УДК 336.7, 338.2

РИСКИ ВНЕДРЕНИЯ ЦИФРОВОГО БЕЛОРУССКОГО РУБЛЯ В ФИНАНСОВОМ СЕКТОРЕ

Малыхина Светлана Игоревна, к.э.н., доцент
Академия управления при Президенте Республики Беларусь
Malykhina Svetlana, PhD in Economics,
Academy of Public Administration under the President of the Republic of Belarus,
s.malykhina@mail.ru

Аннотация. В статье рассмотрены понятие цифровой валюты центрального банка, перспективы внедрения цифрового белорусского рубля, проанализированы ключевые риски, связанные с процессом его внедрения в финансовом секторе, и предложены инструменты их ограничения.

Ключевые слова: цифровой белорусский рубль, финансовый сектор, банк, блокчейн, риски, киберриск, финансовый риск, риск персонала.

Развитие финансовой экономики страны на современном этапе обусловлено важностью обеспечения свободы внутреннего и трансграничного движения капитала как основного фактора производства, что стимулирует создание новых финансовых решений. Необходимость нововведений продиктована современными вызовами, с которыми столкнулись Республика Беларусь и другие страны в результате пандемии Covid-19 и беспрецедентного санкционного давления со стороны коллективного запада, среди них –нарушение функционирования платежных систем, усложнение движения денежных потоков. Чтобы обеспечить безопасное и устойчивое развитие финансового сектора, страны должны находить новые решения.

Одним из таких решений является введение цифровых национальных валют (англ. Central Bank Digital Currencies, CBDC). В общем смысле под такой валютой понимается национальная валюта страны, которая эмитируется центральным банком и существует в безналичной форме [1]. Центральный банк является не только эмитентом цифровой валюты, но и ее регулятором, что открывает широкие возможности для оптимизации затрат на реализацию денежно-кредитной политики страны. Цифровая валюта центрального банка (ЦВЦБ) учитывается на счетах пользователей с помощью записей в распределенном реестре (блокчейне), используя его преимущества.

С распространением цифровизации экономики цифровая валюта рассматривается как средство для осуществления внутренних и трансграничных расчетов с другими странами, в которых процесс ее внедрения находятся на разных стадиях. В Республике Беларусь 31 января 2024 г. Правлением Национального банка одобрена Концепция цифрового белорусского рубля (ЦБР), которая отражает видение регулятором перспектив разработки и внедрения такой валюты в разрезе различных аспектов. В частности, обращено внимание на преимущества введения ЦБР для населения и субъектов хозяйствования, государства, а также финансовой системы. Регулятором ожидается снижение затрат на создание и обеспечение функционирования платежной инфраструктуры, расходов на комиссионные платежи, снижение потребности во внутридневной ликвидности клиентов и потребности в иностранной валюте для трансграничных расчетов, а также создание инновационных финансовых сервисов для клиентов с помощью смарт-контрактов и повышение эффективности финансового рынка.

В то же время в Концепции отмечены *пять основных групп рисков реализации проекта внедрения ЦБР* – технологические (недостаточность производительности блокчейн-платформы, конфиденциальность информации блокчейна, реализация офлайн-режима, возможность подрыва криптозпщиты), риск ликвидности (резкий отток), риск использования комплексов платформы ЦБР (программно-аппаратного и программного), неготовность инфраструктуры (у финансовых и торгово-сервисных организаций) и риски, связанные с легализацией доходов, полученных преступным путем, финансированием террористической деятельности и финансированием распространения оружия массового поражения (ОД/ФТ). В документе предусмотрены инструменты для минимизации (снижения влияния) этих рисков [2]. Анализ документов центральных банков стран-членов ЕАЭС в этой сфере выявил схожие риски, связанные с ЦВЦБ.

Очевидно, что внедрение ЦБР послужит активатором роста одного из *ключевых рисков цифровизации – киберриска*, реализация которого может привести к понесению потерь из-за незаконного доступа лиц к объектам инфраструктуры банка с использованием информационных технологий для нарушения информационной и компьютерной безопасности банка. Важность учета этого риска подтверждает рост киберпреступности во всем мире.

Количество киберугроз и ущерб от хакерских атак стремительно растут с каждым годом. Так, в 2020 г. потери мировой экономики от нарастающей «киберпандемии» составили более USD 1 трлн., или около 1% глобального ВВП., а в 2022 г. по экспертным оценкам – USD 8 трлн. Согласно рейтингу Всемирного экономического форума (ВЭФ), преступная деятельность в киберпространстве входит в пятерку глобальных рисков и угрожает существованию и успешному функционированию целых отраслей [3, 4]. Эти тенденции характерны и для стран СНГ, включая Республику Беларусь.

Исследование «Актуальные киберугрозы в странах СНГ 2023-2024», проведенное известным разработчиком ИТ-продуктов в области кибербезопасности Positive Technologies, показало, что в I квартале 2024 г. количество кибератак на страны СНГ было в 2,6 раза больше по сравнению с аналогичным периодом в 2023 г. Больше всего атак направлено на Россию (73%), Беларусь – на третьем месте (7%). Наибольшему числу атак в странах СНГ подверглись госучреждения (18%), промышленность (11%) и телекоммуникации (10%). В Беларуси профиль топ-3 категорий жертв кибератак несколько иной: на госучреждения направлена каждая пятая кибератака (22%), на промышленность - 14%, на финансовые организации – 11%. Каждая вторая атака (57%) заканчивалась утечкой конфиденциальных данных, в 16% случаев была нарушена основная деятельность, 8% атак привели к прямым финансовым потерям [5].

Результаты проведенного тем же Positive Technologies исследование «Киберугрозы финансовой отрасли 2023—2024» подтвердило, что интерес киберпреступников к клиентам финансовых организаций в последние несколько лет стабильно растет. По данным Банка России, количество мошеннических операций, остановленных банками, во II квартале 2024 г. превысило 16 млн., или половина от количества попыток мошенников украсть деньги за предыдущий год. При этом украдено со счетов физических и юридических лиц около 4,8 млрд рублей, что примерно на четверть выше среднего показателя за предшествующие четыре квартала [6]

На фоне сложной геополитической обстановки российские и белорусские банки, фондовые биржи и операторы платежных систем, которые выполняют важные функции для стабильного функционирования экономики государств и проведения финансовых операций на внутреннем и международном рынке, подвергаются мощным DDoS-атакам, направленным на временное нарушение работы цифровых сервисов. При подобных атаках на блокчейн центрального банка под угрозой может оказаться вся финансовая система страны.

Исходя из необходимости повышения уровня защиты информационной инфраструктуры от внешних и внутренних рисков и угроз, в Республике Беларусь создана и функционирует национальная система обеспечения кибербезопасности страны, в рамках которой за два года уже аттестовано 17 центров кибербезопасности, в т.ч. два крупнейших белорусских банка – ОАО «АСБ Беларусбанк» и ОАО «Белагропромбанк» [7]. Такой системный подход служит действенным инструментом ограничения киберриска и смягчения его последствий.

Важным условием успешного внедрения ЦБР является наличие достаточных ресурсов Национального банка и банков, поскольку значительные затраты могут привести к росту *риска нехватки финансирования.* Так, по оценкам участников платежного рынка России, минимальные затраты на подключение банка к платформе цифрового рубля составят 120–200 млн. руб., что кратно превышает годовой ИТ-бюджет. К операциям с цифровым рублем придется адаптировать практически всю инфраструктуру и системы банка – дистанционное банковское обслуживание (ДБО) для физических и юридических лиц, автоматизированную банковскую систему (АБС), системы комплаенс-контроля и иные, а также обеспечить их кибербезопасность, для чего понадобятся новые, более мощные серверы и программное обеспечение. Ожидается, что финансовые риски будут выше в небольших банках, поскольку их вложения в инфраструктуру для цифрового рубля и обеспечение его функционирования могут быть произведены без отдачи ввиду отсутствия клиентов, использующих эту валюту. Одним из средств ограничения этого риска может стать разработка коробочных решений [8].

Помимо риска нехватки финансовых ресурсов следует обратить внимание на связанный с ним риск дефицита человеческих ресурсов как один из видов *риска персонала.* Основной источник этого риска в белорусских банках – дополнительная потребность в достаточном количестве дорогостоящих высококвалифицированных кадров с необходимым опытом работы, в том числе в сфере технологии блокчейн и смарт-контрактов, на этапах как внедрения ЦБР, так и дальнейшего сопровождения связанной с ним операционной деятельности. Таким образом, ожидается рост затрат банков на поиск и привлечение необходимого персонала. Риск может быть снижен путем организации превентивных мер, среди которых – направление на повышение квалификации действующих ИТ-специалистов, привлечение на практику перспективных студентов профильных вузов с последующим распределением их в банк, создание для персонала условий деятельности, привлекательных не только с финансовой, но и с социальной точки зрения.

В Концепции цифрового белорусского рубля не нашел отражения еще один вид операционного риска – *регуляторный,* источником которого служат изменения в законодательстве, а также связанный с ним *комплаенс-риск,* возникающий в случае несоблюдения норм и требований, установленных законодательством или регулятором. Реализация этих рисков при внедрении цифровой валюты банками также может привести к дополнительным затратам (потерям). В Республике Бела-

русь дорожная карта ЦБР предусматривает его поэтапное внедрение в течение 2024-2026 г.г., включая внесение изменений в законодательство, с оговоркой, что форма и сроки выполнения конкретных работ могут быть изменены [2]. Как правило, для подобных инновационных проектов странового масштаба устанавливаются сроки исполнения и меры за их нарушение. Банк России, которая находится на втором этапе пилотного проекта по внедрению цифрового рубля, уже планирует применять экономические санкции к банкам за несоблюдение сроков подключения к платформе цифрового рубля, что станет возможным после установления этих сроков и иных норм на законодательном уровне [8]. Независимо от того, какие меры будут предусмотрены для белорусских банков в случае нарушения законодательных норм, для предупреждения возникновения этих рисков банкам необходимо включать мероприятия по реализации дорожной карты ЦБР и предусматривать для этого необходимые ресурсы в стратегических планах развития и ежегодных бизнес-планах.

Особые вызовы могут возникнуть при внедрении цифрового рубля в деятельность сложных организационных структур – банковских холдингов, которые включают как финансовых (например, лизинговые и страховые компании), так и нефинансовых участников (например, ИТ-компании). Очевидно, что наиболее эффективным способом реагирования на такие вызовы является включение выявленных и рассмотренных выше рисков внедрения цифрового рубля в общую систему управления рисками и капиталом банковского холдинга, их оценку на консолидированной основе, разработку необходимых мероприятий и контроль со стороны органов управления за ходом их реализации.

Представляется, что ключевая роль в успешном внедрении цифрового белорусского рубля принадлежит наблюдательному совету банка, который принимает решения по вопросам разработки стратегии развития и иных стратегий, контролирует их реализацию и обеспечивает организацию системы управления рисками в рамках корпоративного управления как в банке, так и в банковском холдинге, если банк является его головной организацией. Такой подход будет способствовать внедрению инноваций в финансовом секторе и экономике страны в целом, направленных на повышение качества платежных и расчетных услуг, соответствующих современным запросам населения, субъектов хозяйствования и государства.

Список использованных источников

1. Турбанов А. В. Цифровой рубль как новая форма денег //Актуальные проблемы российского права. – 2022. – Т. 17. – №. 5. – С. 73-90.

2. Концепция цифрового белорусского рубля // Национальный банк Республики Беларусь. URL: https://www.nbrb.by/payment/digital_ruble/ concept.pdf (дата обращения: 17.10.2024)

3. Потери от киберпреступности достигли $1 триллиона в мировом масштабе // Anti-Malware. URL: https://www.anti-malware.ru/news/2020-12-07-1447/34432 (дата обращения: 17.10.2024).

4. Лавров: потери мировой экономики от кибератак могут составить $8 трлн в 2022 году // ТАСС. URL: https://tass.ru/ekonomika/9567725 (дата обращения: 17.10.2024).

5. Актуальные киберугрозы в странах СНГ 2023—2024 // Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-v-stranah-sng-2023-2024/#id6 (дата обращения: 17.10.2024).

6. Киберугрозы финансовой отрасли 2023—2024 // Positive Technologies. URL: https:// https://www.ptsecurity.com/ru-ru/research/analytics/financial-industry-security-h2-2023-h1-2024/#id17 (дата обращения: 17.10.2024).

7. О кибербезопасности;: Указ Президента Респ. Беларусь от 14 фев. 2023г. № 40 // ЭТАЛОН : информ.-поисковая система (дата обращения: 15.10.2024).

8. Цифровой рубль влетит в копеечку // Коммерсантъ. URL: https:// https://www.kommersant.ru/doc/7249032 (дата обращения: 23.10.2024).