления обучаемой модели (детально ее рассмотрение будет приведено несколько позже).

Необходима также проверка на содержание в имени держателя карты по меньшей мере двух букв (цифры и тире в имени являются легитимными), относится ли карта к действующим (карта обладает своим сроком действия), проходит ли номер карты проверку по алгоритму Луна.

Алгоритм Луна (Luhn algorithm) является алгоритмом определения контрольной цифры номера пластиковой карты. Основное его назначение – определение ошибок, причиной которых является непреднамеренное искажение данных. Следует отметить, что по результатам выполнения данного алгоритма можно только с определенной степенью достоверности утверждать о том, что в номере карты отсутствуют ошибки.

Номер пластиковой карты обычно состоит из:

- шести цифр, которые характеризуют тип и организацию, выполнившую выпуск карты;
- до двенадцати цифр, обозначающих персональный банковский счет;
- одной проверочной цифры, вычисленной с помощью алгоритма Луна.

Данный алгоритм был предложен немецким компьютерным специалистом Гансом Луном в 1954 году. Алгоритм Луна базируется на простом правиле вычисления контрольной суммы для проверки идентификационных номеров, в частности, номеров пластиковых карт. Целью разработки алгоритма являлось определение ошибок при вводе номера. В данном алгоритме предусмотрено определение ошибки ввода одной некорректной цифры, а также практически всех перестановок соседних цифр, кроме перестановки 09-90, а также обратной 90-09.

Формула для вычислений достаточно несложна. Для определения контрольной суммы согласно алгоритму Луна необходимым является суммирование всех нечетных цифр последовательности справа налево, после чего к этой сумме прибавляется сумма всех четных цифр, умноженных на 2. При этом, если произведение превышает число 9, из него необходимо вычесть 9.

Алгоритм Луна позволяет также вычислить проверочную цифру, которую можно добавить к исходной последовательности, чтобы была получена корректная последовательность (другими словами, последовательность, контрольная сумма которой оканчивается на 0).

Чтобы определить проверочную цифру, требуется простое добавление «0» к исходной последовательности и вычисление контрольной суммы полученной последовательности с помощью алгоритма Луна. При окончании полученной контрольной суммы на 0 можно утверждать, что проверочная цифра и есть 0, в ином случае для определения проверочной цифры выполняется вычитание последней цифры полученной контрольной суммы из 10.

После этого необходимо выполнить проверку на отнесение определенной транзакции к мошенническим. Выявление признака отнесения платежа к мошенническим может быть произведено с использованием большого количества эвристик. В некоторых компаниях утверждается о применении более двухсот эвристик. Здесь, конечно, нельзя избежать сомнения, что некоторые из эвристик слабо или ничем не подкреплены, либо какие-нибудь эвристики не являются независимыми (представляют собой следствие другой эвристики), либо это вовсе является программной закладкой, ориентированной на улучшение подгона результата под обучающую выборку и слабо или вообще никак не работающей на реальных данных. Действительно, с увеличением количества эвристик можно получить только переобученную модель, ошибочно

определяющую, относится ли транзакция к мошенническим. Вместе с тем, катастрофически падает производительность разработанного приложения.

Исходя из вышеперечисленного, целесообразно перечисление только ключевых и показавших наибольшую эффективность эвристик:

- одна карта соответствует множеству IP, а также обратный случай: один IP соответствует множеству карт;
- один клиент является держателем множества карт (особенно эмитированных различными банками);
- наблюдается несовпадение имени клиента с именем владельца аккаунта на сайте мерчанта (в случае его наличия);
- оплата осуществляется в ночное время (в соответствии с локальным временем клиента);
- наблюдается несовпадение страны клиента со страной владельца аккаунта на сайте мерчанта (в случае его наличия);
- одному клиенту соответствует несколько индексов, алресов электронной почты;
- на одну карту приходится множество покупок или множество неудачных попыток.

Тут же возникает вопрос – как количественно определиться с термином «множество»? Какой период времени может быть отнесен к коротким (10 секунд или три недели)? Как может быть решена проблема неравенства веса фильтра x_1 весу фильтра x_2 при условии, что значения их весов должны изменяться в динамическом режиме в ходе функционирования приложения?

В качестве основного подхода принято пользоваться наивным присвоением фиксированного значения для одного из фильтров (любого) с последующей обработкой таких условий в конструкциях, одна из которых представлена ниже (написанный код является псевдокодом):

```
if (число_карт_с_одного_IP > 5)
{
платеж_статус = отклонен;
return;
}
else
{
if (число_покупок_с_карты_за_30_минут > 10)
{
        платеж_статус = отклонен;
return;
}
else
{
        //выполнение других проверок
}
}
//одобрение платежа с последующим его проведением
```

Очевидно, что подобный подход обладает большим количеством недостатков, что делает конечную стоимость приведенного кода чрезвычайно низкой. На эту стоимость окажут непосредственное негативное влияние потери, вызванные ложными срабатываниями на отклонение вполне корректных и легитимных платежей, а также пропуск фрода, который неизбежно случится при минимальном изменении злоумышленниками собственной стратегии.

Следовательно, единственно приемлемое решение заключается в разработке системы, в которой заложена способность эвристических фильтров к самообучению как на уже накопленной платежной истории, так и на абсолютно новых платежах. Для этого может быть выбран один из широко известных алгоритмов машинного обучения: метод опорных векторов, «случайный лес», нейронные сети, метод k ближайших соседей, наконец, логистическая регрессия.

Теперь следует остановиться на глобальных фильтрах. Под этим названием в данном случае подразумеваются списки, в которых при наличии плательщика проведение всех остальных проверок – а именно валидности платежных данных, проверки на фрод представляется нецелесообразным занятием. К подобным спискам могут быть отнесены такие, как черные списки IP, мерчантов, банковских карт.

Глобальные фильтры могут принадлежать как к статическому, так и к динамическому типу, они могут быть взаимосвязаны как с определением аномальной активности (адрес IP), так и с определенными бизнес-правилами (мерчантом отклоняются все платежи, совершенные из Уругвая) и т.д.

Теперь следует подробнее остановиться на принципах создания классификаторов из обучающих данных. В качестве обучающей выборки целесообразен выбор материала, который получен из действительных транзакций определенной финансовой структуры. Рекомендуемый объем выборки обучающих данных – около одного миллиона, среди которых не менее 10% должны составлять нелегальные (отклоненные транзакции). В каждой транзакции в соответствии с требованиями конфиденциальности выполняется элиминирование всех полей, кроме суммы и суточного времени платежа. Под термином «суточное время» в данном случае следует понимать время создания транзакции без учета даты. Полученный набор данных и получает название «обучающая выборка». Вся совокупность данных после обработки представлена в виде, показанном на Рисунок Error: Reference source not found.5.

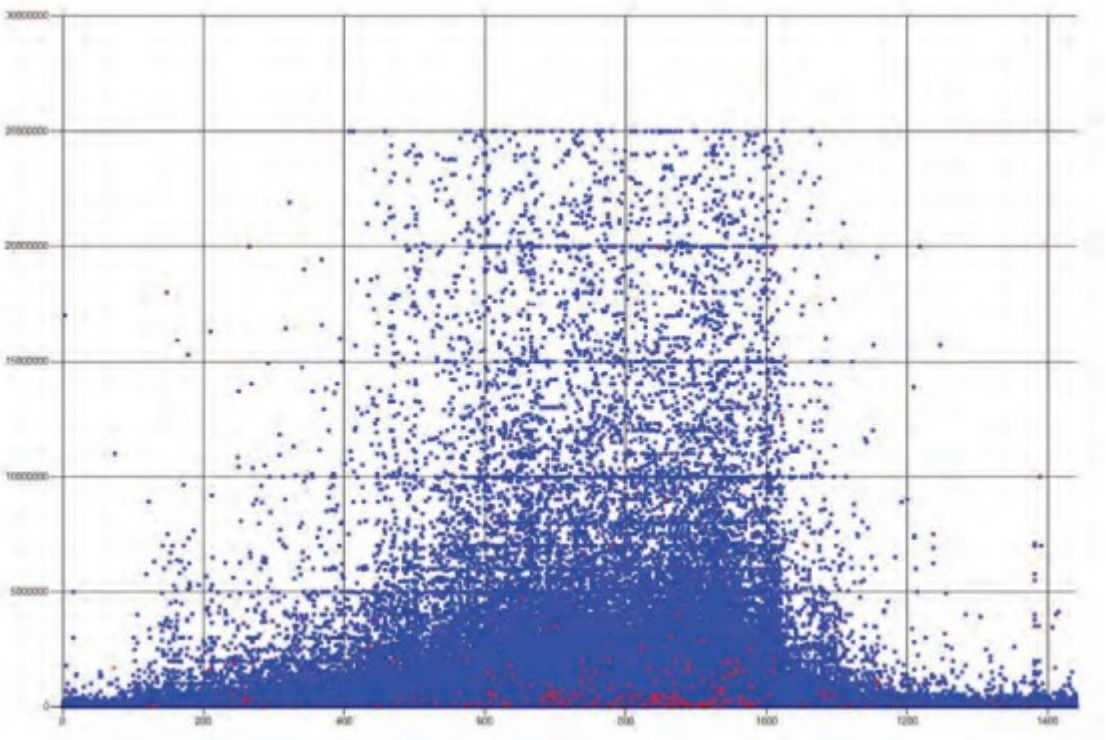


Рисунок Error: Reference source not found.5 – Жизненный цикл транзакций с различными типами риска

В данном случае по вертикальной оси находится сумма транзакции (в условных единицах, у.е.), а по горизонтальной – суточное время транзакции (в минутах). Соответственно, каждая из точек обозначает одну транзакцию, имеющую два параметра: сумма (в у.е.) и суточное время (в минутах). Синим цветом выделены точки, соответствующие легальным транзакциям, красным – транзакциям мошеннического характера (фрод). Под классификатором транзакции мошеннического характера (фрод) понимается в общем случае произвольная область (либо подмножество, как на Рисунок Error: Reference source not found.5), при попадании в которую анализируемая «урезанная» транзакция приобретает статус подозрительной на фрод и остается для последующих исследований на следующей ступени системы фрод-мониторинга. Если же данная транзакция не попадает в область классификатора, то ее относят к легальным и она исключается из дальнейшего рассмотрения. Очевидно, что подобный алгоритм строит наиболее качественные классификаторы при наличии как можно большего количества

красных точек и как можно меньшего количества, соответственно, синих. При изучении методом «естественного интеллекта» обучающей выборки, показанной на Рисунок Error: Reference source not found.5, как визуально (используя большое разрешение), так и с помощью различных метрик можно сделать вывод о слабом отличии в представленной обучающей выборке легальных транзакций от мошеннических. Такой вывод представляется вполне логичным, так как у злоумышленников всегда существует цель маскировки, по крайней мере, по сумме и времени своих транзакций под транзакции легальных реальных пользователей.

3.3 Конфигурирование механизмов защиты и мониторинга

После проведенных в предыдущих разделах данной главы подготовительных действий можно перейти к разработке программной архитектуры антифрод-сервиса, рассмотрению его модульной структуры и основных деталей реализации сервиса подобного рода.

Общая архитектура разрабатываемой системы представлена на Рисунок Error: Reference source not found.6.

Представленный сервис состоит из нескольких приложений, функционирующих в Microsoft Azure. Вариант с размещением с применением облачной платформы вместо размещения на собственном физическом сервере даст возможность с относительно малыми временными затратами осуществить разработку сервиса, соответствующего всем атрибутам качества системы, перечисленным в предыдущем разделе. Кроме того, используя подобный подход, можно добиться существенного снижения первоначальных финансовых затрат на требуемое аппаратное и программное обеспечение.

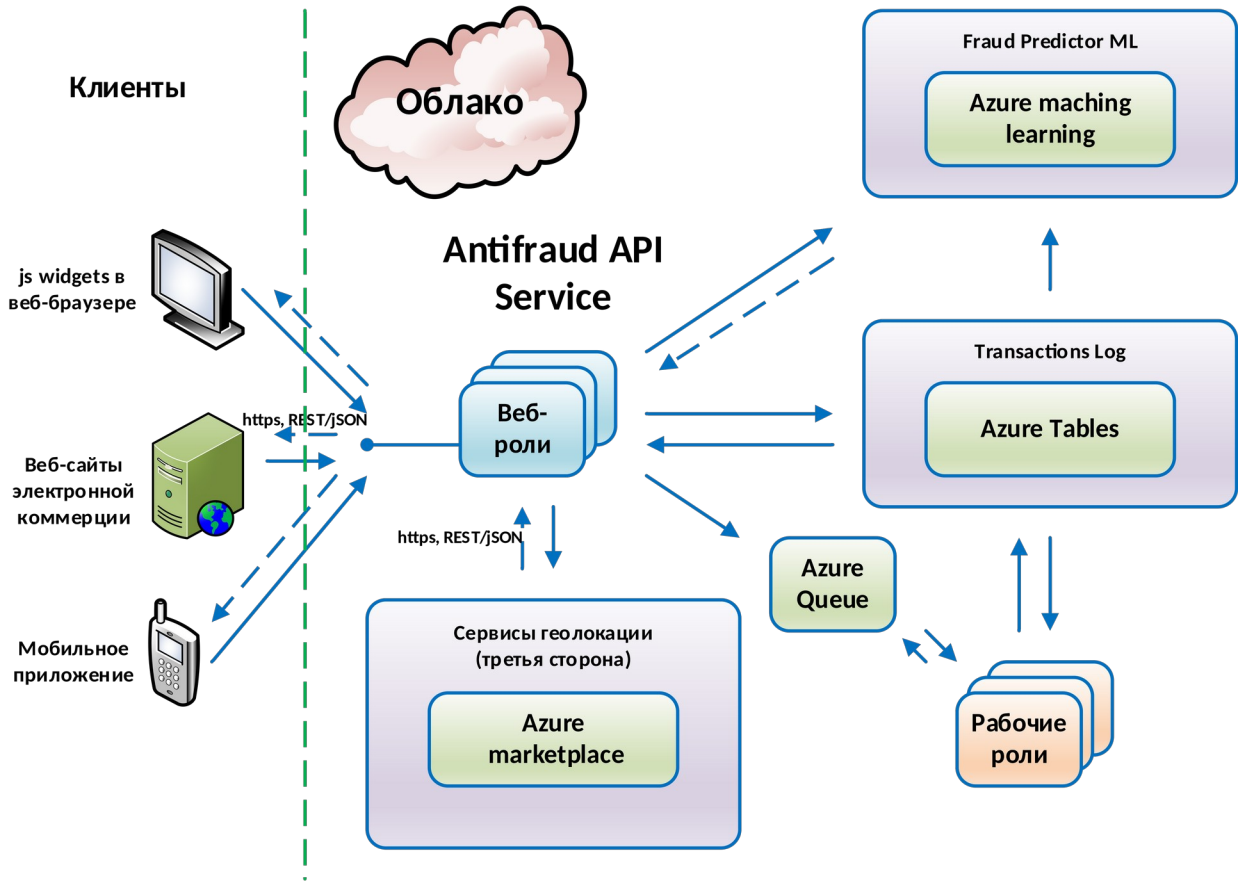


Рисунок Error: Reference source not found.6 – Архитектура разрабатываемого антифрод-сервиса

В разработанный антифрод-сервис входят следующие системы:

- Antifraud API Service – сервис типа REST, осуществляющий предоставление API для взаимодействия с сервисов Fraud Predictor ML;
- Transactions Log (журнал транзакций) – NoSQL хранилище, в котором содержится вся информация о транзакциях;
- Fraud Predictor ML – сервис выявления платежей мошеннического характера, основанный на использовании алгоритмов машинного обучения.

Кроме того, сервис обладает многочисленными программными клиентами (Clients). Они фактически являются веб-приложениями мерчантов, либо js-виджетами, выполняющими вызов REST-сервисов Antifraud API Service.

Принципиальная архитектура взаимодействия перечисленных систем представлена на Рисунок Error: Reference source not found.6.

Инфраструктурой, также как и предметной областью и законодательными документами накладывается достаточное количество ограничений, которые подлежат учету на уровне архитектуры. Ограничения доменного и юридического типа были рассмотрены ранее, теперь же рассмотрению подлежат достоинства и ограничения, обусловленные выбором облачной платформы Microsoft Azure.

При использовании антифрод-системой сервисов Azure – Cloud Service для веб и рабочих ролей, Azure Queue, Azure Table, Azure ML помимо практического полного отсутствия необходимости в начальных финансовых затрат можно говорить о следующих ключевых конкурентных преимуществах:

- наличие высокой доступности: уровень SLA составляет не менее 99,96%;
- обеспечение безопасности хранения: соответствие сертификатам ISO 27001/27002, а также PCI DSS 3.0;
- обеспечение высокой масштабируемости: предусмотрено масштабирование в автоматическом режиме количества рабочих узлов в соответствии с нагрузкой, партицирование таблиц хранилища NoSQL на базе PartitionKey;
- приемлемая отказоустойчивость: доступен (и даже рекомендован) запуск всех рабочих узлов в нескольких экземплярах;
- высокая надежность хранения: существующие системы хранения данных обладают значительной избыточностью.

Кроме этого, можно отметить ряд менее значимых достоинств:

- наличие глубокой интеграции с Microsoft Visual Studio;
- наличие удобного мониторинга приложения.

Однако все эти преимущества (достоинства) стали доступными из-за первоначального замысла разработки антифрод-сервиса под облачные технологии. Таким образом:

- веб и рабочие узлы относятся к stateless (любой ответ не зависит от состояния);
- сетевые взаимодействия осуществляются исключительно в асинхронном режиме и только с использованием retry-политик (Retry Pattern);
- выравнивание нагрузки и гарантированная обработка задач осуществляется с помощью очередей сообщений (паттерн Queue-Based Load Leveling Pattern);
- наличие горизонтального партицирования для хранения структурированных или полуструктурированных данных (Sharding Pattern).

Помимо этого, антифрод-система является так называемой near real-time системой, поэтому в процессе реализации антифрод-сервиса:

- применяются алгоритмы, параллельные по данным (одним из простейших, но обладающих большой эффективностью является алгоритм MapReduce). MapReduce является алгоритмом (фреймворком) для вычисления определенных наборов распределенных задач с применением большого числа компьютеров (называемых в данном случае «нодами»).

Функционирование MapReduce включает два этапа: Map и Reduce, получивших свое название по аналогии с одноименными функциями высшего порядка map и reduce.

На Map-этапе осуществляется предварительная обработка входных данных. Для этого на один из компьютеров (он называется главным узлом – master node) поступают входные данные задачи, после чего он выполняет разделение их на части с последующей передачей другим компьютерам (они называются рабочие узлы – worker node) для обработки предварительного характера.

Суть Reduce-этапа заключается в свертке предварительно обработанных данных. На главный узел поступают ответы от рабочих узлов, после чего, на их основе, происходит формирование результата – решение изначально сформулированной задачи.

Достоинство MapReduce состоит в его возможности распределенного выполнения операций предварительной обработки и свертки. Работа операций предварительной обработки осуществляется независимо друг от друга, они могут выполняться в параллельном режиме (хотя в практических задачах всегда существуют ограничения, связанные с источником входных данных и/или числом используемых процессоров). Аналогично, свертка может выполняться множеством рабочих узлов – для этого необходимым является только выполнение условия, при котором обработка всех результатов предварительной обработки, имеющих одно конкретное значение, выполнялась одним рабочим узлом в один момент времени. Вместе с тем, эффективность данного алгоритма может быть меньше, чем у более последовательных алгоритмов. Применение MapReduce возможно к большим объемам данных, обработка которых может вестись большим числом серверов. Например, MapReduce вполне подходит для решения задачи сортировки петабайта данных, причем время выполнения не будет превышать нескольких часов. Благодаря параллелизму появляются определенные возможности, связанные с восстановлением после частичных сбоев серверов: при возникновении сбоя в рабочем узле, который производит операцию предварительной обработки или свертки, допустима передача его работы другому рабочему узлу (при условии доступности входных данных для осуществляемой операции);

- принимаются меры для предотвращения блокировок лога транзакций (любых распределяемых ресурсов). Для этого к информации о транзакции добавляется поле timestamp;
- удаляются долгие запросы;
- для таких операций, как сохранение единичной записи в логе транзакций, используется подход Push’n’Forget (точность работы алгоритма особенно не пострадает от пропажи одной записи из 10K успешно сохраненных).

Следует также помнить об ограничениях, существующих у любых облачных сервисов:

- технические ограничения: к наиболее частым из них можно отнести максимальный размер сообщения, максимальное число запросов в секунду;
- технологические ограничения: к наиболее ключевым из них относится ограничение по поддерживаемым протоколам взаимодействия с сервисами PaaS.

Далее необходимо кратко остановиться на принципах взаимодействия между компонентами антифрод-сервиса. С точки зрения мерчанта сервис является REST-сервисом, с которым возможно взаимодействие посредством протокола https – Antifraud API Service. Antifraud API Service осуществляет свою работу в кластере, в состав которого входят несколько веб-ролей типа stateless (под веб-ролью в Azure следует понимать слой приложения, играющий роль веб-приложения).

На диаграмме последовательностей (Рисунок Error: Reference source not found.7) выполнено описание возможных взаимодействий мерчанта с каждой из подсистем антифрод-сервиса.

Целесообразно описание работы данной диаграммы по этапам (шагам):

- этап 1: выполняется отправка запроса, содержащего данные о платеже;
- этап 2: осуществление трансформации модели (в терминах MVC);
- этап 3: производится отправка запроса на сервис, отвечающий за предсказание результата платежа;
- этап 4: происходит возврат результата – будет ли проведен платеж (или отклонен);
- этап 5: выполняется сохранение данных;
- этап 6: производится возврат результата клиенту;
- этапы 7, 8: выполнение пересчета и обновления обучающей выборки; после этого происходит переобучение модели;

- этапы 9-12 (могут быть опущены). Со стороны Клиента осуществляется инициация отправки запроса, содержащего данные о результате платежа (для случая, когда результат предсказания не совпадает с реальным результатом платежа, который был передан в запросе).

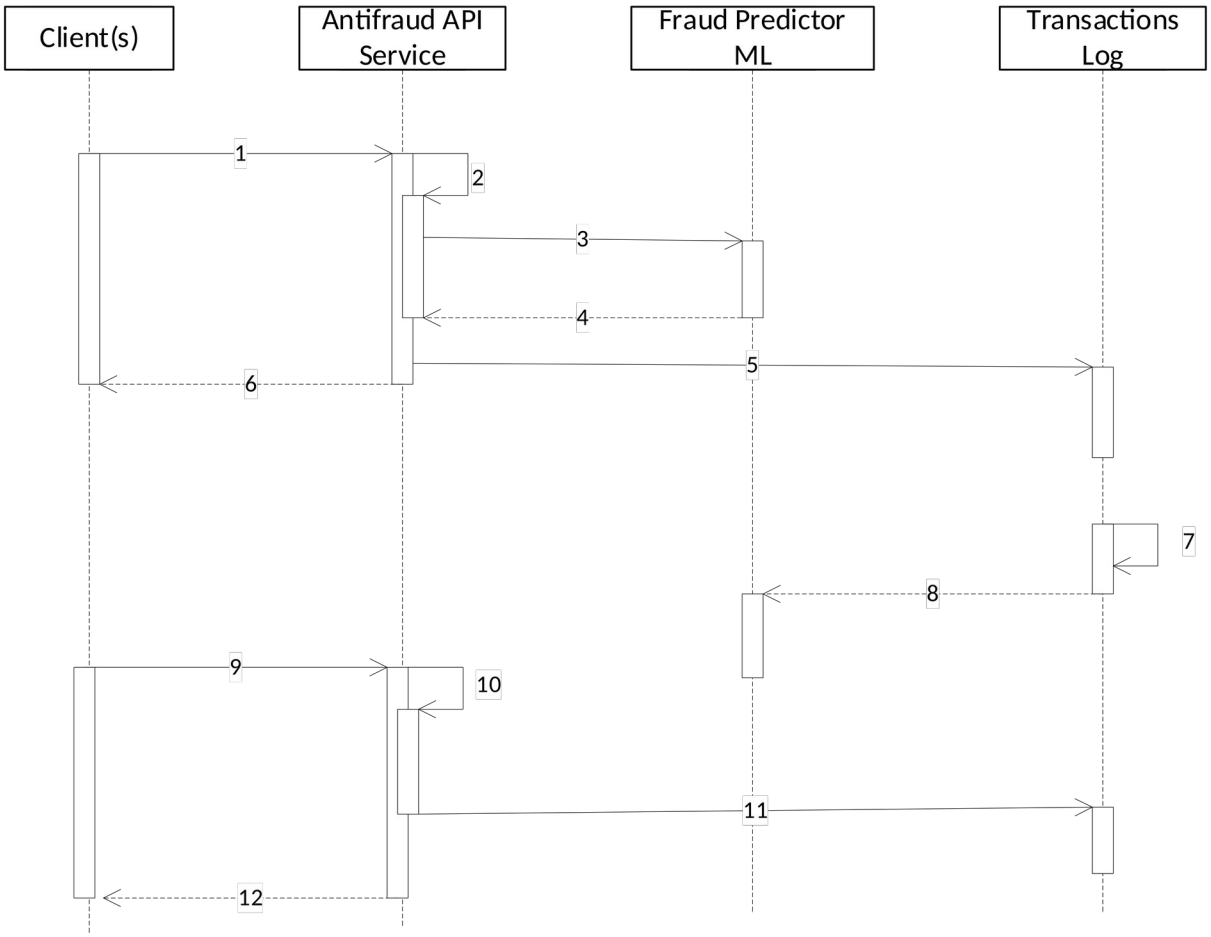


Рисунок Error: Reference source not found.7 – Диаграмма последовательностей взаимодействия подсистем сервиса

Теперь будет выполнено более подробное рассмотрение каждого из этапов.

Запрос от мерчанта подается на Контроллер (в терминах MVC) (этап 1). Далее с полученной моделью (в терминах MVC) происходит следующее:

- трансформация из модели контроллера в доменный объект;
- отправка запроса на внешние геолокационные сервисы (Azure Marketplace) для определения страны в соответствии с индексом плательщика и

страны в соответствии с IP хоста, с которого было зафиксировано поступление запроса на снятие средств с карты;

- выполнение этапа проверки через глобальные фильтры;
- выполнение этапа проверки платежных данных на валидность;
- осуществление предварительного анализа полученной транзакции – выполняется вычисление эвристики для таймфреймов продолжительностью в 5 секунд, 1 минута, 24 часа;
- выполнение сокрытие личных данных держателя карты и платежных данных – фактически, это хэширование имени держателя карты, имени владельца аккаунта на сайте мерчанта, адреса плательщика, его телефона, адреса электронной почты;
- удаление неиспользуемой информации – например, данные, свидетельствующие о сроке действия карты, после этапа 4 будут далее не нужны.

Подробное описание эвристик, глобальных фильтров и признаков валидности данных платежа было выполнено в предыдущем разделе.

На этапе 2 осуществляется трансформация объекта предметной области в объект DTO, который:

- отправляется в сервис Fraud Predictor ML (этап 3);
- после получения ответа от Fraud Predictor ML (этап 4) производится сохранение в лог транзакций данных о транзакции и ее результате (этап 5);
- осуществляется возврат клиенту ответа, касающегося предсказанного результата платежа (отнесен ли он к мошенническим или нет).

Чтобы улучшить качество функционирование алгоритма предсказания, для клиентов является доступным API уточнения результатов транзакции. Например, при несовпадении реального результата проведения платежа со значением, возвращенным разработанной антифрод-системой, у мерчанта есть возможность сигнализировать об этой ситуации путем отправки запроса на

уточнение результатов транзакций (этап 9). Подобные запросы обладают следующими свойствами:

- структура их формата: <transaction_id, transaction_result, last_update_time>;
- выполняется обработка запросов в Merchant API Service и после валидации они поступают в Azure Queue (отказоустойчивый сервис очередей).

Из очереди запросы извлекаются одним из роботов, которые, фактически, являются рабочими ролями типа stateless (под рабочей ролью в Azure следует понимать слой приложения, на который аозложена роль обработчика).

Теперь пришло время детального разбора хранилища данных.

В лог транзакций осуществляется сохранение как данных о транзакциях, так и дополнительной информации, касающейся их (чаще всего, это статистические данные). Лог транзакция является долговременным хранилищем на основе Azure Table (сервис, который может быть описан как отказоустойчивое хранилище типа NoSQL (key-value)).

В логе транзакций содержатся две таблицы:

- таблица, в которой содержатся факты о транзакции. Она называется TransactionsInfo. Ее структура: id транзакции (Row Key), id мерчанта, хэш имени держателя платежной карты (в случае его доступности), сумма платежа, валюта платежа и т.д.;
- таблица, в которой хранятся рассчитанные статистические метрики. Ее название – TransactionsStatistics. В ней содержится информация, характеризующая: сколько раз были осуществлены платежи с данной карты (несколько таймфреймов), количество IP были произведены платежи, значение временного интервала между платежами, с какого времени выполнена регистрация покупателя у мерчанта, сколько раз были осуществлены проведенные (успешные) платежи и т.д.

На этапах 7 и 8 выполняется переобучение модели. Для обучающей выборки берется информация из лога транзакций, поскольку в хранилище лога

располагается последняя актуальная информация, касающаяся платежей и их результатов. Переобучение может осуществляться в соответствии с заранее составленным расписанием, по превышению заданного порога некорректных предсказаний, по появлению фиксированного значения в логе транзакций новых записей.

3.4 Предложения по технологии организации реагирования на инциденты

После разработки проекта антифрод-системы целесообразным является начальное его тестирование. Для этого предлагается обучение четырех моделей с использованием алгоритмов логистической регрессии, метода опорных векторов, дерева решений и персептрона. Из обученных моделей будет выбрана модель, обладающая наибольшей точностью на тестовой выборке, после чего будет осуществлена ее публикация в виде сервиса REST/JSON. После этого необходимо написание программного клиента и проведение нагрузочного тестирования на сервисе REST.

Вначале создается новый эксперимент в Azure ML Studio. Его конечный вид представлен на Рисунок Error: Reference source not found.8. Каждому из элементов эксперимента ставится в соответствие этап последовательности, осуществляемый data scientist в ходе обучения модели.

Далее целесообразно рассмотрение каждого из этапов разработки модели распознавания платежей мошеннического типа с учетом технических деталей, которые были подробно описаны в предыдущем разделе.

Ключевые предположения и концепции, являющиеся полезными для разработки модели, были описаны в первых двух разделах настоящей главы. Следует отметить, что создание качественной гипотезы представляет собой итеративный процесс проб и ошибок, в качестве основы для которого применяются знания, касающиеся как анализируемой предметной области, так и области Data Science.

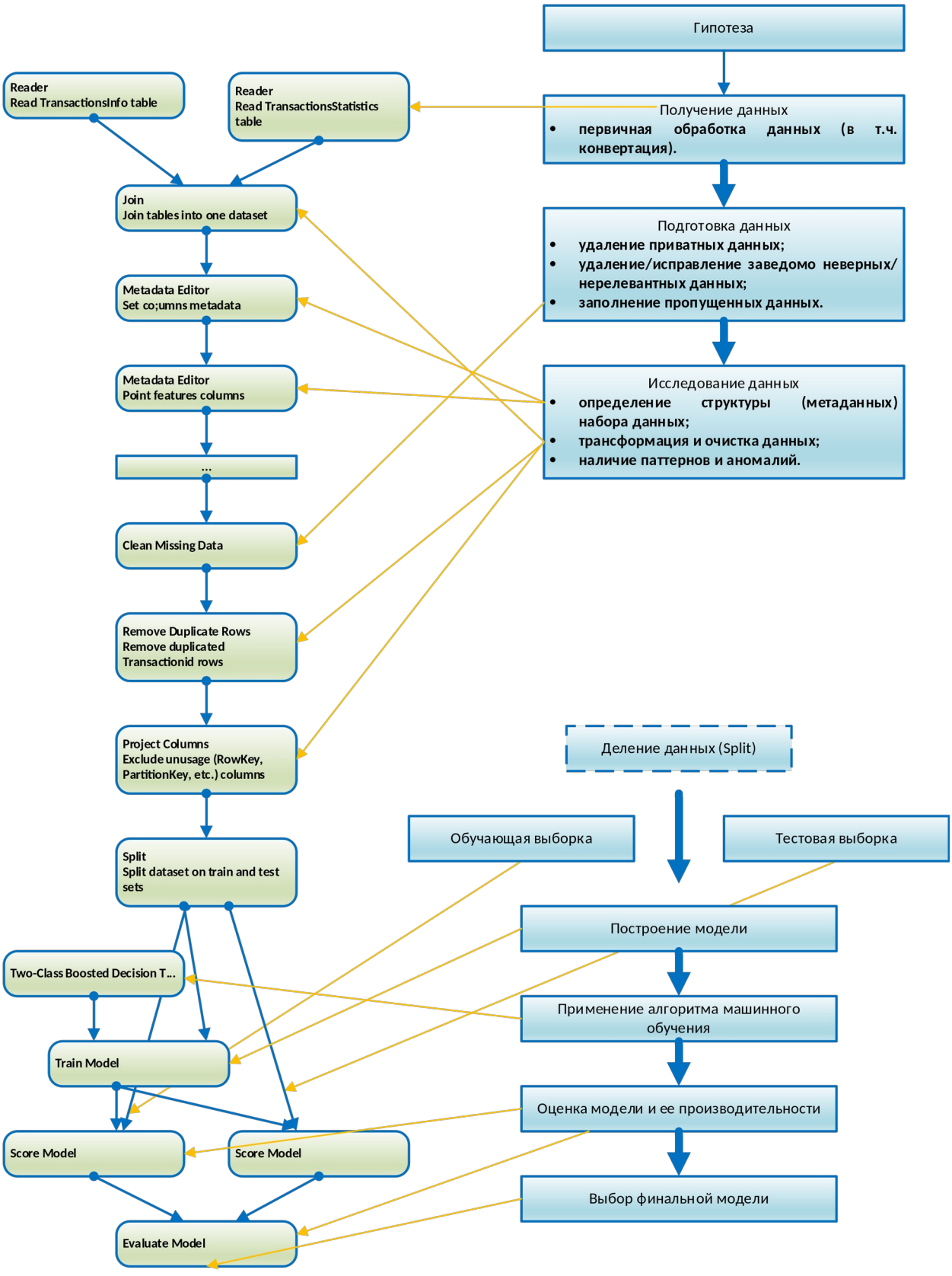


Рисунок Error: Reference source not found.8 – Структура эксперимента

В качестве набора данных для модели, ориентированной на определение платежей мошеннического типа, будет использован лог транзакций, в состав

которого входят две таблицы в NoSQL-хранилище (Azure Table): таблица, содержащая фактическую информацию о транзакциях (TransactionsInfo) и таблица, содержашая предварительно вычисленные статистические метрики (TransactionsStatistics).

Этап получения данных включает в себя загрузку описанных двух таблиц через управляющий элемент Reader.

Далее выполняется Inner Join загруженных таблиц в соответствии с полем TransactioId. Используя элемент управления Metadata Editor, существует возможность указания типов данных (timestamp, integer, string), пометки столбца, в котором содержатся ответы (label), а также столбцов с предикторами (features). Кроме этого выполняется пометка типа шкалы у этих данных: абсолютные, номинальные.

Этап подготовки обладает большой важностью при создании адекватной модели. Можно проиллюстрировать данный тезис на конкретном примере, касающемся валюты платежа, хранение которой осуществляется в виде кодов ISO (тип – целочисленное значение). В кодах ISO используется классификационная (номинальная) шкала. Однако сомнительно ожидать автоматического определения со стороны системы, что в столбце «Currency» осуществляется хранение не целочисленного значения с абсолютной шкалой (другими словами, доступными являются операции типа + и >). Данное правило достаточно неочевидно, и в системе нет никакой информации о нем.

В наборе данных могут содержаться пропущенные значения. В данном случае, определение IP-адреса плательщика и его страны не всегда представляется возможным, поэтому в данных полях могут находиться пустые значения. После проверки имеющегося набора данных выполняется замена пустых значений стран на «undefined», используя при этом элемент управления Clean Missing Data. Этот же элемент управления поможет выполнить удаление строк, в полях держатель карты, валюта или сумма платежа которых

присутствуют пустые значения, поскольку данные строки заведомо заполнены некорректными данными, то есть они являются источником шума в модели.

Следующий этап заключается в удалении из модели неиспользуемых полей: адрес (в данном случае интерес представляет только проверка на совпадение страны плательщика со страной, откуда поступил запрос), хэш имени держателя банковской карты (данный параметр вообще не влияет на ожидаемый результат платежа), PartitionId и RowId (эти поля служебного типа попали в таблицу из Azure Table).

Наконец, используя элемент управления Normalize Data осуществляется ZScore-нормализация данных, в которых содержатся слишком большие числовые значения. Таким значениям может быть сумма платежа (расположенная в столбце TransactionAmount).

Далее выполняется разделение полученного набора данных, соответственно, на обучающую и тестовую выборки. Важно осуществить корректный выбор соотношения данных в обучающей выборке и в тестовой. В данном случае, используя элемент управления Split, в обучающую выборку переносится 75% данных с дополнительным включением режима смешивания данных (установка флага Randomized split) при разделении на поднаборы данных. Благодаря режиму смешивания данных при разделении появляется возможность недопущения «перекосов» в обучающей выборке, появляющихся из-за больших утечек номеров пластиковых карт (и, в результате, аномальной активности фрод-роботов в данный период).

Теперь можно осуществить инициализацию нескольких алгоритмов классификации с последующим сравнением показанных ими результатов (точности) на тестовой выборке. Следует учитывать, что достижение на реальных данных той же производительности, что и на тестовых, абсолютно не всегда возможно. В связи с этим, чрезвычайно важно обладать полной картиной того, что в модели не подверглось учету, каковы причины выдачи тем или иным алгоритмом лучшего или худшего результата, также важно провести

исправление ошибок и выполнить запуск алгоритма обучения еще раз. Данный процесс целесообразно продолжать до тех пор, пока полученная модель с точки зрения точности не станет приемлемой для исследователя.

В Azure ML существует возможность подключения в одном эксперименте сколь угодно большого количества алгоритмов машинного обучения. Это позволяет на этапе исследования осуществить сравнение производительности нескольких алгоритмов для определения того, который в наибольшей степени соответствует решаемой задаче. В данном случае используется нескольку алгоритмов, принадлежащих к так называемой двухклассовой классификации: логистическая регрессия (Two-Class Logistic Regression), метод опорных векторов (Two-Class Support Vector Machine), нейронная сеть (Two-Class Neural Network) и дерево решения, построенное с помощью метода градиентного спуска (Two-Class Boosted Decision Tree).

Для улучшения производительности модели можно воспользоваться еще одной возможностью. Она заключается в настройке алгоритма машинного обучения с применением большего количества параметров, являющихся доступными для настройки алгоритма. Например, для алгоритма дерева решений, построенного с помощью метода градиентного спуска, указывается число деревьев, необходимых для построения, и наименьшее/наибольшее число листьев на каждом из деревьев. В алгоритме нейронной сети настройке подлежат число скрытых узлов, начальные веса и число обучающих итераций.

Заключительный этап состоит в просмотре получившихся данных элемента управления Evaluate Model (соответствует команде Visualize из контекстного меню элемента). Отображение данных представлено для каждого из используемых алгоритмов.

В элементе управления Evaluate Model содержится матрица неточностей (confusion matrix), графики ROC и Precision/Recall, а также рассчитанные параметры точности алгоритма Recall, Accuracy, F1 Score, Precision и AUC. Немного упрощая, требуется выбор алгоритма, значения Precision, AUC и

Accuracy которого наиболее близки к единице, вогнутость графика ROC в сторону оси ординат как для обучающей, так и для тестовой выборки максимальна.

Помимо этого, следует изучить изменения AUC в соответствии с устанавливаемым значением Threshold. Для фрод это является важным, поскольку величина стоимости нераспознанных платежей мошеннического характера (False Positive) значительно превышает величину стоимости платежей, которые ошибочно были приняты за фрод (false Negative).

В такой ситуации требуется подбор значения Threshold, не совпадающего со значением по умолчанию (оно установлено равным 0,5).

Выбирая наиболее соответствующий для выбора эффективной модели определения фрода алгоритм, помимо уровня Threshold необходимо учесть и то обстоятельство, что логика принятия решений для некоторых алгоритмов подлежит воспроизведению (например, алгоритм дерева решения, построенного с помощью метода градиентного спуска), а для некоторых воспроизведение этой логики не представляется возможным (нейронная сеть). Наличие подобной возможности может быть отнесено к критичным если важен ответ на вопрос, по какой причине по заданному прецеденту системой принято конкретной решение.

В результате проведенного эксперимента лучшей точностью обладает алгоритм двухклассовой нейронной сети (Two-Class Neural Network) (показатели точности представлены на Рисунок Error: Reference source not found.9), после него – алгоритм построения дерева решения с помощью метода градиентного спуска (Two-Class Boosted Decision Tree).

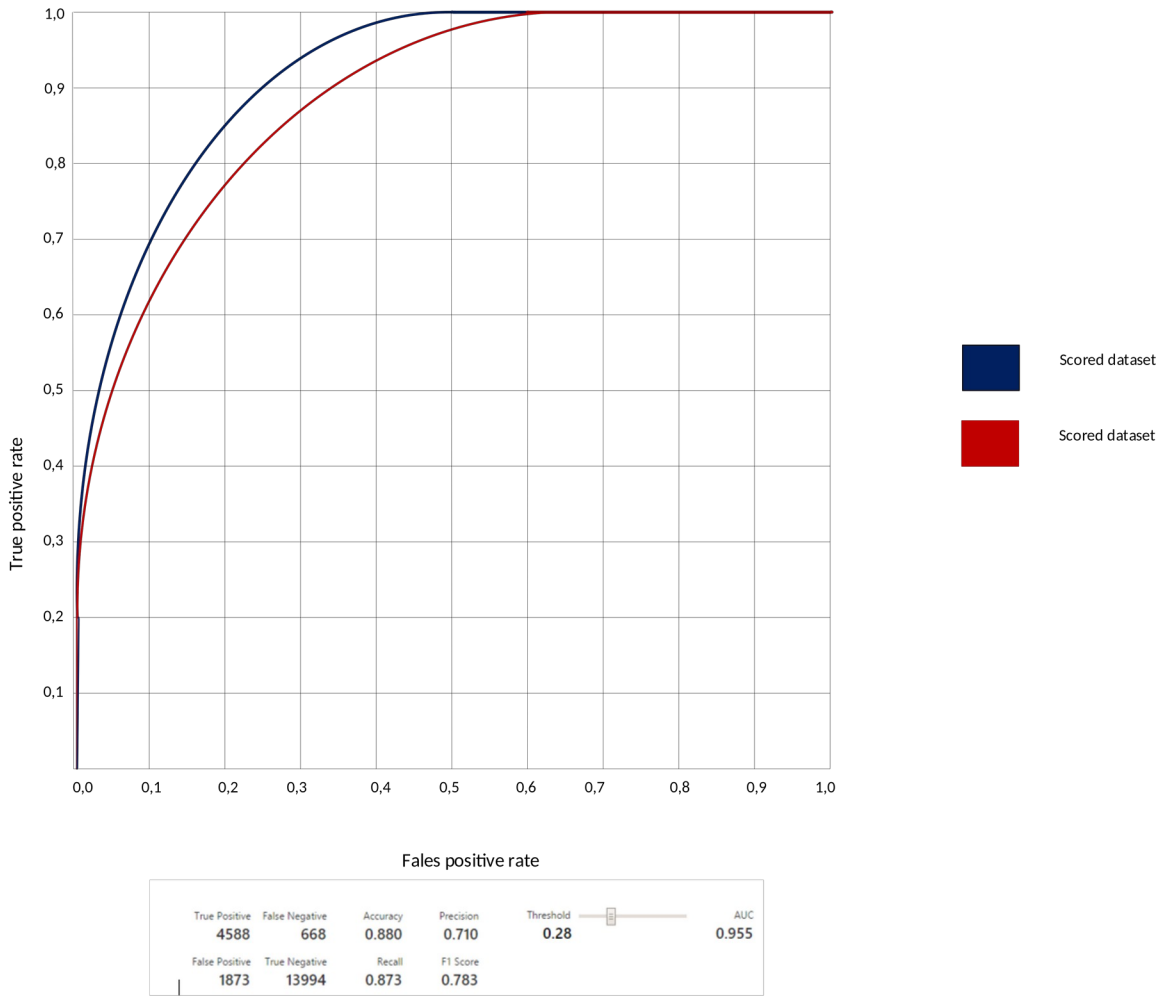


Рисунок Error: Reference source not found.9 – Результаты алгоритма нейронной сети

После получения модели, функционирующей с приемлемой точностью, необходима публикация проведенного эксперимента в виде веб-сервиса. Для операции публикации требуется нажатие кнопки «Publish Web Service» в Azure ML Studio. Далее идет выполнение тривиальных процедур.

Результатом будет являться развертывание Azure ML отказоустойчивого (SLA 99,96%) масштабируемого веб-сервиса. После публикации сервиса будет получен доступ к странице документации по API сервиса, которая называется API help. На ней выполнено общее описание сервиса, а кроме того, описаны форматы ожидаемых входных и выходных сообщений, и примеры вызова данного сервиса на языках высокого уровня Python, C# и R.

Основной принцип вызова разработанного сервиса со стороны программного клиента представлен на Рисунок Error: Reference source not found.10.

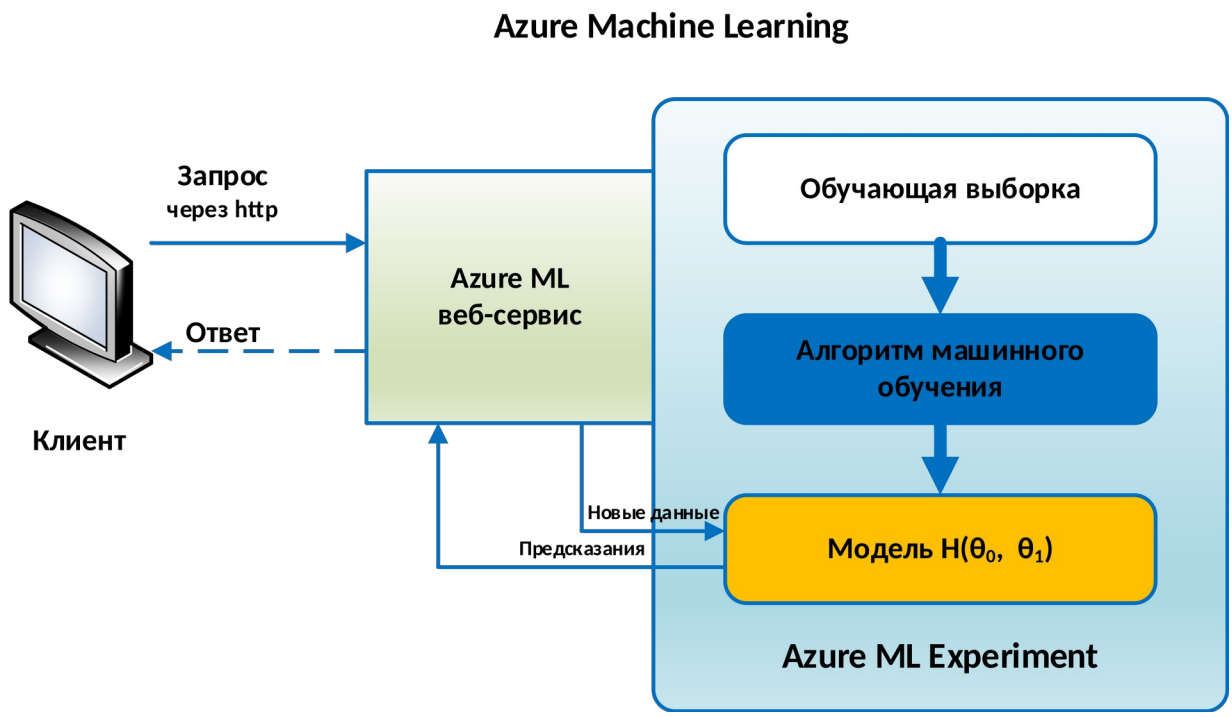


Рисунок Error: Reference source not found.10 – Схема вызова сервиса

Разработанная система, безусловно, обладает рядом ограничений. Так в качестве одного из узких мест можно говорить, непосредственно, о самой системе Azure ML. Поэтому важным является понимание ограничений Azure ML в целом, а также веб-сервисов Azure ML. Однако данный вопрос плохо освещен как в официальной документации, так и в соответствующем community.

Нет практически никакой информации, касающейся throttled policy конечных точек веб-сервиса Azure ML: неизвестно наибольшее допустимое значение параллельных запросов веб-сервису Azure ML (в ходе тестирования эмпирически было проверено значение 25 параллельных запросов на одну конечную точку), а также максимально возможный размер, которым может обладать принимаемое сообщение (это актуально для работы сервиса в пакетном режиме).

Менее важно, однако существует вопрос, связанный с наибольшим допустимым размером входных данных (Criteo Labs был размещен набор данных, имеющий размер в 1 Тб), наибольшим числом прецедентов и предикторов, которые могут быть переданы на вход алгоритма машинного обучения в Azure ML.

Также критически значимым является уменьшение времени ответа веб-сервиса Fraud Predictor ML, а также времени, затрачиваемого на переобучение модели до минимальных значений, однако алгоритм достижения данной цели пока не находит своего отражения в официальной документации.

Резюмируя, можно утверждать, что со стороны антифрод-сервиса отсутствуют ограничения клиентам как в процессе предварительной проверки платежей, так и в последующем изучении результатов предсказаний. Проведение предварительных специфических для бизнес-процесса проверок, а также принятие окончательного решения, касающегося проведения (принятия) или отклонения платежа очевидно являются теми задачами, которые не находятся в сфере ответственности антифрод-системы.

Неважно, какая роль у клиента – платежная система, интернет-магазин, банк, для всех них может быть сформулирован ряд следующих рекомендаций:

- обязательное осуществление проверки платежей, как с применением технологий, принятых в конкретной отрасли (fingerprint и т.д.), так и с применением собственных накопленных о клиенте знаниях (история заказов, например);
- проведение интерпретации результата с использованием следующего алгоритма: при вероятности фрода менее 0,35 оплата может приниматься без 3-D Secure, при значении вероятности в интервале 0,35-0,90 оплата должна приниматься с включенным 3-D Secure, при значении вероятности фрода выше 0,9 платеж должен быть блокирован;
- необходимо осуществлять выбор уровней, описанных выше, основываясь на собственных аналитических исследованиях с систематическим

пересмотром их (выполнение минимизации упущенных выгод и штрафов, причиной которых является фрод).

Заключение

В ходе работы, целью которой является исследование проблемы систем информационной безопасности на основе фрод-мониторинга, были решены все поставленные задачи исследования.

Проведен анализ проблемы использования платежных систем для мошеннических схем. Выяснено, что различного рода злоупотребления и правонарушения в банковской сфере относятся экспертами к значительным угрозам, оказывающим негативное влияние на экономические интересы любого общества. Интенсивное развитие и внедрение актуальных информационных технологий в мире повлекло за собой активизацию процессов формирования глобального информационного пространства, и, как неизбежный результат, привело к появлению новых вызовов и угроз.

Изучены способы и методы реализации мошеннических действий со счетами и банковскими картами. Практика правоохранительных органов свидетельствует о том, что к самому распространенному виду мошенничества с пластиковыми картами относится мошенничество, основанное на применении поддельных карт, и кража реквизитов действующих карт.

Анализ технологий противодействия мошенничеству показал, что в случае использования дистанционного банковского обслуживания, основную роль в борьбе с мошенническими действиями должны играть сами клиенты, которые и осуществляют переводы своих средств на счета сторонних организаций. При этом банки должны предоставлять клиентам полную информацию о возможных вариантах мошенничества и средствах защиты от него.

Исследованы принципы работы антифрод-системы, общую схему функционирования которой можно описать следующим образом: в момент совершения оплаты с помощью банковской карты осуществляется сбор

совокупности показателей определенного типа (у каждой из антифрод-систем они различаются) – это и IP-адрес компьютера, и статистика оплат по данной карте и многое другое.

Выработаны предложения по решению проблем обеспечения защиты в системах обработки больших данных в финансово-кредитных организациях. В результате работы был разработан проект антифрод-системы с использованием облачных сервисов Azur.

Список использованных источников

1. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер (Издание с Поправкой). Дата введения 2018.01.01. М. Стандартинформ, 2020. 34 с.
2. ИСО/МЭК 29115:2013 (ISO/IEC 29115:2013) Информационная технология. Техника безопасности. Схема обеспечения идентификации объекта. Введен: 04.2013. 44 с. – Режим доступа. – URL: https://www.iso.org/ru/standard/45138.html.
3. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». Собрание законодательства Российской Федерации, N 45, 05.11.2012, ст.6257. – Режим доступа. – URL: http://docs.cntd.ru/document/902377706.
4. Приказ ФСТЭК России от 6 декабря 2011 г. N 638. «Требования к системам обнаружения вторжений». Введен в действие: 15.03.2012. – Режим доступа. – URL: https://fstec.ru/normotvorcheskaya/poisk-po-dokumentam/118-tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/prikazy/394-informatsionnoe-pismo-fstek-rossii
5. Центральный банк Российской Федерации. Положение «О требованиях к защите информации в платёжной системе Банка России» от 23.12.2020. N 747-П. – Режим доступа. – URL: http://www.cbr.ru/Queries/UniDbQuery/File/90134/1243.
6. Центральный банк Российской Федерации. Положение «О платежной системе Банка России» от 24 сентября 2020 г. N 732-П. – Режим доступа. – URL: https://www.cbr.ru/PSystem/acts/.

7. Болонин А.И. Мошенничество в электронных платежных системах // Вестник Академии. 2016. № 1. Т. 77-80.

8. Варламова С.Б., Васильев Ю.А. Классификация способов мошеничества в банковских IT-технологиях и современные методы защиты от фрода // Финансовые рынки и банки. 2019. № 2. С. 41-44.

9. Вельц С.В. OMNIREACT - кросс-канальный фрод-мониторинг // Свидетельство о регистрации программы для ЭВМ RU 2018666995, 27.12.2018. Заявка № 2018660981 от 28.09.2018.

10. Верхотуров В.К., Ткаченко С.Н. Использование машинного обучения в системах фрод-мониторинга // В сборнике: Сборник методических рекомендаций по вопросам развития технических и естественных наук. Нижний Новгород, 2019. С. 52-59.

11. Гришина Е.А. Риски в платежных системах: мошеннические схемы в мире банковских карт // Финансы и кредит. 2018. Т. 24. № 6 (774). С. 1280-1291.

12. Журин В.О. Основные проблемы при разработке системы фрод-мониторинга на основе машинного обучения // В сборнике: Научные исследования: теоретико-методологические подходы и практические результаты. Материалы международной научно-практической конференции НИЦ «Поволжская научная корпорация». 2018. С. 210-213.

13. Замятина Е.В., Луценко А.В. Влияние фрод - мониторинга на экономическую безопасность коммерческом банке // В сборнике: Инструменты и механизмы современного инновационного развития. сборник статей Международной научно-практической конференции. 2018. С. 71-75.

14. Кашина Ю.А. Особенности преступлений в сфере безналичных расчетов с использованием банковских карт // Бюллетень науки и практики. 2018. Т. 4. № 5. С. 574-582.

15. Копелиович Д.И., Журин В.О. Сравнительная характеристика систем фрод-мониторинга. Основные подходы к построению механизма

обнаружения // Современные научные исследования и разработки. 2018. № 3 (20). С. 302-304.

16. Левашов М.В., Кухаренко А.В. Эффективность критерия отношения правдоподобия в статистической модели фрод-мониторинга в интернет-банкинге // Вопросы защиты информации. 2018. № 2 (121). С. 66-71.

17. Левашов М.В., Овчинников П.В. Эффективность классификаторов для выявления фрода в финансовых транзакциях // Вопросы кибербезопасности. 2019. № 5 (33). С. 63-69.

18. Ляхова А.О., Элмурадов Т.Д. Мошенничество в интернете и способы защиты от нее // Теория и практика современной науки. 2020. № 3 (57). С. 157-159.

19. Медведева М.Б., Васин М.М. Проблемы защиты от мошенничества в операциях с платежными картами в системе КБО физических лиц и развитие ее законодательного обеспечения // Финансовые рынки и банки. 2019. № 1. С. 30-35.

20. Нечаев А.В. Антифрод системы и принципы их работы // Труды Северо-Кавказского филиала Московского технического университета связи и информатики. 2019. № 2. С. 88-94.

21. Шейнов А.И., Пастухова О.Н. Современные способы выявления мошеннических транзакций в сети интернет // Вестник Тульского филиала Финуниверситета. 2019. № 1-2. С. 311-313.

22. Group-IB — одна из ведущих международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий. – Режим доступа. – URL: https://www.group-ib.ru/about.html

23. Аналитический комплекс «FRAUD RECORDER» // Свидетельство о регистрации программы для ЭВМ RU 2018617465, 25.06.2018. Заявка № 2018613591 от 04.04.2018.

24. Глобальное исследование по вопросам мошенничества в банковской сфере. – М.: ООО «КПМГ Налоги и консультирование». 2019. 28˚с.

25. Программа для ЭВМ система поиска аномалий и построения объектных траекторий в транзакционных данных (СПАПОТ) // Свидетельство о регистрации программы для ЭВМ RU 2020613918, 24.03.2020. Заявка № 2019666822 от 17.12.2019.

26. Расследования высокотехнологичных преступлений Борьба с компьютерными, финансовыми, корпоративными преступлениями по всему миру. – Режим доступа. – URL: https://www.group-ib.ru/

27. Гайкович Ю.В, Першин А.С. Безопасность электронных банковских систем. // М: Единая Европа, 1994 г.

28. Линьков И.И. и др. Информационные подразделения в коммерческих структурах: как выжить и преуспеть. // М: НИТ, 1998 г.

29. Панкратов Ф.Г. Коммерческая деятельность : учеб.для вузов / Ф. Г. Панкратов. - Изд. 8-е, перераб. и доп. // М. : Дашков и Ко, 2015. - 502 с.

30. Петренко С.А. и Курбатов В.А. Политики безопасности компании при работе в интернет // ДМК Пресс, 2011.

31. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / М: Гостехиздат**,** 2016