

ЦИФРОВОЙ РУБЛЬ:

основные ошибки интеграции и как их избежать



Текст

МАРАТ ЦИХМИСТРОВ,
РУКОВОДИТЕЛЬ НАПРАВЛЕНИЯ
ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ
КОМПАНИИ «ИНФОРМЗАЩИТА»

Сложность подключения банка к Платформе цифрового рубля легко недооценить на этапе планирования. За подключением банка к ней стоит отдельный технологический контур с серверами, сетевым оборудованием, TLS-шлюзами, средствами криптографической защиты, удостоверяющими центрами и другими компонентами. Параллельно нужно дорабатывать мобильное приложение, АБС и ДБО, настраивать взаимодействие с внешними сервисами и готовить инфраструктуру к испытаниям. Ошибка в архитектуре или выборе оборудования может обнаружиться уже после закупки, когда ее исправление напрямую влияет на сроки и бюджет.

Над проектом одновременно работают банк, ИБ-интегратор, вендоры бизнес-логики, АБС и ДБО, поставщики оборудования и средств защиты. Их зоны ответственности различаются, но успех зависит от согласованности действий всех участников. Сроки сдвигают не только технические ошибки, но и поздние закупки, несогласованные изменения и решения, принятые без учета смежных систем.

«Информзащита» реализует проекты по цифровому рублю с 2024 года. Практика позволяет выделить ряд проблем, наиболее заметно влияющих на ход подключения. В этой статье мы остановимся только на части таких нюансов — прежде всего на проектировании инфраструктуры, совместимости компонентов и организации работы между участниками проекта.

ПРОЕКТИРОВАНИЕ И ИНТЕГРАЦИЯ ИНФРАСТРУКТУРЫ ЦИФРОВОГО РУБЛЯ

Инфраструктура цифрового рубля формирует внутри банка отдельный сложный контур. В него входят серверы, коммутаторы, межсетевые экраны, TLS-шлюзы, удостоверяющие центры, HSM, средства криптографической защиты, рабочие места обслуживающего персонала и системы мониторинга. Все компоненты должны работать совместно и соответствовать требованиям к безопасности.

Одна из типичных ошибок — начинать с минимальной конфигурации, достаточной для первичного подключения. На старте это сокращает объем закупки, но затем появляются требования к резервированию, кластеризации, автоматизации выпуска сертификатов и росту числа пользователей. Минимальная схема разрастается, а часть решений приходится пересматривать уже по ходу внедрения.

Поэтому проектировать контур имеет смысл от конечной модели, даже если внедрение будет проходить поэтапно. В архитектуре нужно заранее учитывать требования к отказоустойчивости, масштабированию и дальнейшей эксплуатации. Иначе решения, достаточные для первого этапа, впоследствии могут потребовать пересмотра.

Похожая ситуация возникает с переиспользованием существующей инфраструктуры. Банк может быть оснащен HSM, удостоверяющими центрами, межсетевыми экранами и каналами связи, задействованными в СМЭВ, ЕБС, СБП и других системах. Теоретически часть такого оборудования можно рассматривать для нового контура, но каждый случай требует отдельной проверки. Важны назначение устройства, версия прошивки, действующие сертификаты, текущая нагрузка и воз-

возможность очистки или перенастройки устройства. Отдельные элементы рубля в силу законодательных требований в принципе нельзя использовать одновременно для других задач.

Требования к ИБ также критически важно проработать в ходе создания общей архитектуры. Ошибка в выборе продукта СЗИ или СКЗИ может обнаружиться уже после закупки и затронуть не одну позицию в спецификации, а всю архитектуру, схему взаимодействия, документацию и сроки этапов проекта.

Даже корректно подобранные компоненты необходимо проверять в связке, так как формальное соответствие требованиям не гарантирует совместимости конкретных моделей. По этой причине интегратору приходится держать в поле зрения сразу несколько технологических областей. Недостаточно хорошо разбираться только в сетях или только в средствах защиты. Нужна команда, которая понимает серверную инфраструктуру, криптографию, СЗИ и СКЗИ, банковские системы и регуляторные требования и при этом умеет свести все это в одну работающую архитектуру в плотном взаимодействии с производителями оборудования и ПО.

ОРГАНИЗАЦИЯ ПРОЕКТА И ВЗАИМОДЕЙСТВИЕ УЧАСТНИКОВ

Техническая часть не определяет результат сама по себе. Одновременно могут происходить развертывание адаптера, доработка АБС и ДБО, интеграция с ЕСИА и СБП, настройка проверок ПОД/ФТ, создание удостоверяющих центров, внедрение СЗИ и СКЗИ, подготовка инфраструктуры и испытания. Почти ни один из этих потоков нельзя вести полностью автономно.

Задержка в одном элементе быстро отражается на работе соседних. Вендор АБС зависит от готовности интерфейсов, команда ДБО — от интеграции с адаптером цифрового рубля, специалисты по ИБ должны учитывать архитектурные решения, которые принимаются по ходу проекта. Если эти зависимости не учтены заранее, расхождения проявляются уже во время интеграции, когда исправление требует больше времени и денег.

Поэтому интегратор должен видеть весь проект и понимать, какие решения одного участника повлияют на других, где потребуются дополнительные согласования и какие этапы нельзя начинать до завершения предыдущих. Здесь особенно ценен опыт реальных внедрений, где подобные зависимости уже приходилось учитывать.

Для цифрового рубля это критично еще и потому, что эксперименты с непроверенными

конфигурациями быстро начинают влиять на сроки. Нетипичное сочетание СКЗИ, неудачно выбранная архитектура или неподтвержденная совместимость оборудования могут не мешать на этапе проектирования, но создать проблемы на этапе развертывания тестового контура. Чем раньше такие риски снимаются, тем меньше вероятность переделок ближе к запуску.

На сроки влияет и закупочная стратегия. Перенос сроков закупки оборудования ради текущей экономии может обернуться ростом финальной стоимости и пересмотром уже согласованной конфигурации, что при многокомпонентной инфраструктуре и ограниченном бюджете затрагивает и другие части проекта.

Еще один фактор — участие в работе специалистов самого банка. Мероприятия по обеспечению ИБ идут параллельно с доработкой бизнес-функциональности, поэтому проект постоянно требует решений и исходных данных со стороны внутренних команд. Если согласования затягиваются или ключевые специалисты подключаются нерегулярно, эпизодически, общий график начинает сдвигаться даже при слаженной работе подрядчиков.

«Информзащита» с 2024 года ведет проекты по цифровому рублю как единый интеграционный процесс. Компания координирует технические и организационные задачи, связывает между собой инфраструктуру, ИБ, бизнес-логику и работу поставщиков. Для банка это снижает риск ситуации, когда отдельные части проекта формально готовы, но перейти к следующему этапу невозможно из-за общей неработоспособности контура цифрового рубля.

При этом перечисленные в статье ошибки охватывают только часть вопросов, которые приходится учитывать при подключении к Платформе цифрового рубля. Состав и архитектура решения зависят от инфраструктуры конкретного банка, используемых средств защиты, требований к отказоустойчивости, объема автоматизации и многих других факторов. Чего стоит только работа с мобильным приложением банка! На практике почти каждый проект требует глубокой проработки технических и организационных нюансов.

Большая часть серьезных проблем закладывается задолго до запуска, при выборе архитектуры и оборудования, планировании закупок, распределении ответственности и определении последовательности работ. Чем раньше эти решения проверены и увязаны между собой, тем более предсказуемо происходит дальнейшая интеграция.

Б.О