Кредитные организации во всем мире и в России все чаще используют специализированные системы для автоматизированного распознавания сценариев (pattern recognition) подозрительных операций на фондовом, срочном и валютном рынках. Какие подразделения банка могут повысить эффективность своей работы при помощи таких систем? Какой спектр задач решают такие системы в отдельных направлениях их использования? Какие специфические требования к ним наиболее актуальны на сегодняшний день?

Автоматизация мониторинга подозрительных операций при брокерском обслуживании клиентов банка на финансовых рынках

Геннадий БЕЛОВ,
ООО «Атретек», руководитель НИОКР

В качестве примеров таких автоматизированных систем можно назвать иностранные решения для противодействия мошенничеству на финансовых рынках, которые использовались кредитными организациями в России до 2022 г.: NICE Actimize (через DIS Group), ACA Technology, B.Next, Trillium, Kx и др. Однако в условиях гибридной войны и международных санкций такие системы могут быть использованы зарубежными компаниями-разработчиками непредсказуемым образом. Большинство таких систем специализируются исключительно на выявлении сценариев манипулирования и инсайдерской торговли. Но современные реалии требуют от них расширенной функциональности.

Спектр применения автоматизированных систем в кредитных организациях для распознавания подозрительной активности на фондовом, срочном и валютном рынках представлен в таблице.

Финмониторинг

Основные требования к ПВК по ПОД/ФТ для кредитной организации перечислены в Положении № 375-П. При этом аналогичное Положение № 445-П для некредитных организаций распространяет часть

Геннадий БЕЛОВ

Таблица

Применение автоматизированных систем для распознавания подозрительной активности

Направление подозрительной активности на финансовых рынках	Подразделение кредитной организации	Требования законодательства и правоприменительная практика	Виды операций для автоматизированной проверки	Риски, контролируемые при помощи автоматизации
ПОД/ФТ[1]	Финмониторинг/ внутренний контроль	Закон № 115-ФЗ[2], Положение № 375-П[3], Положение № 445-П[4] в части, обязательной для кредитных организаций[5]	В основном внебиржевые сделки, сделки с нерезидентами	Риски финансовых потерь, регуляторные риски, комплаенс-риски
Манипулирование и инсайдерская торговля в России	Контролер ПНИИИ/МР[6]	Закон № 224-ФЗ[7], Указание № 5222-У[8]	Биржевые сделки	Репутационные, регуляторные риски, комплаенс-риски
Манипулирование и инсайдерская торговля вне России	Международный комплаенс	Законодательство в области рыночных злоупотреблений (MAR[9]) в разных вариантах в иностранных государствах и регионах, международная правоприменительная практика	Биржевые и внебиржевые сделки на международных и иностранных торговых площадках	Регуляторные риски, комплаенс-риски, риски утраты контроля над активами

[1] Противодействие легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (Федеральный закон от 07.08.2001 № 115-ФЗ).

[2] Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

[3] Положение Банка России от 02.03.2012 № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

[4] Положение Банка России от 15.12.2014 № 445-П «О требованиях к правилам внутреннего контроля некредитных финансовых организаций в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

[5] Положение № 445-П в части, обязательной для кредитных организаций: «Профессиональные участники, являющиеся кредитными организациями, учитывают признаки группы 32 при включении в перечень признаков, указывающих на необычный характер сделки, в программу выявления в деятельности клиентов операций, подлежащих обязательному контролю, и операций, в отношении которых возникают подозрения, что они осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма».

[6] Противодействие неправомерному использованию инсайдерской информации и манипулированию рынком (Федеральный закон от 27.07.2010 № 224-ФЗ).

[7] Федеральный закон от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации».

[8] Указание Банка России от 01.08.2019 № 5222-У «О требованиях к правилам внутреннего контроля по предотвращению, выявлению и пресечению неправомерного использования инсайдерской информации и (или) манипулирования рынком».

[9] Регламент Европейского Союза от 16.04.2014 № 596/2014 «О рыночных злоупотреблениях (Market Abuse Regulation (MAR)).

Автоматизация мониторинга подозрительных операций при брокерском обслуживании клиентов банка

Окончание таблицы

Направление подозрительной активности на финансовых рынках	Подразделение кредитной организации	Требования законодательства и правоприменительная практика	Виды операций для автоматизированной проверки	Риски, контролируемые при помощи автоматизации
Внутреннее мошенничество: хищения сотрудниками в сговоре с клиентами	Информационная безопасность и внутреннее мошенничество	Российская и международная правоприменительная практика: случаи хищений сотрудников в сговоре с клиентами	Биржевые и внебиржевые сделки на российских, международных и иностранных торговых площадках	Риски финансовых потерь от хищений, репутационные риски, риски использования третьими лицами инфраструктуры кредитной организации в преступных схемах
Сокрытие рыночных рисков сотрудниками в сговоре с клиентами	Риск-менеджмент (рыночные риски)	Международная правоприменительная практика: случаи сокрытия позиции сотрудниками в сговоре с клиентами и контрагентами через многочисленные варианты «парковки позиций»	Биржевые и внебиржевые сделки на российских, международных и иностранных торговых площадках	Рыночные риски
Совершение сделок клиентами из списков	Комплаенс и внутренний контроль	Международные списки: санкционные списки, «правило 50%», предположительные связи, списки Росфинмониторинга, иностранное происхождение, списки публичных должностных лиц и т.п.	Биржевые и внебиржевые сделки на российских, международных и иностранных торговых площадках	Комплаенс-риски, риски утраты клиентами контроля над активами
Использование счетов корпоративного клиента сотрудниками этого клиента для реализации схем отмывания, манипулирования, хищений, сокрытия рыночных рисков	Подразделение по работе с корпоративными клиентами внутри РКО	Предоставление крупным корпоративным клиентам дополнительного комфорта в виде «сервиса проверки качества управления счетом»	Биржевые и внебиржевые сделки на российских, международных и иностранных торговых площадках	Риски хищений, рыночные риски, репутационные риски, комплаенс-риски, риски утраты клиентами контроля над активами
Аудит кредитной организации (внутренний или внешний)	Подразделение внутреннего аудита	Внутренние регламенты в кредитной организации	Биржевые и внебиржевые сделки на российских, международных и иностранных торговых площадках	Риски хищений, рыночные риски, репутационные риски, комплаенс-риски, риски утраты клиентами контроля над активами

Источник: ООО «Атретек» (www.атретек.рф).

своих требований на всех профессиональных участников. В частности, Приложение 3 к Положению № 445-П перечисляет признаки группы 32, указывающие на необычный характер сделки, и прямо распространяет требования к выявлению сделок с этими признаками на кредитные организации.

Геннадий БЕЛОВ

Особенности сценариев, которые подлежат автоматизированному детектированию в рамках требований Положения № 445-П, заключаются, в частности, в том, что в них делается акцент на внебиржевых операциях (например, коды[1] 3202, 3203, 3205, 3206, 3207, 3216, 3221, 3230, 3231, 3232) и операциях с участием банков-нерезидентов или клиентов-нерезидентов (например, коды 3211, 3213, 3215, 3216, 3217, 3218, 3219, 3220, 3228, 3229, 3230, 3231).

Другая особенность этих сценариев Приложения 3 к Положению № 445-П — их кажущаяся простота и отсутствие необходимости использовать сложноструктурированные многоходовые алгоритмы детектирования (такие, например, как сценарии из смежной международной практики в области рыночных злоупотреблений: схемы pump&dump или momentum ignition).

Интересно, что мошенники часто используют для отмывания схемы, перечисленные в кодах 3202, 3203, 3205, 3206, 3207, но при этом не через внебиржевой рынок и не через адресные заявки, а через традиционный биржевой рынок в режиме анонимных торгов. Выявляются такие схемы в режиме анонимных торгов в основном при помощи автоматизированных систем и специализированных алгоритмов, которые используют теорию вероятности и математическую статистику.

Интересно, что мошенники часто используют для отмывания схемы, перечисленные в кодах 3202, 3203, 3205, 3206, 3207, но при этом не через внебиржевой рынок и не через адресные заявки, а через традиционный биржевой рынок в режиме анонимных торгов.

Пример — схема по коду 3203 «Совершение профессиональным участником за свой счет или за счет клиента взаимных сделок, когда стороны таких сделок (профессиональные участники или их клиенты) регулярно меняются, выступая в качестве то продавцов, то покупателей, приобретая/продавая при этом единовременно или по частям одни и те же ценные бумаги и (или) иные финансовые инструменты примерно одного и того же объема (в случае совершения взаимных сделок на внебиржевом рынке и (или) через организаторов торговли на основании двух адресных заявок)».

Эта схема часто применяется именно в режиме анонимных торгов для отмывания и для «выкачивания» средств из кредитной организации, которая находится на грани банкротства.

Важное требование к автоматизированной системе в данном направлении — умение распознавать сценарии с использованием «кросс-инструментов», например схемы с использованием одновременно акций на внебиржевом рынке и опционов на фьючерсы на эти же акции на бирже в режиме анонимных торгов.

[1] Коды вида признака Приложения 3 к Положению № 445-П.

Автоматизация мониторинга подозрительных операций при брокерском обслуживании клиентов банка

Манипулирование и инсайдерская торговля в России

Второе направление использования такого рода автоматизированных систем — детектирование подозрительной активности клиентов в области манипулирования рынком и инсайдерской торговли в России[1]. Согласно п. 4 ст. 12 Закона № 224-ФЗ, участники организованных торгов, имеющие основания полагать, что операция от их имени, но за счет клиента или от имени и по поручению клиента осуществляется с неправомерным использованием инсайдерской информации и (или) является манипулированием рынком, обязаны уведомить Банк России о такой операции.

Особенностью правил по этому направлению является то, что они, во-первых, распространяются прежде всего на биржевые операции и в редких случаях требуют автоматизированного анализа внебиржевых сделок клиентов, во-вторых, почти не совпадают с международной практикой выявления рыночных злоупотреблений (MAR и его аналоги вне Евросоюза).Нельзя не отметить, что рекомендуемые в России правила по этому направлению часто бывают более эффективными для выявления манипуляторов, чем правила европейского MAR.

Порядок уведомления, сроки направления и содержание уведомления определяет Банк России. Соответственно, важным требованием к автоматизированным системам является их умение не просто распознавать подозрительные сценарии, рекомендованные Банком России через Национальный совет финансового рынка (так называемые «критерии НСФР»[2]), но и автоматизированным образом формировать отчет в соответствии с требованиями, заданными Банком России в Указании № 5222-У.

Важным требованием также может быть умение системы не просто генерировать отчеты по набору полей, которые требует Банк России, но и автоматизированным образом формулировать пояснение для регулятора, почему тот или иной сценарий считается подозрительным.

Обычно это самый трудоемкий раздел, требующий «ручной работы» специалиста кредитной организации, и автоматизация этого раздела позволяет серьезно повысить эффективность подготовки отчетов для регулятора.

Важным требованием может быть умение системы не просто генерировать отчеты по набору полей, которые требует Банк России, но и автоматизированным образом формулировать пояснение для регулятора, почему тот или иной сценарий считается подозрительным. Обычно это самый трудоемкий раздел.

[1] https://cbr.ru/inside/inside_detect/table/.

[2] Критерии НСФР: https://rosfinsovet.ru/site/public/elfinder/News/2020-12-17/1_Rekom_%23_21-7-3(3_redakciya)(of_ot_02.12.20)(na_14.12.20).pdf.

Геннадий БЕЛОВ

Манипулирование и инсайдерская торговля вне России

Третье направление — это отдельный класс правил (алгоритмов), связанный с необходимостью выявлять подозрительные операции на финансовых рынках в соответствии с международной правоприменительной практикой в области рыночных злоупотреблений. Правила (алгоритмы детектирования) по этому направлению наиболее сложно структурированы и основываются на требованиях регуляторов в Евросоюзе и других странах.

Здесь важно отметить, что одним из глобальных хабов в области управления активами является Сингапур и требования местного регулятора (Monetary Authority of Singapore) в области детектирования рыночных злоупотреблений[1] не сильно отличаются от требований европейского регулятора. Эта ремарка может показаться неактуальной в сегодняшних условиях, однако большинство регуляторов в других странах Ближнего Востока и Азии также формулируют свои требования близко к требованиям директивы Евросоюза и сингапурского регулятора.

Использование трейдинговой (брокерской) инфраструктуры банка клиентами для реализации схем хищений из крупных компаний в пользу третьих лиц — наиболее распространенная проблема, причем мошенники применяют множество разнообразных схем.

Внутреннее мошенничество на фондовом, срочном и валютном рынках

Как правило, это направление находится в компетенции службы информационной безопасности банка. Оно не связано с выполнением требований регуляторов и относится скорее к добровольному желанию кредитной организации контролировать ситуацию в области мошенничества и хищений по брокерским и собственным операциям. Использование трейдинговой (брокерской) инфраструктуры банка клиентами для реализации схем хищений из крупных компаний в пользу третьих лиц — наиболее распространенная проблема, причем мошенники применяют множество разнообразных схем.

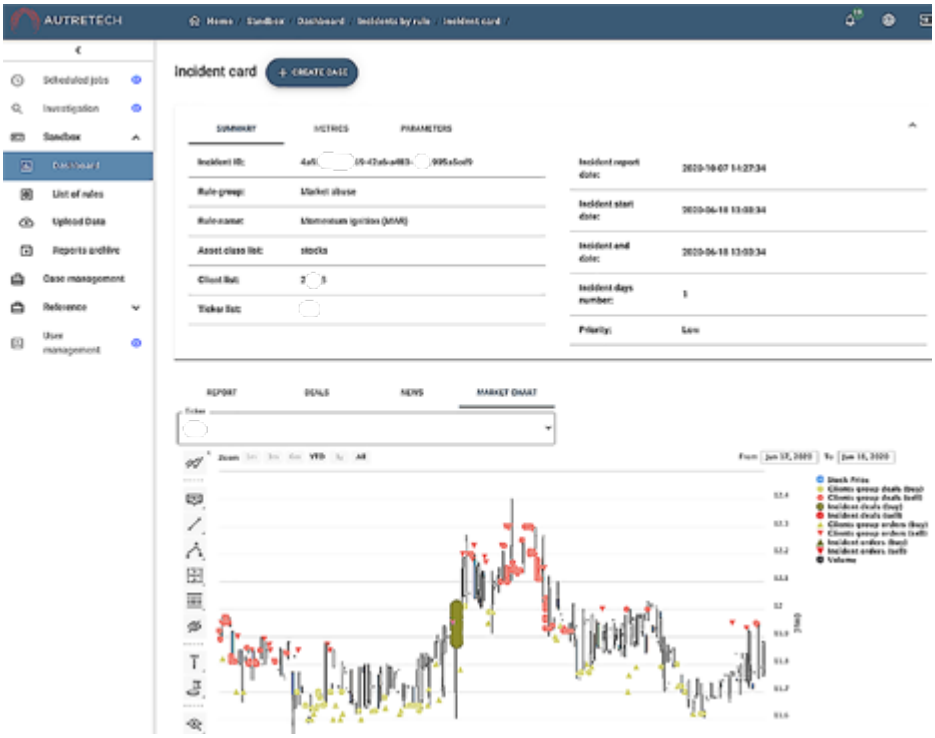
Важное требование к автоматизированной системе по данному направлению — умение осуществлять автоматизированный анализ совокупности совершенных действий/инцидентов, который может быть использован для формирования доказательной базы в судебных разбирательствах и для обеспечения гражданско-правовой ответственности вовлеченных лиц. Система должна не просто находить сценарии, но и позволять обоснованно использовать результаты своей работы в суде.

[1] https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Consultation-Papers/05082019-Control-Against-Market-Abuse/Consultation-Paper-on-Requirements-on-Controls-Against-Market-Abuse.pdf.

Автоматизация мониторинга подозрительных операций при брокерском обслуживании клиентов банка

Рисунок 1

Пример визуализации карточки подозрительного инцидента



Источник: www.атретек.рф.

В настоящее время суды вообще не понимают, «в чем заключается обман и кому причинен ущерб», когда сталкиваются с подобными ситуациями[1].

Противодействие мошенничеству и хищениям при проведении брокерских операций — тема, пока серьезно не анализируемая в России. Вероятно, потому, что масштабы этой проблемы не видны невооруженным глазом, непонятны для судей и пока не привлекают внимание кредитных организаций, предоставляющих брокерское обслуживание розничным и корпоративным клиентам.

Особенностью алгоритмов по второму, третьему и четвертому направлению является то, что они требуют специальной настройки пороговых значений (индивидуального набора настроек для каждого алгоритма) и настройки в зависимости от класса актива. Практика

[1] https://www.rbc.ru/finances/02/03/2018/5a98ee459a79476f524b375f.

Геннадий БЕЛОВ

показывает, что чем больше «регулируемых параметров тонких настроек» в правилах детектирования — тем эффективнее можно минимизировать количество ложных срабатываний системы.

Другая сторона этого подхода заключается в том, что при большом количестве правил (например, 100 алгоритмов) и «регулируемых параметров настроек» (например, в среднем 30 параметров тонких настроек внутри каждого правила) получается уже 3000 таких «регулируемых параметров тонких настроек». Если умножить это число на количество классов активов (например акции, облигации, валюты, фьючерсы, опционы), то получим 15 000 тонких настроек алгоритмов, грамотное выставление которых (с учетом особенностей клиентской базы банка) может эффективно уменьшить количество ложных срабатываний. Такое количество тонких настроек сложно изменять вручную. Оптимальным решением может быть модуль оптимизации тонких настроек с использованием встроенного машинного обучения.

Подразделение контроля рыночных рисков может использовать автоматизированную систему для распознавания многочисленных сценариев «парковки позиций» сотрудниками кредитной организации в сговоре с клиентами и контрагентами.

Контроль рыночных рисков на фондовом, срочном и валютном рынках

Подразделение контроля рыночных рисков (управляют рыночным риском трейдеры) может использовать автоматизированную систему для распознавания многочисленных сценариев «парковки позиций» сотрудниками кредитной организации в сговоре с клиентами и контрагентами.

Такого рода схемы позволяют скрывать рыночные риски в значительных масштабах. Инциденты из этой области редки, но могут сильно повлиять на финансовое состояние кредитной организации и ее рыночную капитализацию.

Наиболее одиозным примером является скандал с банком Societe Generale и его сотрудником Жеромом Кервьелем, который в течение длительного периода скрывал несколько сотен тысяч несанкционированных сделок на финансовых рынках. После обнаружения скрытых рыночных рисков и закрытия позиции объем убытка банка составил около 4,9 миллиардов евро[1]. Воздействие этой истории на капитализацию банка Societe Generale также было огромным. Другой пример (давний, но интересный) — скандал с главным трейдером подразделения Daiwa Bank в Нью-Йорке Тосихидэ Игучи[2], который однажды написал президенту банка «покаянное письмо» о том,

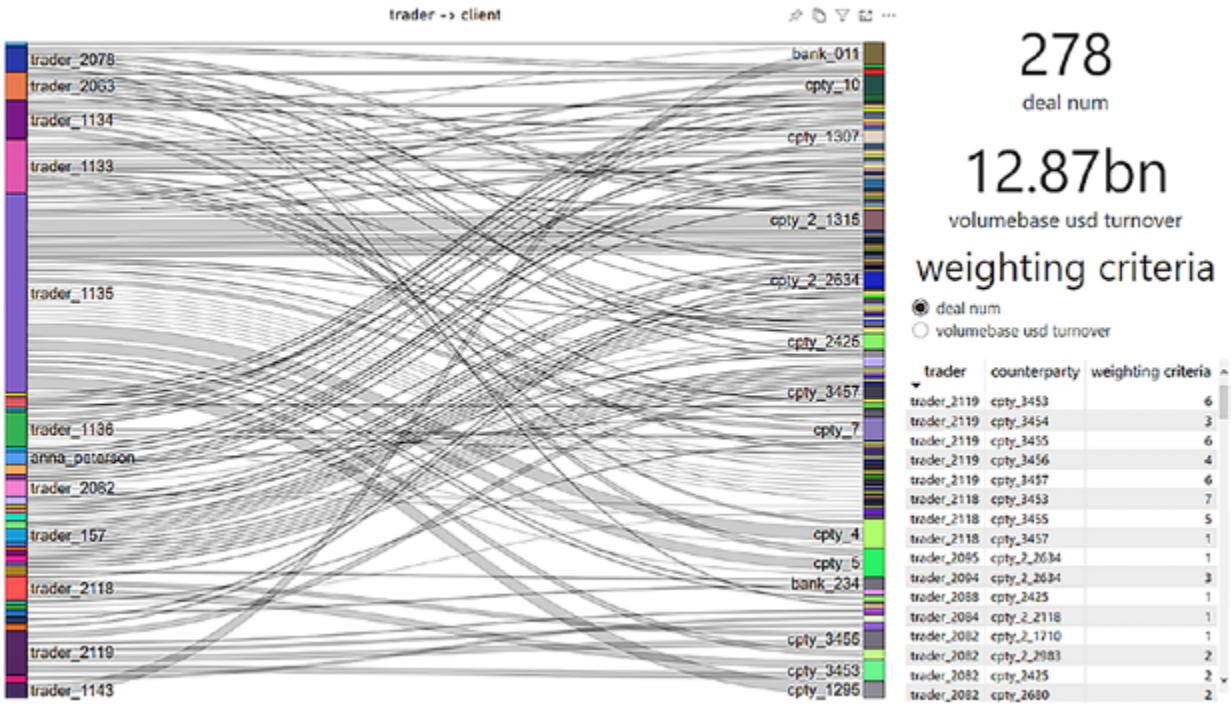
[1] https://quote.rbc.ru/news/article/5e7db83a9a7947b4a08033f8.

[2] https://www.fd.ru/articles/82100-unesennye-treyderom.

Автоматизация мониторинга подозрительных операций при брокерском обслуживании клиентов банка

Рисунок 2

Пример визуализации неявных взаимосвязей между сотрудниками и клиентами



Источник: www.атретек.рф.

что в течение 12 лет скрывал мошеннические схемы и 30 000 фиктивных сделок на финансовых рынках. В течение этих лет и позже его сделки проверяли: аудиторы (несколько лет подряд), специальная комиссия FED США, специальная комиссия Министерства финансов Японии, и никто из проверяющих ничего подозрительного не обнаружил.

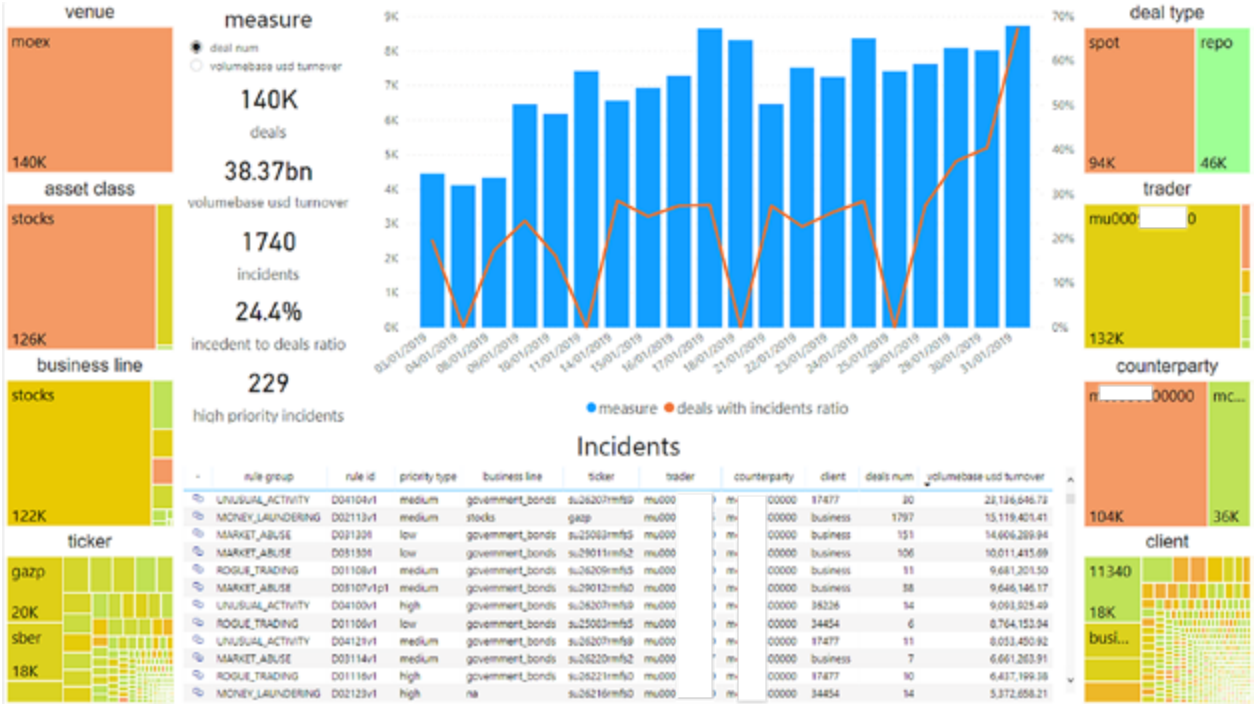
Проверка сделок и заявок клиентов на наличие в списках/токсичность

Такие проверки включают в себя автоматизированные проверки сделок в режиме, близком к реальному времени, на наличие в санкционных списках, списках финмониторинга, списках публичных должностных лиц, «правило 50%», предположительные связи, иностранное происхождение. При этом проверяются не только физические и юридические лица, совершающие сделки, но и их руководители и бенефициары.

Геннадий БЕЛОВ

Рисунок 3

Пример визуализации управленческих отчетов



Источник: www.атретек.рф.

Сервис для крупных клиентов

Крупным корпоративным клиентам может быть предоставлен сервис автоматизированной проверки операций по их счетам на подозрительную активность на финансовых рынках и сформирован отчет об отсутствии скрытых рисков по их счетам и активности на финансовых рынках.

Клиент получает регулярный отчет, подтверждающий, что:

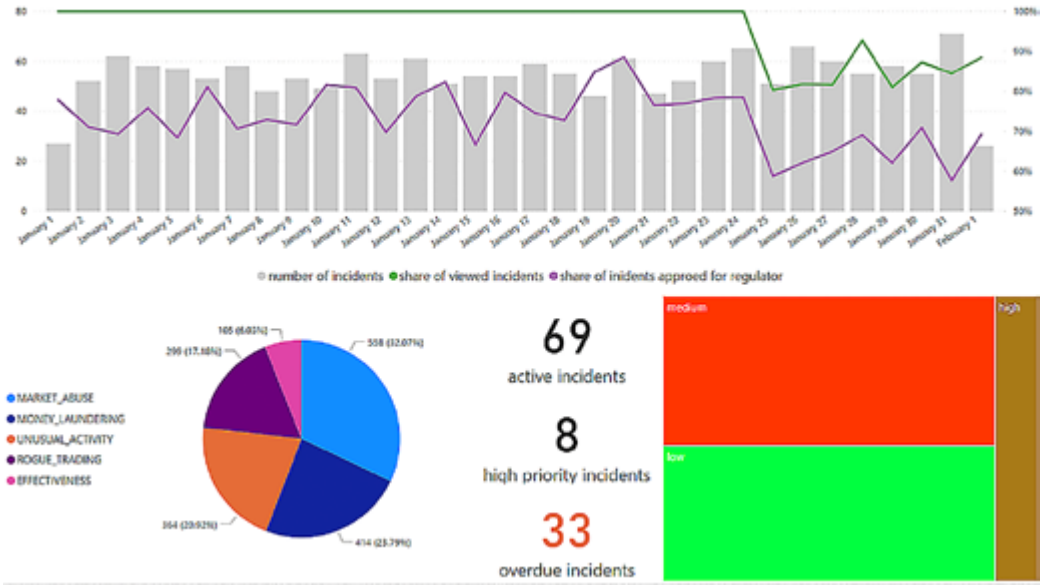
— счета, остатки на счетах и сделки клиента на финансовых рынках не участвовали и не использовались (намеренно или случайно) в схемах хищений или отмывания денежных средств;

— по счетам клиента не обнаружена намеренная или случайная активность с признаками манипулирования и инсайдерской торговли;

— в личные данные клиента не вносились изменения (email, номер телефона и т.п.);

Рисунок 4

Пример визуализации управленческих отчетов



Источник: www.атретек.рф.

— по счетам клиента не обнаружена иная аномальная или подозрительная активность.

Аудит операций кредитной организации на финансовых рынках (внутренний или внешний)

Недостатком внутреннего аудита в кредитных организациях является то, что проводится такой аудит не через анализ 100% сделок и заявок, а на выборках от нескольких сотен до нескольких тысяч сделок за квартал. И это при том, что общее количество сделок и заявок ежедневно (!) может превышать несколько миллионов. Для внутреннего аудита автоматизированная система может стать эффективным инструментом контроля подозрительной активности сотрудников кредитной организации в сговоре с клиентами и контрагентами и позволит выявлять преступные схемы на ранней стадии.

Итак, сформулируем основные цели использования автоматизированных систем такого класса:

1. Минимизировать финансовые, операционные, рыночные, репутационные, регуляторные риски посредством мониторинга

подозрительных операций трейдинговых подразделений банка и клиентов на фондовом, срочном и валютном рынках.

2. Повысить защищенность процессов проведения операций от мошеннических действий сотрудников и клиентов банка.

3. Снизить влияние человеческого фактора на процесс мониторинга операций банка, сократить время выявления инцидентов и реагирования на них, обеспечить оперативное пресечение на ранней стадии/предотвращение мошенничества и недобросовестных практик на фондовом, срочном и валютном рынках.

4. Выявлять внутреннее мошенничество клиентов и сотрудников банка на фондовом, срочном и валютном рынках.

5. Обеспечить соответствие кредитной организации требованиям Законов № 115-ФЗ и № 224-ФЗ по контролю/выявлению подозрительных операций на биржевых и внебиржевых рынках.

Аналогично можно сформулировать задачи, которые решаются при помощи такого рода автоматизированных систем (для достижения поставленных целей):

— предоставление комплексного решения для автоматизированного анализа данных из различных систем банка и внешних источников данных для алгоритмической обработки собственных и клиентских операций на фондовом, срочном и валютном рынках;

— предоставление среды проведения административных расследований и функций инцидент-менеджмента в контексте противодействия мошенничеству на фондовом, срочном и валютном рынках;

— автоматизация процессов подготовки отчетов внутри кредитной организации, аналитических материалов (по итогам алгоритмического анализа).

При этом основным глобальным трендом является переход от систем экспертного типа к системам, дополненным технологиями машинного обучения, которые, однако, используются не для распознавания подозрительных сценариев, а для оптимизации работы такой автоматизированной системы.