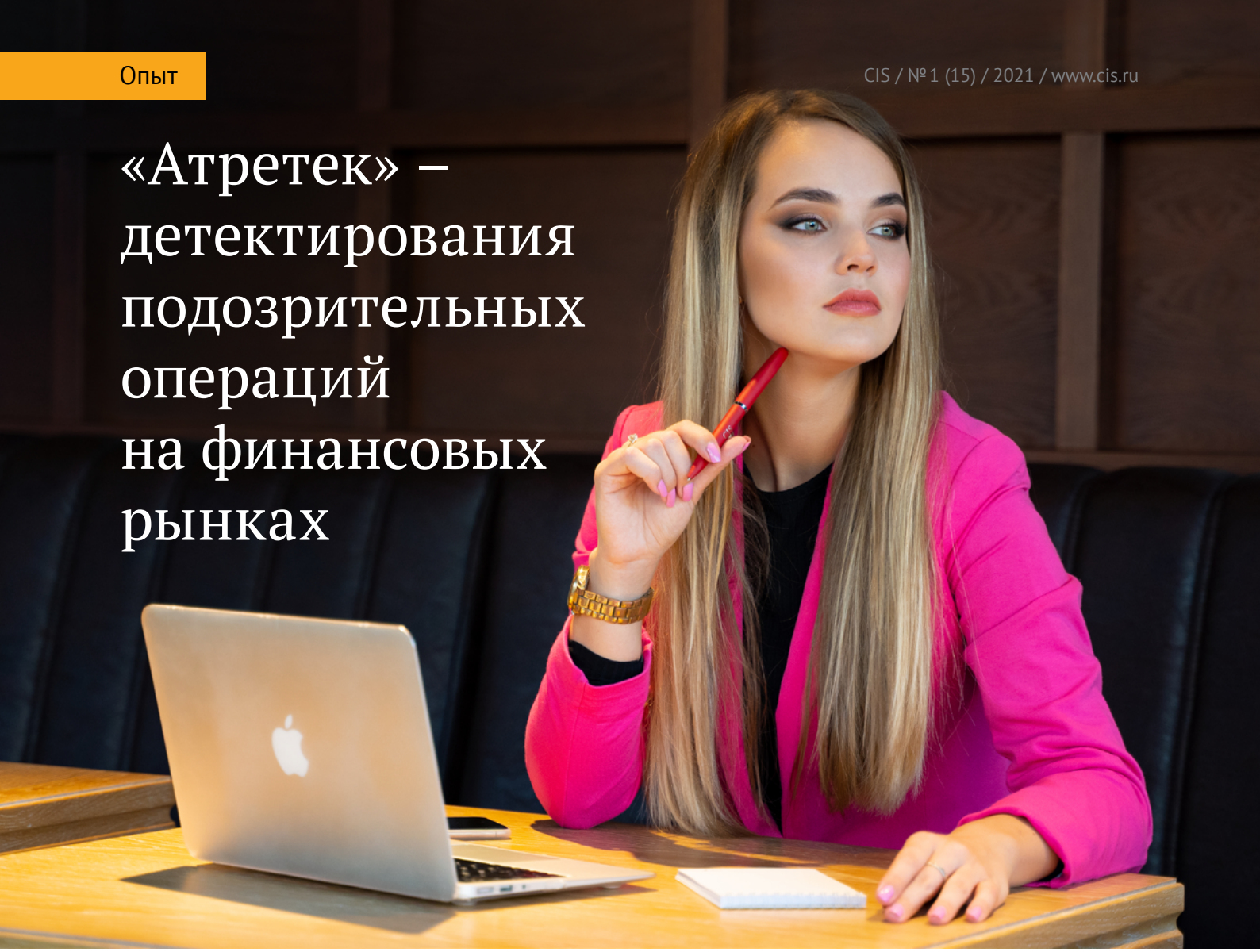
CIS / № 1 (15) / 2021 / www.cis.ru

«Атретек» – детектирования подозрительных операций на финансовых рынках



Геннадий, добрый день! Мы публиковали интервью с Вами примерно 1 год назад. Как развивается система ТАФС и проект «Атретек»? Был ли негативный эффект от пандемии?

Добрый день. Спасибо, что снова пригласили пообщаться. Да, мы не стоим на месте. Пандемия заставляет всех меняться в сторону повышения эффективности. Поэтому, в целом, мы оцениваем эффект пандемии на индустрию цифровых технологий скорее как положительный. Нас это вынудило перейти полностью на «удалёнку», и в нашей команде это привело к сокращению затрат времени на транспорт и расходов на содержание офиса.

Напомню, что проект «Атретек» – это инновационный проект, который направлен на развитие цифровых технологий для комплексного автоматизированного детектирования профучастниками подозрительных операций на финансовых рынках.

В предыдущей статье мы рассказали о том, что наша команда занимается разработкой программного обеспечения, которое решает для своих пользователей две основных задачи: снижение вероятности санкций (штрафы, отзывы лицензий, уголовное преследование) со стороны Регуляторов за несанкционированную активность на финансовых рынках и предотвращение на ранней стадии мошенничества трейдеров, которые в сговоре с клиентами могут реализовывать схемы хищений денег у работодателей.

Что-нибудь с тех пор изменилось? Или Вы идёте вперёд по тем же рельсам? Появились ли у Вас в рамках проекта инновационные разработки или новые направления для инновационных исследований?

Сказать, что ничего не изменилось нельзя, хотя в целом наш проект развивается в рамках первоначальной концепции и изначально принятой стратегии. Но по ходу развития мы обнаружили много направлений внутри проекта, которые изначально казались незначительными.

Например, когда только начинали проект «Атретек» в 2018 году, мы наивно полагали, что самое главное, чтобы система умела автоматизированным образом находить «инцидент». Мы бросили все силы команды на разработку нескольких узкоспециализированных библиотек алгоритмов, которые умеют находить «инциденты». И не просто «инциденты», а «подлинные». К слову, инциденты бывают «ложные» и «подлинные». Ложные инциденты происходят от ложных срабатываний алгоритмов. И это отдельная интересная тема.

С общепринятой точки зрения «инцидентом» принято считать просто недоразумение, неприятное происшествие, даже некое «столкновение». А что такое инцидент по Вашей терминологии?

В терминологии инструкции пользователя нашей системой инцидент – это активность клиента (комбинация заявок/сделок в привязке ко времени, рыночным данным, новостному фону), которая может быть трактуема судом как «противоправное действие» либо трактуема руководством финансового института как «нежелательная активность» со стороны рыночных, репутационных и иных рисков.

Вы называете инцидентом «активность». Но ведь «активность» – это процесс, а при слове «инцидент» скорее приходит на ум результат, а не процесс. Разве не так?

Вы абсолютно правы, в общепринятом смысле это так и есть. Но если детально и глубоко посмотреть на то, что выявляет наша система, это будет похоже и на процесс, и на результат, как бы парадоксально это не звучало.

В терминологии «Общебанковское противодействие мошенничеству» (например, ДБО, пластиковые карты и т.п.) – инцидент – это, скорее, некое событие, которое происходит одномоментно. Например, перевод денежных средств со «спящих счётов» пенсионеров в пользу третьих лиц. На финансовых рынках инциденты – это не одномоментные события, а схемы, которые реализуются мошенниками в течение некоторого периода или иначе «интервала времени». Иногда это несколько секунд, а иногда это схемы, длящиеся несколько месяцев. Но практически никогда инцидент не бывает представлен разовой одномоментной транзакцией.

Приведите примеры. Что это за схемы, которые длятся то секунды, то несколько месяцев. О чём речь?

Самые одиозные примеры имели место не в текущем году. Но зато они были наиболее масштабные с точки зрения количества транзакций. Один из первых в современной истории резонансных случаев по данной теме был связан с трейдинговой активностью японского Daiwa Bank в США. Главный трейдер этого банка однажды вдруг раскаялся (интересно, что для него стало катализатором?) и написал «покаянное письмо» президенту Daiwa Bank о том, что в течение 12 лет скрывал мошеннические схемы и около 30000 фиктивных сделок на финансовых рынках. Все его транзакции проверяла специальная комиссия FED США и специальная комиссия Министерства Финансов Японии, не говоря уже о том, что до этого его торговую активность несколько лет подряд проверяла группа Больших аудиторов. И ни одна проверка не смогла обнаружить ничего подозрительного. В итоге оказалось, что убыток банка от активности Toshihide Iguchi (имя трейдера) превысил 1 млрд $. О чём это может говорить? О том, что любая отдельно взятая транзакция сама по себе может представлять инцидент в очень редких случаях. Поэтому её невозможно выявить «вне схемы» и тем более невозможно остановить на уровне «до нажатия кнопки трейдером».

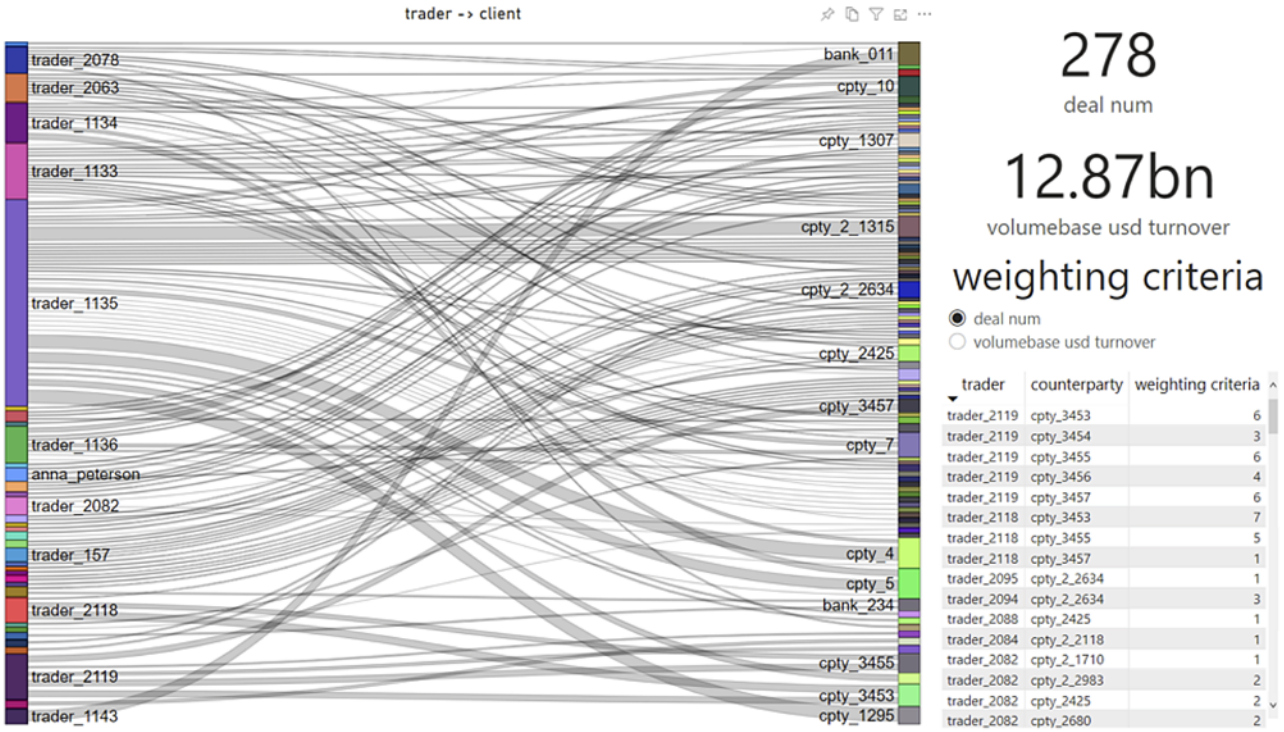
Да, в предыдущем интервью Вы ещё упоминали случай с Жеромом Кервелем из Societe Generale с убытком от его активности более чем на 7 млрд $, а также пример хищения российских трейдеров на 150 млн $ в банке «Открытие».

Поучается что один инцидент – это всегда серия сделок, которая может быть растянута по времени на несколько месяцев?

Вы абсолютно правы. Инцидент – это почти всегда серия сделок и заявок, которая растянута по времени и может быть выявлена только как цельный сценарий через реконструкцию мышления мошенника. В международной профессиональной литературе это называется «pattern recognition». Поэтому, при общении со службой безопасности того или иного профучастника в России или за рубежом нас не сразу понимают, когда мы говорим, что в большинстве ситуаций система выявляет то, что невозможно «перехватить на этапе нажатия кнопки». То есть подобную активность, конечно, можно выявить на ранней стадии и остановить. Но это не «перехват» отдельной транзакции, а выявление на ранней стадии серии сделок и заявок, которые распределены по времени и совокупно формируют подозрительный сценарий. Мы это называем «распознавание сценария», но не претендуем на корректность перевода.

Вы упомянули «мы наивно полагали, что самое главное, чтобы система умела находить «инцидент». В чём была наивность?

При разработке системы ТАФС наша команда старалась чётко фокусировать усилия на том, что называется её «ценность для пользователя» (в нашем контексте «added value»). Наивность заключалась в том, что несколько лет назад мы полагали, что вся ценность заключается в том, чтобы уметь не пропускать подлинные (не ложные) инциденты и эффективно отсеивать лож-



ные, чтобы приобретатель лицензии мог минимизировать ресурсы, выделяемые на анализ выявленных системой инцидентов.

Звучит логично. И что здесь не верно?

Здесь нет ошибки. Но оказалось, что этот функционал лишь минимально необходимый ингредиент в приготовлении блюда под названием «ценность» для пользователя. Необходимый ингредиент, но недостаточный.

Другие ингредиенты включают в себя в первую очередь способность системы автоматизированным образом формировать отчёты. Как оказалось, этот функционал имеет наиболее высокую ценность. Это должен быть не просто отчёт со списком номеров подозрительных сделок или заявок, совсем нет. Ценный для пользователя отчёт должен обладать несколькими критично важными качествами:

1) формироваться системой по заданному расписанию, в режиме близком к реальному времени;
2) удовлетворять требованиям регулятора;
3) может быть использован в качестве улики для суда.

А в чём сложность формировать отчёт, удовлетворяющий требованиям регулятора? Это же, скорее всего, какие-то всем известные формы для заполнения. Разве сложно автоматизировать их заполнение из данных о сделках и заявках, вошедших в инцидент?

Для того чтобы удовлетворить требования регулятора, необходимо своевременно отправлять ему отчёты по заранее известной форме. В Европе этот формат называется STOR («Suspicious Transaction and Order» template report to Regulator). В России это указание Банка России от 14.09.2020 г. № 5549-У «О требованиях к содержанию уведомлений, предусмотренных 224-ФЗ, а также о порядке и сроках представления в Банк России указанных уведомлений».

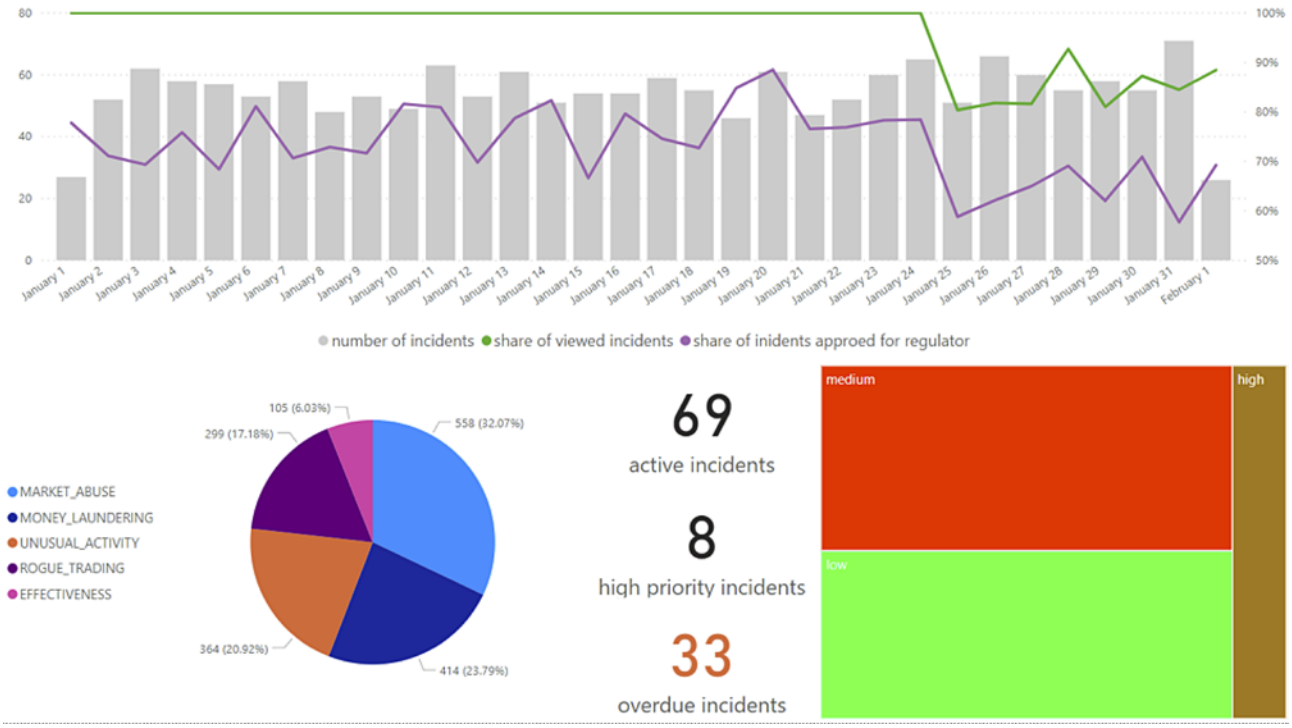
Основная сложность автоматизированного заполнения полей по форме STOR заключается в поле Reasons for the suspicion. В этом поле должно быть чётко и недвусмысленно изложены основания для подозрений.

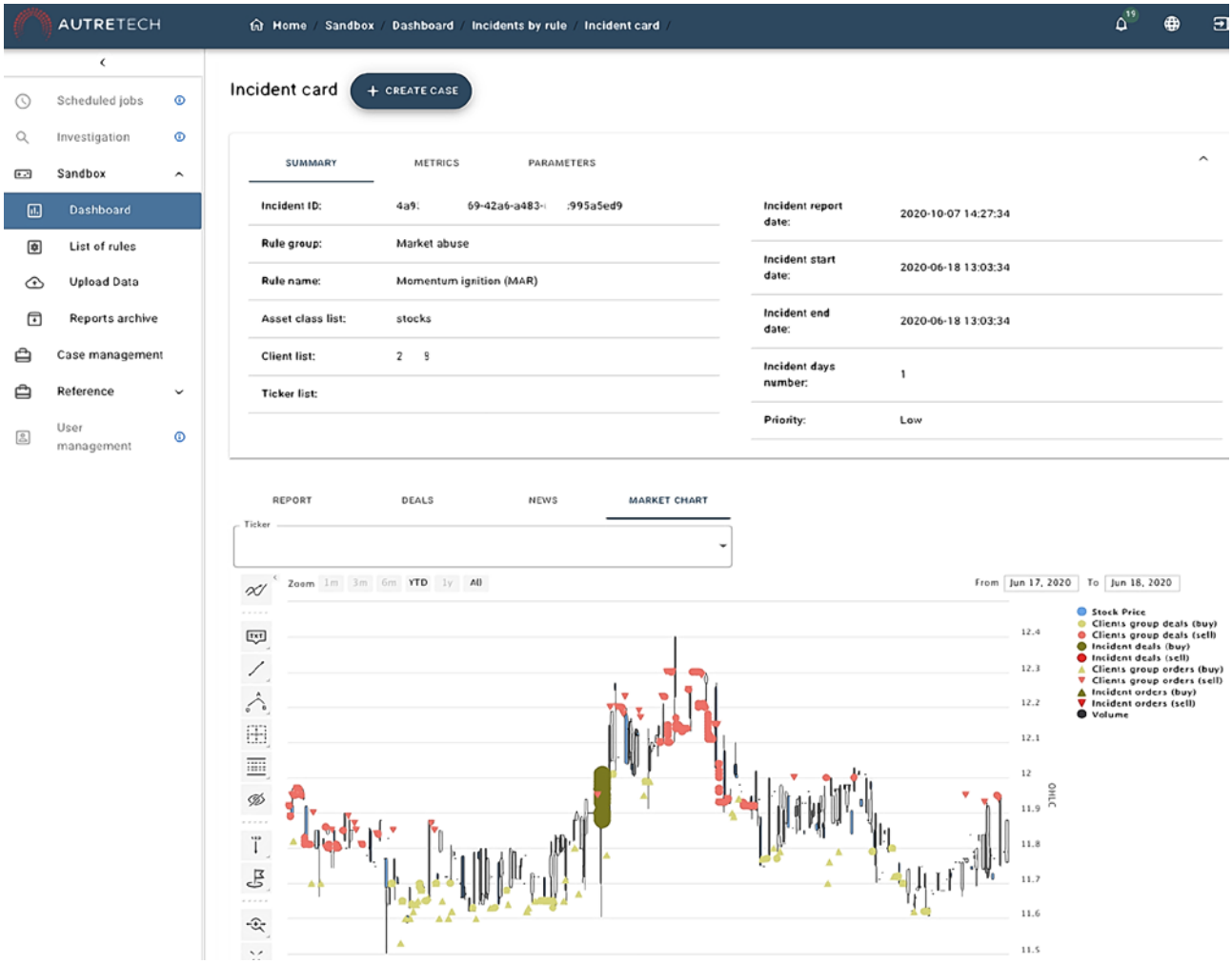
Аналогичное поле есть и в требованиях к отчёту российского регулятора: «Описание признаков неправомерного использования инсайдерской информации и (или) манипулирования рынком потенциально нестандартной операции» и «Вывод, сделанный участником организованных торгов по результатам проведённого им анализа каждой потенциально нестандартной операции».

Эти поля требуют аналитической обработки с участием специалиста, который хорошо ориентируется не только в том, как на практике работают трейдеры и клиенты и как они принимают свои решения о выставлении заявок. Такой специалист должен дополнительно иметь представление о многочисленных практических способах манипулирования и иного мошенничества на финансовых рынках. Он должен уметь реконструировать логику мошенника, уметь обрабатывать данные по сделкам и заявкам при помощи методов математической статистики и теории вероятности. Специалистов, которые имеют в своём арсенале полный набор таких компетенций на рынке, прямо скажем, не много.

Хорошо, допустим, подготовка отчёта для регулятора требует наличие специалиста с таким редким набором компетенций. Но ведь банк или брокер могут себе позволить найм таких сотрудников или воспитание собственных кадров из выпускников, например мехмата МГУ. В чём проблема?

Основная проблема заключается в том, что у крупного брокера может по формальным признакам формироваться несколько десятков и даже несколько сотен инцидентов ежедневно. Специалист с требуемым набором уникальных компетенций должен по каждому подозрительному инциденту скрупулёзно провести анализ «вручную» (с использованием современных систем бизнес-аналитики) и «вручную» изложить своё мнение в полях Reasons for the suspicion для MAR, в полях «описание признаков» и «вывод по результатам анализа».





Да, это действительно звучит как не простая задача даже для подготовленного специалиста. Что Вы можете посоветовать в такой ситуации?

Мы не берёмся давать совет. На наш взгляд, эта задача не может быть решена «вручную» через увеличение штата аналитиков с редким набором компетенций. Внутри нашей команды мы провели целую серию брейнстормингов, и в результате разработали собственную методику автоматизированного заполнения этих полей.

В самом деле? А это не будет выглядеть для Регулятора как формальная отписка, если он будет видеть типовое повторяющееся клише в поле «причина для подозрений», которое Ваша система заполняет автоматизированным образом?

Нет, мы научили систему готовить отчёты так, что повторений практически не будет, если речь не идёт о действительно полностью повторяющихся сценариях. Если говорить точнее, то в нашу систему встроен движок генерации многовариантных ответов, основанных именно на реконструкции логики мошенника. Ответы выстроены по понятной, хотя и многовариантной логике. Всё что остаётся сделать сотруднику Комплаенс – это проверить предложенную системой формулировку и выбрать из всего списка инцидентов те, которые, по его мнению, предназначены для отправки Регулятору, то есть не являются ложными срабатываниями.

К слову говоря, мы научили систему минимизировать число ложных срабатываний, но свести это число к нулю практически невозможно по многим причинам. Анализ этих причин в применении к финансовым рынкам – отдельная тема, которую мы с удовольствием можем обсудить позже.

По Вашим словам, Вы научили систему готовить логически понятные ответы. Но, Вы упомянули, что хороший отчёт должен не только удовлетворять требованиям Регулятора, но и может быть использован в качестве улики для суда. Этому Вы тоже сумели «научить» Вашу систему?

Вы задаёте очень актуальный вопрос. Пока у нас есть только многочисленные наработки по этой теме. И они ещё не объединены в единое стройное автоматизированное решение, имеющее в качестве основы математические теоремы или критерии, на которые можно опираться в суде. Такой критерий Колмогорова-Смирнова например, используется для проверки простых гипотез о принадлежности анализируемой выборки некоторому полностью известному закону распределения. Мы привлекаем для обсуждений этих вопросов специалистов из академических кругов. Но всё же полагаем, что это скорее относится к области «разработки завтрашнего дня». Формирование улик для суда на основе срабатываний алгоритмов в области финансовых рынков – суперинтересная задача. Над решением этой задачи сейчас трудимся не только мы, но и профильные команды специалистов во всём мире.

AUTRETECH

Геннадий Белов
Генеральный директор, ООО «Атретек»

www.tafs.pro