Борьба с обналичиванием – инструменты контроля и анализа

Глубокое исследование банками деятельности клиента, приостановление сомнительных операций, отказ в обслуживании сомнительному клиенту – это не разовая акция, и не региональная специфика нашей страны, это глобальная тенденция. Наличные платежи уходят в прошлое, растет мощность вычислительной техники и пропускная способность линий связи. Настает новая эпоха – эпоха финансовой прозрачности. В США уже больше 5 лет действует программа FATCA, в Евросоюзе есть программа CRS. Ещё 10 лет назад получить сведения об имуществе заемщика было проблемой, сейчас есть база залоговых автомобилей, бесплатная онлайн, есть сведения из Росреестра, доступные в течение нескольких часов за 350 рублей.

Банки наделяются правом и обязанностью контролировать платежи клиентов. Увеличивается число и разнообразие черных списков. Помимо списка террористов от РФМ, появились список решений МВК по ПОД/ФТ, список ФРОМУ, ЦБ выпускает списки неблагонадежных компаний и участников сомнительных операций, Правительство опубликовало «украинский» список.

Пусть не «ноздря в ноздрю» с европейскими странами и США, а с отставанием в несколько лет, но мы идем к глобальному контролю финансовых транзакций. И этот контроль регулятор возложил на плечи кредитных организаций, им же и разбираться со всеми вытекающими последствиями.

Осенью 2018 года Центральный Банк РФ распространил среди банков рекомендательное письмо, в котором обозначил новые подходы к борьбе с обналичиванием.

Эти подходы носят революционный характер. Ключевое в новых рекомендациях - переход от послед-контроля совершенных операций к онлайн проверке и приостановке операций в ходе их исполнения. Есть и еще одна очень важная особенность, не выведенная в письме напрямую, но следующая из его текста.

Критерии сомнительности операций не будут ни закрепляться законодательно, ни проходить согласование и регистрацию в Минюсте, ни даже публиковаться в открытых источниках, а только доводиться до банков в индивидуальном порядке на условиях неразглашения. И эти критерии будут комплексными, учитывающими одновременно и профиль клиента банка, и характер операции, и использовать их в работе надо будет практически на следующий день после получения.

Все вместе – новый вызов и для кредитных организаций, и для банковской автоматизации.

Неисполнение рекомендаций в области контроля сомнительных операций приводит, как правило, к введению ограничений в деятельности банка, дополнительным мерам контроля со стороны Банка России и даже отзыву лицензии. Почти в половине случаев отзыва лицензий первой (основной) причиной указывается нарушение нормативных актов Банка России в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Для банка риск неисполнения этих требований можно смело назвать неприемлемым. Но, с другой стороны, выполнение требований регулятора ведет к дополнительным операционным издержкам, никак напрямую не связанных с банковским бизнесом. В первую очередь, разрастается штат контролирующих подразделений. А это уже новые риски, связанные как с человеческими ошибками, так и с потенциальной подверженностью человека влиянию со стороны, вплоть до коррупционной составляющей. Замкнутый круг – одни риски порождают другие.

Однако, эта ситуация не безнадежна. Решение проблемы, снижающее и риски, и издержки существует. Оно лежит в плоскости грамотной автоматизации, отвечающей следующим требованиям: минимизация ручного труда и человеческого фактора, масштабируемость под задачи банка, оперативная реакция на новые требования регулятора, которые, как мы видим из мировой практики, будут становиться все более комплексными и глобальными.

Исходя из этих тенденций, компания «ПрограмБанк» разработала решение **«ПрограмБанк.ФинМониторинг»**, отвечающее на все вызовы времени.

Во-первых, предлагаемое решение отделено от АБС банка. Совершенно ни к чему грузить такое, и без того ресурсоемкое, приложение, как АБС, новыми, достаточно серьезными, задачами по обработке и хранению информации. Здесь важен принцип разнесения вычислительных мощностей – контроль транзакций не должен тормозить работу подразделений, занимающихся вводом информации. К тому же, огромное количество данных, собранных из многочисленных источников, необходимых для анализа профилей клиентов и платежей, само по себе является *big data* со всеми вытекающими последствиями.

Хранение и обработка собранной информации, контроль платежей осуществляются в **«ПрограмБанк.ФинМониторинг»**. В соответствии с настраиваемыми регламентами необходимая информация (в первую очередь фактически исполненные платежи по счетам клиентов) загружается из АБС и сохраняется в хранилище **«ПрограмБанк.ФинМониторинг»**. Таким образом, минимизируется обмен информацией между АБС и **«ПрограмБанк.ФинМониторингом»**, а также транзакционные издержки на стороне АБС.

Вынесенное за рамки АБС решение, дополнительно, соответствует рекомендации регулятора отделить системы безопасности и антифрода от систем анализа сомнительных операций. Такая рекомендация вызывает вопросы, ведь очевидно, что конечный результат мошеннической деятельности — это вывод средств клиента на сомнительные фирмы или счета физических лиц. Поэтому **«ПрограмБанк.ФинМониторинг»** может, при соответствующей адаптации, также использоваться и для целей антифрода.

Тем не менее, по умолчанию система настроена именно на контроль платежей с точки зрения финмониторинга, в соответствии с требованием регулятора.

Во-вторых, не зря выше сказано про многочисленные источники данных, из которых можно черпать информацию о клиенте и его контрагентах.

Чем больше источников, тем полнее портрет клиента и точнее анализ. И это тоже тенденция – количество обязательных для использования источников будет только расти.

Поэтому в решение **«ПрограмБанк.Финмониторинг»** заложены гибкие интеграционные возможности. В базовое решение входит интеграция с такими агрегаторами данных, как **Контур-Фокус**, **Спарк**; интеграция с ФНС через **СМЭВ** (ЕГРЮЛ, ЕГРИП, реестр МСП); импортируется список «отказников», возможен импорт других «черных списков».

И, конечно, основным контрагентом по обмену информацией является АБС банка. **«ПрограмБанк.ФинМониторинг»** может работать с любой существующей на рынке АБС.

В-третьих, в **«ПрограмБанк.ФинМониторинг»** реализованы гибкие подходы к настройке контроля и анализа операций. При этом, инструментарий сделан легким и удобным для банковских методологов.

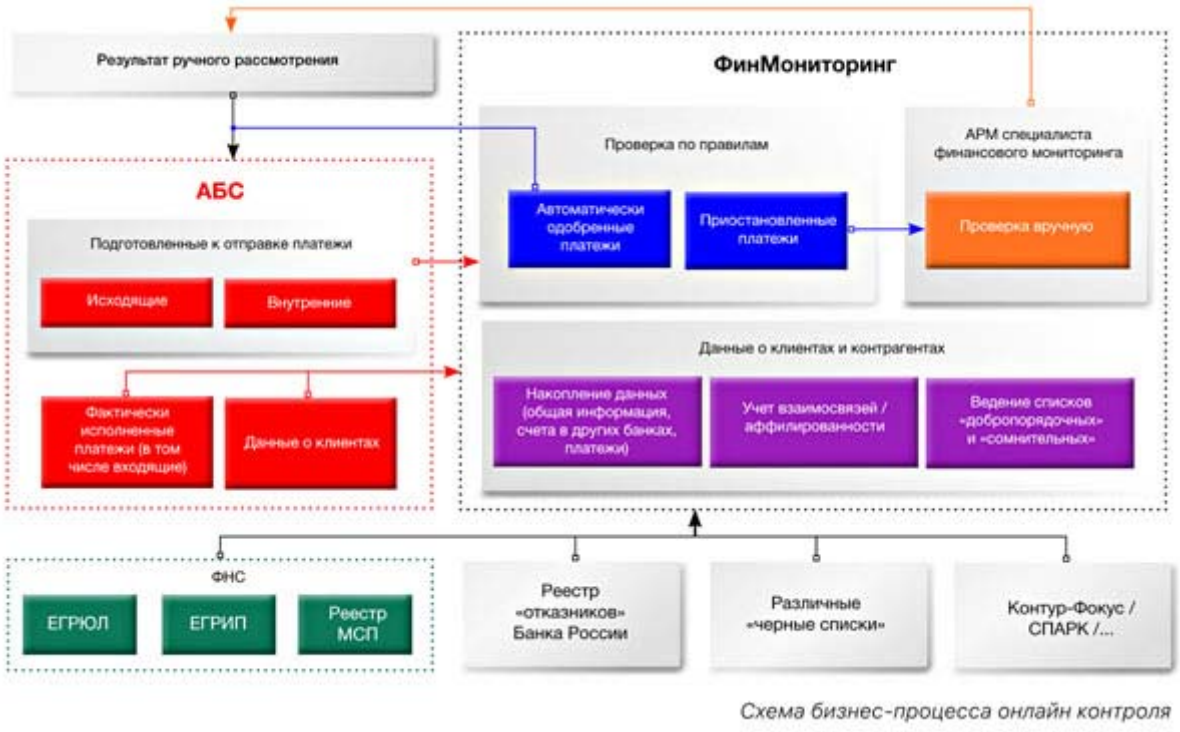
В целях минимизации ошибок предусмотрены такие удобства, как маркирование метрик и контрольных значений раз личными цветами, проверка синтаксиса (подчеркивание нераспознанных выражений), а всплывающие подсказки (описание метрики платежа или клиента,

описание контрольного значения и его собственно значения) всегда подскажут назначение применяемых сущностей. И, конечно, ускорят ввод правил подсказки при вводе части слова (автоподстановка).

Мы все знаем, что внедрение любого нового программного продукта в банке часто тормозится из-за отсутствия навыков его настройки. Понимая эту проблему, «ПрограмБанк» в составе решения передает и готовые профили сотрудников банка, и комплект правил контроля, соответствующих букве и духу упомянутого ранее рекомендательного письма Банка России, а также семинара, посвященного применению новых требований в кредитных организациях.

В базовой поставке настроены правила, позволяющие отлавливать следующие типы операций:

- веерное распределение денежных средств юридических лиц по счетам физических лиц и ИП с их последующим обналичиванием;
- смена назначения платежа, сопровождаемая «ломкой» НДС;
- смена назначения платежа, направленная на покупку наличной торговой выручки у оптово-розничных предприятий.



Базовые сущности системы «ПрограмБанк.Финмониторинг».
Объекты, метрики, правила, события, триггеры.

Настроенные правила можно использовать *as is*. Но можно применять их и как образец при внедрении собственных методик.

В-четвертых, решение **«ПрограмБанк.Финмониторинг»** призвано максимально автоматизировать процессы контроля – не только рабочие места, но все цепочки необходимых взаимодействий – бизнес-процессы.

Необходимое и минимально достаточное количество профилей сотрудников банка в системе – три: администратор, методолог финмониторинга и специалист того же подразделения. Администратор поддерживает систему в рабочем состоянии, методолог разрабатывает и настраивает правила контроля, специалист отрабатывает задачи ручного контроля.

Почему контроль нельзя отдавать на усмотрение сотрудникам операционного отдела? Приоритетная задача операциониста - наиболее точно ввести информацию, предоставленную клиентом; дополнительная автоматизация контролей финмониторинга при вводе данных может

побудить работника невнимательно вводить сведения и, в результате, ввести их с ошибкой. Срабатывание триггеров финмониторинга может побудить работника к сговору с клиентом, направленному на сокрытие информации.

Методологию нельзя отдавать на откуп техническому работнику (специалисту финмониторинга) – из-за свойственного техническим работникам желания «контролировать все самостоятельно вручную», как правило, происходит раздувание штата, и связанные с обилием ручного труда ошибки. Человеку свойственно ошибаться, это неотъемлемое качество ручного труда, и автоматизированная система должна его учитывать. Со всей необходимостью получаем разделение ролей - методолог и технический работник.

Алгоритмы нельзя менять бесследно.
Должно выполняться правило 4 рук. Следовательно, опять разделение ролей: методолог и администратор. Итого, в системе три базовых роли.

Но, если банку нужно большее разнообразие ролей, он легко может себе их настроить в рамках предлагаемого решения.

В двух словах, как выглядит весь процесс:

1. **«ПрограмБанк.ФинМониторинг»** получает из АБС подготовленные к исполнению клиентские платежи и другую необходимую информацию.
2. Информация о клиентах и их контрагентах, обслуживающихся в других банках, автоматически дополняется данными из внешних источников.
3. На основе полученной информации выполняются проверки по правилам, вычисляются метрики по соответствию триггерам и профилю риска клиента.
4. Результат проверки – решение о возможности исполнения операции передается в АБС, таким образом, платежи «вне подозрений» не тормозятся и исполняются практически без задержки.
5. А вот приостановленные платежи уже проверяются специалистами финансового мониторинга Банка вручную. Ими же принимаются обеспечительные меры по минимизации рисков ПОД/ФТ.

По платежу, приостановленному системой на основании правил контроля, специалист может, как принять решение об отказе в проведении платежа, так и разрешить провести платеж. История решений сохраняется в системе для последующего анализа, при необходимости.

Кстати, о других ролях и неожиданных возможностях.

Предложенное решение можно задействовать и для других целей, кроме снижения рисков исполнения рекомендаций регулятора.

Например, предлагаемый в базовой поставке модуль **«ПрограмБанк.ФинМониторинг»** офлайн проверки легко настроить на анализ операций и ведение профиля клиента с целью разработки индивидуальных предложений, а это уже реальная работа на бизнес банка.

Таким образом, решение **«ПрограмБанк.ФинМониторинг»** позволяет построить процессы банка, связанные с онлайн проверкой подозрительных платежей без необходимости переобучать операционистов или увеличивать в несколько раз штат отдела финансового мониторинга. Решение является достаточно гибким, чтобы перенастраивать его для взаимодействия с любой АБС и получения информации из любого источника внешних данных. Реализованные при поставке системы правила уже соответствуют существующим требованиям Банка России, и могут быть перенастроены под новые правила как силами банка, так и в рамках сопровождения системы.

Это все делает **«ПрограмБанк.Финмониторинг»** хорошим подспорьем для банков.