

Цифровому рублю нужна доверенная инфраструктура

Никто не станет, спорить с тем, что одной из самых острых тем 2023 года в области цифровизации банковского сектора является запуск платформы цифрового рубля. А внутри этой повестки выделяется трек обеспечения ИБ

IT-ландшафт платформы цифрового рубля (ЦР) обусловлен двухуровневой (розничной) его моделью при которой Банк России выступает в качестве верхнеуровневого оператора платформы и эмитента ЦР. Он же управляет счетами клиентов.

На втором уровне находятся финансовые посредники, которые предоставляют доступ к цифровым кошелькам, поскольку клиенты не имеют возможности доступа напрямую в ЦБ. Посредники наделены функцией конвертации рублей и предоставления своим клиентам инструмента для доступа к платформе ЦР. Кроме того, они должны выполнять процедуры, предусмотренные законодательством в сфере ПОД/ФТ и т.д.

Сейчас на этапе начального этапа «пилота» насчитывается 13 участников — финансовых организаций. В тестировании участвуют около 600 физлиц и 30 юрлиц в 11 городах России. Уже совершено примерно 10 тыс. операций. В первом квартале 2024 года рамки «пилота» будут расширены. К нему подключатся еще 15 банков, а количество физлиц достигнет нескольких тысяч.

Вести с полей

Рамочное регулирование инфраструктуры ЦР описано Банком России в Положении N820-П «О платформе цифрового рубля» от 3 августа 2023 года. В частности, предусматривается появление уровня смарт-контрактов, которые позволят осуществлять «расчеты с условиями». Кроме того, должна появиться возможность работы с ЦР без доступа к интернету и появление иных инновационных сервисов. На этапе «пилота» ЦР пока выполнят исключительно расчетную функцию.

С целью систематизации требований к ИБ Банком России в июле 2023 года опубликован проект Положения «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля». Требования к защите распространяются на автоматизированные системы, ПО, средства вычислительной техники, а также на телекоммуникационное оборудование. Эксплуатация перечисленного обеспечивается участником платформы цифрового рубля с целью формирования, подготовки, обработки, передачи и хранения защищаемой информации.

Согласно проекту Положения, банкам надлежит использовать электронную подпись, подтверждающие документы на которую выданы удостоверяющим центром ЦР Банка России (УЦ). Кроме того, в документе описаны требования к мобильному и интернет-банку клиента, с помощью которых будут совершаться операции с цифровыми рублями.

Участники пилотного проекта информируют о том, что проект с ЦР является одним из самых сложных в силу высоких затрат как на разработку импортозамещенных прикладных решений, так и инвестиций в сопутствующую ИБ-инфраструктуру, к которой предъявляются жесткие требования. Практической информации от участников пилота крайне мало, поэтому любая информация «с полей» крайне важна.

ВБА информирует

На десятом международном Форуме ВБА-2023 **Алексей Александров,** генеральный директор компании SDK Systems, входящей в консорциум iCAM Group, погрузился в конкретику в области защиты информации ЦР в коммерческих банках, исключая зону ответственности Банка России: «Согласно серии национальных стандартов ГОСТ 57580.х "Защита информации финансовых организаций" подлежат защите персональные данные пользователей ЦР — клиентов банка, данные об операциях, включая связанные с ними, а также ключевая информация средств криптографической защиты информации (СКЗИ) и другая конфиденциальная информация о системе цифрового рубля».

Как известно, указанный ГОСТ предполагает регулярный аудит инфраструктуры банка с привлечением сторонней компании-аудитора лицензиата ФСТЭК на соответствовали требованиям документа. Периодичность проверки пока официально не объявлена. Модель угроз, по данным участников рынка, также будет утверждена ФСБ в скором будущем. Пока перечисленное находится в «серой зоне» регулирования.

В список технологических сегментов ЦР в банках-участниках входит адаптер цифрового рубля, состоящий из контуров обработки и контроля, подчиненный удостоверяющий центр, пользовательские интерфейсы, включая мобильное и web- приложение, а также каналы передачи данных. По мнению представителя SDK Systems, одним из наиболее серьезных вызовов является построение УЦ.

«Банк-участник пилотного проекта должен развернуть подчиненный Удостоверяющий центр с использованием программно-аппаратного комплекса (ПАК) УЦ, сертифицированный ФСБ по классу КС3. Назначение — выдача сертификатов ключей проверки электронных подписей пользователей ЦР. Мы в своих проектах, внедряя удостоверяющий центр, ориентируемся на продукт компании КриптоПро, сертифицированный по классу КС3», — пояснил Алексей Александров.

В своей презентации, эксперт разъяснил, что каждый пользователь ЦР должен пройти идентификацию и получить сертификат в удостоверяющем центре банка-участника. В мобильное и web-приложение должно быть встроено СКЗИ (ПМ БР) для работы с ключами пользователя ЦР, а канал до банка-участника защищается с помощью ГОСТ TLS. И TLS применительно к web, и КС3 (и выше) для УЦ, работающих на ОС Windows, являются одними из множества болевых точек ИБ и импортозамещения. Дополнительные проблемы создает и требование к тому, чтобы контура обработки и контроля имели свои собственные сетевые сегменты с СКЗИ класса КС3, а также обслуживались отдельными сотрудниками.

Роман Карпов, директор по стратегии и развитию технологий Axiom JDK успокаивает: «Отечественная среда исполнения Java включает готовые конфигурации российских TLS

МНЕНИЕ ЭКСПЕРТА



Павел Обрезумов, заместитель директора по развитию продуктов Центра цифровых решений для бизнеса компании BSS

Вызовы проекта цифрового рубля для банков

В первую очередь обращает на себя внимание масштаб затрат, понесенных банками на реализацию «пилота» по цифровому рублю. Безусловно, надо делать поправку на то, что данная работа была новаторской (это предполагает повышенные расходы на возможные эксперименты и ошибки), а также выполнялась многими банками в формате самостоятельной разработки (которая, очевидно, дороже, чем использование тиражируемого IT-решения). Но даже с учетом этих факторов минимальный бюджет на реализацию проекта может кратно превышать весь IT-бюджет небольшого банка за год.

Ответом на данный вызов видится появление на рынке тиражируемых решений по поддержке цифрового рубля. Ведущие вендоры уже активно идут в этом направлении (в том числе и компания BSS, создавшая решение по поддержке цифрового рубля в ДБО). Тем не менее пока цифровой рубль существует в рамках пилотирования, оценить масштаб рынка решений по цифровизации работы с цифровым рублем и как следствие оценить, насколько цена таких решений станет доступной широким слоям банков, пока трудно.

Другой серьезный вызов — комплексность проекта по внедрению цифрового рубля и вытекающая отсюда потребность в специальных компетенциях у банков. В соответствии с требованиями Банка России проект внедрения цифрового рубля требует развертывания в банке отдельных решений по информационной безопасности, а также прохождения ряда процедур в этой области. При этом пока результат таких работ ограничен применением только в отношении цифрового рубля — например, используемый для работы с цифровым рублем удостоверяющий центр банк не вправе применять для каких-то иных нужд. В целом, бескомпромиссный подход Банка России к обеспечению информационной безопасности цифрового рубля абсолютно понятен и правилен, однако хочется надеяться, что по мере расширения проекта будут предложены пути выполнения требований, доступные для разного спектра возможностей банков.

(SSL) сертификатов в дополнение к обновлениям безопасности и критическим патчам (CPU). При установлении защищенных TLS-соединений с цифровыми сервисами, использующими сертификаты Минцифры, подключение Java-приложений произойдет автоматически, если они работают на Axiom JDK Pro в отличие от приложений, работающих на Oracle Java, других JDK и самосборках OpenJDK».

Станислав Шилов, директор по развитию продуктов Центра цифровых решений для бизнеса компании BSS, комментируя для «Б.О» вопрос: «Насколько будет сложна на следующих этапах "пилота" внедрения ЦР задача построения удостоверяющих центров для средних и малых банков?», ответил: «Задача не простая, как в силу необходимости дополнительных инвестиций в построение собственного УЦ, так и в силу необходимости наличия соответствующих кадров, которых в небольшом банке без своего УЦ, скорее всего, нет. Но при этом она вполне решаема».

Вебинар АРБ и опыт Ингосстраха

15 ноября 2023 года Ассоциация российских банков (АРБ) в партнерстве с компанией BSS провела вебинар «Цифровой рубль и реализации в ДБО функционала, необходимого для работы с новой цифровой валютой», запись которого доступна на канале Ассоциации в YouTube.

Вебинар дал исчерпывающие ответы инженеров из BSS по уже наработанным ими практикам трансформации имеющихся в банках систем ДБО для работы с ЦР согласно требованиям Банка России. В частности, реализована типовая web-версия ДБО для юридических лиц с платежным функционалом, а также полным набором операций для открытия кошелька и регистрации сертификата ключа, а также обмена безналичных средств банка на ЦР. Срок выполнения проекта составил три месяца.

Андрей Тужилин, технический директор банка Ингосстрах, в режиме вопросов и ответов рассказал о полученном опыте. Его выступление также доступно в записи на канале АРБ. ИБ-специалистам стало интересно то, что он опроверг расхожее мнение о возможности аутсорсинга: «Никакой облачной подписи не предусмотрено. Сейчас ключи хранятся надежным образом у клиента в мобильном приложении Банка России или на не извлекаемых носителях, если это web».

Что будет дальше? И Андрей Тужилин, и представители BSS говорят об оффлайн режиме использования ЦР, а также о крайне полезном инструменте — смарт-контрактах. Станислав Шилов добавил: «Компания BSS очень чутко относится ко всем инновационным инициативам и стремится максимально их поддерживать. Поскольку мы видим существенную синергию между дистанционными каналами банка и инфраструктурой цифрового рубля, включая и возможность его использования в смарт-контрактах, планируем работать в данном направлении». Б.О

Российская Java готова к работе с цифровым рублем

В платежных системах, в том числе в платформе цифрового рубля, крайне важны отсутствие уязвимостей, минимизация времени простоев, а также повышенный уровень ИБ. Роман Карпов, директор по стратегии и развитию технологий Axiom JDK поделился с «Б.О» лучшими практиками



— Какова статистика по обнаружению и скорости устранения уязвимостей?

— Обновления безопасности Axiom JDK выходят ежеквартально. В год в OpenJDK закрывается порядка 100 уязвимостей разного уровня критичности.

В этой связи стоит вспомнить ситуацию с библиотекой Log4J, давшую начало глобальной «киберпандемии» в конце 2021 года. Она осложнилась тем, что даже если в коде, написанном в организации ее не было, библиотека могла наследоваться. Внедрение цикла безопасной разработки (РБПО/SDLC) в совокупности с технической поддержкой от вендоров, разрабатывающих продукты на основе Open Source, как раз являются требованиями ФСТЭК к подобным решениям. Поэтому наши инженеры выпустили патч, который позволял блокировать эксплуатацию этой уязвимости и который можно было применить на работающей Java-системе.

— Как обеспечивается безопасность рантайма?

— Безопасность среды исполнения Java обеспечивается промышленным процессом разработки РБПО. Это статический и динамический анализ исходных кодов, а также применение доверенных компиляторов при формировании бинарного дистрибутива Axiom JDK. Для систем с повышенными требованиями по безопасности дополнительно может потребоваться контроль запускаемых jar/war файлов. Поэтому финансовым организациям будет проще контролировать операционную надежность ПО на всех этапах жизненного цикла в соответствии с требованиями Положения Банка России № 716-П.

Необходимо отметить, что все сборки проходят тщательное QA/QC-тестирование перед каждым релизом. Повышенная стабильность Java-приложений обеспечивается благодаря современным сборщикам мусора, включая Shenandoah и ZGC, а технология Axiom Runtime Container Pro позволяет создавать микроконтейнеры с высокой скоростью запуска и работы. Инженеры Axiom JDK оказывают помощь в режиме 24/7 на русском языке. Все это позволяет минимизировать время простоя в соответствии с требованиями Положения № 787-П и обеспечить бесперебойную работу банковской инфраструктуры.

Среди публичных кейсов стоит отметить компанию НСПК, которая перевела процессинг, клиринг и систему лояльности ПС «Мир» на Axiom JDK Pro. В этом году наше сотрудничество расширилось. В настоящее время более 50 различных систем НСПК работают на нашей Java с SLA 99,999%, в том числе СБП, через которую за сутки проводится более 18 млн операций по данным на июль этого года.

— Имеется ли допуск регуляторов для работы с цифровым рублем?

— Продукты Axiom JDK соответствуют всем необходимым требованиям. Сертификат ФСТЭК подтверждает, что среда разработки и исполнения Java Axiom JDK Certified может использоваться при создании систем, требующих четвертого уровня доверия (СЗИ УД4):

Это единственная среда разработки и запуска Java-приложений, разрешенная регулятором к применению в системах с повышенными требованиями к ИБ. В ходе проверки соответствия было подтверждено отсутствие в СЗИ Axiom JDK Certified недокументированных возможностей и наличие требуемых функций безопасности, произведен контроль архитектуры продукта и полный анализ его исходного кода, включая фаззинг-тестирование. Инженерная команда Axiom JDK инвестировала десять человеко-лет в разработку сертифицированного продукта и верификацию трех Гб программного кода.

Что касается криптографии, Axiom JDK является доверенной средой функционирования для криптопровайдера КриптоПро, что отражено в соответствующих формулярах ФСБ. Б.О

реклама