УДК 332.1:338.47:336.71:004.9 DOI: 10.14451/1.251.158

Open Banking и CBDC: баланс между прозрачностью и рисками отмывания доходов

© 2025 **Николаев Дмитрий Александрович**
Доцент, кандидат экономических наук, доцент Кафедры экономической безопасности и управления рисками Факультета экономики и бизнеса. Финансовый университет при Правительстве РФ, Москва.
E-mail: DNikolaev@fa.ru

© 2025 **Терютина Яна Павловна**
Студент Факультета экономики и бизнеса. Финансовый университет при Правительстве РФ, Москва.
E-mail: yateryutina@mail.ru

Ключевые слова: открытый банкинг, цифровая валюта центрального банка, CBDC, цифровизация, финансовая система, кибербезопасность, AML, приватность, финтех.

Развитие открытого банкинга и CBDC в условиях цифровой трансформации финансового сектора создает новые возможности и риски (кибербезопасность, AML, приватность). Исследование анализирует институциональные и технологические аспекты функционирования, а также зарубежный и отечественный опыт. Предложены рекомендации для регуляторов и рынка, направленные на стандартизацию, развитие мониторинга и повышение грамотности, что позволит снизить угрозы, укрепить доверие и обеспечить эффективное внедрение технологий.

Введение

Трансформация финансовой системы под влиянием цифровизации и геополитической нестабильности становится определяющим фактором развития мировой экономики. На фоне растущего спроса на безопасность, скорость и удобство финансовых услуг ключевым направлением развития становится внедрение концепций открытого банкинга (Open Banking) и цифровых валют центральных банков (CBDC). Эти инновации, с одной стороны, предоставляют широкие возможности для оптимизации транзакционных издержек, повышения эффективности контроля и автоматизации процессов, а с другой — создают новые риски, связанные с ростом киберпреступности, усложнением схем отмывания доходов и нарушением приватности.

В этой связи особую актуальность приобретает задача поиска баланса между стимулированием технологического развития, повышением финансовой прозрачности и минимизацией рисков, связанных с использованием цифровых финансовых инструментов в незаконных целях. Проблема приобретает особую значимость для

экономики, так как неконтролируемое распространение децентрализованных инструментов или неэффективное регулирование цифровых активов может создать новые каналы оттока капитала, стимулировать развитие теневой экономики и снизить устойчивость финансовых систем.

В Российской Федерации проектирование и внедрение Open Banking и CBDC рассматривается как приоритетная задача Банка России и Ассоциации Финтех. Однако несмотря на активные дискуссии и разработку концепций, ряд вопросов, касающихся гармонизации регуляторных подходов, унификации стандартов, обеспечения кибербезопасности и защиты прав потребителей, остаются недостаточно изученными. Это создает необходимость проведения комплексного исследования, направленного на выявление и анализ рисков, связанных с внедрением Open Banking и CBDC, а также на разработку практических рекомендаций для минимизации этих рисков и обеспечения устойчивого развития финансовой системы страны и, как следствие, региональных экономик.

Целью данного исследования является анализ перспектив и рисков, связанных с внедрением Open Banking и CBDC в контексте региональной и отраслевой экономики, а также разработка научно обоснованных рекомендаций для регуляторов и участников рынка, направленных на достижение баланса между технологическим развитием и обеспечением финансовой безопасности.

Материалы и методы

Для достижения поставленной цели использовались методы анализа нормативных документов, научной литературы, компаративного и системного анализа, статистического анализа и экспертных оценок. Информационной базой исследования послужили нормативные акты Банка России, Федеральной службы по финансовому мониторингу (Росфинмониторинг), международных организаций (ФАТФ, Базельский комитет по банковскому надзору), а также законодательство стран, имеющих опыт внедрения Open Banking и CBDC.

Результаты исследования и их обсуждение

Финансовая система переживает период глубокой трансформации под воздействием цифровизации и других меняющихся факторов внешней среды, которые влияют на потребительские запросы в безопасности и удобстве сервисов. В российской практике на передний план выходят такие концепции, как открытый банкинг (Open Banking) и цифровая валюта центрального банка (CBDC), которые призваны повысить эффективность, прозрачность и доступность финансовых услуг.

С одной стороны, открытые интерфейсы и цифровые валюты расширяют возможности для анализа транзакций, автоматизации контроля и внедрения инновационных сервисов. С другой — они создают новые угрозы: рост киберпреступности, усложнение схем отмывания доходов, риски нарушения приватности и усиления государственного контроля. Таким образом, баланс между повышением прозрачности и минимизацией рисков отмывания доходов становится ключевым вызовом для регуляторов и участников рынка [1].

В Российской Федерации проектирование среды открытого банкинга находится в зоне ответственности Центрального банка совместно с Ассоциацией Финтех. В подготовленной ими концепции внедрения открытых API на финансовом рынке рассмотрены понятия открытого банкинга как «модель, предполагающая получение поставщиками услуг банковских и платежных данных о клиенте, а также осуществление банковских операций по его поручению» [3, с. 3]. В рамках официальной трактовки Ассоциации Финтех и Банка России концепция открытого банкинга позиционируется как частный случай более общей экосистемы «Открытых API».

Проведенный в Концепции компаративный анализ зарубежных практик позволяет сформулировать вывод о том, что развитие открытых API в международном контексте преимущественно сосредоточено на стадии открытого банкинга, что подчеркивает его роль в качестве драйвера данной экосистемы. Внедрение открытых API

часто обусловлено государственной политикой, направленной на повышение фискальной прозрачности и обеспечение всеобъемлющей подотчетности экономических агентов перед налоговыми органами.

Что касается российской специфики, то отечественная практика внедрения открытого банкинга направлена на «преобразования из только лишь кредитной организации в полноценную экосистему, которая может предоставлять первоклассные услуги: доставки, розничной торговли, страхования, продажи услуг и т.п. Таким образом, инициатива по созданию открытого банкинга в Российской Федерации исходила изначально не от правительства, как в Европе, а от ведущих игроков рынка снизу» [8, с. 261].

Для конечных потребителей внедрение этих технологий означает рост конкуренции между банками и финтех-компаниями, что стимулирует улучшение условий обслуживания, снижение тарифов и появление новых сервисов. Например, клиенты получат возможность в одном приложении видеть все свои финансовые продукты, даже если они открыты в разных организациях, вести учет расходов и доходов, планировать бюджет. При этом управление личными данными становится более прозрачным: именно клиент решает, кому и на каких условиях предоставлять доступ к информации, а строгие требования к информационной безопасности повышают уровень защиты при получении финансовых услуг.

Для участников рынка открытый банкинг упрощает доступ к клиентским данным, что повышает конкурентоспособность небольших игроков и финтех-компаний. Использование единых стандартов снижает затраты на интеграцию, уменьшает количество ошибок и ускоряет запуск новых продуктов. Появляются новые цифровые каналы привлечения клиентов, в том числе через сервисы-агрегаторы и маркетплейсы, что расширяет охват аудитории. Дополнительным преимуществом становится рост доверия к финтех-компаниям, поскольку они обязаны соблюдать требования по кибербезопасности, а единые правила обмена данными делают взаимодействие между всеми участниками прозрачным и предсказуемым.

Для государства внедрение открытых API способствует созданию условий для развития конкуренции, так как переход клиентов между поставщиками услуг упрощается. Это стимулирует появление новых бизнес-моделей, основанных на цифровизации клиентского пути и интеграции комплексных предложений. В результате формируется благоприятная среда для инновационных решений не только в финансовом секторе, но и в экономике в целом. Кроме того, использование сервисов на базе открытых API повышает финансовую доступность и грамотность граждан: они получают инструменты для анализа доходов и расходов, более осознанного выбора продуктов и доступа к широкому спектру услуг [3, с. 15].

Несмотря на очевидные преимущества, связанные с внедрением открытых API и сопутствующее повышение уровня прозрачности финансового рынка, имплементация концепции открытого банкинга сопряжена со значительным спектром рисков. Данные риски потенциально определяют усложнение задач в области обеспечения кибербезопасности, а также создают предпосылки для эксплуатации инфраструктуры в целях легализации доходов, полученных преступным путем:

1. Поскольку открытые API становятся ключевым элементом взаимодействия между банками, финтех-компаниями и другими сервисами, они существенно расширяют поверхность возможной атаки [7, с. 346]. Ошибки при разработке интерфейсов, недостаточная аутентификация или уязвимости в протоколах передачи данных могут быть использованы злоумышленниками для кражи учетных данных, доступа к конфиденциальной информации клиентов и проведения мошеннических операций. Чем больше сторонних провайдеров подключено к экосистеме, тем возрастает вероятность того, что слабое звено,

которое запустит «эффект домино», окажется внутри инфраструктуры. Например, если сторонний сервис, имеющий доступ к клиентским данным через API, окажется скомпрометированным, атака может распространиться на связанные с ним системы, где идентификационные данные и токены доступа будут использованы для входа в другие приложения. Особенностью данного процесса является его нелокальный характер: исходная уязвимость не обязательно возникает в крупнейшем или наиболее защищённом элементе инфраструктуры, но может быть реализована через периферийного участника, безопасность которого не соответствует столь же высоким стандартам. В результате взлом небольшого финтех-стартапа или агрегатора данных способен привести к угрозе для крупных банковских институтов и их клиентов, создавая цепочку взаимосвязанных инцидентов.

2. Одно из преимуществ открытого банкинга в том, что он способствует развитию экосистемы, где клиент может одновременно пользоваться услугами нескольких поставщиков. Такая структура, с одной стороны, удобна для клиента, с другой — она затрудняет отслеживание происхождения средств. Предположим, клиент получает средства на свой счет в банке-А. Далее он с помощью сервиса агрегатора переводит часть суммы в финтех-приложение для инвестиций, ещё часть — в электронный кошелёк в банке-В, а остаток — на предоплаченную карту. В итоге для системы противодействия отмыванию доходов картина выглядит как цепочка разрозненных переводов небольшими суммами, проведённых через несколько посредников. Источник первоначального поступления средств маскируется, а выявить конечного выгодоприобретателя становится крайне затруднительно. Эти операции происходят быстро и в разных системах, которые используют разные стандарты мониторинга, что позволяет злоумышленникам использовать схемы для легализации доходов или финансирования незаконной деятельности. Например, существенной проблемой в данной многоуровневой экосистеме является отсутствие унифицированных стандартов маркировки транзакций. В разных странах и даже внутри отдельных банков используются различные классификаторы платежей, коды операций и форматы передачи данных. Так, в Европейском союзе действует стандарт ISO 20022, предусматривающий внедрение методологии передачи данных с детализированным описанием назначения платежа, включая возможность добавления уникальных идентификаторов для каждой транзакции. Однако во многих странах за пределами ЕС по-прежнему применяются устаревшие форматы — SWIFT MT-сообщения или локальные классификаторы, которые не интегрируются с другими форматами и содержат меньше данных, которые не всегда позволяют однозначно определить цель перевода или его связь с конкретным видом операции. В Российской практике собственный стандарт для передачи сообщений имеет Национальный расчетный депозитарий (НРД) и крупные банки с разветвленной филиальной сетью также разрабатывают собственные стандарты для обмена с филиалами. Другими словами, если платёжное поручение сначала поступает в банк через НРД, затем по системе SWIFT MT-сообщений передаётся в другой российский банк, а после оформляется трансграничный перевод с использованием стандартов ISO, то банковские системы как минимум дважды вынуждены «транслировать» исходное сообщение в иной формат, обеспечивая при этом корректность передачи всей информации, чтобы она была однозначно интерпретирована каждым участником цепочки. Эта задача сама по себе крайне затратна и сложна, но её сложность возрастает многократно при появлении в процессе дополнительных стандартов [10].
3. В условиях открытого банкинга в обработке транзакций участвуют разные звенья: банки, финтех-компании, платежные провайдеры и сервисы аналитики. Это усложняет

определение того, кто несёт ответственность за соблюдение требований AML, защиту данных и предотвращение утечек. Проблема усугубляется отсутствием единых стандартов: даже внутри одной страны реализация API может различаться, а на международном уровне — ещё больше. Разные подходы к безопасности, аутентификации и обмену данными создают почву для регуляторного арбитража, когда злоумышленники намеренно используют слабые юрисдикции для проведения сомнительных операций.

Таким образом, внедрение Open Banking, несмотря на его потенциал, сопряжено с существенными издержками в сфере противодействия отмыванию доходов. Сложность экосистемы, разнородность участников и нормативная фрагментация усиливают вероятность злоупотреблений и затрудняют формирование единой системы надзора. В этой связи представляется необходимым обратиться к другому направлению цифровой трансформации финансового сектора — цифровым валютам центральных банков (CBDC), которые разрабатываются в условиях институционального контроля и претендуют на роль инструмента укрепления прозрачности и управляемости денежного обращения.

Создание цифровых валют ЦБ обусловлено недавним бумом на криптовалюты, так как «криптовалюты поставили финансовых аналитиков центробанков перед задачей перехвата инициативы у частных эмитентов и создания подобного криптовалютам инструмента, но централизованно эмитируемого государством, а не распределённой децентрализованной частной сетью» [2, с. 42]. К тому же, важным отличием цифровой валюты ЦБ является ее режим анонимности: в то время как криптовалютные транзакции зачастую не требуют обязательной идентификации сторон, CBDC предполагает возможность установления правил персонифицированного учета и отслеживания операций, что обеспечивает дополнительный потенциал в сфере противодействия отмыванию доходов и финансированию незаконной деятельности. Более того, CBDC не обладает свойствами спекулятивного актива, поскольку ее стоимость жестко привязана к национальной валюте и не подвержена высокой волатильности, характерной для большинства частных цифровых валют.

Несмотря на то, что цифровые валюты центральных банков проектируются как инструмент под полным контролем государства, их использование в трансграничных расчетах открывает новые возможности для обхода традиционных барьеров финансового регулирования. CBDC могут стать альтернативным каналом проведения международных операций в обход существующих систем межбанковских расчетов (например, международная система SWIFT), что создает риск их применения в целях ухода от санкционных ограничений, нелегального вывода капитала и финансирования противоправной деятельности.

Например, Иран в условиях многолетних санкций активно ищет альтернативные каналы международных расчетов и с 21 июня 2024 года Центральный банк Ирана объявил о запуске пилотного проекта «цифрового риала». Одной из ключевых задач заявляется упрощение трансграничных платежей, особенно в торговле с Китаем и Россией. При создании механизма интероперабельных расчетных платформ, которые позволяют цифровым валютам центральных банков (CBDC) взаимодействовать напрямую без использования традиционной корреспондентской сети SWIFT у государства появится возможность проводить трансграничные расчёты в обход существующей санкционной инфраструктуры. В случае, если цифровой риал получит доступ к подобным платформам — например, через двусторонние соглашения о взаимном приёме и клиринге CBDC как система платежей в местных валютах между Аргентиной и Бразилией — Sistema de Monedas Locales (SML) [4], либо посредством участия в многосторонних инициативах по созданию «мостов» для цифровых валют (CBDC bridges), как проект MBridge (Multiple CBDC Bridge), создавшего мост между Китаем, Таиландом и ОАЭ — CBDC может стать инструментом обхода ограничений международных санкционных режимов, поскольку

новые расчетные инфраструктуры ещё не имеют единых правил регулирования и контроля, сопоставимых с действующими в глобальной системе.

Важным дискуссионным аспектом внедрения CBDC является проблема приватности. В отличие от наличных средств, цифровая валюта фиксирует каждую транзакцию, что позволяет государству в теории получать полный доступ к финансовой истории гражданина. Наиболее яркий пример представляет Китай, где цифровой юань интегрируется в более широкую систему социального контроля под предлогом удобства и борьбы с «теневой экономикой» [11, с. 356]. Ключевым элементом выступает интеграция e-CNY с национальными системами идентификации и социального рейтинга на основе сквозного контроля «1) за процессом регистрации пользователей цифровой валюты и владельцев электронных кошельков; 2) за хранением данных о трансакциях, совершаемых с использованием цифровых кошельков; 3) за выполнением функций анализа операций с цифровой валютой (концепция двух баз данных и трех дата-центров)» [6, с. 54]. Каждая транзакция привязана к конкретному пользователю, что исключает анонимность и позволяет формировать детализированный поведенческий профиль гражданина. Более того, технологическая инфраструктура позволяет вводить ограничения на использование средств: например, устанавливать временные рамки для расходования, ограничивать круг контрагентов или виды товаров и услуг, доступных для оплаты. Такие механизмы уже апробировались в пилотных проектах, где цифровой юань использовался для адресных субсидий, которые невозможно потратить на иные цели.

Подобная архитектура существенно изменяет характер финансовых отношений между государством и гражданином. Это создает предпосылки для тотальной прозрачности частной финансовой жизни, что может оказывать сдерживающее влияние на поведение граждан и формировать так называемый «эффект самоконтроля», когда пользователи воздерживаются от определённых действий из-за страха перед возможными санкциями или ухудшением социального рейтинга. Вдобавок эксперты выделяют как крупную проблему — «постепенная «маргинализация наличных денег», которая может привести к ограничению доступности денежных средств» [5, с. 19]. В научной литературе подобные практики трактуются как усиление функций надзора государства, что, с одной стороны, способствует сокращению теневой экономики, но с другой — вызывает серьёзные вопросы относительно защиты прав личности и соблюдения принципа финансовой автономии [9].

При этом чрезмерное ограничение приватности представляет собой самостоятельный риск для функционирования CBDC. Недоверие к системе со стороны граждан и бизнеса способно существенно снизить уровень её использования и подорвать доверие к национальной финансовой инфраструктуре в целом. Более того, высокая концентрация персонализированных данных в руках государства или центрального банка повышает вероятность злоупотреблений и утечек, а также делает такую систему привлекательной целью для киберпреступников. Таким образом, проблема приватности в контексте CBDC выходит за рамки этического и правового измерения, превращаясь в фактор, напрямую влияющий на эффективность внедрения цифровых валют и устойчивость финансовой системы.

В условиях дуальности вопроса внедрения открытого банкинга и цифровых валют центральных банков (CBDC) особую актуальность приобретает формирование системы практических рекомендаций, направленных на обеспечение баланса между инновационным развитием финансовых технологий и сохранением устойчивости финансовой системы. Ниже предлагается комплекс мер, ориентированных на снижение выявленных рисков и создание условий для безопасного и эффективного функционирования данных инноваций в национальном и международном контексте.

1. Одним из ключевых факторов безопасного функционирования открытого банкинга является разработка и внедрение единых

технических стандартов для API, через которые осуществляется обмен данными между банками, финтех-компаниями и другими участниками финансовой экосистемы. Стандартизация должна включать обязательные требования к шифрованию данных как при их передаче, так и при хранении, что предотвращает возможность перехвата или модификации информации злоумышленниками. Не менее важным элементом является внедрение многофакторной аутентификации для всех участников системы. Это предполагает использование не только пароля, но и дополнительных факторов идентификации (например, биометрии, одноразовых кодов или аппаратных токенов), что существенно повышает уровень защиты пользовательских данных. Для поддержания устойчивости и своевременного выявления угроз необходимо регулярно проводить тестирование на проникновение и аудит безопасности API. Такие мероприятия позволяют обнаруживать слабые места инфраструктуры, оценивать риски эксплуатации уязвимостей и своевременно внедрять корректирующие меры.

2. Эффективное управление рисками требует сочетания юридической чёткости и гармонизации нормативных стандартов. Необходимо закрепить механизмы распределения ответственности между банками, финтех-компаниями и провайдерами сервисов, чтобы ускорить выявление нарушений и реагирование на инциденты в сфере противодействия отмыванию доходов и информационной безопасности. Одновременно важна унификация регуляторных подходов, как на национальном, так и на международном уровне, для снижения рисков регуляторного арбитража. В качестве примера может служить практика Европейского союза (PSD2), где действуют единые правила защиты данных и аутентификации, обеспечивающие согласованность требований ко всем участникам финансовой экосистемы.
3. Для повышения эффективности контроля рекомендуется внедрение интеллектуальных аналитических платформ, способных отслеживать и анализировать межсервисные транзакционные связи в режиме реального времени. Такие платформы используют алгоритмы искусственного интеллекта и машинного обучения, которые позволяют выявлять нетипичные схемы перемещения средств, включая переводы через несколько банков, агрегаторов и электронных кошельков. Также они способны определять аномалии в поведении клиентов на основе исторических данных и паттернов транзакций и моментально формировать предупреждения и отчёты для специалистов AML. Предсказывая потенциальные направления злоупотреблений, они позволяют проактивно корректировать правила мониторинга.
4. Для эффективного функционирования CBDC критически важно установить чёткие юридические рамки, регулирующие порядок обработки персонализированных транзакционных данных и ограничивающие возможности государства в использовании финансовой информации граждан. Одним из ключевых элементов такой политики является внедрение независимого надзора за деятельностью центрального банка и других уполномоченных органов. Независимые органы смогут оценивать корректность обработки данных, соблюдение процедур анонимизации и ограничение доступа к персонализированной информации, что повышает доверие граждан к системе.
5. Даже при высоком уровне национального контроля CBDC остаются доступными для трансграничных расчетов, что открывает потенциальные возможности для обхода традиционных финансовых механизмов и ограничений. Для минимизации этих рисков критически важно формирование глобальных стандартов функционирования CBDC. Такой подход предполагает комплексное сотрудничество между центральными банками, международными финансовыми организациями и региональными объединениями. Основные направления стандартизации включают:

согласование правил трансграничных расчетов (включая требования к идентификации сторон, AML/KYC-процедуры и контроль операций с высокой стоимостью), унификацию технических протоколов, разработку общих процедур мониторинга и обмена информацией, создание механизмов реагирования на инциденты и координации действий.

6. В контексте развития цифровых валют центральных банков целесообразно дополнить существующие рекомендации акцентом на создании международных механизмов сотрудничества в сфере противодействия отмыванию доходов. Даже при наличии различий в национальных подходах к обеспечению приватности, центральные банки могли бы обмениваться агрегированными метаданными и унифицированными индикаторами риска, которые не содержат персональных данных, но позволяют выявлять аномальные транзакции и подозрительные модели поведения. Под унифицированными индикаторами риска в международной практике понимаются стандартизированные критерии, которые позволяют идентифицировать потенциально подозрительные операции независимо от юрисдикции и специфики локального регулирования. В отличие от персональных данных, эти индикаторы строятся на анализе поведенческих характеристик транзакций: атипичных сумм и частоты переводов, нестандартных маршрутов движения средств, высокой степени фрагментации платежей, а также использования транзакционных цепочек через юрисдикции с низким уровнем прозрачности. Введение таких индикаторов на глобальном уровне позволило бы центральным банкам создавать систему раннего предупреждения о возможных случаях отмывания доходов при сохранении приватности пользователей. Например, если в цепочке платежей выявляется повторяющийся паттерн дробления суммы на десятки микропереводов, проходящих через несколько стран, это может быть отмечено в качестве «сигнала риска» и передано между регуляторами без раскрытия конкретных имён или счетов. Практическая значимость унифицированных индикаторов проявляется в том, что они дают возможность гармонизировать меры AML даже при различиях в национальных подходах к защите данных. Схожие механизмы уже реализуются в рамках рекомендаций ФАТФ (FATF), где указываются red flags для криптовалютных операций, применимые в разных странах и аналогичный подход мог бы быть институционализирован в сфере CBDC, что обеспечило бы баланс между эффективностью надзора и сохранением доверия пользователей к системе.
7. Недостаточная информированность граждан о механизмах защиты данных и возможных угрозах увеличивает вероятность вовлечения клиентов в мошеннические схемы и снижает эффективность систем противодействия отмыванию доходов. Для минимизации этих рисков рекомендуется разработка комплексных образовательных программ, направленных на повышение финансовой и цифровой грамотности пользователей.

Заключение

На основе проведённого анализа можно сделать вывод о необходимости комплексного подхода к внедрению данных технологий. В частности, стандартизация API и повышение киберустойчивости являются ключевыми мерами для минимизации угроз открытого банкинга. Одновременно интеллектуальный мониторинг транзакций и повышение цифровой грамотности пользователей создают дополнительные уровни защиты, позволяя не только выявлять подозрительные схемы, но и снижать вероятность вовлечения граждан в финансовые риски. В контексте CBDC критически важно обеспечить международную координацию, разработку унифицированных стандартов трансграничных расчетов и строгую политику защиты приватности, что позволит сочетать прозрачность и эффективность денежного обращения с сохранением доверия граждан. То есть только при соблюдении баланса между технологическим развитием и институциональными гарантиями безопасности инновации смогут безболезненно интегрироваться в финансовую

систему. В этом контексте открытый банкинг и CBDC становятся не только технологическими инновациями, но и механизмами укрепления принципов цивилизованного бизнеса, где конкуренция сочетается с прозрачностью, а эффективность — с соблюдением прав и интересов всех участников рынка.

Библиографический список

1. *Вахабова М. Х.*, *Мажигова Е. М.*, *Хутова Л. А.* Цифровая валюта и значение выпуска цифровой валюты центральным банком // Экономика и управление: проблемы, решения. — 2025. — Т. 10, 6(159). — С. 182—187. — DOI: 10.36871/ek.up.p.r.2025.06.10.019. — EDN LWNBYI.
2. *Городецкая О. Ю.*, *Гобарева Я. Л.* Цифровой рубль: история развития и его специфические особенности // Финансовые рынки и банки. — 2024. — № 1. — С. 42—47. — EDN LZCWYW.
3. Концепция внедрения открытых API на финансовом рынке / Банк России. — URL: https://cbr.ru/Content/Document/File/142114/concept_09-11-2022.pdf (дата обр. 03.10.2025).
4. Меж долларом и юанем: Аргентина и Бразилия переходят на единую валюту... снова / Российский совет по международным делам. — URL: http://duma.gov.ru/media/files/J6heDenfnD5oGqAvN8aGA9fIPsAsgHhX.pdf (дата обр. 03.10.2025).
5. *Морозко Н. И.* Политика Народного банка Китая в условиях введения цифрового юаня // Банковское дело. — 2024. — № 6. — С. 16—19. — EDN LVJHFY.
6. *Навой А. В.* Перспективы трансформации системы международных расчетов в Российской Федерации на базе цифровых валют центральных банков // Финансовый журнал. — 2024. — № 2. — С. 43—58. — DOI: 10.31107/2075-1990-2024-2-43-58. — EDN EQEKII.
7. *Сипратов Р. О.* Пути минимизации рисков в рамках применения открытых интерфейсов API в банковской системе России // Финансовая экономика. — 2022. — № 12. — С. 343—347. — EDN LTPMUA.
8. *Солуянов А. А.* Использование открытых API для проведения платежей и открытый банкинг // Риск: ресурсы, информация, снабжение, конкуренция. — 2025. — С. 255—266. — DOI: 10.56584/1560-8816-2025-1-255-266. — EDN IGFALE.
9. *Тхалиджоков А. С.* Исследование взаимного влияния цифровых валют центральных банков и цифровых финансовых активов // Вестник Академии знаний. — 2025. — 2(67). — С. 832—838. — EDN OWFCHZ.
10. Что такое ISO 20022 и его применение для стандартизации платежных сообщений / R-Style Softlab. — URL: https://www.softlab.ru/blog/iso-20022 (дата обр. 03.10.2025).
11. *Шаталова Е. П.* Цифровые валюты центральных банков: опыт внедрения // Финансовые рынки и банки. — 2024. — № 5. — С. 353—359. — EDN KHYPTE.