● при доступе к платформе цифрового рубля осуществляется "строгая" двухсторонняя аутентификация прямых участников с использованием ключей, сертифицированных УЦ БР, по защищенным каналам взаимодействия, реализованным с применением сертифицированных ФСБ России СКЗИ.

В части обеспечения защиты данных на платформе цифрового рубля:

● применение СКЗИ, сертифицированных ФСБ России, для обеспечения целостности и достоверности данных на платформе Банка России при подписании транзакций с цифровым рублем;

● создание цифровых рублей исключительно с применением эмиссионного ключа Банка России. Эмиссионный ключ Банка России регистрируется в специально выделенном УЦ БР для эмиссии;

● применение комплекса технологических мер защиты информации: логический контроль, структурный контроль, контроль дублирования, контроль авторства и т.д.;

● на участках, где невозможно применение сертифицированных СКЗИ, предусмотрено применение специальных технологических мер, обеспечивающих целостность данных для операций с цифровым рублем;

● организация контроля целостности смарт-контрактов и прав доступа к возможности их запуска.

При развитии платформы цифрового рубля особое внимание в части информационной безопасности будет уделено обеспечению операционной надежности и киберустойчивости на всех стадиях жизненного цикла цифрового рубля.

В схеме на рис. 1 отражены процессы взаимодействия участников в соответствии с вышеизложенными подходами к обеспечению информационной безопасности.

Но, как писал "Коммерсант"[2], серьезным препятствием для финансовых организаций становится отсутствие четких требований к уровню защиты информации в отношении цифрового рубля. Сейчас инфраструктура, поддерживающая обслуживание ЦВЦБ, строится по классу КС2 СКЗИ, но вполне вероятно, что уровень будет повышен до КС3 или КВ и КА, и тогда затраты банков могут стать несоразмерно большими.

В технологическом аспекте эксперты видят риск недостаточной производительности технологии распределенных реестров, осложняющийся дефицитом микроэлектронных компонентов, а также риск сложности реализации решения по обеспечению конфиденциальности в распределенных реестрах.

Стоит отметить, что на платформе цифрового рубля будет обеспечена конфиденциальность информации об операциях клиентов и защита их персональных данных, но при этом расчеты в цифровом рубле не предполагают анонимности платежей. Со стороны финансовых организаций, обеспечивающих проведение клиентских операций в цифровом рубле, будут выполняться процедуры, предусмотренные законодательством в сфере ПОД/ФТ/ФРОМУ. В этом смысле степень конфиденциальности операций на платформе цифрового рубля будет обеспечена на уровне не ниже, чем при существующем механизме безналичных платежей.

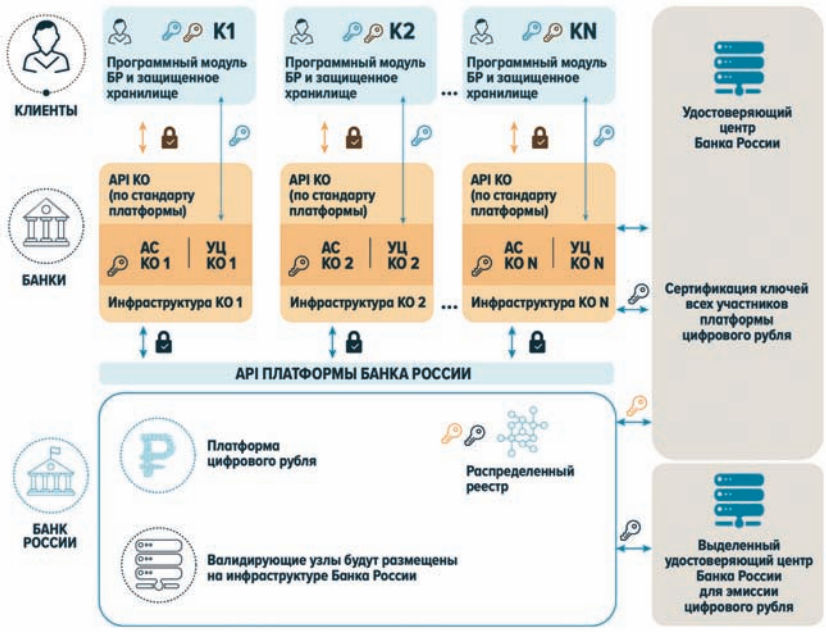

Рис. 1. Подходы к информационной безопасности и конфиденциальности. Источник: Банк России

Если все планы реализуются, то с 1 апреля 2023 г. цифровой рубль должен появиться в экономическом пространстве[3].

Опыт пилотирования ЦВЦБ в Казахстане

В Казахстане недавно завершился[4] пилотный проект введения своей ЦВЦБ – цифрового тенге. В целом финансовой инфраструктуре удалось поддержать вполне комфортный для пользователей уровень производительности при совершении транзакций, хотя и частично за счет организационных мер и ограничений.

Оптимизация производительности не являлась главным фокусом пилотного проекта, но в рамках нагрузочного тестирования разработанной платформы проводились замеры пропускной способности и времени ответа. Результаты пилотного проекта показали, что производительность платформы на уровне показателей платежных систем является одним из ключевых вызовов на будущее. На следующем этапе платформа ЦВЦБ Казахстана потребует глубокой проработки вопросов производительности: повышения пропускной способности, сокращения длительности обработки транзакции, решения вопроса увеличения длительности обработки транзакции при увеличении истории и т.п.

В силу незрелости технологии и отсутствия значительного количества промышленных внедрений существует риск того, что платформа не позволит обеспечить производительность, сопоставимую с существующими решениями национального уровня, например с карточными системами. На текущий момент технологические платформы демонстрируют допустимые результаты по производительности, сопоставимые с существующими системами (например, системами быстрых платежей), но их приемлемость для продуктивного решения пока не тестировалась в условиях, приближенных к реальным.

В части информационной безопасности в отчете по пилотному проекту внедрения ЦВЦБ отмечено, что пока отсутствует полное понимание относительно наиболее безопасной реализации систем защиты на уровне платформы цифровой валюты. В качестве возможных мер предлагаются алгоритмическая криптозащита, безопасность на основе аппаратного или программного обеспечения и их комбинация. Каждый вариант несет определенные риски с точки зрения достигаемого уровня защиты, сложности реализации и поддержки ввиду "гонки вооружений" между атаками и защитой. Безопасность на уровне пользователя эксперты отнесли к "последней миле" – мобильным приложениям, смарт-картам и прочим пользовательским устройствам и технологиям. ●

[2] *https://www.kommersant.ru/doc/5736579*
[3] *https://www.interfax.ru/business/878411*
[4] *https://digital-tenge.payfintech.kz/digital-tenge*

Ваше мнение и вопросы присылайте по адресу is@groteck.ru