## Министерство образования и науки Республики Казахстан

## Комитет науки

ТОО «НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ ИННОВАЦИОННОЙ ЭКОНОМИКИ»

|  |  |  |
| --- | --- | --- |
| УДК 338:004;330.47;338:002.6  № госрегистрации 0118PK00753  МРНТИ 06.54.51  Инв. №: АР05136146 |  | Утверждаю  Директор НИИИЭ  к.э.н., доцент  \_\_\_\_\_\_\_\_\_\_\_\_К.О. Нургалиева  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2018 г. |

ОТЧЕТ

О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

по теме:

ОБЛАЧНЫЕ ПРИЛОЖЕНИЯ В УПРАВЛЕНИИ ИНФОРМАЦИОННЫМИ ПОТОКАМИ НА ФИНАНСОВЫХ РЫНКАХ

(промежуточный)

Руководитель темы PhD, доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.С. Аубакиров

подпись, дата

Алматы 2019

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель темы,

СНС, PhD, доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.С. Аубакиров (введение, заключение)

(подпись, дата)

Исполнители темы \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е.К. Толенбеков (раздел 1-2, заключение)

(подпись, дата)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г. Р. Молдаш (раздел 2)

(подпись, дата)

Нормоконтролер \_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.Р. Качиев

(подпись, дата)

СОДЕРЖАНИЕ

|  |  |
| --- | --- |
| Введение | 4 |
|  |  |
| 1 Исследование современного состояния развития web-технологий и облачных технологий на финансовом рынке РК | 6 |
| * 1. Современное состояние развития web-технологий | 6 |
| * 1. Облачные технологии на финансовом рынке | 9 |
| 1. Определение круга задача по приему, передаче и хранению больших данных | 13 |
| * 1. Понятие противодействия отмыванию преступных доходов и финансированию терроризма (под/фт) и методы оценки | 13 |
| * 1. Мониторинг применения облачных технологий в платежных организациях | 16 |
| 2.3 Системы управления бизнес-правилами, основанные на теории графов для анализа транзакций в реальном времени | 19 |
| * 1. Поиск аномалий в пользовательском поведении на основе истории проведенных транзакций | 25 |
| * 1. Визуализация потока транзакции в виде графов с помощью современных инструментов | 29 |
| Заключение | 37 |
| Список использованных источников | 38 |
| Приложение А. Календарный план работ |  |
| Приложение Б. Перечень опубликованных работ по теме за 2019 год |  |
| Приложение В. Список использованных зарубежных информационных ресурсов |  |
| Приложение Г. Форма ФМ-1 |  |

ВВЕДЕНИЕ

Активно растет число трансакций, построенных на обмене продукцией или на использовании альтернативных валют в рамках онлайн-платформ; широкое распространение получает совершенно новый тип проведения финансовых операций между устройствами без участия человека. Нарастает важность проблем кибербезопасности, защиты персональных данных, идентификации личности в информационном пространстве при совершении трансакций. Объем венчурных инвестиций в финансовые технологии увеличился за последние 5 лет, что подтверждает рост интереса к технологическим инновациям в данной сфере. Активно развиваются компании за пределами традиционной индустрии финансовых услуг.

28 августа 2009 года президент Казахстана подписал закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма". 9 марта 2010 года этот закон вступил в силу. С этого момента начинается деятельность Комитета по финансовому мониторингу как национального подразделения финансовой разведки.

В 2020 году Республике Казахстан предстоит пройти второй раунд взаимных оценок, в рамках которой ЕАГ будет оценена система финансового мониторинга Казахстана [1]. ЕАГ будет оценивать соответствие правовой и институциональной системы ПОД/ФТ Республики Казахстан установленным международным стандартом ФАТФ и присваивать стране рейтинги технического соответствия и эффективности системы. Присвоенные рейтинги накладывают определенные обязательства, невыполнение которых может привести к санкциям экономического характера, применяемых к стране. Согласно международным стандартам ФАТФ, каждая страна должна оценить свои риски отмывания денег и финансирования терроризма. С этой целью на уровне закона создана правовая основа для проведения такой оценки, приняты необходимые подзаконные правовые акты [2], которые определяют правила проведения такой оценки рисков отмывания денег и финансирования терроризма в Казахстане и по результатам которой предусматривают принятие на уровне Правительства решения, направленного на минимизацию выявленных рисков.

Ежегодно требования законодательства к субъектам финансового мониторинга ужесточаются, усиливаются санкции за позднее обнаружение ненадежных операций. Организациям грозят не только значительные репутационные потери, но и риски выплат высоких штрафов, приостановление деятельности и даже лишение лицензии. Крупные компании выполняют до 20 млн транзакций в день, в то время как обнаружение подозрительных операций связано с ручной работой, что может вызвать риск ошибок и ложных срабатываний. Именно поэтому крайне важна разработка и внедрение высокотехнологичных AML-систем, отвечающих всем современным тенденциям и требованиям цифровой экономики. Среди современных инструментов AML можно отметить big data, machine learning, AI. Этот инструментарий позволяет совершенствовать риск-ориентированные подходы и дает возможность успевать за развитием технологий отмывания денег.

Аббревиатура ПОД/ФТ дословно расшифровывается как «противодействие отмыванию денег и финансированию терроризма» (зарубежный аналог AML/CFT – Anti-money laundering and combating the financing of terrorism). Под этим термином принято понимать сложившуюся международную систему борьбы с легализацией преступных доходов и финансированием терроризма, включающую национальные подразделения финансовой разведки, надзорные и правоохранительные органы, межправительственные структуры и организации [3].

Ключевым элементом ПОД/ФТ служит сбор сведений о подозрительных операциях и ненадлежащих клиентах службами внутреннего контроля банков, страховых компаний, организаций – участников рынка ценных бумаг и др. подотчетных структур. Противодействием и регулированием данной проблемой занимается межправительственная организация ФАТФ (FATF) которая формирует мировые стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризма (ПОД/ФТ), а также занимается оцениванием соответствия национальных систем ПОД/ФТ этим стандартам.

Для того что бы Казахстан в полной мере выполнял как требования Законодательства, так и требования международной организации ФАТФ, возникает необходимость в создании системы по противодействию отмыванию денег и финансированию терроризма для Платежных организаций, которая будет соответствовать всем стандартам.

1. Исследование современного состояния развития web-технологий и облачных технологий на финансовом рынке РК
   1. Современное состояние развития web-технологий

Современные инновации и новые инициативы в области веб-разработки, от текущих разработок по ИИ через машинное обучение до блокчейна и криптовалюты, влияющих на мировую экономику. Действительно, когда дело доходит до технологий, все так непостоянно и непредсказуемо. Время от времени прогресс и прорывы удивляют нас и меняют наш мир. Цифровая революция продолжает определять тенденции и искушать нас новыми технологиями, от которых разработчики и программисты повсюду будут без ума. Люди всегда рады узнать о наиболее востребованных языках / платформах, а также о последних обновлениях веб-дизайна и программных приложений.

ИИ или боты. Искусственный интеллект (ИИ) — это интеллект, отображаемый машинами для имитации человеческого интеллекта и выполнения когнитивных функций, таких как способность учиться, собирать данные, анализировать информацию, понимать эмоции или решать сложные проблемы. Потребность в коммуникационных решениях с поддержкой искусственного интеллекта, решениях для автоматизации нескольких задач и аналитики станет более распространенной в этом году.

Уже сейчас мы видим, как чат-роботы, виртуальные помощники (такие как Amazon Alexa, Apple Siri и Microsoft Cortana, Яндекс Алиса) и голосовые роботы помогли бизнесу вовлечься и изменили социальное взаимодействие. Их развитие дало возможность универсальному каналу для цифрового обслуживания клиентов и гарантированной согласованности между голосом, чатом, обменом сообщениями и веб-сайтами.

С помощью исследований в области машинного обучения (ML) и искусственных нейронных сетей (ANN), ИИ может достичь своих желанных целей - успешно симулировать подлинную человеческую эмпатию и демонстрировать общие знания.

ИИ широко применяют в таких областях как: образование, здравоохранение, бизнес, безопасность, в индустрии моды и др.

JavaScript остается наиболее популярным языком в течение последних шести лет, и он продолжает развиваться согласно отчету Stack Overflow 2018. Развитие его фреймворков, библиотек за последние годы доказало, что у него есть что предложить на рынке. Неудивительно, что это лучший язык для разработчиков, поскольку он обеспечивает совершенно новый опыт гибкости, сложности и мощи.

Angular – JavaScript фреймворк созданный компанией Google, целью которого является создание фреймворков, наиболее подходящих для разработки приложений. Он быстро разрабатывается и хорошо работает с другими библиотеками, поскольку позволяет модифицировать и заменять функции в соответствии с уникальным рабочим процессом разработки. Кроме того, он легко расширяется, читается и восприимчив к будущим изменениям в WEB API. Команда Angular проделала большую работу по улучшению Angular на протяжении многих лет. Теперь с Angular v8 можно автоматически добавлять или удалять полифилл отраженных метаданных, а его обновленный интерфейс командной строки предлагает пользователям вводить общие команды.

React – это JavaScript библиотека, поддерживаемая Facebook и большим сообществом разработчиков и компаний [4]. Он создает интерактивные пользовательские интерфейсы, которые отлично подходят для одностраничных приложений и мобильных приложений. Кроме того, он может использовать данные и разрешать изменения даже без перезагрузки страницы. по сравнению с Angular, React имеет впечатляющий виртуальный DOM, который легче изучать и обеспечивает бесценную производительность.

Vue.js - это библиотека с открытым исходным кодом для создания пользовательских интерфейсов и одностраничных приложений. Ее создал Эван Ю, основатель Vue Technology LLC, который ранее работал в Google, используя Angular в своих проектах [5]. Благодаря своей популярности Vue.js теперь признан одним из лучших фреймворков за свою красоту и почти совершенство. Он легче, проще в использовании и эффективнее по сравнению с React, функции которого очень похожи на него. Кроме того, он имеет богатую библиотеку компонентов, стабильные API, отличную поддержку прокси и уникальную анимацию SVG.

Progressive Web App. Прогрессивные веб-приложения (или PWA) по-прежнему являются частью самых популярных веб-тенденций 2019 года. Эти современные веб-приложения загружаются как обычные веб-страницы или веб-сайты, но имеют высокий уровень функциональности. Они могут загружаться мгновенно, независимо от состояния сети и выбора браузера, потому что они построены с прогрессивным улучшением - стратегией веб-дизайна, которая в первую очередь делает основной контент веб-страницы.

PWA обеспечивает мгновенную, независимую и надежную работу пользователей без проблем с кэшем. Это безопасно, потому что оно используется через HTTP, чтобы предотвратить отслеживание содержимого и подделку данных. Кроме того, PWA прост в использовании, удобен в установке и простоте, что расширяет возможности существующих веб-технологий благодаря сервисным работникам и другим встроенным функциям. Он может быть передан через URL-адрес и может повторно привлечь пользователей с помощью веб-push-уведомлений.

Мобильные адаптированные сайты — это сайты, которые хорошо работают на смартфонах. Они используют сенсорное управление и могут поместиться на маленьких экранах для быстрой навигации. Кроме того, они быстро загружаются благодаря своим фантастическим функциям, которые сокращают ввод данных.

В 2016 году команда Google создала собственный первый поисковый индекс, оптимизированный для мобильных устройств. Это один из лучших подходов Google, позволяющий посетителям смартфонов предоставлять пользователям одинаковое качество обслуживания при отображении результатов поиска независимо от используемого ими устройства.

Хотя аппаратные средства и пользовательский интерфейс различаются для настольных компьютеров и мобильных устройств, многие компании приняли стратегию запуска цифрового трафика и повышения конкурентоспособности своего веб-сайта. Это мудрый шаг для количества пользователей мобильных телефонов в мире. Ожидается, что к 2020 году он достигнет пятимиллиардной отметки, сообщает Statistica.com.

Блокчейн Технология. Благодаря Сатоши Накамото, неизвестному человеку, который создал и разработал биткойн, мы вступили в эру биткойнов [6]. И из этого вытекает технология Blockchain, расцвет которой все еще очевиден в наши дни. Блокчейн - это открытая и распределенная бухгалтерская книга, известная своей защищенной конструкцией, децентрализованным консенсусом и блоками с измененным сопротивлением. Он предназначен для снижения финансовых затрат бизнеса, сокращения частоты расчетов по транзакциям и улучшения движения денежных средств, подкрепленных прозрачными записями / данными.

Поскольку она управляется одноранговой сетью, у нее есть строгий протокол для межузловой связи и новый процесс проверки блоков, благодаря которому она получила звание «Первая и самая надежная глобальная криптовалютная компания».

Кибербезопасность. С тех пор как утечки данных, киберугрозы, взлом сайтов и кража данных представляют собой ужасную угрозу, скрывающуюся в самых мрачных тенях технического прогресса и научного прогресса, 2019 год не станет исключением. Таким образом, кибербезопасность не исчезнет в ближайшее время.

Кибербезопасность или защита информационных технологий (ИТ-безопасность) — это компьютерные системы защиты от кражи, нарушения работы или неправильного направления, а также от повреждения оборудования, программного обеспечения или электронных данных [7].

Эксперты по ИТ-безопасности предполагают, что эти киберпреступники не остановятся, чтобы искать уязвимости и жертв. Имея это в виду, отдельным лицам, компаниям, сообществам и отраслям необходимо укрепить свою систему безопасности для защиты своей личной информации, серверов и баз данных. Поэтому для борьбы с кибер вызовами современного мира необходимы упорные решения.

Веб индустрия проделывает большую работу, придумывая новые фреймворки, тенденции дизайна и разработки мобильных веб-приложений, чтобы удовлетворить постоянные требования и ожидания человечества. И несмотря на некоторые неудачи и недостатки, он продолжает процветать, процветать и улучшаться.

1.2 Облачные технологий на финансовым рынке РК

Международный опыт применения сервисной модели информатизации. В большинстве передовых стран мира разработаны и реализуются стратегии или комплексные программы информационного развития как общества в целом, так и отдельных сфер деятельности. Облачные вычисления являются одним из наиболее популярных направлений развития инфокоммуникационной отрасли. По всему миру операторы связи развёртывают вычислительные платформы для предоставления облачных сервисов крупным корпорациям, компаниям малого и среднего бизнеса и частным пользователям [8].

Согласно данным исследования Citrix и IDC, проведенного в 2017 году, во всём мире 94% компаний активно готовятся к переходу на облачные технологии: они занимаются либо пересмотром и трансформацией, либо модернизацией своих сетевых инфраструктур, чтобы упростить доставку приложений.

Основные цели перехода компаний от локальной модели к концепции доставки приложений через облако — повышение безопасности и снижение затрат, в том числе за счёт оптимизации работы IT-отделов и специалистов. В ходе исследования также была выявлена высокая потребность в комплексном подходе при реализации стратегии доставки приложений. Большинство организаций (98%) склоняются к единому решению вместо интеграции различных систем от нескольких производителей.

Исходя из принятой в современном мире классификации, облачные сервисы предоставляются в следующих моделях:

* Программное обеспечение как услуга (SaaS, англ. Software-as-a-Service) – модель, в которой потребителю предоставляется возможность использования прикладного программного обеспечения провайдера, работающего в облачной инфраструктуре и доступного из различных клиентских устройств или посредством тонкого клиента, например, из браузера (например, веб-почта) или посредством интерфейса программы.
* Платформа как услуга (PaaS, англ. Platform-as-a-Service) – модель, когда потребителю предоставляется возможность использования облачной инфраструктуры для размещения базового программного обеспечения для последующего размещения на нём новых или существующих приложений (собственных, разработанных на заказ или приобретённых тиражируемых приложений).
* Инфраструктура как услуга (IaaS, англ. Infrastructure-as-a-Service) –предоставляется как возможность использования облачной инфраструктуры для самостоятельного управления ресурсами обработки, хранения, сетями и другими фундаментальными вычислительными ресурсами, например, потребитель может устанавливать и запускать произвольное программное обеспечение, которое может включать в себя операционные системы, платформенное и прикладное программное обеспечение.

Мировой рынок облачных решений и услуг растет интенсивно. Согласно результатам исследования мирового рынка облачных услуг, проведенного аналитической компанией Gartner, в 2016 году продажи инфраструктурных IaaS-решений поднялись на 56%, чему способствовал растущий спрос на услуги перевода ИТ-инфраструктуры в облако и высокопроизводительные нагрузки, вроде искусственного интеллекта, Интернета вещей и аналитики. По исследованию, проведенному в 2011г., 80% организаций Европы, использующих облачные технологии, снизили свои расходы на 10-20%. За счет применения облачных технологий снижаются капитальные и текущие (эксплуатационные) расходы и повышается уровень использования оборудования, который на данный момент составляет 10% в государственном секторе. Т.е. фактически 90 % закупленного оборудования в государственном секторе Европы простаивает, а значит, используется неэффективно.

Позитивную тенденцию в развитии облачных технологий можно наблюдать и в Казахстане. Развитие отечественной цифровой инфраструктуры и достижение скоростей в 10–30 Мбит/с сделало целесообразным использование облачных технологий. В республике в основном используются программные продукты от крупных поставщиков, непосредственно казахстанских разработок немного [9].

Отечественные IT-компании, работающие на рынке, в большинстве своем являются интеграторами, то есть оказывают услуги по конфигурации существующего решения под нужды конкретного бизнеса, и это не зависит от того, использует клиент облачную или «коробочную» версию. Тем не менее казахстанские разработчики программного обеспечения тоже все чаще предлагают облачные сервисы.

Поиск облачных IaaS-провайдеров Казахстана позволил сформировать список основных компаний, предоставляющих эти услуги [10].

* «ИТ-ГРАД» – международный сервис-провайдер, который предоставляет облачные услуги на территории Казахстана с 2015 года. Является первым сервис-провайдером VMware на территории СНГ, работает много лет на этом рынке. Предоставляет IaaS-услуги (виртуальный дата-центр Vmware vDC, виртуальная СХД), и облачные услуги в модели SaaS (почта, антивирус, 1С, корпоративный портал и другие). Открыла официальное представительство и размещает оборудование на территории РК.
* iD Host – хостинговая площадка АО «Казахтелеком». Предоставляет услуги IaaS – vDC (виртуальный дата-центр), а также услуги хостинга (Windows и Linux), VPS (VDS) (виртуальный выделенный сервер), Colocation (аренда юнита и стойки), аренду физического оборудования, виртуальную СХД, облачные услуги (почта, телефония, конференц-связь и другие). Крупный провайдер, лидер на рынке Казахстана с высоким качеством услуг, ориентирован на серьезные enterprise-проекты.
* «Казтелепорт» – дочерняя организация Народного банка Казахстана. Предоставляет услуги IaaS – vDC (виртуальный дата-центр), а также VPS (VDS), Colocation (аренда юнита и стойки), виртуальная СХД, облачные услуги (видеоконференции и виртуальная 1С). Провайдер имеет два собственных ЦОД, что обеспечивает высокую отказоустойчивость (Disaster recovery plan), и является официальным облачным провайдером Vmware.
* cloud24.kz – ТОО «Интернет решения». Изначально облачный провайдер, не имеющий своего ЦОД и предоставляющий услуги IaaS и SaaS. Основное направление IaaS – VPS (VDS), а также облачные услуги (почта, коммуникации, корпоративный портал, БД) с использованием платформы Microsoft Hyper-V.
* AHOST.kz – дата-центр ТОО «Академсеть». IaaS-провайдером можно назвать с натяжкой, хоть компания и заявляет об этом. Предоставляет услуги VPS (VDS), VDI (виртуальное рабочее место), Colocation, аренда физического оборудования, виртуальная СХД, облачные услуги (почта, хостинг «Битрикс» и другие).

Существуют казахстанские разработки для электронного документооборота, решения на базе корпоративных порталов, разработки на медицинскую тему - из последнего можно привести в пример облачный сервис для медицинских центров - «Электронная клиника MedElement». Чтобы использовать эту информационную систему, медучреждению нужен только доступ в интернет - и можно автоматизировать все основные процессы: ведение электронного расписания приемов, заполнение медицинских карт, создание и ведение электронной базы пациентов и приемов, автоматическое формирование экономической и статистической отчетности.

Государственные органы и национальные компании активно внедряют облачные электронные системы документооборота и прочие облачные сервисы. Крупные компании, чаще всего банки, повсеместно разворачивают собственные корпоративные ЦОДы. К примеру, «Казахтелеком» запустил услугу облачного видеонаблюдения во всех областных центрах, а также городах Алматы и Астана, позволяющую каждому клиенту получать доступ к видео с камер наблюдения. При этом сама облачная платформа расположена в ЦОД в Павлодаре.

Несмотря на это, констатируют в КИРИ, в настоящее время рынок облачных технологий в РК тяжело назвать зрелым. Согласно данным комитета по статистике МНЭ РК, только 0,4% предприятий используют облачные IT-услуги.

По информации iKS-Consulting, основными игроками на рынке коммерческих ЦОД являются государственные органы или операторы связи. Лидером рынка коммерческих ЦОД является «Казахтелеком», которому принадлежат более 50% стоек в дата-центрах.

Доля облачных услуг в структуре доходов дата-центров РК растет, но при этом половина дохода ЦОД по-прежнему приходится на услуги коллокации и выделенного сервера. Основными факторами, которые влияют на особенности развития рынка дата-центров в республике, являются низкая плотность населения и географическая удаленность крупных городов, а также малый объем казахстанского контента. На рисунке 1 представлена популярность облачных сервисов для бизнеса РК.



Рисунок 1 - Популярность облачных сервисов для бизнеса РК

Примечание – Составлено на основе источника [10]

1. Определение круга задача по приему, передаче и хранению больших данных
   1. Понятие противодействия отмыванию преступных доходов и финансированию терроризма (под/фт) и методы оценки

В рамках данной главы рассматриваются понятия и ключевые элементы противодействия отмыванию денег и финансирования терроризма (далее – ПОД/ФТ). Проводится обзор межгосударственной организации FATF (ФАТФ) и региональных групп по типу ФАТФ: методики, стандарты и рекомендации. Выявляются преимущества и недостатки систем AML. Рассматривается текущее состояние Республики Казахстан по отношению к ПОД/ФТ.

Ключевым элементом ПОД/ФТ служит сбор сведений о подозрительных операциях и ненадлежащих клиентах службами внутреннего контроля банков, страховых компаний, организаций – участников рынка ценных бумаг и др. подотчетных структур. Противодействием и регулированием данной проблемой занимается межправительственная организация ФАТФ (FATF) которая формирует мировые стандарты в сфере противодействия отмыванию преступных доходов и финансированию терроризма (ПОД/ФТ), а также занимается оцениванием соответствия национальных систем ПОД/ФТ этим стандартам. Основным инструментом ФАТФ в реализации своего мандата являются 40 рекомендаций в сфере ПОД/ФТ, которые подвергаются ревизии в среднем один раз в пять лет. На рисунке 2 представлены страны с высоким уровнем риска, и которые находятся под постоянным мониторингом ФАТФ.

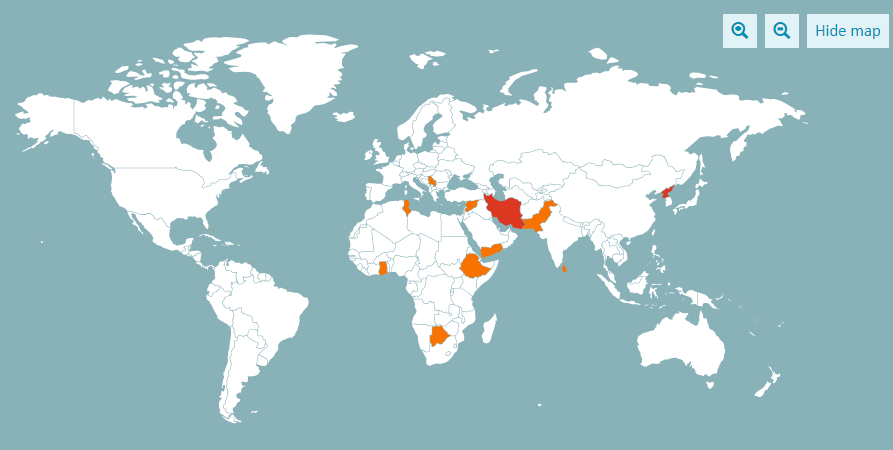


Рисунок 2 – Страны с высоким уровнем риска и которые находятся под постоянным мониторингом ФАТФ

Наблюдается одна особенность в странах-членов организации ФАТФ. Согласно их законодательству о борьбе с отмыванием денег, ответственность за выполнение этих процедур лежит на финансовых и иных учреждениях, а отнюдь на преступниках. Тем более — не на правительственных органах. В связи с этим на финансовые учреждения, такие как банки, биржи, инвестиционные компании, ломбарды, нотариусов, финансовые компании — возложены функции агентов финансового мониторинга. Они обязаны формировать и поддерживать эффективные риск-ориентированные процедуры, гарантирующие выявление рискованных операций и обозначение подозрительных участников финансового обращения. Информацию о выявленных рискованных операциях и их участниках агенты финансового мониторинга передают в орган финансового мониторинга (государственная структура со специальным статусом), который, в свою очередь, оценивает наличие криминальной компоненты в таких операциях и далее передает информацию в правоохранительные органы для реагирования. На время выяснения криминальности той или иной операции агент финансового мониторинга обязан заблокировать ее проведение, включая блокирование (замораживание) участвующих в данной операции активов. Одним из базовых принципов AML является [KYC — «Знай своего клиента»](https://hashtelegraph.com/kyc/) термин означающий, что субъекты финансового мониторинга должны идентифицировать и установить личность контрагента прежде чем проводить финансовую операцию. Это требование распространяется на получение разумно полных сведений о контрагентах-юридических лицах, характере их бизнеса и отдельных хозяйственных операций, для обеспечения которых проводится финансовая операция. В настоящее время требования и стандарты, направленные на реализацию этого принципа, устанавливаются на уровне национального законодательства, нормативных документов банковских регуляторов и международных организаций, таких как ФАТФ.

В задачи ФАТФ входит [3]:

* Выработка рекомендаций в области борьбы с отмыванием денег и финансированием терроризма.
* Проведение взаимных оценок в странах-участницах на предмет соответствия национальных законодательств и действующей практики в области борьбы с отмыванием денег и финансированием терроризма Рекомендациям ФАТФ.
* Изучение ситуации в странах, которые активно используются международной организованной преступностью для отмывания преступных доходов и финансирования терроризма. Взаимоотношения с такими странами руководство ФАТФ строит на основе «регионального подхода», т.е. взаимодействие с отдельными странами и группами стран постепенно переводится в плоскость сотрудничества с Региональными группами по типу ФАТФ (РГТФ).
* Организация и проведение на регулярной основе в различных странах мира конференций, симпозиумов и семинаров по финансовым и юридическим вопросам, а также проблемам в сфере законодательства в области противодействия отмыванию денег и финансированию терроризма (ПОД/ФТ).

ФАТФ регулярно проводит оценки выполнения своих рекомендаций. Составляемые по итогам этих мероприятий отчеты и доклады руководство организации направляет странам-участницам для передачи своим компетентным органам. На рисунке 3 представлены страны участники ФАТФ.

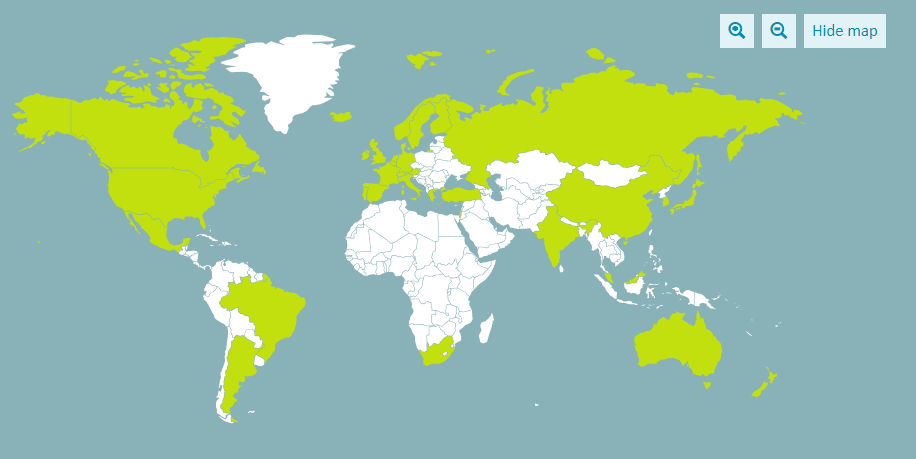


Рисунок 3 – Страны участники ФАТФ

Так же существует Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма является региональной группой по типу ФАТФ и объединяет Беларусь, Казахстан, Китай, Кыргызстан, Россию, Таджикистан, Туркменистан и Узбекистан. Статус наблюдателя в ЕАГ предоставлен 17 государствам и 15 международным и региональным организациям. Деятельность ЕАГ направлена на оказание содействия государствам региона в создании надлежащих правовых и институциональных основ противодействия отмыванию денег и финансированию терроризма, соответствующих стандартам ФАТФ. В рамках этой деятельности ЕАГ проводит взаимные оценки соответствия национальных противолегализационных систем своих государств международным стандартам; анализирует типологии в сфере легализации преступных доходов и финансирования терроризма с учетом особенностей Евразийского региона, а также реализует программы технического содействия государствам-членам группы, включая обучение кадров. На рисунке 4 представлены страны участники ЕАГ.

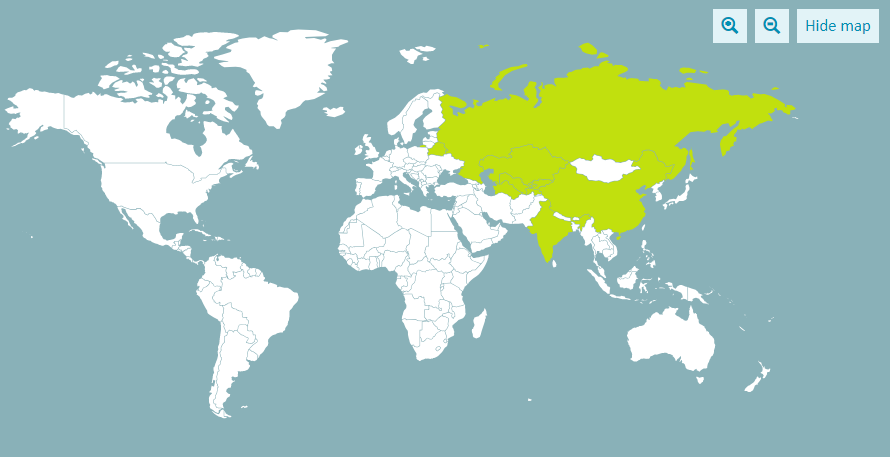


Рисунок 4 – Страны участники ЕАГ

* 1. Мониторинг применения облачных технологий в платежных организациях

Противодействие легализации доходов, полученных преступным путем (Anti-Money Laundering, или AML), является одной из наиболее актуальных проблем, которые стоят сегодня перед кредитными организациями.

AML-решение позволяет:

* Идентифицировать клиентов:

1. Сбор обязательной информации о клиентах. Ведение и периодическое обновление анкет клиентов.
2. Определение категории риска причастности клиента к «отмыванию» в зависимости от собранной информации, а в дальнейшем изменение категории риска в зависимости от деятельности клиента.

* Выявлять лиц, причастных к террористической деятельности:
  + 1. Проверка клиента на причастность к террористической деятельности.
    2. Проверка контрагентов в расчетных операциях клиентов на причастность к террористической деятельности. Приостановка расчетных операций. Отказ клиентам в обслуживании.
    3. Ведение и обновление списков террористов.
* Вести список публичных должностных лиц.
* Реализовать документооборот для отдела финансового мониторинга. Автоматизация процесса расследования инцидентов.
* Снизить количество ложных срабатываний за счет гибкой настройки сценариев.
* Произвести интеграцию с банковскими системами. Поддержка основных стандартов индустрии.
* Выявлять операции клиентов, подлежащие обязательному контролю.
* Выявлять необычные операции и сделки, а также мошеннические схемы, распределенные территориально и растянутые во времени.
* Предотвращать мошеннические операции.
* Подготовить обязательную и аналитическую отчетность.

На сегодняшний день, на рынке существует много AML решений, которые помогают субъектам финансового мониторинга, соблюдать все требования, указанные в законе «О противодействии отмывания денег и финансирования терроризма» и требования ФАТФ, тем самым оберегая их от карательных санкций, значительных репутационных потерь и, наконец, прекращения деятельности, но каждое из решений имеет определённые преимущества недостатки. Существующие AML-решения не способны обрабатывать операции в режиме онлайн. Интеллектуальный анализ выполняется фильтрацией транзакций в соответствии с определенными правилами, т.е. на него влияют установленные ограничения. Все отфильтрованные транзакции считаются «законными» и не проходят процедуру анализа. Существующие AML-системы рассматривают только индикаторы, непосредственно связанные с операцией или ее участниками, и не учитывают косвенных показателей. В результате возникают ложные срабатывания и ошибки.

В рамках проводимого в данной статье анализа, существующих AML систем, учитываются следующие функциональные возможности:

* обработка и анализ транзакций в автономном режиме;
* автоматизация мониторинга финансовых процессов организации;
* расширенный анализ данных клиентов;
* оценка надежности юридических лиц через базу данных;
* высокая скорость принятия решений;
* возможность автоматической корректировки алгоритмов анализа данных с целью выявления устойчивых закономерностей, а также прямых и косвенных связей между объектами;
* рассмотрение официальных требований Законодательства страны;

Системы используют следующие исходные данные для анализа:

* сведения о транзакции;
* подробную информацию о контрагентах сделки;
* историю транзакций (график транзакций);
* отрезок пути транзакции для тренировки системы (набор транзакций с тегами «подозрительный / соответствующий»).

На рынке представлены следующие решения: SAS AML, Oracle Mantas AML, Nice Actimize AML, FLEXTERA. В основном, среди данных систем можно выделить следующие преимущества [9]:

* полная автоматизация мониторинга финансовых процессов организации, включая оценку подозрительных транзакций, проведение расследований;
* применение принципа KYC;
* анализ сценария;
* высокая скорость принятия решений о подозрительных операциях;
* предоставление трафика средств в транзакциях в виде графика;
* конструктор отчетов.

А также, следующие недостатки систем:

* обработка и анализ транзакций возможны только в режиме отсрочки;
* невозможность самообучения системы по фактическим данным – только путем ручной корректировки правил;
* отсутствие анализа для расширенного уровня данных по юридическим лицам – участникам сделок;
* чрезвычайно высокая стоимость лицензирования, внедрения и владения. Решение могут себе позволить только крупные банки.

Казахстан с 2004 года является членом Евразийской группы по противодействию легализации преступных доходов и финансированию терроризма (ЕАГ) региональная группа по типу ФАТФ.

28 августа 2009 года президент Казахстана подписал закон "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма". 9 марта 2010 года этот закон вступил в силу. С этого момента начинается деятельность Комитета по финансовому мониторингу как национального подразделения финансовой разведки. В 2011 году Комитет стал полноправным членом в Группе подразделений финансовой разведки "Эгмонт", которая объединяет подразделения финансовой разведки более 151-ти юрисдикции и представляет своим членам возможность обмена информацией с целью борьбы отмыванием денег и финансированием терроризма. С начала своей деятельности Комитет ведет постоянный диалог с субъектами финансового мониторинга. Выполнение международных стандартов ФАТФ является обязательным для любой страны – члена ООН в соответствии с Резолюцией Совета Безопасности ООН.

Такое регламентированное участие государственных органов, субъектов финансового мониторинга и профессиональных объединений субъектов является важнейшим условием всестороннего и успешного исследования по оценке рисков. В проведении оценки рисков в Казахстане принимают участие государственные органы, профессиональные объединения субъектов финансового мониторинга и субъекты финансового мониторинга. «Государственные органы привлекают к участию в оценки свои подведомственные научно - исследовательские и академические институты.

Казахстан выполняет следующие шаги по улучшение мероприятий по противодействию отмыванию денег и финансирования терроризма: 1) Вступление в региональную группу ФАТФ; 2) Создание нормативно правовой базы по ПОД/ФТ; 3) Применение автоматизированных решений. Один из таких решений является программный продукт от Казахстанской компании ТОО «Prime Source».

Система, созданная компанией ТОО «Prime Source», подходит только под определенные субъекты финансового мониторинга, такие как: Банки второго уровня, биржи и страховые организации. Но перед Уполномоченным органом так же должны отчитываться и платежные организации. Существующие системы AML не подходят для Платежных организаций, так как при регистрации, необходим только сотовый номер телефона, который во многих странах никак не регистрируется.

Ежегодно требования законодательства к субъектам финансово мониторинга ужесточаются, усиливаются санкции за позднее обнаружение ненадежных операций. Организациям грозят не только значительные репутационные потери, но и риски выплат высоких штрафов, приостановление деятельности и даже лишение лицензии. Крупные компании выполняют до 20 млн транзакций в день, в то время как обнаружение подозрительных операций связано с ручной работой, что может вызвать риск ошибок и ложных срабатываний. Именно поэтому крайне важна разработка и внедрение высокотехнологичных AML-систем, отвечающих всем современным тенденциям и требованиям цифровой экономики. Среди современных инструментов AML можно отметить big data, machine learning, AI. Этот инструментарий позволяет совершенствовать риск-ориентированные подходы и дает возможность успевать за развитием технологий отмывания денег.

* 1. Системы управления бизнес-правилами, основанные на теории графов для анализа транзакций в реальном времени

Управление бизнес-правилами – это технология создания, поддержания и размещения сервисов принятия решений на основе правил. Системы управления бизнес-правилами позволяют разработчикам и бизнес-пользователям быстро и легко разрабатывать правила, ориентированные на принятие решений. Например, для банка может работать правило:

* If перевод осуществляется за пределы банка
* then рассчитать комиссию в размере 1,5%.

Для мобильных операторов, может быть:

* If клиент использует тарифный план «Вечерний»
* and звонок после 17:00
* then рассчитать стоимость звонка 0.05 за минуту.

Для реализации этих правил используются BRMS-системы (business rules management systems - BRMS).

BRMS системы описывают логику принятия решений в виде системы бизнес - правил. Бизнес-правила указывают на выполнение некоторых действий в случае выполнения определенных условий. BRMS система позволяет менеджерам вынести решение вместе с заказчиками, которое будет удовлетворять обе стороны и соответствовать бизнес-логике предприятия. Доступность правил позволяет бизнес-пользователям быстро выполнять изменения, не вовлекая ИТ специалистов [11].

В общем виде бизнес-правило представляется в форме утверждения вида: eсли (условия), то (список действий), иначе (альтернативный список действий) и сразу же сохраняется в виде кода как показано на рисунке 5.

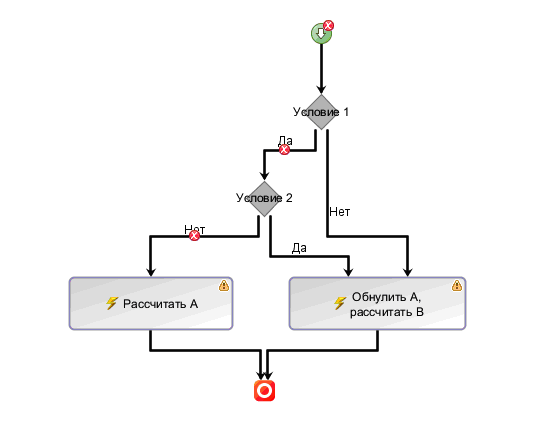


Рисунок 5 – Блок-схема и код бизнес-правил

Примечание – Составлено на основе исследований

Доступность правил позволяет бизнес-пользователям быстро выполнять изменения. Результатом становится повышение гибкости бизнеса, быстрое реагирование на динамику рынка и предоставление клиентам новых возможностей [12].

Основными преимуществами использования BRMS являются:

* система позволяет легко и гибко автоматизировать логику принятия решений в рамках бизнес-процессов компании;
* повышается прозрачность логики принятия решений в компании;
* снижается зависимость от программистов для внесения изменений в работу информационных систем;
* увеличивается контроль реализованной бизнес-логики;
* быстро реагирует на динамику рынка и предоставляет клиентам новых возможностей;
* в BRMS хранится вся история изменения бизнес-логики.

Возможности BRMS систем:

* Управление задачами сотрудников (возможность объединять отдельные задачи в бизнес-процессы, управлять переходами от одной задачи к другой, переназначать задачи и назначить их на группы, функциональные подразделения).
* Возможность оперативно отслеживать ход исполнения задач.
* Возможность подключения к системе партнеров (например, коллекторских агентств, партнеров по оценке и т.д.) и полный контроль за их деятельностью со стороны сотрудников Вашей компании (сотрудники видят на какой стадии находится процесс и задачи партнеров).

Также присутствуют компоненты тестирования и анализа правил [13]. Использование систем управления бизнес-правилами является важной частью системы управления принятием решений в организации. Топ BRMS системы 2019 года показано в Таблице 1.

Таблица 1 – Топ BRMS систем 2019 года

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Название | Документация/  Исходный код | Интерфейс/  Юзабилити | Стоимость |
| 1 | Drools | + | + | бесплатно |
| 2 | Red Hat News | - | + | платно |
| 3 | IBM | - | - | бесплатно |
| 4 | FICO | - | + | бесплатно |
| 5 | Agiloft | - | - | платно |
| 6 | Bosch | - | + | бесплатно |
| 7 | Sas | - | + | бесплатно |

К компонентам BRMS систем, которые указаны на рисунке 6 относится:

* сервер исполнения бизнес правил.
* инструмент ведения правил (репозитория), предоставляющего бизнес-пользователям удобный и функциональный интерфейс для хранения, создания и изменения бизнес логики.

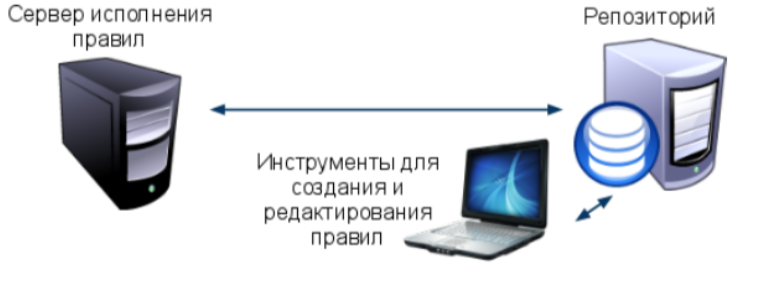


Рисунок 6 – Компоненты BRMS систем

Данный список охватывает основных поставщиков BRMS-решений [14]. Исходя из анализа, мы поработали и протестировали BRMS систему Drools и запустили в Eclipse.

Drools - это процессор правил с открытым кодом, написанный на Java и выполняющий правила в соответствии с алгоритмом Рете [15].

Алгоритм Рете – функционирует как сеть, которая предназначена для хранения большого объёма информации и обеспечивает значительное сокращение времени отклика. Рете алгоритм обеспечивает повышение быстродействия, что при изменении действии мгновенно знает, какие правила нужно применить [16].

Основные характеристики алгоритма Рете:

* Уменьшает или устраняет определенные типы избыточности за счет использования совместного использования узлов
* Он сохраняет частичные совпадения при выполнении объединений между различными типами фактов.
* Работает очень быстро

Единственным недостатком алгоритма Рете является большой объём памяти. Сеть Рете состоит из альфа и бета-подсетей. Левая сторона (альфа) формирует дискриминационную сеть, отвечающую за отбор элементов рабочей памяти (альфа-памяти), основанный на простых условиях сравнения атрибутов с фактами. Если элемент рабочей памяти успешно сопоставлен с условиями правил, он передается на следующий узел сети. Следовательно, все элементы рабочей памяти, представляющие одну сущность, пересекают данную ветвь узлов дискриминационной сети. Правая (бета) сторона графа выполняет объединение различных элементов рабочей памяти и записывает результат в бета-память [17]. Пример дерева решений показан на рисунке 7.

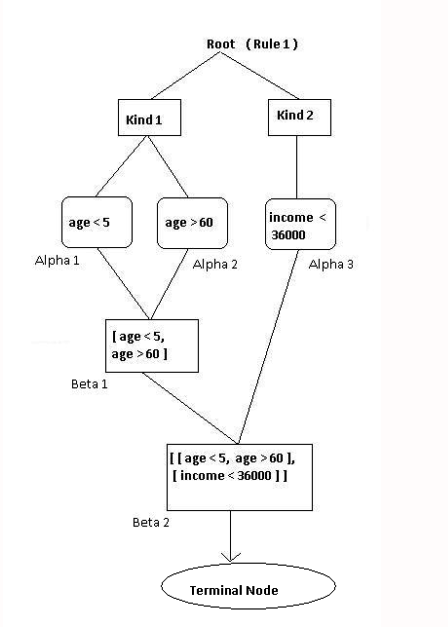
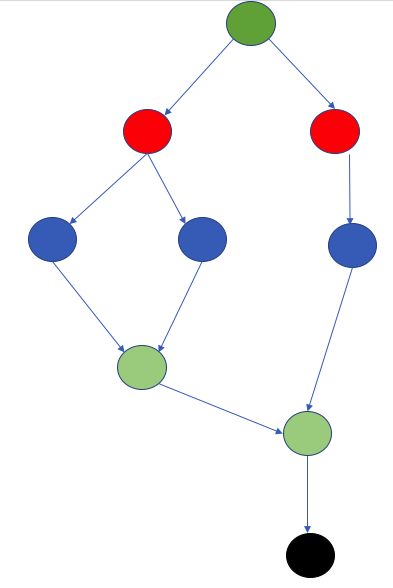
 

Рисунок 7 – Дерево решений Рете

Примечание – Составлено на основе источника [18]

В примере дерева решений Рете:

* Зеленый – точка входа
* Красный – название класса
* Синий – условия по отдельности (альфа узел)
* Зеленый - бета-узел (используется для объединения несколько условии)
* Черный – выход(ответ)

Ниже приведены правила которые мы использовали для тестирования в Eclipse :

* Если платеж равен или превышает 7 000 000 тенге, взять в контроль;
* Если платеж 7 000 000 тенге дроблен на 2 в течение месяца, взять в контроль;
* Если число транзакций у пользователя превышает среднее число транзакций среди пользователей, необходимо взять в контроль;
* Если переводы от одного физического лица нескольким при отсутствии явных признаков родственных связей между отправителем и получателями, взять в контроль;
* Если переводы от нескольких физических лиц одному при отсутствии явных признаков родственных связей между отправителями и получателем, взять в контроль;
* Если в течение 6 часов было совершено больше 3-х транзакции на один счет, взять в контроль.

Мы написали наши правила в Drools-rules и вытащили Rete tree как показано на рисунке 8.

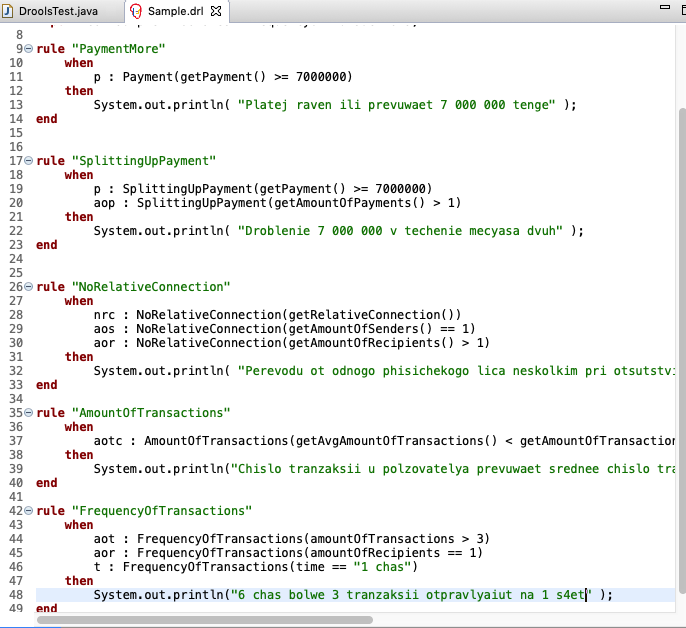
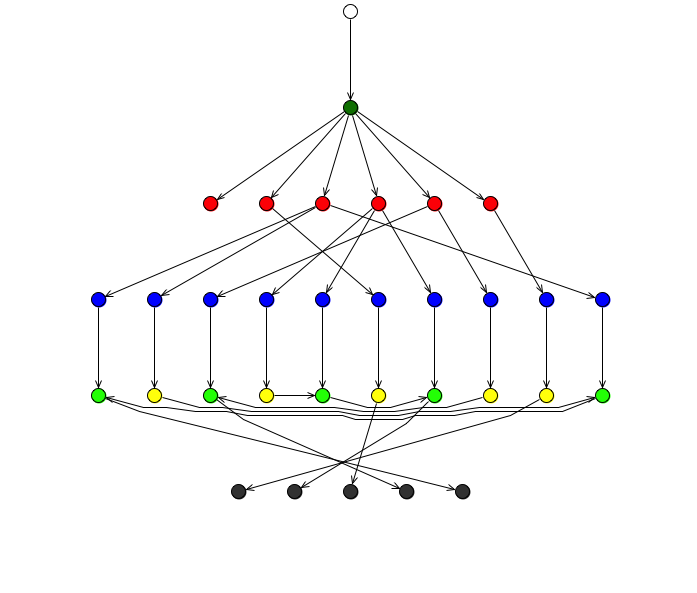
 

Рисунок 8 – Пример кода на Eclipse с использованием Drools

Примечание – Составлено на основе исследований

В нашем дереве решений Рете:

* Зеленый – точка входа
* Красный – название класса
* Синий – условия по отдельности
* Желтый – альфа узел (альфа память)
* Зеленый - бета-узел (используется для объединения несколько условии)
* Черный – выход (ответ)

BRMS-система позволяет легко и гибко автоматизировать логику принятия решений в рамках бизнес-процессов компании. Ценность BRMS заключается в том, что на ее основе можно создавать эффективные и воспроизводимые решения, которые работают быстрее и требуют меньшего уровня технической поддержки [19].

Системы управления бизнес-правилами, как средства моделирования, выполнения и проектирования оперативных решений, позволяют автоматизировать логику принятия решений в организациях сферы предоставления услуг. Данные системы успешно применяются в различных секторах экономики, в том числе и на рынке предоставления услуг связи населению.

* 1. Поиск аномалий в пользовательском поведении на основе истории проведенных транзакций

На первый взгляд в качестве подхода к решению задачи поиска аномалий сводится к обучению с учителем, а точнее к бинарной классификации наблюдений, где наблюдения помечаются как «типичное наблюдение»/«аномалия». Такой подход имеет следующие сложности и проблемы: маркировка наблюдений и несбалансированная выборка [20]. Маркировка наблюдений - при подготовке данных необходимо произвести маркировку наблюдений. Каждое наблюдение должно быть причислено к определенному классу, в данном случае к классам «типичное наблюдение»/«аномалия». Зачастую данный процесс становится затруднительным или невозможным, из-за малочисленности и неоднозначности наблюдений минорного класса. Несбалансированная выборка — это такая выборка содержит наблюдения одного класса в разы превосходящие в количестве наблюдений второго класса. Данная проблема представляет затруднения для моделей машинного обучения из-за недостатка данных. Имеются различные решения проблемы несбалансированной выборки, такие oversampling и undersampling.

В данных методах наблюдения минорного класса копируются, дополняя количество до размеров мажорного класса, или наблюдения мажорного класса удаляются до размера минорного класса. Данные подходы не всегда гарантируют соответствие получаемой выборки с реальными распределениями. Несбалансированной выборкой считается выборка, в которой наблюдения минорного класса составляют менее 10% общего количества наблюдений в выборке.

Следующий подход представляет собой обучение моделей без учителя. Для данной задачи подходят методы кластеризации. В основе идеи лежит разбиение наблюдений на различные классы на основе характеристик [21]. При данном подходе «типичные» наблюдения будут образовывать крупные кластеры, а «аномалии» будут считаться выбросами или одиночными объектами, не причисленными к определенному кластеру. Большинство методов кластеризации основываются на расстояниях между объектами в многомерном пространстве признаков.

EM-алгоритм. Данный алгоритм относится к вероятностным [22]. Каждое наблюдение относится к кластеру с определенной степенью вероятности. В контексте задачи поиска аномалий, предполагается что основные наблюдения относятся к определенному распределению/кластеру (смеси распределений/нескольким кластерам), аномалия относится к иному распределению с иной плотностью. Для решения задачи необходимо восстановить плотность распределения, на основе имеющийся выборки с помощью данного алгоритма.

DBSCAN. Данный алгоритм относится к плотностным [23]. Наблюдения, которые имеют n наблюдений в радиусе e обозначаются основными и находятся в пределах кластера. Наблюдения, имеющие менее n других наблюдений в радиусе e, но имеющие основные среди них, обозначаются пограничными и находятся на границе кластера. Наблюдения, имеющие менее n других наблюдений в радиусе e, но не имеющие основных среди них, обозначаются шумовыми и находятся вне кластера. В качестве гиперпараметров алгоритму передаются радиус области e и количество наблюдений n. Шумовые наблюдения в контексте задачи признаются аномалиями.

Isolation Forest. В основе алгоритма лежит бинарное дерево, изолирующее каждое наблюдение, из которых строится лес [24]. Алгоритм строит деревья до тех пор, пока в каждом листе не останется по одному единственному наблюдению, тем самым изолируя каждый объект в многомерном пространстве. Следующим шагом вычисляется оценка аномалии. Идея состоит в том, что чем меньше глубина пути до изоляции объекта, тем больше вероятность того, что он является аномалией.

Задачу поиска аномалий также можно решить при помощи проектирования нейронных сетей. В основе данной идеи лежит способность рекуррентной нейронной сети сохранять состояния предыдущих наблюдений [25,26,27]. Нейронная сеть пытается предсказать следующее наблюдение. Если реальное наблюдение соответствует предсказанному, но то наблюдение считается типичным, если наблюдение не соответствует предсказанному, то наблюдение признается аномальным.

Решением указанных проблем является создание интеллектуальной автоматизированной системы сбора-анализа и распределения больших неструктурированных данных финансовых потоков в облачной среде. Методы автоматического обнаружения аномалий помогут выявлять отклонения и показывать потенциальные рисковые денежные потоки. Задача поиска нетипичных объектов в выборке, называемых аномалиями, широко распространена в различных сферах, таких как медицина, маркетинг, информационная безопасность, различные движения финансовых средств и другие. Аномалиями называются различные выбросы, экстремальные значения, объекты с отличающимися совокупными характеристиками, иначе говоря, наблюдения из распределения, отличного от основной выборки. Аномалии могут иметь различный характер влияния и интерпретацию, все однозначно попадают определение «не типичного» наблюдения. Яркими примерами аномалий могут быть зафиксированные отклонения в работе двигателей, взлом информационных систем, кража аккаунтов, мошенничество. В качестве проблемы было выбрано определение попыток мошенничества с помощью нахождения аномалий среди переводов денежных средств. Аномалиями в данной постановке являются отклонения от общих характеристик транзакций. При нахождении аномалий, последние передаются финансовым специалистам для установки факта мошенничества.

Для данной задачи подходят методы кластеризации. В основе идеи лежит разбиение наблюдений на различные классы на основе характеристик. При данном подходе «типичные» наблюдения будут образовывать крупные кластеры, а «аномалии» будут считаться выбросами или одиночными объектами, не причисленными к определенному кластеру. Большинство методов кластеризации основываются на расстояниях между объектами в многомерном пространстве признаков.

Введём несколько определений. ε - максимальное расстояние между соседними объектами, minPts - минимальное количество соседних объектов, необходимых для образования кластера.

Объект p∈X называется ядровым, если в ε-окрестности точки p находятся MinPts объектов (включая сам объект p). Эти объекты называются напрямую достижимыми из p.

Объект q∈X называется достижимым из p, если существует путь p1,...,pn, где p1=p и pn=q, а каждый объект pi+1 напрямую достижим из pi. Таким образом вся объекты в пути, кроме объекта q, должны быть ядровыми.

Выбросами (или шумом) называются все объекты, недостижимые ни из одного другого объекта.

Кластером является множество ядровых точек, достижимых друг из друга, а также граничные неядровые точки, которые достижимы из любой ядровой точки кластера.

Описание алгоритма

* + - * Выбираем необработанный объект p.
      * Отмечаем объект p как обработанный.
      * Находим соседние объекты в ε-окрестности объекта p.
      * Сравниваем количество соседних объектов с MinPts, определяя, является ли p ядровым объектом:
      1. Если объект p является ядровым, то создаём новый кластер и запускаем поиск в ширину из данного объекта по другим непосещённым объектам, находя все объекты кластера.
      2. Если объект p не является ядровым, то отмечаем его как выброс (или шум).
* Если присутствуют необработанные объекты, то возвращаемся к шагу 1.

Выборка состоит из более 28 000 транзакций в определенный промежуток времени. Каждая транзакция представляет собой перемещение денежных средств от одного счета другому. Признаками наблюдений являются сумма, дата, канал перевода, тип транзакции, провайдер.

Данные были проанализированы, после чего был проведен разведочный анализ данных (exploratory data analysis). В ходе анализа был выведен дополнительный признак, отражающий время с момента последнего перевода с определенного счета.

Была проведена очистка данных. Категориальные данные были приведены к числовым значениям. Были выявлены переводы с помощью технических и системных счетов, которые не представляют интереса в рамках данной задачи, поэтому они были исключены из общей выборки, в следствии чего объем был сокращен до ≈12 000 наблюдений. Данные были стандартизированы.

Наблюдения были кластеризированы с помощью алгоритма DBSCAN. В ходе кластеризации алгоритмом было выявлено 23 кластера и шумовые точки. На рисунке 9 показана гистограмма плотности принадлежности наблюдений к кластерам.

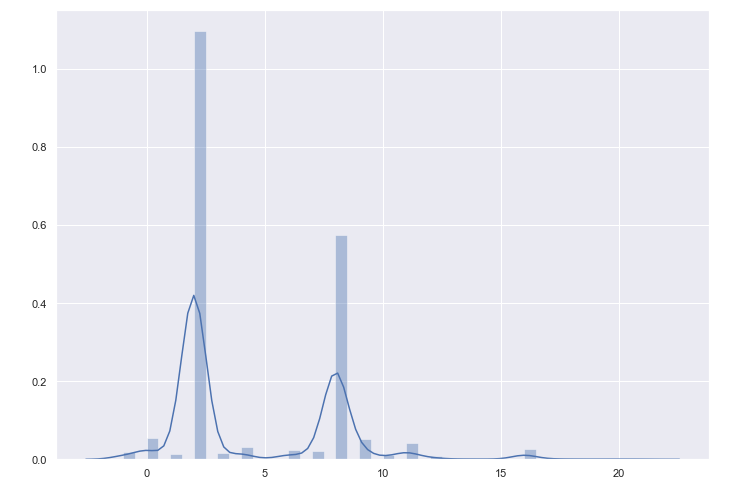


Рисунок 9 - Гистограмма принадлежности наблюдений к кластерам

Как видно из гистограммы, основной объем наблюдений принадлежит 6 кластерам. Построена визуализация наблюдений в двумерное пространство согласно принадлежности к кластерам с помощью метода t-SNE. На рисунке 10 представлена визуализация наблюдений в двумерном пространстве.

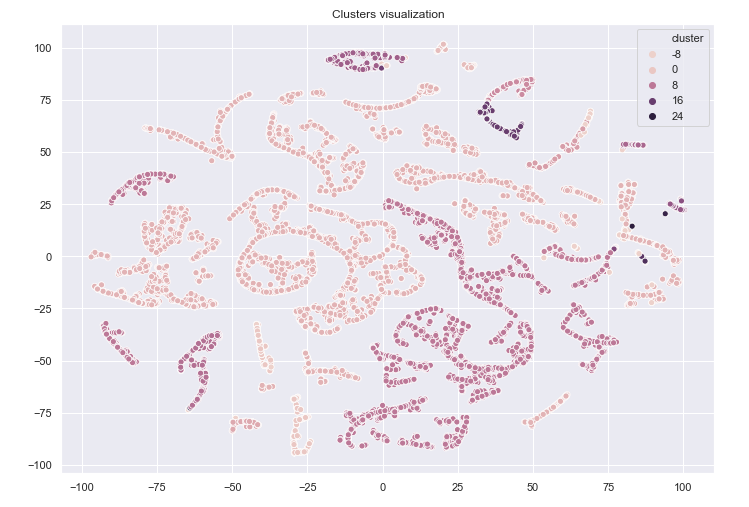


Рисунок 10 - Визуализация наблюдений в двумерное пространство

Как видно из визуализации, большинство групп составляют ленточные кластеры. На визуализации нет четкого разделения типичных наблюдений и аномалий. Имеет смысл провести повторную очистку данных и разведочный анализ данных. Было выявлено 131 шумовые точки, не принадлежащие ни одному кластеру. Также был проведен анализ шумовых точек, который показал, что их определение не является интерпретируемым, что также указывает на повторный анализ данных и кластеризацию.

* 1. Визуализация потока транзакции в виде графов с помощью современных инструментов

Визуализация информации предназначена для представления больших, абстрактных, полуструктурированных данных, которые очень сложно интерпретировать в более понятном и удобочитаемом виде для человека. Графы являются универсальным средством представления абстрактной информации. Самыми подходящими для нашего исследования являются силовые алгоритмы изображения графов также называемые пружинными. Эти алгоритмы популярны так как: они интуитивно понятны и подходят для построения произвольных графов, они легко интерпретируемы и их можно запрограммировать так как они описаны подробно и зачастую имеют псевдокод, также из этого следует что их можно кастомизировать под свои предпочтения и такие графы выглядят эстетически красиво.

Традиционные силовые алгоритмы широко приняты для анализа данных в области рисования графов. Они относятся к графам как к физическим системам. К каждому элементу применяются соответствующие силы такие как сила пружины, сила тяжести и т. д. (для вершин и ребер), чтобы держать их на правдоподобном и читаемом расстоянии которые показаны на рисунке 11.

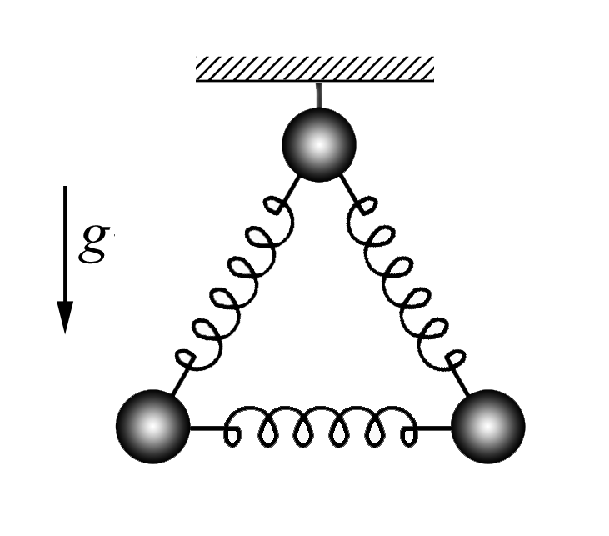


Рисунок 11 - Представление физической системы графа

Процесс останавливается, когда достигается нулевая или минимизированная энергия между элементами. Концепция была впервые введена Тутте на основе барицентрического представления. Существенные методы компоновки пружины, основанные на силе пружины, аналогичны тем, которые предусмотрены в законе Гука. Силы отталкивания среди всех вершин, а также силы притяжения между соседними вершинами. В качестве альтернативы, пружинные силы могут вычисляться на основе графика теоретических расстояний. Графики, построенные с помощью силовых алгоритмов, имеют тенденцию быть эстетически приятными, демонстрирует симметрию и в большинстве случаев создают макеты без пересечения для плоских графиков, но у них большое время выполнения из-за их больших обозначений O [28].

Задачей работы является найти наиболее подходящий алгоритм для рисования социальных связей мессенджера «Телеграм».

Целью исследования является обзор алгоритмов визуализации графов для выбора наиболее оптимального из них. Данное действие нужно для реализации алгоритма на серверной стороне. После чего можно рисовать граф по заранее подготовленным данным на клиентской стороне.

Методы:В этом разделе представлены экспериментальная методология и соответствующие алгоритмы, а также экспериментальные гипотезы.

С точки зрения техники, это исследование включает в себя три аспекта:

* Описание алгоритма
* Граф моделей
* Эстетические критерии для графических макетов
* Силовые алгоритмы. В рамках оценки были выбраны четыре алгоритма:
* FR (Фрухтерман и Рейнгольд)

Алгоритм Фрухтермана и Рейнгольда является традиционным силовым алгоритмом, который является модификацией модели пружинного алгоритма Eades (Eades, 1984). Этот алгоритм создает эстетически приятные двумерные изображения графов, проводя упрощенное моделирование физических систем. В этом методе вершины представлены стальными кольцами, а ребра рассматриваются как пружины, алгоритм учитывает силу между каждыми двумя вершинами. Силы притяжения продолжают меняться посредством перемещения узлов, пока энергия не будет минимизирована состоянием завершения всей «механической системы». Хотя константа, которая определяет, как далеко перемещается один шаг узла должна быть определена заранее, окончательный макет может вообще не достичь равновесия. FR простой, элегантный, интуитивно понятный, эффективный и имеющий одинаковую длину ребра и разумное время обработки алгоритм [29]. У этого алгоритма есть два принципа описанные ниже:

* + Вершины, соединенные ребром, должны быть нарисованы рядом друг с другом.
  + Вершины не должны быть нарисованы слишком близко друг к другу.

В этом алгоритме предположим, что fa и fr - силы притяжения и отталкивания, соответственно, d расстояние между двумя вершинами и k - радиус пустой области вокруг вершины, тогда

fa(d) = d2 / k (1)

fr(d) = -k 2 /d (2)

Для данного графа G = (V, E) объединенная сила, приложенная к вершине v:

F(v) = ∑ (𝑢,𝑣)∈𝐸 𝑓𝑎, 𝑢𝑣 + ∑ (𝑢,𝑣)∈𝑉∗𝑉 𝑓𝑟，𝑢𝑣  (3)

* FA (ForceAtlas). Алгоритм компоновки FA (Bastian, Heymann & Jacomy, 2009) - это метод пространственной компоновки в категории силовые алгоритмы, направленные на придание сети четкой формы (пространственная локализация), наряду с интеграцией между различными методами, такими как моделирование Барнса-Хата, зависящая от степени силы отталкивания, локальной и глобальной адаптивной температуры. Он предназначен для реальных сетей, таких как веб-сети, предоставляя универсальный и интуитивно понятный способ локализации сетей. Алгоритм компоновки FA придает больший вес качеству схемы, чем скорость, с которой он был рассчитан [4]. Это особенно точно в случае больших

сетей. Алгоритм FA предлагает настройки в реальном времени, включая скорость, гравитацию, отталкивание, автостабилизацию, инерцию или настройку размера [30]. Силовая модель FA похожа на FA2, как описано ниже.

* FA2 (ForceAtlas2). FA2 основан на FA, но предлагает больше возможностей и инновационных оптимизаций, которые делают его очень быстрым алгоритмом компоновки.

Внедрение адаптивных локальных и глобальных скоростей обеспечивает хорошие показатели для сети менее 100 000 узлов. Опытным путем наблюдалось, что FA2 был в лучшем случае с сильно кластеризованными сетями [31].

Сила притяжения fa между двумя связанными узлами n1 и n2 линейно зависит от расстояния d (n1, n2), сила отталкивания Fr пропорциональна произведению угла плюс один (deg + 1) из двух узлов n1 и n2.

fa(n1, n2) = d(n1,n2) (4)

fr(n1, n2) = kr (𝑑𝑒𝑔(𝑛1 )+1)(𝑑𝑒𝑔(𝑛2 )+1) / 𝑑(𝑛1,𝑛2 ) (5)

Для данного графа G = (V, E) объединенная сила, приложенная к вершине v:

F(v) = ∑ (𝑢,𝑣)∈𝐸 𝑓𝑎, 𝑢𝑣 + ∑ (𝑢,𝑣)∈𝑉∗𝑉 𝑓𝑟，𝑢𝑣  (6)

* LinLog. Ноак предложил энергетические модели LinLog, которые могут естественно представлять кластерную структуру графов группирование плотно связанных узлов и разделение разреженных узлов. Модели включают узел отталкивания LinLog и ребро-отталкивание LinLog, чьи схемы минимальной энергии отражают кластерную структуру графов с соблюдением двух четко определенных критериев кластеризации и отталкивания краев в моделях энергии. LinLog избегает или уменьшает смещение в сторону группировки узлов с высокой степенью при использовании вместо или в дополнение к отталкиванию узла [32].

Для графа G = (V, E) для чертежа p и двух узлов u, v ∈ V длина разностного вектора p (u) −p (v) называется евклидовым расстоянием u и v в p и обозначается через || p (u) −p (v) || [6].

ULinLog(p) = ∑(𝑢,𝑣)∈𝐸 ||𝑝(𝑢)− 𝑝(𝑣)|| + ∑(𝑢,𝑣)∈𝑉∗𝑉 𝑙𝑛||𝑝(𝑢)− 𝑝(𝑣)|| (7)

Ноак определяет энергетическую модель ((притяжение, отталкивание) -модель) макета как показатель степени, взятый расстоянием в формулы, используемые для расчета притяжения и отталкивания (лог рассматривается как 0-й степени) [33]. (притяжение, отталкивание) - Модель FA (1, -1) занимает промежуточное положение между LinLog Ноака (0, -1) и алгоритмом Фрухтермана и Рейнгольд (FR) (2, -1). ForceAtlas2 (FA2) основан на FA, но предлагает больше возможностей и инновационных оптимизаций, которые делают его очень быстрым алгоритмом компоновки. Способность FA2 показывать кластеры лучше, чем у FR, но хуже, чем у LinLog [33].

Используя методы интеллектуального анализа данных, можно выявить несколько стратегий для выявления узлов с повышенным риском мошенничества. Одним из популярных методов является использование мер централизованности – степени (in-degree, out-degree, all-degree), близость (closeness) и межцентральность (betweenness centrality) – которые являются способами выявления наиболее значимых социальных актеров [32]. Степени централизованности В реальной жизни мы часто считаем людей, имеющих много связей, важными. Аналогично и в социальном графе, актеры, у которых много контактов, считаются важными. Поэтому централизованность является мерой измерения важности узла в сети. Степень центральности C d для узла v i в неориентированном графе равна

Cd(vi) = Σn di (8)

Где:

di - степень (число соседних ребер) узла vi .

Входящая степень (in-degree) - эта мера подсчитывает количество входящих связей, то есть, сколько раз клиент действовал как продавец. Во взвешенной версии значения входящих дуг суммируются. (Взвешенная) входящая степень для общего узла gi представляется уравнением:

(Di(gi)) =Σn xji  (9)

Исходящая степень (out-degree) – эта мера подсчитывает количество исходящих связей, то есть количество случаев, когда клиент выступает в качестве должника. Взвешенная исходящая степень общего узла g i представлен уравнением:

(Do(gi)) =Σ xji (10)

Общая степень - при помощи этой меры подсчитывается число связей, объединяющих узел с другими узлами, независимо от их направленности. Во взвешенной версии фактор риска вычисляется как сумма весов всех дуг, связанных с одним узлом. Эта мера заменяет входящие и исходящие степени в неориентированных сетях. (Взвешенная) общая степень для общего узла g i в направленном графе представлена уравнением 11:

(DA(gi)) = Σn(xij + xji) (11)

Существует разные способы выделения сообществ. Далее следует перечисление основных способов. Betweenness — алгоритм, основанный на коэффициенте «централизации посредничества», определяемом как число кратчайших путей между всеми парами вершин, проходящих через определенное ребро [33]. Если между вершинами N кратчайших путей, то каждое ребро добавляется N 1 к значению коэффициента. Чем больше значе ние, тем вероятнее, что ребро соединяет вершины из разных сообществ. Например, когда разные группы связаны одним ребром, все кратчайшие пути от одного сообщества к другому проходят через это ребро. Этот алгоритм является одним из первых алгоритмов по выделению сообществ в сетях. Данный метод разработан Ньюманом и Гирваном и работает по следующей схеме:

* Подсчет коэффициентов “центральности по посредничеству” на всех ребрах графа.
* Поочередное удаление ребер с самым большим коэффициентом.
* Сообществами считаются оставшиеся компоненты связности.
* Процедура удаления связей завершается, когда достигает максимума модулярность результирующего разбиения.

Обработка данных включает в себя установление настроек, выбор атрибутов, группировка узлов в Сообщества. Данный анализ позволяет проследить пути выведения денег заграницу, размыв деньги в многочисленных счетах, обратное введение в страну, зачислив на другие счета. Каждый из этих этапов сопровождается группой тесно связанных банковских счетов, которые будут формировать сообщества.

Был проведён сравнительный анализ существующего программного обеспечения для визуализации графов: python networkX, Gephi, D3JS. Анализ проводился на 28000 транзакциях с участием 20000 контрагентов.

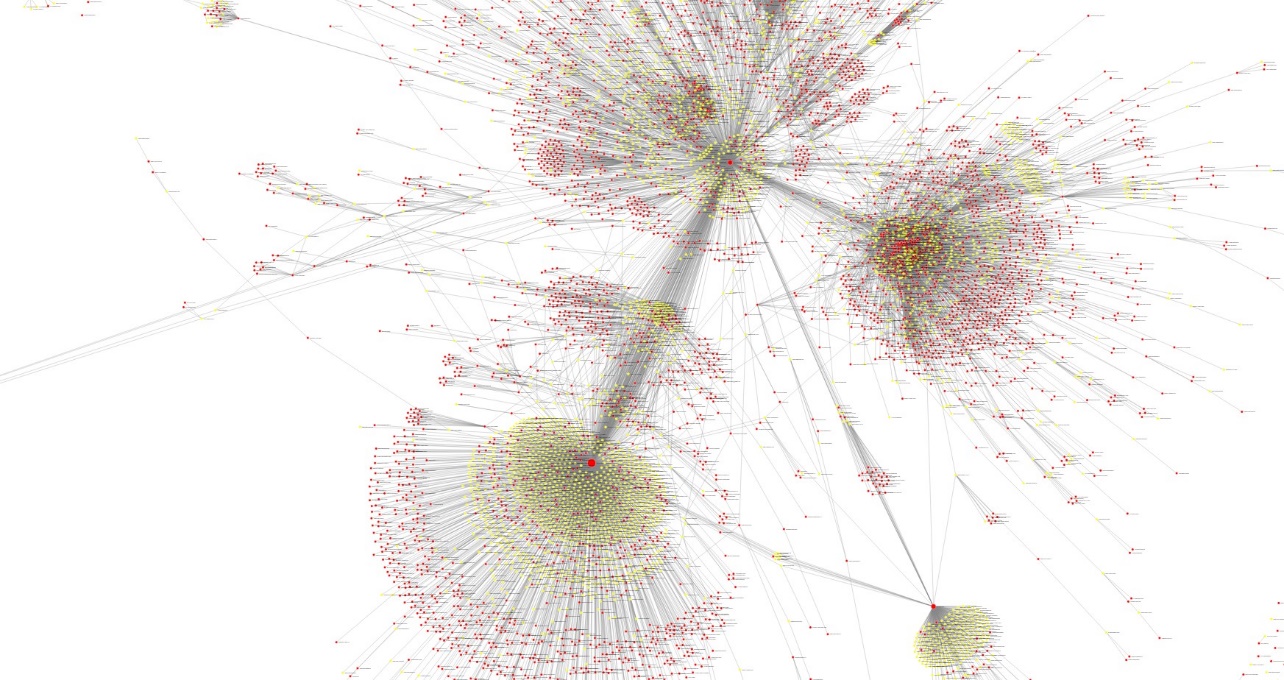


Рисунок 12 – Визуализация на d3js

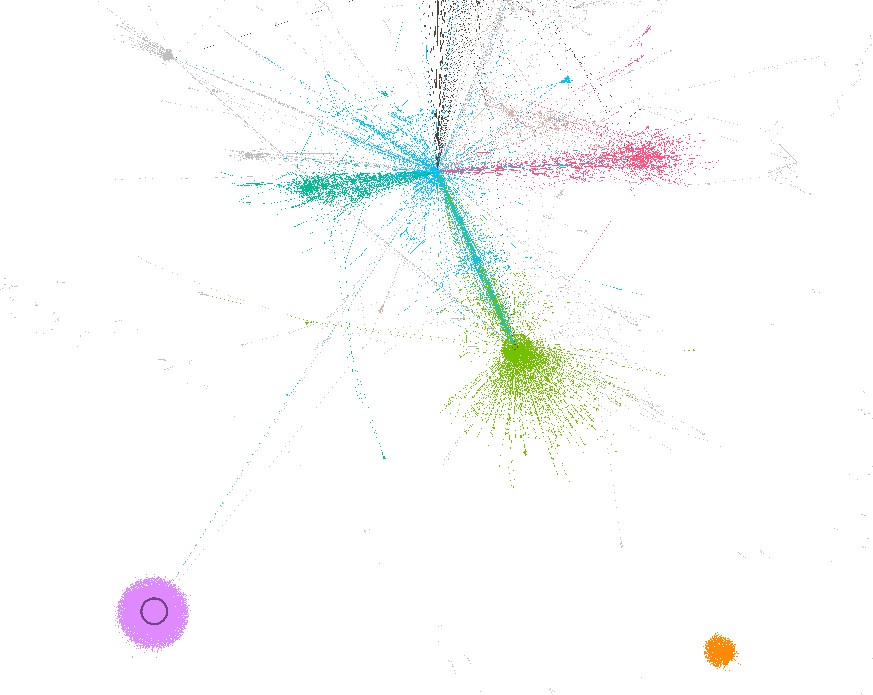


Рисунок 13 – Визуализация на Gephi

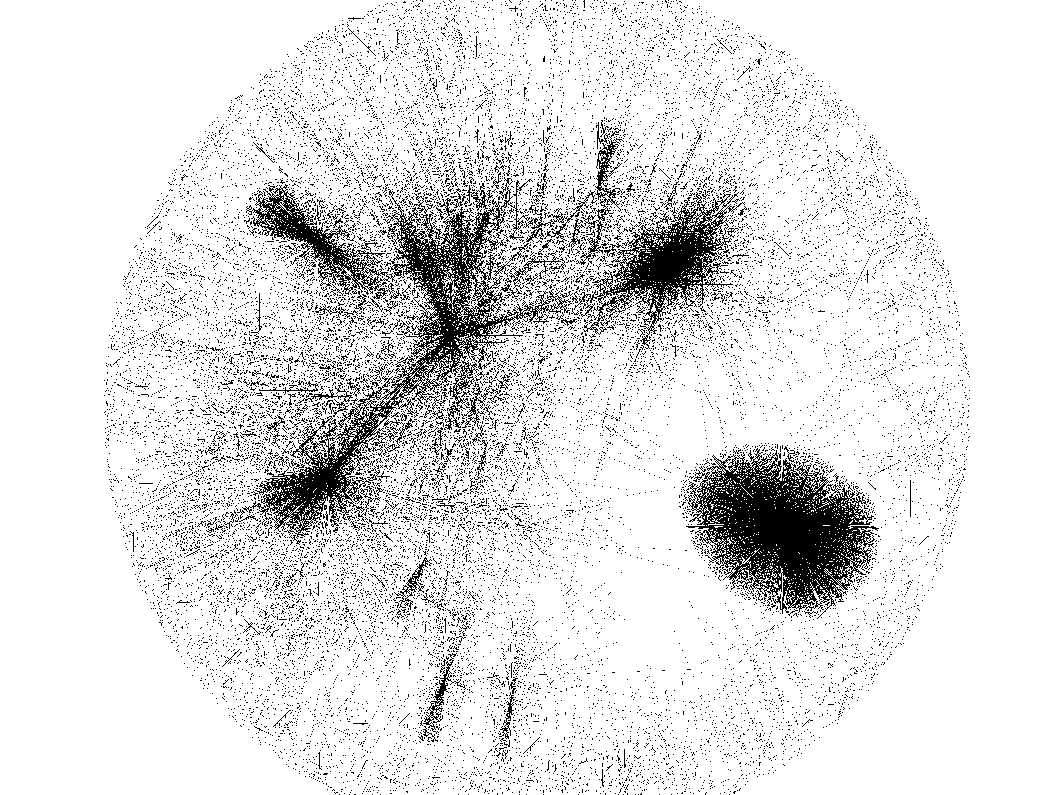


Рисунок 14 – Визуализация на python networkC

В исследовании проводился анализ целесообразности использования методов интеллектуального анализа данных при отслеживании отмывания денег для увеличения эффективности мониторинга отмывания денежных средств. Граф на рисунках 1, 2 и 3 показывает, что при выведении денежных средств, два узла имеют наибольшее число связей с другими узлами. Из этих счетов выводится наибольший объем денежных средств. Эти узлы также взаимосвязаны друг с другом. Весь этот процесс говорит о многочисленных транзакциях между определенными счетами, целью которых является скрытие следов отмывания денег. На графе видно обособленное сообщество, узлы которого также имеют внутренние связи. Учитывая тесные связи между узлами этого сообщества, крайне малочисленные связи с узлами других сообществ, а также отдаленность от основного графа, можно утверждать, что счета данного сообщества являются заграничными счетами. В это сообщество деньги поступают из одного счета, проводится манипуляция перекладывания денег между счетами этого сообщества, затем деньги выводятся в Сообщество 1, которое является крупнейшим, внутри этого сообщества деньги также перекладываются и возвращаются в стартовые узлы. Таким образом, социальные графы позволяют отслеживать отмывание денег в банковской сфере

Проводился анализ целесообразности использования методов интеллектуального анализа данных при отслеживании отмывания денег для увеличения эффективности мониторинга отмывания денежных средств. Визуализация продемонстрировала способность выполнять задачу мониторинга транзакций денежных средств. Выявлены недостатки существующих платформ при работе с большим количеством транзакций. Подсчета всех коэффициентов, построения графа и визуализация является ресурсоемкой задачей и требуется распараллеливания на платформах высокопроизводительных вычислений.

ЗАКЛЮЧЕНИЕ

Согласно подпункту 12 п 1, ст3, гл2 Закона РК «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (с изменениями и дополнениями по состоянию на 02.04.2019 г.) платежные организации являются субъектом финансового мониторинга и должны предоставлять информацию о «подозрительных транзакциях» по форме п2 ст10 гл2 Закона уполномоченному органу (Комитет финансового мониторинга РК).

Для того что бы Казахстан в полной мере выполнял как требования Законодательства, так и требования международной организации ФАТФ, возникает необходимость в создании системы по противодействию отмыванию денег и финансированию терроризма для Платежных организаций, которая будет соответствовать всем стандартам. Так же, создание данной системы становится возможным в связи с тем, что в Казахстане с 2019 года, все граждане должны произвести регистрацию своего сотового номера телефона к своему ИИН. Проведенный анализ нормативно правовой базы, выявляет необходимость создания системы, которая будет проводить оценку транзакции на рискованность (от низко-рискованной до высоко-рискованной), тем самым помогая экспертам в оценивании рисков.

Проведен анализ целесообразности использования методов интеллектуального анализа данных при отслеживании отмывания денег для увеличения эффективности мониторинга отмывания денежных средств. Визуализация продемонстрировала способность выполнять задачу мониторинга транзакций денежных средств. Выявлены недостатки существующих платформ при работе с большим количеством транзакций. Подсчета всех коэффициентов, построения графа и визуализация является ресурсоемкой задачей и требуется распараллеливания на платформах высокопроизводительных вычислений. Были выделены 3 метода кластеризации и 1 метод построения модели нейронных сетей для решения задачи определения аномалий. Были собраны данные в размере 28000 наблюдений. В ходе очистки данных количество наблюдений сократилось до 12000. При выполнении кластеризации алгоритмом DBSCAN, объекты были сгруппированы в 23 кластера и 131 объект оказался не причисленным ни к одному кластеру. Поверхностный анализ 131 шумовых объектов не показал интерпретируемость характера аномалий, из чего следует что данный эксперимент не показал достаточный результат.

В рамках дальнейшего исследования по данной теме, планируется написание Технического задания и формирование критериев для создания оптимальной системы для бесперебойной работы Платежных организаций, а также разработка прототипа информационной системы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

* + - 1. Официальный сайт евразийской группы по противодействию легализации преступных доходов и финансированию терроризма. – URL: https://eurasiangroup.org/ru/general-information/ (дата обращения: 01.05.19)
      2. Официальный интернет-ресурс Комитета по финансовому мониторингу Министерства финансов Республики Казахстан. - URL: https://kfm.gov.kz/ru/regulatory-framework/is-the-current-legislation/ (дата обращения: 01.05.19)
      3. Официальный сайт международной организации FATF. - URL: http://www.fatf-gafi.org. (дата обращения: 01.05.19)
      4. React в действии. Тиленс Т.М. – Санкт-Петербург: Питер, 2019. – 368 c.
      5. Vue.js up and running. Macrae C. - New York: - O'Reilly Media, 2019. – 174 p.
      6. Bitcoin. Больше, чем деньги. Форк А. – М: - Продюсерский центр Александра Гриценко, 2017 г. – 290 c.
      7. Нормативная база и стандарты в области информационной безопасности. Учебное пособие. Родичев Ю.А. – Санкт-Петербург: Питер, 2018. – 256 c.
      8. KPMG в Казахстане и Центральной Азии Отчет по отрасли информационно-коммуникационных технологий в Республике Казахстан. АО «Национальный инфокоммуникационный холдинг «Зерде».
      9. Прогноз: Облачные вычисления — способ уменьшить расходы и повысить производительность. – URL: http://expertonline.kz
      10. IaaS в Казахстане. Рынок и провайдеры. - URL: https://iaas-blog.it-grad.ru
      11. Информационные технологии. Романова Ю., Музычкин П. – М: Юрайт, -2018. – 291 с.
      12. Business Rules Management Systems Maximizing Value with an Enterprise-Level Strategy. Decision Management for The Summit Point Group. Bhogaraju P. – 2009, 215 p.
      13. Обзор IBM WebSphere ILOG JRules. – URL: https://www.ibm.com/ru/events/presentations/11kz/Kulak%202\_ILOG%20JRules.pdf (дата обращения: 01.10.2019).
      14. Business Rules Management Systems (BRMS). – URL: https://www.trustradius.com/contract-management (дата обращения: 01.10.2019).
      15. Реализация бизнес-логики: Введение в проект Drools. Рапп Н.А. – 2004. - 195 с.
      16. Rete algorithm. – URL: https://subscription.packtpub.com/book/application\_development/9781847196064 (дата обращения: 01.10.2019).
      17. Интеллектуальные системы. Бессмертный И., Платонов А. – М: Юрайт, - 2018. – 243 с.
      18. Introduction to Rete algorithm. – URL: https://webcache.googleusercontent.com/ (дата обращения: 01.10.2019).
      19. Business Rules Management and Service oriented architecture. Ian Graham. N: Wiley, – 2007. – 292 p.
      20. Anomaly Detection Survey. – URL: https://arxiv.org/pdf/1901.03407.pdf (дата обращения: 21.10.2019).

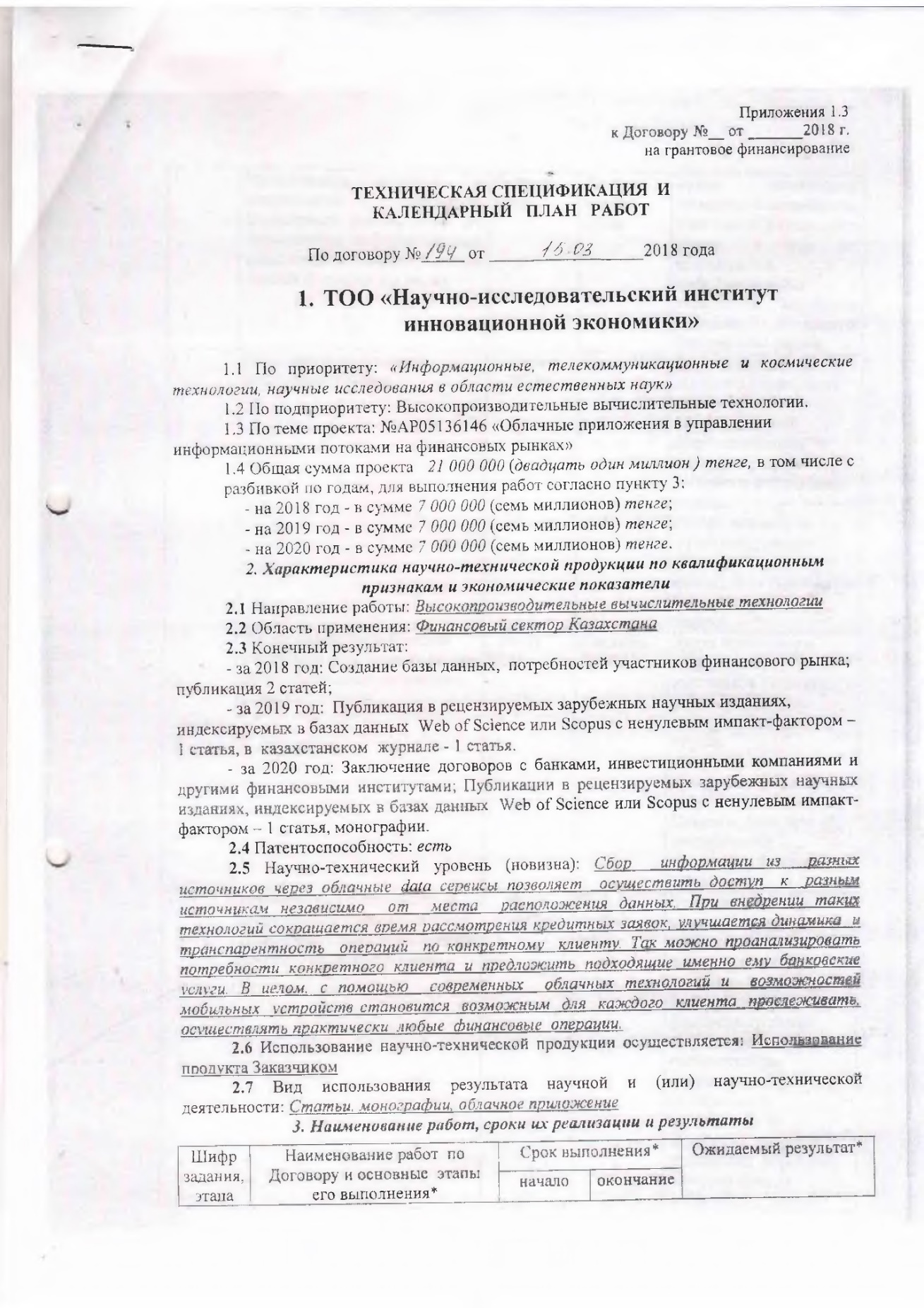
21 Network Anomaly Detection Using One Class Support Vector Machine. – URL: https://pdfs.semanticscholar.org/4d40/5c9d9dc537881479ad2709fad69131b940a2.pdf (дата обращения: 21.10.2019).

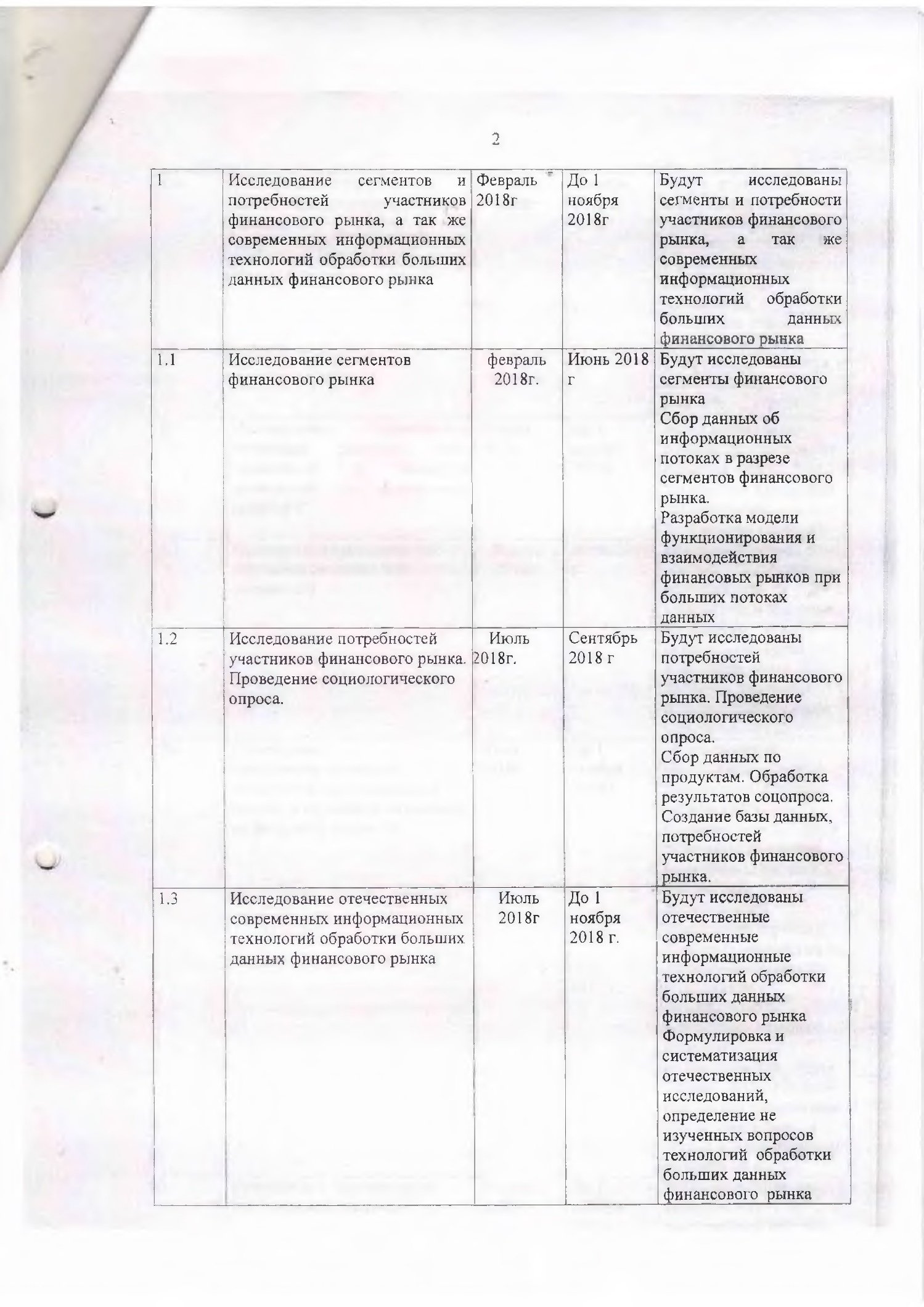
* + - 1. EM overview. – URL: http://web.mit.edu/6.435/www/Dempster77.pdf (дата обращения: 21.10.2019).

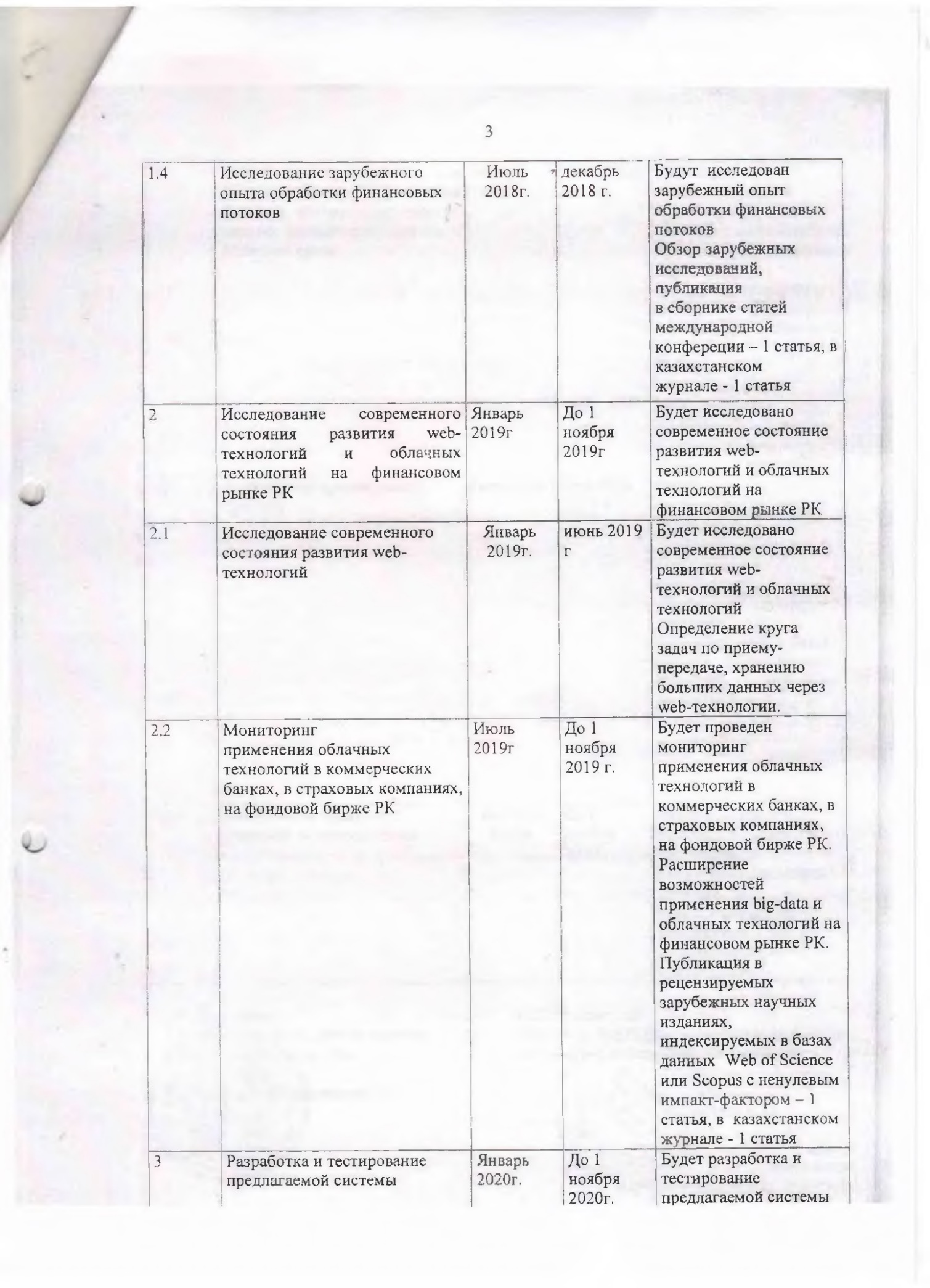
1. DBSCAN (temperature anomaly). – URL: https://www.researchgate.net/publication/233919690\_Anomaly\_Detection\_in\_Temperature\_Data\_Using\_DBSCAN\_Algorithm (дата обращения: 21.10.2019).
2. Isolation Forest. – URL: https://arxiv.org/pdf/1811.02141.pdf (дата обращения: 22.10.2019).
3. LSTM. – URL: http://ai.dinfo.unifi.it/paolo//ps/tnn-94-gradient.pdf (дата обращения: 22.10.2019).
4. LSTM Anomaly Detection. – URL: https://arxiv.org/ftp/arxiv/papers/1802/1802.00324.pdf (дата обращения: 22.10.2019).
5. LSTM Unsupervised Anomaly Detection. – URL: https://arxiv.org/pdf/1710.09207.pdf (дата обращения: 01.10.2019).
6. Force-directed Drawing Algorithms. S. G. Kobourov. - Handb: - Graph Draw, 2013. – 408 p.
7. Graph Drawing by Force-Directed Placement. Software Practice and Experience. T. M. J. Fruchterman, E. M. Reingold, 1991.- 1164 p.
8. Gephi: An Open Source Software for Exploring and Manipulating Networks. M. Bastian, S. Heymann, and M. Jacomy. Third International AAAI Conference on Weblogs and Social Media, 2004. – 579 p.
9. Force Atlas 2, A Graph Layout Algorithm for Handy Network Visualization. M. Jacomy, S. Heymann, T. Venturini, and M. Bastian, 2011. – 365 p.
10. Energy Models for Graph Clustering. A. Noack, J. Graph., 2007. – 425 p.
11. An Energy Model for Visual Graph Clustering. A. Noack, 2003. – 436 p.
12. Gephi: An Open Source Software for Exploring and Manipulating Networks. M. Bastian, S. Heymann, and M. Jacomy, 2004. – 579 p.

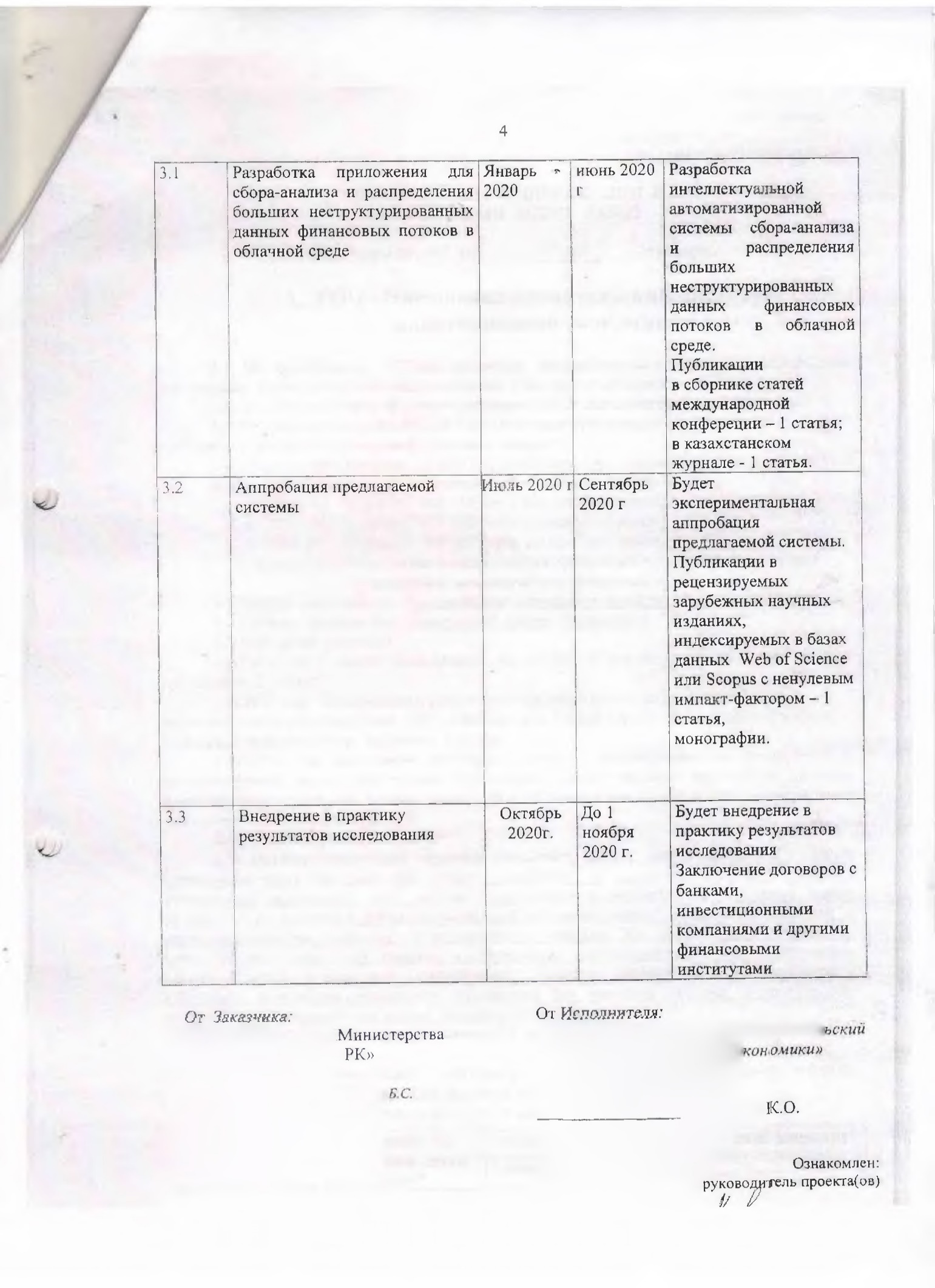
ПРИЛОЖЕНИЕ А

Календарный план работ









ПРИЛОЖЕНИЕ Б

Перечень опубликованных работ по теме за 2019 год

|  |  |  |
| --- | --- | --- |
| № | Выходные данные работ | Ссылка |
| 2019 год | | |
| 1 | Адилова К., Аубакиров С., Абенов Ж., Анализ требований к системам по противодействию отмыванию денег и финансированию терроризма в Казахстане. Матер. IV Международная научно-практическая конференция «Информатика и прикладная математика», - Алматы. С. 143-147. | Копия прилагается |
| 2 | Адилова К., Аубакиров С., Обзор текущего состояния по противодействию отмыванию денег и финансированию терроризма в Казахстане. Научный журнал «Вестник университета Туран». №4 (78), 2019 | [В](http://vital.lib.tsu.ru/vital/access/services/Download/vtls:000631597/SOURCE1) печати |
| 3 | Толенбеков Е., Аубакиров С., Абенов Ж., Абдулкаримова К, Анализ потока финансовых транзакций с помощью построения графов. Казахский национальный педагогический университет имени Абая ВЕСТНИК Серия «Физико-математические науки». №3 (67), 2019г. | В печати |

ПРИЛОЖЕНИЕ В

Список использованных зарубежных информационных ресурсов

1 Springer Link // https://link.springer.com/

2 Scopus // https://www.scopus/

3 Web of Science // https://apps.webofknowledge.com/

4 Cornell University Library // https://arxiv.org/

5 РМЭБ // http://rmebrk.kz/

6 Mendeley // https://www.mendeley.com/

7 Cyberleninka // https://cyberleninka.ru/

8 Google Scholar // https://scholar.google.com/

9 ResearchGate // https://www.researchgate.net/

ПРИЛОЖЕНИЕ Г

### Форма ФМ-1

Подозрительные транзакции, которые попадают под первую категорию риска, должны быть направлены в Комитет по финансовому мониторингу Министерства финансов Республики Казахстан, посредством заполнения форы ФМ-1 и отправки ее через АРМ СФМ или WEB СФМ. В данной форме необходимо заполнить следующие поля:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | | № реквизита | Наименование | | Содержание |
|  | | 1 | 2 | | 3 |
|  | | 1 | Сведения о форме ФМ-1 | |  |
|  | | 1.1 | Номер формы ФМ-1\* | | 1.Номер:  2. Связь с иной формой ФМ-1 (при наличии):  2.1. Номер связанной формы ФМ-1: 2.2. Дата связанной формы ФМ-1: |
|  | | 1.2 | Дата формы ФМ-1\* | |  |
|  | | 1.3 | Вид документа (нужное подчеркнуть)\* | | 1. Новое сообщение  2. Корректировка непринятого сообщения (с указанием номера корректируемого сообщения)  3. Запрос замены сообщения (с указанием номера сообщения) |
|  | | 1.4 | Состояние операции (нужное подчеркнуть) | | 1. Совершено (время завершения операции)  2. Продолжается (время начала операции)  3. Приостановлено (время приостановки операции субъектом финансового мониторинга)  4. Не совершено |
|  | | 1.5 | Основание для подачи сообщения (нужное подчеркнуть)\* | | 1. Равна или превышает пороговую сумму 2. Подозрительная операция  4. Совпадение с перечнем организаций и лиц, связанных с финансированием терроризма и экстремизма: 4.1. Приостановление расходных операций по банковским счетам 4.2. Приостановление исполнения указаний по платежам и переводам без использования банковского счета 4.3.Блокирование ценных бумаг 4.4.Отказ в проведении иных операций 4.5Социальные выплаты и обязательные платежи в бюджет |
|  | | 2 | Сведения о субъекте финансового мониторинга, направившем форму ФМ-1 | |  |
|  | | 2.1 | Код субъекта финансового мониторинга\* | |  |
|  | | 2.2 | Субъект финансового мониторинга\* | | 1.1. Организационная форма:  1.2. Наименование:  1.2.1. Фамилия: 1.2.2. Имя:  1.2.3. Отчество (при наличии): |
| 2.3 | ИИН/БИН\* | | |  | |
| 2.4 | Адрес местонахождения | | | 1. Область (в том числе гг. Алматы и Астана): 2.Район:  3.Населенный пункт (город/поселок/село), за исключением гг. Алматы и Астаны:  4.Наименование улицы/проспекта/микрорайона:  5.Номер дома:  6.Номер квартиры/офиса (при наличии): 7. Почтовый индекс: | |
| 2. | Документ, удостоверяющий личность (для физических лиц)\* | | |  | |
| 2.6.1 | Номер и серия документа, удостоверяющего личность (для физических лиц)\* | | | 1.Номер:  2. Серия (при наличии): | |
| 2.6.2 | Кем выдан документ, удостоверяющий личность (для физических лиц)\* | | |  | |
| 2.6.3 | Когда выдан документ, удостоверяющий личность (для физических лиц)\* | | |  | |
| 2.7 | Ответственное должностное лицо | | | 1. Фамилия:  2. Имя:  3. Отчество (при наличии): | |
| 2.7.1 | Должность ответственного должностного лица | | |  | |
| 2.8 | Контактные телефоны\* | | |  | |
| 2.9 | Электронная почта | | |  | |
| 3 | Информация об операции, подлежащей финансовому мониторингу | | |  | |
| 3.1 | Номер операции\* | | |  | |
| 3.2 | Код вида операции\* | | | 1. Код:  2. Информация об имуществе, подлежащем государственной регистрации:  2.1. Вид имущества:  2.2. Регистрационный номер имущества: | |
| 3.3 | Код назначения платежа \* | | | 1. Код назначения платежа:  2. Невозможно установить | |
| 3.4 | Количество участников операции\* | | |  | |
| 3.5 | Код валюты операции\* | | |  | |
| 3.6 | Сумма операции в валюте ее проведения\* | | |  | |
| 3.7 | Сумма операции в тенге\* | | |  | |
| 3.8 | Основание совершения операции\* | | |  | |
| 3.9 | Дата и номер документа, на основании которого осуществляется операция | | | 1. Дата:  2. Номер документа: | |
| 3.10 | Код признака подозрительности операции | | |  | |
| 3.11 | 1-й дополнительный код признака подозрительности операции (при наличии) | | |  | |
| 3.12 | 2-й дополнительный код признака подозрительности операции (при наличии) | | |  | |
| 3.13 | Описание возникших затруднений квалификации операции как подозрительной | | |  | |
| 3.14 | Дополнительная информация по операции | | |  | |
| 4 | Сведения об участниках операции, подлежащей финансовому мониторингу | | |  | |
| 4.1 | Участник (нужное подчеркнуть)\* | | | 1. Плательщик по операции  2. Получатель по операции  3. Представитель плательщика  4. Представитель получателя  5. Лицо от имени и по поручению  6. Выгодоприобретатель | |
| 4.2 | Клиент субъекта финансового мониторинга (нужное подчеркнуть)\* | | | 1. Не является  2. Является | |
| 4.3 | Вид участника\* | | |  | |
| 4.4 | Резидентство | | |  | |
| 4.5 | Тип участника операции (нужное подчеркнуть)\* | | | 1. Юридическое лицо  2. Физическое лицо  3. Индивидуальный предприниматель | |
| 4.6 | Иностранное публичное должностное лицо (нужное подчеркнуть) | | | 1. Не является  2. Является  3. Аффилиированный (-ая) с иностранным публичным должностным лицом | |
| 4.7 | Банк участника операции\* | | | 1.1. Местонахождение филиала: 1.2. Наименование банка:  1.2.1. Наименование СДП: 1.3. Код банка/филиала: 1.4. Номер счета участника: 1.5. Сведения о корреспондентских счетах, участвующих в операции: 1.5.1. Местонахождение банка: 1.5.2. Наименование банка: | |
| 4.8 | Наименование участника операции (для юридических лиц)\* | | | 1. Участник:  1.1. Организационная форма:  1.2. Наименование:  2. Невозможно установить | |
| 4.9 | Учредители участника (для юридических лиц) | | | 1.1. Организационная форма:  2.1. Наименование:  1.2.1. Фамилия:  1.2.2. Имя:  1.2.3. Отчество (при наличии):  2. Резидентство: | |
| 4.10 | Первый руководитель (для юридических лиц) | | | 1. Фамилия:  2. Имя:  3. Отчество (при наличии): | |
| 4.12 | ОКЭД | | |  | |
| 4.13 | ИИН/БИН | | |  | |
| 4.14 | Ф.И.О. (для физических лиц и индивидуальных предпринимателей) | | | 1.1. Фамилия:  1.2. Имя:  1.3. Отчество (при наличии):  2.1. Невозможно установить | |
| 4.15 | Документ, удостоверяющий личность | | |  | |
| 4.16 | Номер и серия документа, удостоверяющего личность | | | 1. Номер:  2. Серия (при наличии): | |
| 4.17 | Кем выдан документ, удостоверяющий личность | | |  | |
| 4.18 | Когда выдан документ, удостоверяющий личность | | |  | |
| 4.19 | Дата рождения (для физических лиц и индивидуальных предпринимателей) | | |  | |
| 4.20 | Место рождения (для физических лиц и индивидуальных предпринимателей) | | |  | |
| 4.21 | Юридический адрес (для юридических лиц - юридический адрес, для физических лиц - адрес места регистрации) | | | 1. Область (в том числе гг. Алматы и Астаны):  2. Район:  3. Населенный пункт (город/поселок/село, за исключением гг. Алматы и Астаны):  4. Наименование улицы/проспекта/ микрорайона:  5. Номер дома:  6. Номер квартиры/офиса (при наличии):  7. Почтовый индекс: | |
| 4.22 | Номер контактного телефона | | |  | |
| 4.23 | Электронная почта | | |  | |
| 4.24 | Фактический адрес (для юридических лиц - адрес местонахождения, для физических лиц - адрес места проживания) | | | 1. Область (в том числе гг. Алматы и Астаны):  2. Район:  3. Населенный пункт (город/поселок/село, за исключением гг. Алматы и Астаны):  4. Наименование улицы/проспекта/ микрорайона:  5. Номер дома:  6. Номер квартиры/офиса (при наличии):  7. Почтовый индекс: | |
| 4.25 | Дополнительная информация об участнике операции | | |  | |

Карточки рисков

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 01 | | | |
| Наименование | Транзакция 7 000 000 | | | |
| Описание особенностей, назначение | Предполагается что недобросовестным гражданином был совершена транзакция равная или превышающая 7 000 000 тенге либо равной сумме в иностранной валюте, эквивалентной 7 000 000 тенге или превышающей ее, согласно главе 2, статьи 4, пункта 1 Закона О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, данную транзакцию необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1 | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Разовая сумма транзакции, Сумма транзакции в течении 2 недель. | | | |
| Единица измерения | тг | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 02 | | | |
| Наименование | Дробление транзакции 7 000 000 тг | | | |
| Описание особенностей, назначение | Предполагается что недобросовестным гражданином были совершены транзакции равная или превышающая 7 000 000 тенге либо равной сумме в иностранной валюте, эквивалентной 7 000 000 тенге или превышающей в течении 1-2 месяцев, согласно главе 2, статьи 4, пункта 1 Закона О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, данную транзакцию необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1. | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Сумма транзакции в течении 1-2 месяцев. | | | |
| Единица измерения | тг | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 03 | | | |
| Наименование | Совершение клиентом сложной транзакции | | | |
| Описание особенностей, назначение | Предполагается что недобросовестным гражданином были совершены транзакции с необычно крупной суммой и не имеющей очевидного экономического смысла и видимой законной цели согласно главе 2, статьи 4, пункта 4, подпункта 1 Закона О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, данную транзакцию необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1.  В данном случае необходимо учитывать скачок в 3-4 раза больше среднемесячной суммы пользователя в течении 1-3 месяцев; | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Среднемесячная сумма транзакции в течении 1-3 месяцев. | | | |
| Единица измерения | тг | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 04 | | | |
| Наименование | Совершение пользователем транзакции с участием лиц из стран с низким рейтингом ПОД ФТ | | | |
| Описание особенностей, назначение | Предполагается что недобросовестным гражданином была совершена транзакция (перевода\ получения) от или к пользователю проживающему (имеющему код города) в странах с низким рейтингом ФАТФ, согласно главе 2, статьи 4, пункту 4, подпункту 4) Закона О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, данную транзакцию необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1. | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции, БД ПОД\ФТ,  https://kfm.gov.kz/ru/to-help-sps/a-list-of-states-(territories)-that-do-not-perfor ; | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Код города страны | | | |
| Единица измерения | Нет | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 05 | | | |
| Наименование | Совершение транзакции публичными лицами | | | |
| Описание особенностей, назначение | Предполагается что публичным лицом (например: занимающую позицию в местном управлении города) была совершена транзакция на сумму превышающую среднемесячный размер транзакции, данную транзакцию необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1. | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции, | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Код города страны | | | |
| Единица измерения | Нет | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 06 | | | |
| Наименование | Совершение транзакции публичными лицами | | | |
| Описание особенностей, назначение | Предполагается что публичным лицом (например: занимающую позицию в местном управлении города) среднемесячная частота транзакций была увеличена в 2-3 раза, данного пользователя необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1. | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции, | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Код города страны | | | |
| Единица измерения | Нет | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Код | 07 | | | |
| Наименование | Совершение транзакции согласно схемам | | | |
| Описание особенностей, назначение | Предполагается что публичным лицом (например: занимающую позицию в местном управлении города) среднемесячная частота транзакций была увеличена в 2-3 раза, данного пользователя необходимо рассмотреть и при необходимости передать на рассмотрение в Уполномоченный орган посредством отправления формы ФМ-1. | | | |
| Источники данных для расчета | БД Системы, Сведения о транзакции, | | | |
| Участвует в расчете второго контура | Нет | | | |
| Значение риска | Код города страны | | | |
| Единица измерения | Нет | | | |
| Ранжирование по уровням | № | Наименование | Нижняя граница | Верхняя граница |
| 1 | Высокий (Красный) | 1 | 9999 |
| 2 | Средний (Желтый) | Нет | Нет |
| 3 | Низкий (Белый) | Нет | Нет |
| Периодичность расчета первого контура | По событию: при обновлении локальной БД и совершении транзакции | | | |