

На уровне безопасности

Защита инфраструктуры цифрового рубля в банках

Текст

РИММА БАДМАЕВА,
ВЕДУЩИЙ МЕНЕДЖЕР ПРОДУКТОВ «ИНФОТЕКС»

Проект по цифровому рублю сейчас находится на стадии «пилота». В нем принимает участие ограниченный круг банков и граждан. Проект курирует Банк России, который получает от участников «пилота» вопросы о необходимых доработках и запросы о сдвиге сроков широкого внедрения цифрового рубля. Учитывая это, Банк России принял решение несколько позже перейти к массовому внедрению цифрового рубля. Однако уже сейчас ведутся работы по подготовке его внедрения и отрабатываются все детали. Когда проект станет массовым, крупнейшие банки должны будут обеспечить своим клиентам возможность проводить операции с цифровым рублем: открывать и пополнять счета цифрового рубля, делать переводы, компании должны будут принимать оплату в цифровых рублях

При выполнении операций с цифровым рублем особое внимание будет уделяться вопросам информационной безопасности. Требования к обеспечению защиты информации для участников платформы цифрового рубля были зафиксированы в Положении № 833-П «О требованиях к обеспечению защиты информации для участни-



фото: InfoText

ков платформы цифрового рубля», вступившем в силу 1 января 2024 года. Документ в том числе определяет порядок применения и классы средств криптографической защиты информации (СКЗИ), которые используются как на стороне участников, так и на стороне пользователей платформы.

Для граждан операции с цифровым рублем будут доступны в мобильном приложении банков — участников платформы цифрового рубля. Именно в мобильном приложении пользователи смогут проводить операции с цифровым рублем через собственные цифровые кошельки. Для реализации криптографической защиты в приложение будет

встроен программный модуль Банка России (ПМ БР), в ядре которого сертифицированные СКЗИ класса КС1. По сути, программный модуль — это надстройка в виде API для работы СКЗИ с мобильным приложением банка. Здесь применяется только отечественная криптография, соответствующая принятым стандартам безопасности Банка России.

Участие компании «ИнфоТеКс» в проекте цифрового рубля началось несколько лет назад с разработки по заданию Банка России версии ПМ БР с сертифицированным СКЗИ ViPNet OSSSL. На первом этапе разработали сам модуль и реализовали функцию шифрования и формирования электронной подписи (ЭП). В рамках второго этапа добавили функцию защиты канала передачи данных путем организации TLS-соединений с использованием алгоритмов ГОСТ. За время участия в проекте были разработаны несколько версий ПМ БР. Финальную версию для встраивания компания «ИнфоТеКс» передала в конце 2024 года.

На стороне коммерческих банков, участников платформы цифрового рубля, в соответствии с 833-П также применяются СКЗИ: для организации TLS-соединений должны использоваться средства класса КС2, для шифрования — средства класса КС3, для формирования и проверки ЭП — средства ЭП класса КС3. Обращаем внимание, что в цифровом рубле используется УНЭП — усиленная неквалифицированная электронная подпись. Компания «ИнфоТеКс» разработала комплексное решение для защиты инфраструктуры цифрового рубля финансовых посредников. Для организации TLS-соединений мы предлагаем шлюз безопасности ViPNet TLS Gateway. Для формирования и проверки ЭП разработан шлюз ViPNet PKI Service на базе сертифицированной платформы ViPNet HSM.

Помимо этого для защиты трафика в инфраструктуре банка могут применяться шлюзы безопасности ViPNet Coordinator HW, для разделения или выделения сегментов цифрового рубля внутри инфраструктуры банка — межсетевой экран следующего поколения (NGFW) ViPNet xFirewall 5.

Для того чтобы обеспечить участников информационного взаимодействия необходимым количеством сертификатов, на стороне банков также должны быть организованы два удостоверяющих центра (УЦ) — в целях выпуска сертификатов для подписи и в целях выпуска сертификатов безопасности. УЦ при этом должны быть сертифицированы по классу КС3. В настоящее время обсуждается возможность снижения затрат банков на внедрение цифрового рубля в части реализации единого подчиненного удостоверяющего центра: на стороне Банка России или

Все продукты решения ViPNet для защиты инфраструктуры цифрового рубля интегрированы в систему ДБО «iBank» компании «БИФИТ». Благодаря нашему партнерству коммерческие банки получают готовое комплексное решение для участников платформы цифрового рубля

на стороне единого оператора. Предложение Ассоциации банков России поддержал Банк России, поэтому, возможно, будут изменения в части организации УЦ. Для реализации функций УЦ может использоваться ViPNet Удостоверяющий центр 4, который может работать совместно с ViPNet HSM для хранения ключей ЭП УЦ.

Для автоматизации выпуска сертификатов из мобильного приложения банка с аутентификацией через ЕСИА разработан сервис автоматизации выпуска сертификатов ViPNet CABCS — комплекс технических и программных средств, предназначенный для выпуска сертификатов пользователей платформы цифрового рубля. ViPNet CABCS обеспечивает автоматизированный процесс выпуска сертификатов безопасности и сертификатов ЭП. В его состав входит криптошлюз ViPNet EDI Soap Gate. Программно-аппаратный комплекс ViPNet EDI Soap Gate предназначен для осуществления обмена электронными сведениями по каналам СМЭВ и взаимодействия с ЕСИА с применением ЭП, сертифицирован по классу КС3, что соответствует действующим требованиям Банка России. ViPNet CABCS также включает в себя ViPNet EDI Flow — программный комплекс, который обеспечивает взаимодействие с ViPNet EDI Soap Gate и удостоверяющими центрами. ViPNet EDI Flow является управляющим компонентом ViPNet CABCS и обеспечивает выполнение всех процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователей платформы цифрового рубля.

Все продукты решения ViPNet для защиты инфраструктуры цифрового рубля интегрированы в систему ДБО «iBank» компании «БИФИТ». Благодаря нашему партнерству коммерческие банки получают готовое комплексное решение для участников платформы цифрового рубля.

Также хочется напомнить, что при встраивании СКЗИ финансовые организации обязаны пройти оценку влияния. Соответствующие работы может проводить аккредитованная испытательная лаборатория, имеющая право и опыт проведения тематических исследований (сертификационных испытаний) программных и программно-аппаратных средств на соответствие требованиям ФСБ России.