**НАЗВАНИЕ**

**Сергеева Вероника Александровна**,  
студентка ИФЭБ НИЯУ МИФИ  
**Соколов Александр**  
студент ИФЭБ НИЯУ МИФИ  
**Федоров Николай Михайлович**,  
студент ИФЭБ НИЯУ МИФИ

*Аннотация: в статье рассматриваются*

*Ключевые слова:* риск легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма, банки, кредитные организации, риски, цифровые технологии, алгоритм мониторинга транзакций, цифровые алгоритмы, ПОД/ФТ.

*Annotation: in article important questions ……are considered.*

*Keywords:* *the risk of legalization (laundering) of proceeds of crime and the financing of terrorism, banks, credit organizations, risks, digital technologies, an algorithm for monitoring transactions, digital algorithms, AML / CFT.*

Риск легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма – это риск, связанный с вероятностью придания клиентами банка правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученным преступным путем, и финансирования терроризма, которые не только нарушают законодательство и влекут наложение соответствующих санкций на банк, но и наносят удар по его репутации [1]. Предотвращение данного риска является одной из приоритетных задач в сфере ПОД/ФТ. На сегодняшний день достижение этой цели зависит от грамотности и организованности мер ПОД/ФТ, принимаемых кредитными организациями.

История насчитывает достаточно примеров, когда кредитные организации не осуществляли должного контроля в данной сфере и, как следствие, были закрыты. Например, банк Риггс, известный тем, что занимался личными финансовыми делами многих президентов США и многих посольств в Вашингтоне, прекратил свою деятельность в связи с выявленными попытками отмывания денег в 2005 году.

Другой пример - Danske Bank, крупнейший коммерческий банк Дании, объявил о прекращении банковской деятельности в России и странах Балтии. Причиной этого стали обвинения в незаконном отмывании денег в Эстонии и признание банка самым коррумпированным банком в 2018 году.

Примеры показывают нам несоблюдение требований ПОД / ФТ различными банками. Итак, что мешает банкам принимать эффективные меры по пресечению деятельности по ОД и ФТ?

При борьбе с финансированием терроризма и отмыванием денег особое внимание уделяется связям между физическими лицами, между юридическими лицами, а также между физическими и юридическими лицами. В целом, основные проблемы, возникающие у банков при установлении этих связей, связаны с недостатками в следующих областях:

1. Несовершенная проверка клиентов, а именно неполные или отсутствующие профили клиентов. Данное обстоятельство является наиболее слабым звеном банка. Отсутствие полноты информации о клиенте может сильно затруднить всесторонний анализ подозрительных транзакций. Предоставление услуг для фиктивных фирм, в которых личности конечных бенефициаров неизвестны, может еще больше усложнить процесс мониторинга.
2. Слабая проверка банков-корреспондентов:

Банки часто осуществляют транснациональные транзакции через банки-корреспонденты. Подразумевается, что банки проводят комплексную проверку банков-корреспондентов в отношении рисков ОД и ФТ, а также постоянный мониторинг транзакций на счетах в иностранных корреспондентских банках, но с практической точки зрения мониторинг часто бывает слабым или поверхностным.

1. Мониторинг транзакций:

Мониторинг транзакций считается основой ПОД / ФТ. Несмотря на то, что в большинстве банков системы мониторинга выполняют автоматические проверки всех операций, недостатки данной автоматизации проявляются при работе с большим объемом данных. Система мониторинга транзакций создает оповещения на основе алгоритмов, определенных для пороговых значений транзакций и исходя из поведенческих аномалий. Но поскольку большинство этих алгоритмов уже устарело, они не могут осуществлять мониторинг постоянно совершенствующихся методов ОД / ФТ, что приводит к большому количеству ложных срабатываний. Таким образом, банки настраивают систему мониторинга транзакций так, чтобы уменьшить поток поступающих оповещений.

В феврале 2016 года Базельский комитет по банковскому надзору выпустил пересмотренный набор руководящих принципов о том, как банки должны учитывать риски, связанные с ОД и ФТ, при разработке общей архитектуры управления рисками. Руководство «О должной осмотрительности клиентов», изданное Группой разработки финансовых мер по борьбе с отмыванием денег в 2017 году, позволяет использовать упрощенные меры должной осмотрительности клиентов, такие как электронная проверка личности для снижения риска ОД / ФТ. В 2017 году регулирующие органы США выпустили также набор указаний по поводу обновления структуры управления рисками для повышения ее эффективности, в котором указываются такие меры, как повышение долларовых порогов в операциях с денежными средствами, а также предоставлены более широкие возможности для обмена информацией между банками, например, прямой обмен необработанными, зашифрованными данными с РегТехом для уменьшения его зависимости от банков при проведения финансовых расследований. Согласованные действия и взаимодействие между банками будут способствовать повышению их осведомленности и стимулированию эффективного контроля во вопросе управления риском легализации отмывания доходов, полученных преступным путем, и финансированию терроризма.

По мере того, как растут требования к надлежащей проверке клиента и обмену информацией между финансовыми организациями, цифровые технологии начинают играть ключевую роль в борьбе с ОД и ФТ.

На рынке появились новые алгоритмы, встроенные в искусственный интеллект и инструменты аналитики, которые позволяют банкам и иным финансовым организациям достичь большей прозрачности транзакций. Эти алгоритмы собирают и просматривают данные о клиентах, а также помогают при углубленной проверке новых клиентов. Благодаря прогнозированию и возможностям машинного обучения, существуют платформы и алгоритмы, которые позволяют банкам легко отслеживать глобальные транзакции.

Цифровые технологии могут помочь банкам получить информацию в реальном времени для управления рисками ОД и ФТ. Данные технологии предлагают достаточно простые процессы проверки, что позволяет значительно сократить расходы. Благодаря обобщению данных из нескольких источников, цифровые технологии помогают банкам и иным финансовым организациям разрабатывать стратегии для управления рисками. Эти технологии не только снижают затраты и упрощают процессы ПОД / ФТ, они помогают банкам увеличить доходы и обеспечить защиту конфиденциальности данных.

Цифровые алгоритмы, охватывающие процессы регистрации, мониторинга и проверки клиентов, обеспечивают единый доступ к различным внутренним и внешним источникам информации, включая базы данных управления взаимоотношениями с клиентами (базы данных CRM). Автоматизированный отбор на предмет нарушений санкций, статуса публичного должностного лица (статуса PEP), упоминаний в прессе, а также информации о бенефициарном праве во всех источниках значительно повышает эффективность проверки клиентов. Собственные базы данных юридических и физических лиц из разных регионов дают большие преимущества в обнаружении и проверке бенефициарных собственников.

Некоторые алгоритмы осуществляют проверку качества данных, что позволяет банкам стандартизировать форматы данных, исправлять ошибки в именах, а также дедуплицировать записи клиентов из разных источников. Это также позволяет с большей точностью устанавливать связи и отношения между клиентами и предприятиями. Инструменты визуализации помогают сотрудникам банка легко обмениваться сложными сетями отношений между различными заинтересованными сторонами.

Алгоритмы мониторинга транзакций широко используют расширенный набор инструментов аналитики и искусственный интеллект для мониторинга, присвоения рейтингов рисков, вывода предупреждений, управления рабочими процессами предупреждений, а также для отчетов о подозрительных транзакциях. Банки могут выбрать автоматизацию мониторинга в режиме реального времени или выполнять мониторинг в режиме пакетной обработки.

Большинство цифровых технологий поставляется с предопределенными алгоритмами и сценариями обнаружения для конкретной области и предлагает возможности настройки для фильтрации на основе оценок риска клиента или транзакции.

На основе вышеперечисленного, можно с уверенностью заметить, что многие из представителей сферы ПОД/ФТ надеются на установление более широкого диалога среди регуляторов, органов финансовой разведки и компаний РегТеха.

До сих пор, все усилия в сфере ПОД/ФТ направлены на регуляцию банковской сферы, принятия различных нормативных актов для банков по ПОД/ФТ, что делает процесс обмена информацией расплывчатым и недостаточным, в то время как банковской сфере сейчас в первую очередь необходимо двигаться в направлении принятия комплексного подхода к оценке рисков, позволяющей более целостно понимать риски ОД/ФТ. Регуляторы в выработке мер должны обратить внимание на отсутствие стандартизации, возможности расширения сотрудничества между финансовыми организациями и необходимости постоянно искать новые решения, которые будут способны бросать вызов современным угрозам.

Новые технологии, такие как моделирование, могут успешно устранять пробелы в мониторинге банковских операций, но и, что не менее важно, позволяет делать это более быстро и менее затратно. Банки должны понимать, что партнерство с регуляторами и компаниями, у которых имеется опыт в аналитике, поможет создать совершенно новый подход к задачам предотвращения риска ОД/ФТ в кредитной организации.

**Список литературы:**

1. В.И. Корнейчук. Управление риском легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма. [Электронный ресурс]: – Режим доступа: <https://cyberleninka.ru/article/v/upravlenie-riskom-legalizatsii-otmyvaniya-dohodov-poluchennyh-prestupnym-putem-i-finansirovaniya-terrorizma> (Дата обращения: 05.11.2019)
2. WNS Extending Your Enterprice. Saurav Banerjee, Nitin Kashyap. Can the digital revolution help banks counter money laundering and terrorist financing? [Электронный ресурс]: – Режим доступа: <https://vk.com/doc165655350_524072234?hash=288c50a8a173fe6fb3&dl=89f5d67bdf842760f3> (Дата обращения: 05.11.2019)
3. Система Orange Business Services. Чем AI помогает банкингу. [Электронный ресурс]: – Режим доступа: <https://www.orange-business.com/ru/blogs/get-ready/bezopasnost/Chem-ai-pomogaet-bankingu> (Дата обращения: 05.11.2019)
4. Cистема Payhawk. Why banks should not be responsible for KYC and anti-money-laundering. [Электронный ресурс]: – Режим доступа: <https://payhawk.io/blogs/why-banks-shouldnt-be-responsible-for-kyc-and-anti-money-laundering/> (Дата обращения: 05.11.2019)