УДК 336.7 **DOI: 10.34670/AR.2026.64.55.067**

Методика пресечения финансовых правонарушений с использованием цифровых активов в кредитных учреждениях

Коробков Денис Алексеевич

Студент,
Финансовый университет при Правительстве Российской Федерации,
125167, Российская Федерация, Москва, Ленинградский просп., 49;
e-mail: Korobkov@mail.ru

Смирнов Валерий Валерьевич

Кандидат экономических наук, доцент,
Финансовый университет при Правительстве Российской Федерации,
125167, Российская Федерация, Москва, Ленинградский просп., 49;
e-mail: Korobkov@mail.ru

Аннотация

В статье рассматривается проблема противодействия финансовым правонарушениям с использованием цифровых активов в российских кредитных организациях. Авторами предложена экономико-математическая модель оценки интегрального риска клиента и транзакции, основанная на линейной аддитивной свертке семи факторов. Целью статьи является разработка экономически обоснованной методики риск-ориентированного контроля операций с цифровыми активами в кредитных организациях, позволяющую дифференцировать клиентов и транзакции по уровню риска без полного запрета на проведение таких операций, подтверждение гипотезы о целесообразности разработки такой модели. Методами исследования выступают экономико-математическое моделирование, сценарный анализ, сравнительный анализ и анализ финансовой отчётности. В результате работы была построена семифакторная модель интегрального риска клиента и транзакции, разработан алгоритм работы подразделения с такой моделью, выполнен сценарный расчет NPV. Выводы: выдвинутая гипотеза была частично подтверждена. Предложенная модель эффективна только для крупных системно значимых и подсанкционных банков.

Для цитирования в научных исследованиях

Коробков Д.А., Смирнов В.В. Методика пресечения финансовых правонарушений с использованием цифровых активов в кредитных учреждениях // Экономика: вчера, сегодня, завтра. 2026. Том 16. № 4А. С. 686-699. DOI: 10.34670/AR.2026.64.55.067

Ключевые слова

Цифровые активы, криптовалюта, финансовые правонарушения, кредитные организации, финансовый мониторинг, ПОД/ФТ, риск-ориентированный контроль, экономико-математическая модель, блокчейн-аналитика.

Введение

Цифровая трансформация финансового сектора за последнее десятилетие привела к появлению и стремительному распространению криптовалют, токенов и иных цифровых активов (далее – ЦА). Децентрализованная природа, трансграничность и высокая скорость расчётов, обеспечиваемые технологией блокчейн, открыли новые возможности для инвестиций и привлечения капитала. Однако значительная часть операций с ЦА до сих пор находится вне правового поля, а их теневой сегмент продолжает расти. Анонимность, необратимость транзакций, отсутствие единого регулятора оказались привлекательными как для законных участников рынка, так и для мошенников, эффективно адаптировавших такие активы под криминальную среду.

Легализация доходов, полученных преступным путём, уклонение от уплаты налогов, финансирование терроризма и обход санкционных ограничений – основной, но не полный перечень угроз, с которыми столкнулась глобальная финансовая система. Центральное место в противодействии этим угрозам занимают кредитные организации, которые являются основным регулятором таких транзакций, и через которые осуществляется финальная стадия обналичивания преступных доходов, их интеграция в легальную экономику.

В Российской Федерации сложилась парадоксальная ситуация. С одной стороны, государство признаёт значимость цифровых активов и создаёт отдельные элементы регулирования, но, одновременно, в отношении наиболее массового и проблемного сегмента криптовалют до сих пор сохраняется политика сдерживания, которая на практике оборачивается не снижением, а ростом криминальных рисков.

Основная часть

Традиционные методики финансового мониторинга, эффективные при работе с классическими банковскими операциями, зачастую оказываются бессильны перед анонимными и скоростными транзакциями с цифровыми активами. Платформа «Знай своего клиента» анализирует только фиатные потоки и не имеет доступа к блокчейн-данным. AML-системы кредитных организаций не способны отследить, что поступлению рублей на счёт физического лица предшествовала продажа криптовалюты на нелегальной P2P-площадке или вывод средств с санкционной биржи.

В результате возникает устойчивое противоречие между необходимостью эффективно пресекать правонарушения с использованием цифровых активов и отсутствием сбалансированных, экономически обоснованных методик, которые могли бы быть интегрированы в повседневную деятельность кредитных организаций.

Цифровые активы, в свою очередь, являются не просто новой технологией, а принципиально иным классом финансовых инструментов. Обобщая подходы, представленные в научной литературе, можно определить цифровой актив как экономический актив нематериальной природы, существующий в цифровой форме, обладающий стоимостью и способный к гражданскому обороту. [Лосева, 2021]

Их интеграция в хозяйственный оборот трансформирует технологические особенности в конкретные финансовые угрозы для кредитной организации, которые можно разделить на несколько категорий.

Рыночные риски, включают в себя: риск волатильности, который проявляется в отсутствии

у ЦА внутренней стоимости, что создаёт угрозу для банка в сфере инвестиций и обесценивании залоговых обеспечений; риск неправильной оценки стоимости ЦА, который исходит из предыдущего риска; риск ликвидности, проявляющийся в невозможности быстро конвертировать актив в фиат без существенных потерь и дополнительных рисков, особенно на территории стран, которые вводят запреты на оборот ЦА.

Операционные и технологические риски, выражающиеся в зависимости банка от нерегулируемых или слабо регулируемых провайдеров, таких как криптобиржа, сбой, взлом или банкротство которых ведут к заморозке операций и потере активов, по которым банк выступал либо как держатель, либо как посредник.

Основной категорией в данном исследовании выступают криминальные риски и риски в сфере ПОД/ФТ. Реализация этого риска влечёт наиболее тяжёлые последствия для кредитной организации: отзыв лицензии, многомиллионные штрафы, репутационные потери. Он консолидирует в себе негативный потенциал прочих рисков и создаёт для банка безвыходную ситуацию, в которой он либо вводит недостаточно жёсткий контроль, сопровождающийся санкциями регулятора, либо полностью исключает возможность проводить транзакции с ЦА, что создаёт упущенную выгоду для кредитной организации.

Вместе с тем, было бы неверным рассматривать любую операцию с цифровыми активами как заведомо противоправную, так как значительная часть пользователей ЦА использует их в добросовестных целях: для долгосрочного инвестирования, хеджирования валютных рисков, участия в легальных краудфандинговых проектах, а также для трансграничных переводов с низкими комиссиями. Добросовестность таких клиентов подтверждается наличием прозрачной цепочки происхождения средств, отсутствием связей с теневыми площадками и готовностью предоставлять подтверждающие документы по запросу банка.

Игнорирование этого обстоятельства ведёт к прямо противоположному эффекту: тотальная блокировка всех операций с ЦА, без различения их природы и целей, влечёт за собой массовый отток добросовестных клиентов, рост репутационных рисков и упущенную выгоду для банка. Итоговая задача кредитной организации заключается не в тотальном запрете, а в выстраивании такой системы мониторинга, которая позволяет отделять добросовестных клиентов от недобросовестных, концентрируя усилия на действительно опасных транзакциях.

Кредитные организации имеют определённые инструменты для противодействия финансовым правонарушениям с использованием цифровых активов, но их эффективность и надёжность не позволяют бороться с мошенничествами на приемлемом уровне. Платформа «Знай своего клиента» и традиционные AML-системы, которые сейчас используются в банках созданы для классических банковских операций и не позволяют просматривать всю цепочку транзакций с ЦА. Банк видит лишь финальную стадию движения средств - зачисление на карту физического лица от множества отправителей с последующим снятием наличными. Проследить, что этим зачислениям предшествовала продажа криптовалюты на нелегальной P2P-платформе или вывод средств с криптобиржи, находящейся под санкциями, такие системы не способны.

Помимо технологических проблем, существуют и правовые барьеры. Федеральный закон № 259-ФЗ запрещает использование цифровой валюты в качестве средства платежа на территории России, но при этом не регулирует порядок её купли-продажи, обмена, дарения и наследования. [Федеральный закон № 259-ФЗ, 2020] Криптовалюта не признаётся имуществом в классическом гражданско-правовом смысле, однако на неё распространяются общие нормы об обязательствах. На практике это означает, что банк обязан контролировать то, что юридически

не определено. [Брисов, Аббасова, 2023] В отношении ЦФА также сохраняются проблемы: они являются нерейтингуемыми, отсутствуют обязательные требования по раскрытию информации для эмитентов, технологии разных операторов несовместимы, что создаёт риски утраты прав на актив при смене оператора или техническом сбое. [Мнацаканян, Гамиловская, 2024]

Даже если банк на основании косвенных признаков заподозрил клиента в причастности к криптовалютному обналичиванию, формирование неопровержимой доказательной базы для регулятора или правоохранительных органов остаётся крайне сложной задачей. Банк не может предоставить выписку по криптокошельку, не может подтвердить, что средства поступили именно от продажи криптовалюты, а не от иных источников.

Это позволяет сделать вывод о том, что современная система противодействия финансовым правонарушениям с использованием цифровых активов в российских кредитных организациях переживает неопределённо-запретный период. Запрет на использование криптовалюты в качестве средства платежа не остановил её оборот, но вытеснил его в теневой сегмент, где контроль становится практически невозможным. Фрагментарность надзорных функций, технологическая ограниченность традиционных AML-систем и правовая неопределённость статуса цифровых активов создают устойчивые пробелы, делающие контроль малоэффективным.

Международный опыт, в частности модель Объединённых Арабских Эмиратов, где создана многоуровневая система лицензирования криптовалютной деятельности с чётким разделением компетенций между федеральным регулятором SCA и региональным регулятором VARA, показывает, что альтернатива запретительному подходу существует. Признание криптовалют объектом прав, создание регулируемых точек входа в фиатную систему и стимулирование прозрачности вместо штрафов и блокировок позволяют сделать рынок более контролируемым. Правовое регулирование криптовалюты в ОАЭ,www…]

Для российских кредитных организаций это означает необходимость разработки определённой модели, в рамках которой банк должен не пытаться блокировать всё, что связано с цифровыми активами, а учиться дифференцировать клиентов и операции по уровню риска, концентрируя основные ресурсы на действительно опасных транзакциях и кошельках.

Чтобы разработать такую модель, требуется отталкиваться от нескольких базовых принципов, вытекающих из специфики объекта контроля и особенностей функционирования кредитных организаций в этой сфере:

- Приоритет риск-ориентированного подхода, подразумевающий концентрацию кредитных организаций на тех клиентах и операциях, которые демонстрируют повышенные индикаторы риска
- Экономическая целесообразность
- Многофакторность оценки транзакций
- Динамичность и адаптивность правонарушений в реалиях цифровизации и появления новых способов совершения финансовых правонарушений

Эти принципы предопределяют сам состав факторов риска, которые следует включить в экономико-математическую модель, и их также можно разделить по трём группам.

Клиентские факторы риска, такие как вид деятельности клиента, продолжительность существования клиента в базе кредитных организаций, его кредитный рейтинг и юрисдикция регистрации.

Транзакционные факторы риска, привязанные к конкретной транзакции и оценивающиеся в момент её совершения, либо в ходе последующего мониторинга. К ним также требуется отнести

сумму и частоту операций, связи с однодневками или организациями с критически низким рейтингов доверия (имеются ввиду сервисы-миксеры и другие платформы, позволяющие стирать реальные данные владельца кошелька).

Внешние факторы риска, независящие от действий самого клиенты, но влияющие на оценку риска по операции, вроде регуляторного статуса ЦА, санкционного статуса контрагента (далее – КА) и общеэкономическая обстановка, влияющая на временный рост рисков для банка.

На базе вышеописанных факторов предлагается построить модель, основанную на принципах линейной аддитивной свертки, т.к. это обеспечит прозрачность расчёта, простоту интерпретации итоговых результатов и возможность последующей корректировки весовых коэффициентов без изменения всей архитектуры модели:

$$\mathrm{R} = \sum_{i=1}^{n} w_i \times x_i \qquad (1)$$

где: R – интегральный риск от 0 до 1;

w_i – весовой коэффициент фактора i;

x_i – нормированная оценка фактора i от 0 до 1;

n – количество учитываемых факторов.

Выбор линейной формы обусловлен требованиями прозрачности расчета и простотой интерпретации результата для сотрудников подразделений финансового мониторинга. Ключевые факторы, шкалы их оценки и весовые коэффициенты, полученные экспертным путем и готовые к калибровке на исторических данных, представлены в таблице 1.

Таблица 1 – Перечень факторов, шкалы оценки и весовых коэффициентов

№	Фактор риска	Шкала оценки x_i	Вес w_i
1	Наличие связи с криптосервисами с низким рейтингов доверия	0 – нет связи; 0,5 – косвенная связь (несколько транзакций); 1 – прямая связь	0,25
2	Использование анонимных криптовалют	0 – не используются; 0,5 – единичные транзакции; 1 – регулярное использование	0,2
3	Несоответствие объёма и характера операций заявленному виду деятельности клиента	0 – полное соответствие; 0,5 – незначительные отклонения; 1 – явное несоответствие	0,15
4	Юрисдикция КА	0 – страны ЕАЭС или ЕС (кроме офшора); 0,5 – офшорные зоны; 1 – страны с высоким уровнем коррупции	0,15
5	Частота и объём операций, не достигающих порога обязательного контроля (600 тыс руб. в соответствии с 115 ФЗ)	0 – отсутствие дробления; 0,5 – незначительные намёки на дробление; 1 – дробление крупных сумм	0,15
6	Наличие негативной информации о клиенте	0 – отсутствует; 0,5 – несколько эпизодов; 1 – наличие подобной информации в большом объёме	0,05
7	Продолжительность предоставления услуг клиенту	0 – более 3 лет; 0,5 – от 6 месяцев до 3 лет; 1 – менее 6 месяцев	0,05
Итого			1,00

Источник: создано автором.

Наибольший вес присвоен фактору связи с потенциально нелегальными сервисами, так как он является прямым индикатором участия в схемах легализации. Вторым по значимости является использование анонимных криптовалют, изначально проектируемых для ухода от

мониторинга. Несоответствие операций заявленному виду деятельности, юрисдикционный фактор имеют равный вес, так как оба характеризуют структурные особенности деятельности клиента, которые имеют возможность выходить за рамки конкретной транзакции. Сюда же относится и дробление сумм, потому что он является значимым в любой модели для оценки рисков, но недостаточно специфичен для ЦА и в равной степени используется в классических схемах обналичивания. Наименьший вес получили негативная информация и срок обслуживания, так как эти факторы не обязательно означают причастность клиента к правонарушениям, совершаемым мошенниками, но являются их неотъемлемой частью.

Для верной интерпретации интегрального риска R были найдены пороговые значения (Таблица 2).

Таблица 2 – Шкала пороговых значений

Уровень риска	Диапазон значений R	Характеристика	Действия кредитной организации
Низкий	$0 \leq R < 0,3$	Операции не содержат явных индикаторов правонарушений	Автоматический пропуск транзакций без дополнительных проверок
Средний	$0,3 \leq R < 0,7$	Выявлено сочетание факторов, требующих углублённого анализа	Ручная проверка операций, дозапрос подтверждающих документов, сокращение периода плановых проверок до 1 раза в месяц
Высокий	$R \geq 0,7$	Операции демонстрируют явные признаки отмывания/обналичивания	Отказ в проведении операции, заморозка счета, направление отчета в Росфинмониторинг, возможное расторжение договора

Для иллюстрации работы приведённой модели рассмотрим гипотетического клиента – юридическое лицо, которое подписало с кредитной организацией договор на открытие счёта 4 месяца назад - $x_7 = 1$. Деятельность клиента не вызывает подозрений, но его расчётный счёт показывает регулярные поступления от физических лиц с последующим переводом на криптобиржу, которая не включена в реестр операторов ЦФА - $x_3 = 1$. При проверке адресов кошельков через открытые базы данных обнаружена связь с миксером - $x_1 = 1$. Анонимные криптовалюты клиентом не используются - $x_2 = 0$. КА находятся в юрисдикции стран ЕАЭС - $x_4 = 0$. Дробления денег нет - $x_5 = 0$. Негативная информация отсутствует - $x_6 = 0$.

Исходя из этих вводных данных, приведённая модель выводит следующий уровень риска по клиенту:

$$R = 0,25 \times 1 + 0,2 \times 0 + 0,15 \times 1 + 0,15 \times 0 + 0,15 \times 0 + 0,05 \times 0 + 0,05 \times 1 = 0,45$$

Клиент из приведённого примера попадает в зону риска среднего уровня, который не влечёт санкций, но каждая операция с ЦА требует ручной проверки, а банк вправе запросить подтверждение легальности транзакций.

Для внедрения модели в деятельность банков необходимо регламентировать действия финмониторинга алгоритмом из четырёх (пяти - при среднем риске) этапов, автоматизировав максимум процессов и оставив для ручного анализа лишь узкие места, требующие профессионального суждения.

Первый этап - идентификация операции как потенциально связанной с ЦА по формальным признакам вроде использования определённых терминов в назначении платежа, реквизитов получателей или поведенческих паттернов вроде переводов физлицам с последующим списанием, а также данных от поставщиков информации о подозрительных адресах. При отсутствии признаков операция обрабатывается в общем порядке для фиатных средств.

Второй этап - автоматический сбор данных для расчёта интегрального риска. Система

определяет значение x_i по каждому фактору, сопоставляя данные с порогами. Если сопоставление невозможно, транзакция передаётся аналитику для дальнейшего анализа.

Третий этап - вычисление интегрального показателя, сравнение с вышеописанными порогами, присвоение уровня риска и, при необходимости, отправка запроса на дополнительный анализ или заморозку счёта.

Четвёртый этап, являющийся ситуационным, включает запрос аналитику, который в установленный срок собирает дополнительную информацию и принимает решение на основе собранной информации и выявленных им рисков клиента. Аналитик получает доступ к клиенту, запрашивает пояснения и документы, оценивает их достоверность, при необходимости проверяет открытые/закрытые источники и принимает итоговое решение: разморозить транзакцию, продлить срок её рассмотрения, отказать и направить в Росфинмониторинг.

Пятый этап – ежеквартальный, в первое время, или ежегодный, когда система докажет свою эффективность, анализы работы разработанной модели уполномоченным лицом по следующим параметрам:

– доля операций в каждой зоне риска - отклонение от ожидаемого распределения свидетельствует о некорректной калибровке;
– частота ложноположительных и ложноотрицательных срабатываний - ложный сигнал ведёт к репутационным избыткам и излишней трате рабочей силы, исходя из чего оба случая требуют пересмотра весовых коэффициенты модели или добавления новых факторов;
– время обработки операций со средним риском - превышение нормы говорит о недостаточной квалификации аналитика, в связи с чем ему требуется назначить прохождение дополнительных курсов, либо взять на его место более квалифицированного специалиста, так как модель и отрасль относительно новая, и недостаточный уровень знаний системе может привести к огромным убыткам в кредитной организации.

На основе результатов руководитель подразделения может корректировать параметры модели, обеспечивая её адаптивность к новым схемам нарушений и экономическую эффективность в долгосрочной перспективе.

Экономическая эффективность предлагаемой методики определяется затратами на её внедрение и последующее сопровождение. В рамках данного исследования рассматриваются три сценария при единых вводных: активы банка — 20 млрд руб., количество клиентов — 20 тыс., имеется собственное IT-подразделение, но существует лимит расходов на дорогостоящее ПО. Помимо этого, для расчёта дохода на одного клиента используется финансовая отчётность Банка ВТБ с 2023 по 2025 год с дальнейшими расчётами издержек.

Первый сценарий. Банк не внедряет специализированные инструменты блокчейн-аналитики, а опирается исключительно на традиционную AML-систему, ориентированную на фиатные потоки. Выявление операций с цифровыми активами проводится верхнеуровнево — по формальным признакам в назначении платежа и при поступлении запроса от надзорного органа.

Поскольку затраты на оборудование отсутствуют, единственные издержки банка связаны с регуляторными рисками и упущенными доходами. Банки, не обеспечивающие должного контроля за операциями с ЦА, рискуют получить штрафы от Банка России в размере от 300 тыс. до 500 тыс. руб. Для сценария принимается сумма возможных штрафов за неисполнение обязанностей в сфере ЦА — 3 млн руб. [Кодекс РФ об административных правонарушениях,

2001]

Штрафы влекут репутационные потери, из-за которых от 15% до 20% клиентов перестают пользоваться услугами банка, что создаёт эффект упущенной выгоды[Regulatory and Operational Risk in UK Retail Banking, www...]

Для расчёта итоговых издержек по этому сценарию используется финансовый отчёт ВТБ, количество клиентов и доход на одного клиента. В нашем банке 20 000 клиентов, из них 10% заинтересованы в цифровых активах и транзакциях с ними (такой процент обусловлен растущей популярностью ЦА), а 25% их транзакций связаны с ЦА. На основе этого рассчитана упущенная выгода — 4,5 млн руб. Штрафы по 115-ФЗ приняты в сумме 3 млн руб., репутационные потери — 32 млн руб. (вычислены через средний процент оттока клиентов из банков со снизившейся репутацией после инцидента).

Итоговые издержки за 2025 год составили 39,6 млн руб., за 2024 год — 81,1 млн руб., за 2023 год — 41,3 млн руб. Относительно активов банка суммы невелики, однако они носят трудно прогнозируемый характер, и по мере популяризации ЦА, их узаконивания государством и роста числа клиентов издержки будут увеличиваться.

Второй сценарий. Банк приобретает годовую лицензию на одну из основных зарубежных платформ блокчейн-аналитики — Chainalysis KYT. В минимальной комплектации ПО обойдётся примерно в 10 млн руб. в год, в максимальной — в 25 млн руб. (в зависимости от уровня специалиста, курсов повышения квалификации и прочих издержек, по которым невозможно дать точную оценку). В данном сценарии берётся среднее значение итоговой стоимости — 17,5 млн руб. в год. [KYT (Know-Your-Transaction), www…]

При этом у банка снижается риск наложения штрафов или отзыва лицензии, а качество мониторинга оказывается высоким, поскольку купленное ПО выявляет все связи с нелегальными или заблокированными сервисами, а также риски клиента. С другой стороны, из-за действующих санкционных ограничений и вероятных будущих ограничений существует опасность прекращения поддержки ПО со стороны зарубежной организации на территории РФ, что делает такие траты высокорисковым шагом для банка среднего размера. Кроме того, система не будет автоматизирована, и потребуются дополнительные расходы на её интеграцию и автоматизацию.

В третьем сценарии банк переходит на гибридный формат мониторинга цифровых активов: внедряет модель, разработанную в данном исследовании, и использует платные сервисы зарубежной блокчейн-аналитики только для высокорисковых операций. При этом расходы на такие сервисы становятся не ежегодными, а возникают по факту обращения по конкретной операции.

Создаётся программный модуль, который рассчитывает интегральный риск по выделенным факторам и обеспечивает интеграцию с ЗСК. Собственное IT-подразделение банка может не иметь навыков программирования, поэтому стоимость оценивается по средней ставке аутсорс-разработки — 3500 руб./час. KYT (Разработка программного обеспечения, www...] При штате в 10 человек и 8-часовом рабочем дне это даёт 69 млн руб., округляется до 70 млн руб./год (с учётом возможных переработок и непредвиденных ситуаций). Разработка сложного ПО занимает более года; в данном случае срок установлен в 2 года, что позволяет и разработать ПО, и интегрировать его с ЗСК, и внедрить в систему, и исправить ошибки, неизбежные при разработке. Итоговая стоимость разработки — 140 млн руб.

Два курса обучения для сотрудников, работающих с системой, а также для внутренних IT-специалистов — 258 тыс. руб. [Разработка программного обеспечения, www...]

Точечные платные запросы к платформам блокчейн-аналитики стоят от 50 до 500 руб. в

зависимости от глубины проверки; для расчётов берётся средняя цена — 250 руб. Поскольку нельзя точно предсказать количество операций и объём попадающих в красную зону, рассматривается один из наихудших вариантов: из 10 000 операций с ЦА 1000 оказывается связана с финансовыми правонарушениями. В этом случае затраты на точечные запросы составят 250 тыс. руб. в год. В зависимости от реального числа запросов и объёма операций с ЦА расходы могут расти, но они не достигнут стоимости покупки полноценной лицензии.

Совокупные затраты в первый год (с предоплатой всей системы) — 140,5 млн руб., в дальнейшем они снижаются до 250 тыс. руб. Эти затраты могут возрасти при росте подозрительных операций или при доработке системы силами той же аутсорс-компании, но увеличение будет минимальным и происходит только с ростом размера банка.

На первый взгляд, столь крупные капитальные вложения в третьем сценарии с предлагаемой моделью выглядят экономически неоправданными на фоне покупки годовой лицензии за 17,5 млн руб. Однако если купленная лицензия перестанет действовать из-за санкций или прекращения обслуживания, потребуется время на поиск новой системы блокчейн-аналитики, в течение которого транзакции не будут отслеживаться, а значит, возникнет риск штрафов или отзыва лицензии.

Экономический эффект от внедрения такой системы выражается не столько в прямом доходе, сколько в предотвращённых потерях, которые были рассчитаны в первом сценарии — 39,6 млн руб., округлим до 40 млн руб.

Для корректного сравнения сценариев необходимо учесть, что в базовом сценарии банк несёт скрытые потери, а в сценариях 2 и 3 эти потери частично или полностью предотвращаются. Используются следующие допущения:

– Сценарий 1: прямые затраты отсутствуют, непредотвращённые потери и чистая выгода соответственно составят минус 40 млн руб./год.
– Сценарий 2: ежегодные затраты — 17,5 млн руб./год, предотвращённые потери — 40 млн руб./год, чистая выгода — 2 млн руб./год.
– Сценарий 3: капитальные затраты — 69 млн руб. в первые два года, затем ежегодные операционные затраты — 0,25 млн руб., предотвращённые потери — 40 млн руб. Чистая выгода в первые два года с учётом аренды лицензионного ПО на этот срок составит -86,5 млн руб./год, начиная с 3-го года — 39,75 млн руб./год.

Формула расчёта для NPV в сценариях:

$$DCF_t = CF_t \times \frac{1}{(1+r)^t} \quad (2)$$

где: DCF_t – дискретный денежный поток за период t;

CF_t – чистый денежный поток (прибыль/ предотвращённый или непредотвращённый убыток) за период t;

r – ставка дисконтирования;

t – номер года.

Расчёт проводится для трёх сценариев на 10 лет в целях рассмотрения долгосрочной перспективы, также используется ставка дисконтирования в 10% (Таблица 3).

Первый сценарий даёт отрицательный NPV за десять лет - минус 245,76 млн руб. Такой сценарий не просто убыточен, но и опасен для непрерывности деятельности банка: из-за обилия штрафов он может лишиться лицензии.

Второй сценарий показывает положительный NPV - 138,24 млн руб., с ежегодной чистой прибылью 22,5 млн руб., т.е. даже при подорожании лицензии банк остаётся далёк от точки безубыточности.

Таблица 3 – Расчет NPV для трех сценариев

Год	Коэффициент дисконтирования (10%)	Сценарий 1	Сценарий 2	Сценарий 3
1	0,909	-36,36	20,4525	-42,2685
2	0,826	-33,04	18,585	-38,409
3	0,751	-30,04	16,8975	29,85225
4	0,683	-27,32	15,3675	27,14925
5	0,621	-24,84	13,9725	24,68475
6	0,564	-22,56	12,69	22,419
7	0,513	-20,52	11,5425	20,39175
8	0,467	-18,68	10,5075	18,56325
9	0,424	-16,96	9,54	16,854
10	0,386	-15,44	8,685	15,3435
NPV		-245,76	138,24	94,58025

Третий сценарий даёт NPV 94,5 млн руб., и, с финансовой точки зрения, для малого банка разработанная методика экономически менее целесообразна, чем покупка готовой лицензии, но есть факторы, делающие её более предпочтительной:

– невозможность купить лицензию из-за санкций вынудит банки использовать либо неполноценные российские аналоги, либо предложенную разработку, на внедрение которой уйдёт время;
– обслуживание крупных клиентов, активно работающих с ЦА, упущенные комиссионные доходы которых будут значительно выше;
– включение банка в перечень системно значимых кредитных организаций, обслуживание гособоронзаказа или критической инфраструктуры, так как требования информационной безопасности могут запрещать передачу данных о транзакциях третьим лицам.

На основе этого анализа сценариев можно сформулировать практические рекомендации для кредитных организаций с проведением транзакций с ЦА, которые позволят им более эффективно соблюдать правила в сфере ПОД/ФТ.

Для малых банков наиболее рационально отказаться от капиталоёмкой собственной разработки и перейти к готовому сервису блокчейн-аналитики, желательно российскому, в целях минимизации санкционных и валютных рисков. Достаточно базового функционала в виде проверки адресов по чёрным спискам и присвоения уровня риска. Также можно комбинировать бесплатные публичные инструменты вроде открытых блокчейн-обозревателей и публичных реестров подозрительных адресов. Это не требует лицензионных платежей, но увеличивает ручную нагрузку на аналитиков и даёт лишь базовый уровень защиты, но даже такой минимальный контроль снижает регуляторные риски по сравнению с полным отсутствием мониторинга, т.к. банк может документально подтвердить регулятору, что предпринимал разумные усилия для выявления сомнительных операций.

Для средних, крупных и системно значимых банков целесообразна разработка модели по предлагаемой методике, но с поэтапным финансированием, без предоплаты всех суммы за готовую систему. Это позволит распределить инвестиции во времени, оценить эффективность на ранних стадиях и решить дальнейшие действия по проекту: продолжать его или остановить, без существенной потери всех вложенных средств. Рекомендуется три этапа:

– Первые 4–5 месяцев отводятся на создание минимально жизнеспособного продукта, который сможет проводить расчёты интегрального риска по нескольким ключевым

факторам и будет иметь интеграцию через API с несколькими бесплатными блокчейн-обозревателями.

– Следующие 6–7 месяцев ведётся разработка расширенной модел и с полным набором из семи вышеописанных факторов, интеграция с платформой «Знай своего клиента» и платными API для углублённой проверки, разработка интерфейса для аналитиков.
– Последние 6–10 месяцев проводится опытная эксплуатация ПО, калибровка весовых коэффициентов на исторических данных, обучение персонала, выпуск финальной версии.

Для банков, попавших под санкции, лишённых доступа к зарубежным платформам, обслуживающих критическую инфраструктуру и госкорпорации, собственная разработка становится обязательной. В этом случае рекомендуется не копировать полный функционал Chainalysis, а создать узкоспециализированную модель под актуальные для российского рынка схемы нарушений, дополняя её новыми функциями по мере проверки временем.

Независимо от выбранного сценария, все кредитные организации обязаны провести обучение персонала с внутренним экзаменом, организовать регулярный пересмотр весовых коэффициентов и порогов на основе анализа подозрительных операций, запросов Росфинмониторинга и изменений в законодательстве, а также наладить обмен информацией с другими банками через отраслевые ассоциации для формирования единой базы подозрительных криптоадресов и нелегальных обменников. Как вариант, можно дополнить ЗСК новым функционалом, интегрировав в него просмотр клиентов по операциям с ЦА.

Также ЦБ и Росфинмониторинг активно запрашивают информацию о применяемых инструментах контроля за Ц, и внедрение любой из модели должно быть документально оформлено и представлено регулятору. Рекомендуется заранее готовится пакет документов, включающих методику оценки риска, журнал срабатываний и решений, и акты об обучении, чтобы при проверке продемонстрировать добросовестность и принятие всех разумных мер по ПОД/ФТ, даже если отдельные операции с ЦА были пропущены. [Как ЦБ РФ контролирует оборот цифровых активов?, www...]

Отдельно для банков, принявших решение о собственной разработке, рекомендуется рассмотреть возможность коммерциализации созданного программного модуля. Рыночный спрос на инструменты блокчейн-аналитики в России существенно превышает предложение, особенно в сегменте средних и малых банков, которые не могут позволить себе ни покупку зарубежной лицензии, ни разработку личного ПО. Если банк-разработчик предложит такую лицензию на рынке, то сможет не только окупить свои затраты на разработку за счёт продаж лицензий, но и получить дополнительный доход, превратив центр затрат в центр прибыли. Для малых и средних банков это снизит порог выхода на проведение транзакций в сфере ЦА, упростит покупку лицензии и будет гарантировать качественный надзор за операциями с ЦА.

Заключение

Проведённое исследование подтвердило выдвинутую гипотезу, но лишь отчасти: разработанная экономико-математическая модель интегрального риска и алгоритм риск-ориентированного контроля позволят некоторым кредитным организациям более эффективно управлять операциями с цифровыми активами, сокращая издержки на мониторинг без полного запрета на проведение таких транзакций.

Предложенная модель, действительно, обеспечивает прозрачность расчёта, простоту

интерпретации и возможность калибровки весовых коэффициентов на исторических данных, а разработанный пятиэтапный алгоритм формализует действия подразделения финансового мониторинга от идентификации операции до регулярного анализа эффективности модели, при этом ключевым новшеством является гибридный подход, включающий в себя комбинацию бесплатных публичных источников и точечных платных API-запросов, что минимизирует постоянные операционные издержки, но её финансовая эффективность создаёт барьеры для входа в эту отрасль.

Для малых кредитных организаций наиболее финансово выгодным является второй сценарий с приобретением годовой лицензии на зарубежную (желательно отечественную) платформу блокчейн-аналитики. Третий сценарий даёт более низкий NPV, но становится более предпочтительным при невозможности покупки лицензии из-за санкций, обслуживании крупных клиентов, активно работающих с ЦА, или включении банка в перечень системно значимых организаций с требованиями информационной безопасности, запрещающими передачу данных третьим лицам.

Независимо от выбранного сценария, все кредитные организации обязаны провести обучение персонала с внутренним экзаменом, организовать регулярный пересмотр весовых коэффициентов и порогов на основе анализа подозрительных операций и запросов Росфинмониторинга, а также наладить информационный обмен с другими банками через отраслевые ассоциации для формирования единой базы подозрительных криптоадресов.

Дальнейшие направления исследований могут включать калибровку весовых коэффициентов модели на основе реальных исторических данных российских банков, разработку методов автоматической идентификации новых схем правонарушений с использованием машинного обучения, а также создание отраслевого стандарта обмена данными о подозрительных криптоадресах между кредитными организациями и регулятором, но ключевым объектом остаётся внедрение подобной модели на основе более выгодных финансовых условий для кредитных организаций, так как разработанная модель эффективно только для малой части банков.

Библиография

1. Брисов Ю.В., Аббасова Л.А. Цифровая валюта в России: правовые основы и бизнес-перспективы // Digital Law Journal. 2023. Т. 4, № 3. С. 72-88.
2. Как ЦБ РФ контролирует оборот цифровых активов? // Финансовый университет при Правительстве Российской Федерации. URL: https://www.fa.ru/university/structure/university/uso/press-service/press-releases/kak-tsb-rf-kontroliruet-oborot-tsifrovykh-aktivov/
3. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_34661/
4. Лосева О.В. Цифровые активы: экономический, юридический и технологический контексты // Имущественные отношения в Российской Федерации. 2021. № 11 (242). С. 42-51.
5. Мнацаканян Л.С., Гамиловская А.А. Риски цифровых финансовых активов // Вестник Алтайской академии экономики и права. 2024. № 6. С. 345-352.
6. Правовое регулирование криптовалюты в ОАЭ // WhiteSquare. URL: https://www.whitesquarepartners.com/ru/news/pravovoe-regulirovaniye-kryptovalyty/
7. Разработка программного обеспечения // RESOLVENTA. URL: https://resolventagroup.ru/uslugi/razrabotka-programmnogo-obespechenija/
8. Сколько стоит запустить первый онлайн-курс: рассчитываем минимальный бюджет // МедиаМетологии. URL: https://netology.ru/blog/11-2023-edm-how-much-does-it-cost/
9. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации».
10. Финансовые результаты по РСБУ // ВТБ. URL: https://www.vtb.ru/ir/statements/report-rsbu/

11. KYT (Know-Your-Transaction) // Chainalysis. URL: https://www.chainalysis.com/product/kyt/
12. Regulatory and Operational Risk in UK Retail Banking: Assessing Lloyds Banking Group's Long-Term Exposure to Mis-Selling Scandals // AInvest. URL: https://www.ainvest.com/news/regulatory-operational-risk-uk-retail-banking-assessing-lloyds-banking-group-long-term-exposure-mis-selling-scandals-2510/

Methodology for Suppressing Financial Offenses Using Digital Assets in Credit Institutions

Denis A. Korobkov

Student,
Financial University under the Government of the Russian Federation,
125167, 49, Leningradskiy ave., Moscow, Russian Federation;
e-mail: Korobkov@mail.ru

Valerii V. Smirnov

PhD in Economics, Associate Professor,
Financial University under the Government of the Russian Federation,
125167, 49, Leningradskiy ave., Moscow, Russian Federation;
e-mail: Korobkov@mail.ru

Abstract

The article examines the problem of countering financial offenses using digital assets in Russian credit institutions. The authors propose an economic-mathematical model for assessing the integral risk of a client and a transaction, based on a linear additive convolution of seven factors. The aim of the article is to develop an economically justified methodology for risk-oriented control of operations with digital assets in credit institutions, allowing for the differentiation of clients and transactions by risk level without a complete ban on conducting such operations, and to confirm the hypothesis on the expediency of developing such a model. The research methods include economic-mathematical modeling, scenario analysis, comparative analysis, and analysis of financial statements. As a result of the work, a seven-factor model of the integral risk of a client and a transaction was constructed, an algorithm for the work of a department with such a model was developed, and a scenario-based NPV calculation was performed. Conclusions: the hypothesis put forward was partially confirmed. The proposed model is effective only for large systemically important and sanctioned banks.

For citation

Korobkov D.A., Smirnov V.V. (2026) Metodika presecheniya finansovykh pravonarusheniy s ispol'zovaniem tsifrovykh aktivov v kreditnykh uchrezhdeniyakh [Methodology for Suppressing Financial Offenses Using Digital Assets in Credit Institutions]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 16 (4A), pp. 686-699. DOI: 10.34670/AR.2026.64.55.067

Keywords

Digital assets, cryptocurrency, financial offenses, credit institutions, financial monitoring, AML/CFT, risk-oriented control, economic-mathematical model, blockchain analytics.

References

1. Brisov, Y. V., & Abbasova, L. A. (2023). Tsifrovaya valyuta v Rossii: pravovye osnovy i biznes-perspektivy [Digital currency in Russia: Legal framework and business prospects]. *Digital Law Journal*, 4(3), 72-88.
2. Chainalysis. (n.d.). *KYT (Know-Your-Transaction)*. https://www.chainalysis.com/product/kyt/
3. Code of the Russian Federation on Administrative Offenses No. 195-FZ of December 30, 2001. (2001). https://www.consultant.ru/document/cons_doc_LAW_34661/
4. Federal Law No. 259-FZ of July 31, 2020 "On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation". (2020).
5. Financial results under RAS. (n.d.). *VTB*. https://www.vtb.ru/ir/statements/report-rsbu/
6. How does the Central Bank of the Russian Federation control the circulation of digital assets? (n.d.). *Financial University under the Government of the Russian Federation*. https://www.fa.ru/university/structure/university/uso/press-service/press-releases/kak-tsb-rf-kontroliruet-oborot-tsifrovykh-aktivov/
7. Legal regulation of cryptocurrency in the UAE. (n.d.). *WhiteSquare*. https://www.whitesquarepartners.com/ru/news/pravovoe-regulirovaniye-kryptovalyty/
8. Loseva, O. V. (2021). Tsifrovye aktivy: ekonomicheskiy, yuridicheskiy i tekhnologicheskiy konteksty [Digital assets: Economic, legal and technological contexts]. *Property Relations in the Russian Federation*, (11), 42-51.
9. Mnatcakanyan, L. S., & Gamilovskaya, A. A. (2024). Riski tsifrovykh finansovykh aktivov [Risks of digital financial assets]. *Bulletin of the Altai Academy of Economics and Law*, (6), 345-352.
10. Regulatory and operational risk in UK retail banking: Assessing Lloyds Banking Group's long-term exposure to mis-selling scandals. (n.d.). *AInvest*. https://www.ainvest.com/news/regulatory-operational-risk-uk-retail-banking-assessing-lloyds-banking-group-long-term-exposure-mis-selling-scandals-2510/
11. Software development. (n.d.). *RESOLVENTA*. https://resolventagroup.ru/uslugi/razrabotka-programmnogo-obespechenija/
12. How much does it cost to launch your first online course: Calculating the minimum budget. (n.d.). *MediaMetologies*. https://netology.ru/blog/11-2023-edm-how-much-does-it-cost/