ФИНАНСЫ

Методы борьбы с отмыванием средств в транзакциях с цифровым рублем

Methods of Combating Money Laundering in Digital Ruble Transactions

DOI: 10.12737/2306-627X-2022-12-4-50-54 Получено: 14 августа 2023 г. / Одобрено: 22 августа 2023 г. / Опубликовано: 25 декабря 2023 г.

Аникиевич А.М.

Аспирант, кафедра мировых финансовых рынков и финтеха, ФГБОУ ВО «Российский экономический университет им. Г.В. Плеханова», г. Москва, e-mail: anikievich-sasha@yandex.ru

Anikievich A.M.

Postgraduate Student, Department of Global Financial Markets and Fintech, Plekhanov Russian University of Economics, Moscow, e-mail: anikievich-sasha@yandex.ru

Аннотация

В статье представлен комплексный анализ современных методов противодействия отмыванию денежных средств при проведении транзакций с цифровым рублем. Учитывая растущее внедрение цифровых технологий и усиление роли электронных платежей, становится очевидной необходимость адаптации механизмов финансового контроля. Статья освещает ключевые проблемные аспекты в сфере безопасности транзакций с цифровой валютой и демонстрирует актуальные методы их решения.

Ключевые слова: отмывание денежных средств, цифровой рубль, транзакции, цифровые технологии, электронные платежи, финансовый контроль.

Abstract

The article presents a comprehensive analysis of modern methods of combating money laundering in transactions with digital ruble. Given the growing adoption of digital technologies and the increasing role of electronic payments, the need to adapt financial control mechanisms becomes obvious. The article highlights key problematic aspects in the field of security of digital currency transactions and demonstrates actual methods of their solution.

Keywords: money laundering, digital ruble, transactions, digital technologies, electronic payments, financial control.

ВВЕДЕНИЕ

В последние годы мы стали свидетелями значительных перемен в мировой финансовой системе. Цифровые валюты разных стран набирают обороты, становясь потенциальным будущим мировой экономики. Одной из ключевых инициатив в этом направлении является попытка интеграции денежно-кредитной политики с современными финансовыми технологиями, зародившимися на стыке экономики и компьютерных наук. Многие центральные банки как ведущих мировых держав, так и развивающихся стран, рассматривают возможность переформатирования своих денежных систем с применением новых цифровых токенов.

Важной особенностью данных цифровых валют, известных как цифровые валюты центральных банков, является то, что они могут быть официально приняты на национальном уровне. Дело в том, что за их выпуск отвечает главное финансовое ведомство страны, что автоматически подразумевает поддержку их стоимости государственным фиатом и прямое стимулирование их использования через государственную политику.

Внедрение цифровых валют не происходит без препятствий. Одним из ключевых вопросов, требующих решения, является проблема отмывания денежных средств. Транзакции с цифровой валютой предоставляют уникальные возможности для нелегальных действий, поскольку они становятся быстрее, сложнее для отслеживания и менее прозрачными в сравнении с традиционными финансовыми операциями.

Целью данной статьи является анализ методов борьбы с отмыванием средств в транзакциях с цифровым рублем. Изучаются как преимущества, так и риски, связанные с использованием цифрового рубля, и предлагаются рекомендации по улучшению механизмов надзора и контроля для обеспечения безопасности и прозрачности транзакций с цифровыми валютами.

Задачи исследования:

1) определение концептуальных основ и функциональных характеристик цифрового рубля;
2) оценка действующих подходов к надзору и контролю над цифровыми операциями;
3) исследование стратегий и методик, применяемых для нелегитимных операций в сфере цифровых валют;
4) разработка рекомендаций по оптимизации и усилению мер борьбы с неправомерными финансовыми действиями при использовании цифрового рубля.

Научная новизна данного исследования заключается в комплексном анализе специфики цифрового рубля, методик отмывания средств при его использовании и разработке рекомендаций для усовершенствования механизмов регулирования и контроля над цифровыми транзакциями.

МЕТОДЫ ИССЛЕДОВАНИЯ

Статья базируется на Федеральном законе № 115-ФЗ «О противодействии легализации доходов, полученных преступным путем». А.А. Симаков и В.В. Неелов в своей работе описывают схемы преступлений с использованием криптовалюты, ключевым этапом которых является конвертация в рубли. В то же время В.И. Соловьев, В.К. Конторович, В.Г. Феклин приходят к выводу, что для предотвращения таких преступлений необходимо добиться раскрытия информации о покупателе в статье «О возможности осуществления контроля за оборотом цифровых финансовых активов». А.Б. Сергеев говорит о преимуществах и недостатках понижения порога контроля за финансовыми сделками: с одной стороны, должно повысится количество выявленных фактов отмывания денег, но, с другой стороны, возникают проблемы в квалификации действия как отмывания доходов, поскольку можно считать их как распорядительные действия для удовлетворения своих потребностей. Данная статья агрегирует указанные работы и рассматривает их исключительно с точки зрения транзакций с цифровым рублем.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

После внесения изменений в соответствии с Федеральным законом № 340 от 24.07.2023 в России появился новый дополнительный инструмент для поддержания денежной системы страны — цифровой рубль, выпускаемый Центральным банком. Предполагается его расширенное использование как среди населения, так и предприятий, что делает актуальным изучение его особенностей, преимуществ и потенциальных рисков, а также воздействия на финансовую инфраструктуру страны, в первую очередь на банковскую систему.

Цифровой рубль (ЦВЦБ, *CBDC*) — это валюта, не имеющая наличной формы и выпускаемая Банком России в форме цифрового кода, которая также входит в состав денежной базы наряду с наличными деньгами и резервами коммерческих банков [2, с. 2–3].

Цифровой рубль относится к так называемым розничным ЦВЦБ, т.е. цифровым валютам, предназначенным для массового использования населением и предприятиями, в отличие от оптовых ЦВЦБ, которые предназначены для проведения крупных платежей банками и другими финансовыми посредниками [8, с. 84]. Таким образом, цифровой рубль можно рассматривать как цифровую наличность, поскольку он сочетает в себе удобство электронных денег и надежность банкнот с точки зрения отсутствия риска дефолта их эмитента.

Любая крупная экономика, которая создаёт и вводит цифровую валюту, вероятно, столкнется с новыми рисками финансовых преступлений. По сравнению с физическими деньгами, цифровой рубль в определенных отношениях облегчит регулирующим органам борьбу с отмыванием денег, а его ключевые технические аспекты будут препятствовать некоторым традиционным незаконным финансовым методам [5, с. 104–106]. Но цифровой рубль, тем не менее, станет заманчивой мишенью для недобросовестных участников расчетов, как государственных, так и негосударственных, которые смогут соответствующим образом адаптировать свои методы. В частности, уникальные технические функции, которые цифровой рубль добавит к бумажным деньгам, такие как программируемость кошелька [10, с. 110] и микротранзакции (возможность совершать транзакции в объемах ниже копейки), позволят реализовать более изощренные схемы отмывания денег.

Перед специалистами по противодействию отмывания денег стоит задача точно настроить мониторинг операций с учетом возможностей цифрового рубля. Понимая новую эволюционную фазу денег, законодательные органы должны установить соответствующие стандарты соответствия [3, с. 8], чтобы обеспечить высокий уровень честности в индустрии финансовых технологий, которая, вероятно, будет развиваться вокруг приложений для цифрового рубля. Предвидя появление новых слоев финансовых преступлений, органы финансового регулирования в сотрудничестве с частным сектором должны применять ответные меры, учитывающие цифровые инновации, и смягчать неизбежные проявления противоправного поведения, которые будут связаны с платформами цифрового рубля.

Первый уровень управления цифровым рублем, на котором Центральный банк контролирует разработку цифровой валюты и распределяет ее между провайдерами платежных систем, скорее всего столкнется со значительными угрозами кибербезопасности. Политикам необходимо устранить критические уязвимости кибербезопасности в достаточной степени, прежде чем развертывать систему *CBDC*. Анализ рисков кибербезопасности цифрового рубля заслуживает отдельного рассмотрения, выходящего за рамки данной статьи.

В рамках нашего обсуждения мы будем исходить из того, что первый уровень *CBDC* достаточно защищен с точки зрения кибербезопасности. На втором уровне мы рассмотрим операции конечных пользователей друг с другом через программное обеспечение провайдеров платежных систем.

Уровень взаимодействия провайдера платежной системы с пользователем будет общедоступным и круглосуточно используемым в розничной торговле. Таким образом, он будет представлять собой широкую мишень для незаконного отмывания денег.

Для финансовых регуляторов факт участия цифрового рубля в незаконных операциях может иметь как положительный, так и отрицательный характер. Хорошая новость заключается в том, что цифровой рубль, скорее всего будет препятствовать прямому криминальному использованию. Субъекты незаконной деятельности в большинстве случаев предпочтут наличные деньги, поскольку они будут оставаться анонимными, в то время как цифровой рубль будет иметь документированную идентификацию, привязанную к каждому цифровому кошельку и, следовательно, к каждой транзакции.

Хотя правоохранительные органы не будут иметь прямого доступа к этой информации в режиме реального времени, эти данные представляют собой цифровой «след», который потенциально может быть получен правоохранительными органами [6, с. 2837]. Таким образом, преступники, использующие цифровой рубль, не смогут действовать в условиях полной анонимности, как в случае с наличными деньгами.

Мошенники должны будут либо взять на себя риск совершения операций под своим настоящим именем, либо создавать поддельные документы, красть чьи-то учетные данные либо уговаривать доверчивого человека разрешить им использовать цифровой кошелек.

Плохая новость заключается в том, что, поскольку цифровой рубль будет широко распространен среди торговцев и будет обладать некоторыми новыми техническими возможностями, такими как микроплатежи, преступники все равно захотят воспользоваться им. Поэтому финансовым органам следует ожидать, что они столкнутся с продуманными схемами отмывания денег. Риск финансовых преступлений в отношении цифрового рубля заключается не столько в том, что пользователи платят за незаконную деятельность, сколько в том, что преступники переводят незаконные доходы в систему [7, с. 243–245].

В частности, нелегальные субъекты скорее всего приспособятся к внедрению цифрового рубля, разработав более сложные схемы отмывания денег, предусматривающие обмен наличных денег и анонимных цифровых токенов на цифровой рубль.

Правоохранительные органы уже давно понимают «многослойность» как ключевой компонент процесса отмывания денег, независимо от технологии. За многослойностью операций следует интеграция, казалось бы, чистых средств обратно в официальную финансовую систему. Когда появились кредитные карты и онлайновые платежи, такие как PayPal, они привнесли новые виды незаконной деятельности, начиная от мошенничества и афер и заканчивая кражей личных данных и тщательным отмыванием денег. По всей видимости, цифровой рубль ожидает аналогичный путь.

Отмыванию денег с помощью цифровой валюты будут способствовать четыре фактора: денежные мулы, наличие соучастников, простота трансграничных операций и наличие криптовалютных бирж, не отвечающих требованиям законодательства [4, с. 86]. Преступные субъекты скорее всего будут использовать некоторые или все эти элементы для сокрытия незаконных денежных операций.

Нижеприведенная ситуация иллюстрируют, каким образом мошенники могут вливать доходы от финансовых преступлений в систему цифрового рубля и как финансовые органы могут противодействовать такой деятельности.

Ситуация: террористы финансируют цифровые услуги с помощью цифровых кошельков. В этом случае террористическая группа создает поддельную ИТ-компанию для прикрытия покупки услуг, необходимых для поддержки кибер- и медиаопераций и внутренних коммуникаций. Поскольку организаторы терроризма не могут легко приобрести кошельки с цифровым рублем в связи с тем, что провайдеры платежных систем знают своего клиента, они просят соучастников поделиться данными о кошельках. Реальные продавцы не проверяют личности людей, просто приобретающих их услуги. Таким образом, террористы приобретают ежемесячные ИТ- и медиауслуги на кошельки своих соучастников. Учитывая программируемость кошелька, террористы могут управлять платежами через несколько кошельков, переводя денежные потоки из одного кошелька в другой [9, с. 107–108].

Провайдеры платежных систем являются основной линией обороны против этих действий. Если соучастников нельзя явно уличить в связи с террористами, то они могут не вызвать подозрений в процессе проверки клиента при приобретении кошелька. Провайдеры должны проводить мониторинг транзакций, чтобы выявить возможные подозрительные действия — обращение к кошелькам в неожиданном географическом положении или другие необычные действия.

В современной методологии анализа цифровых транзакций выделяются разнообразные подходы, обусловленные спецификой и сложностью данной

области. При проведении исследований данных транзакций используются такие виды анализа, как корреляционный, кластерный, факторный и графовый.

Применяя корреляционный анализ, исследователи стремятся выявить взаимосвязи между различными параметрами транзакций. Осуществляя данный анализ, можно определить связи между разными транзакциями, что, в свою очередь, позволяет выделить потенциальных нарушителей или злоумышленников.

Применение кластерного анализа обусловлено необходимостью группировки транзакций на основе определенных критериев. Группируя транзакции по таким параметрам, как объем, время проведения и местоположение, можно выявить группы транзакций, вызывающие подозрения. Данный метод анализа способствует классификации транзакций, создавая удобные для изучения категории и выделяя аномальные или нестандартные паттерны поведения.

Факторный анализ направлен на выявление скрытых переменных, которые могут влиять на транзакции. Он позволяет определить ключевые факторы, оказывающие наибольшее воздействие на характер транзакций, исследуя их взаимное влияние и взаимодействие.

Графовый анализ применяется для визуализации и анализа структуры взаимодействий между различными элементами системы транзакций. Он позволяет изучать связи между отдельными узлами в сети, выявляя наиболее активные и значимые точки взаимодействия.

Осложняющим фактором может стать использование мошенниками нехостингового кошелька, который, хотя и имеет идентификатор, не отслеживается так тщательно, как хостинговый кошелек. Для снижения этой угрозы необходимо разработать специальные правила и архитектуру для нехостинговых кошельков.

Кроме того, сотрудники правоохранительных органов и спецслужб должны выявлять финансовые связи с такими мошенническими группировками путем выявления и расследования поставщиков, используемых группировкой.

ОБСУЖДЕНИЕ И ЗАКЛЮЧЕНИЕ

В связи с тем, что Центральный банк находится на ранней стадии изучения цифровой валюты, сейчас самое подходящее время для решения вопросов, связанных с рисками и последствиями внедрения цифровой валюты. В дополнение к важнейшему вопросу о технической безопасности цифрового рубля политикам необходимо изучить, на какой основе лучше всего разрабатывать и внедрять эту технологию. В значительной степени эти рамки должны учитывать неизбежные эффекты второго и третьего порядка влияния на финансовую преступность и отмывание денег, которые будет происходить с участием цифрового рубля.

Ниже приведены основные способы, с помощью которых политики и широкая общественность могут подготовиться к этим событиям.

Необходимо интегрировать риски в национальную систему противодействия легализации (отмыванию) доходов, полученных преступным путем. В настоящее время банки контролируют механизм противодействия отмыванию денег в отношении традиционной валюты с помощью их внутренних систем. Изначально Центральный банк предложил распространить эту ответственность на банки также в области цифрового рубля, включив данное предложение в специализированную концепцию. В настоящее время только Банк России способен осуществлять контроль за соблюдением Федерального закона № 115-ФЗ при работе с цифровым рублем [1]. Он создает и управляет всеми счетами, имея возможность просмотра всех транзакций на своей платформе.

Необходим более широкий общественный диалог по вопросам конфиденциальности финансовых данных и обеспечения конституционной защиты. Необходимо организовать деятельность рабочей группы, состоящей из представителей государственного и частного секторов, чтобы предложить систему обеспечения конфиденциальности данных. В состав этой группы должны войти представители банковской отрасли, специалисты по финансовым технологиям и ИТ-технологиям, юристы по вопросам конфиденциальности. Рабочая группа должна оценить жизнеспособность нехостинговых кошельков в системе цифрового рубля, рассмотреть вопрос о том, какую дополнительную ответственность, если таковая имеется, должны нести продавцы, если они принимают цифровой рубль в качестве платежного средства.

Необходимо установить более жесткие стандарты для платежных систем. Регулирующим органам следует рассмотреть возможность повышения требований к таким компаниям, претендующим на получение лицензии в качестве провайдеров платежных систем. Сектор виртуальных активов отстает в соблюдении требований законодательства. Регулируемые криптобиржи, желающие добавить цифровой рубль в свои цифровые активы, должны иметь лицензию.

Перспектива создания цифрового рубля Центрального банка открывает широкие возможности для финансовых инноваций, эффективности и инклю-

зивности. Когда цифровая валюта будет развернута в такой крупной экономике, как российская, это приведет к непредвиденным последствиям. Законодательные, правоохранительные органы и общество в целом должны как можно лучше предвидеть эти опасности. Дальнейшая цифровизация экономики приведет к появлению новой сферы коммерции. Вслед за ней возникнут и новые криминальные схемы. Но при достаточных усилиях этому можно противостоять.

Литература

1. Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 № 115-ФЗ (последняя редакция) [Электронный ресурс]. — URL: https://www.consultant.ru/document/cons_doc_LAW_32834 (дата обращения: 28.10.23).
2. *Kosse A., Mattei I.* (2023). Making headway-Results of the 2022 BIS survey on central bank digital currencies and crypto. URL: https://www.bis.org/publ/bppdf/bispap136.htm (accessed 27.10.23).
3. *Рябинин В.В*. Правовое регулирование цифровой валюты и цифровых финансовых активов [Текст] / В.В. Рябинин // Актуальные вопросы бухгалтерского учета и налогообложения. — 2021. — № 3. — С. 67–74.
4. *Сергеев А.Б*. Порог легализации денежных средств, приобретенных преступным путем, как критерий уголовной ответственности [Текст] / А.Б. Сергеев // Социум и власть. — 2012. — № 1. — С. 85–87.
5. *Ситник А.А*. Цифровые валюты: проблемы правового регулирования [Текст] / А.А. Ситник // Актуальные проблемы российского права. — 2020. — Т. 15. — № 11. — С. 103–113.
6. *Сергеев В.М*. Цифровой рубль как средство противодействия теневой экономике в Российской Федерации [Текст] / В.М. Сергеев, М.М. Шадурская, О.А. Бойтуш // Креативная экономика. — 2021. — № 15. — С. 2827–2843.
7. *Соловьев В.И*. О возможности осуществления контроля за оборотом цифровых финансовых активов [Текст] / В.И. Соловьев, В.К. Конторович, В.Г. Феклин // Проблемы экономики и юридической практики. — 2022. — Т. 18. — № 5. — С. 242–247.
8. *Сорока Э.Ю*. Правовая природа цифровых финансовых активов в законодательстве Российской Федерации [Текст] / Э.Ю. Сорока // Вопросы российского и международного права. — 2021. — Т. 11. — № 9-1. — С. 84.
9. *Симаков А.А*. Схемы преступлений с использованием криптовалюты [Текст] / А.А. Симаков, В.В. Неелов // Закон и право. — 2020. — № 5. — С. 106–109.
10. *Татоян А.А*. Экономико-правовая природа цифровых финансовых активов [Текст] / А.А. Татоян // Образование и право. — 2022. — № 1. — С. 107–111.

References

1. Federal Law «On Combating Legalization (Laundering) of Proceeds of Crime and Financing of Terrorism» of 07.08.2001 no. 115-FZ (latest edition). URL: https://www.consultant.ru/document/cons_doc_LAW_32834 (accessed 28.10.23). (in Russian)
2. Kosse A., Mattei I. (2023). Making headway-Results of the 2022 BIS survey on central bank digital currencies and crypto. URL: https://www.bis.org/publ/bppdf/bispap136.htm (accessed 27 of October 2023).
3. Ryabinin V.V. Legal regulation of digital currency and digital financial assets. Aktual'nye voprosy buhgalterskogo ucheta i nalogooblozheniya [Actual issues of accounting and taxation], 2021, no. 3, pp. 67–74. (in Russian)
4. Sergeev A.B. The threshold of legalization of criminally acquired funds as a criterion of criminal liability. Socium i vlast' [Society and power], 2012, no. 1, pp. 85–87. (in Russian)
5. Sitnik A.A. Digital currencies: Problems of legal regulation. Aktual'nye problemy rossijskogo prava [Actual problems of Russian law], 2020, no. 15(11), pp. 103–113. (in Russian)
6. Sergeev V.M., Shadurskaya M.M., Boitush O.A. The digital ruble as a means of countering the shadow economy in the Russian Federation // Kreativnaya ekonomika [Journal of Creative Economy], 2021, no. 15, pp. 2827–2843. (in Russian)
7. Soloviev V.I., Kontorovich V.K., Feklin V.G. On the possibility of controlling the circulation of digital financial assets // Problemy ekonomiki i yuridicheskoj praktiki [Problems of Economics and Legal Practice], 2022, v. 18, no. 5, pp. 242–247. (in Russian)
8. Soroka E.YU. Legal nature of digital financial assets in the legislation of the Russian Federation // Voprosy rossijskogo i mezhdunarodnogo prava [Issues of Russian and international law], 2021, v. 11, no. 9-1, p. 84. (in Russian)
9. Simakov A.A., Neelov V.V. Cryptocurrency crime schemes // Zakon i parvo [Law and rights], 2020, no. 5, pp. 106–109. (in Russian)
10. Tatoyan A.A. The economic and legal nature of digital financial assets // Obrazovanie i parvo [Education and rights], 2022, no. 1, pp. 107–111. (in Russian)