Как будет защищен цифровой рубль?

Пользователями платформы цифрового рубля (ПлЦР), которая разрабатывается для доступа к новой форме национальной валюты, будут физические и юридические лица, участниками — финансовые посредники (коммерческие банки), оператором платформ — Банк России. О защите информационного взаимодействия участников ПлЦР рассказала Римма Бадмаева, ведущий менеджер продуктов ИнфоТеКС


Фото: ИнфоТеКС

— Римма, как обычный пользователь будет взаимодействовать с ПлЦР?
— В мобильном приложении банка появится интерфейс для совершения операций с цифровым рублем. Криптографическую защиту передаваемых данных в мобильном приложении будет обеспечивать программный модуль Банка России, в ядре которого — сертифицированные средства криптографической защиты информации (СКЗИ) класса КС1. По сути, программный модуль — это надстройка в виде API для работы СКЗИ с мобильным приложением банка.

— Какие основные функции предлагает программный модуль Банка России?
— Благодаря программному модулю Банка России операции с цифровым рублем будут защищаться с применением функций электронной подписи (ЭП) и шифрования, а взаимодействие с инфраструктурой банка — по защищенному каналу путем организации TLS-соединений с использованием российской криптографии. Несколько лет назад компания «ИнфоТеКС» по заданию Банка России разработала версию программного модуля с сертифицированным СКЗИ ViPNet OSSL. На первом этапе был создан сам модуль и реализована функция шифрования и формирования ЭП. В рамках второго этапа мы добавили функцию организации TLS-соединений с использованием алгоритмов ГОСТ. Именно эта реализация сейчас является основной и применяется банками.

— Как будет организована защита информации на стороне банков?
— Программный модуль Банка России организует TLS-соединения, формирует подпись, шифрует. Естественно, что на стороне банка должна быть ответная часть, также использующая СКЗИ для проверки ЭП, шифрования и расшифрования данных. По требованиям Банка России на стороне финансовых посредников для организации TLS-соединений должны использоваться СКЗИ класса КС2, для шифрования — СКЗИ класса КС3, для формирования и проверки ЭП — средства ЭП класса КС3. В ПлЦР используется УНЭП — усиленная неквалифицированная электронная подпись. Для того чтобы обеспечить участников информационного взаимодействия необходимым количеством сертификатов, на стороне банков также должны быть организованы два удостоверяющих центра (УЦ) — для выпуска сертификатов для подписи и для выпуска сертификатов безопасности. УЦ при этом должны быть сертифицированы по классу КС3.

Компания «ИнфоТеКС» разработала комплексное решение для защиты инфраструктуры цифрового рубля. Для организации TLS-соединений мы предлагаем шлюз безопасности ViPNet TLS Gateway. Для формирования и проверки ЭП — ViPNet PKI Service, который разработан на базе сертифицированной платформы ViPNet HSM. Для построения инфраструктуры открытых ключей и реализации функций УЦ используется ViPNet Удостоверяющий центр 4, который может работать совместно с ViPNet HSM. Для автоматизации выпуска сертификатов из мобильного приложения используется сервис автоматизации выпуска сертификатов, в состав которого входит шлюз электронного документооборота ViPNet EDI Soap Gate. Б.О