informzashchita

Цифровой рубль: общие ошибки и частые вопросы

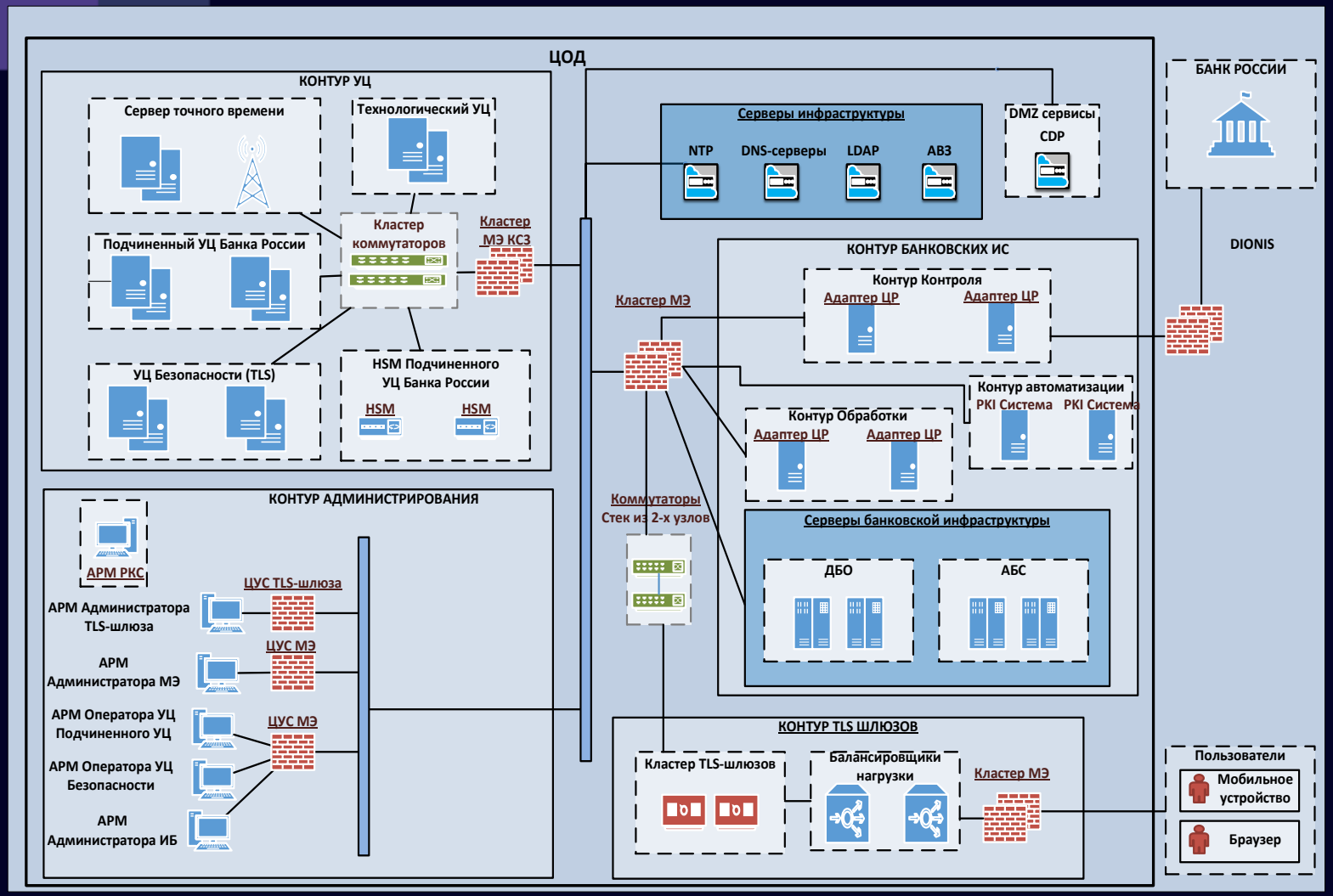
Частые вопросы

1. Существуют ли готовые типовые решения для Цифрового рубля?

2. Какой срок нужно заложить для реализации Цифрового рубля в Банке?

3. Можно ли переиспользовать существующие в банке УЦ и устройства (МЭ, HSM, коммутаторы и шлюзы)?

Пример архитектуры



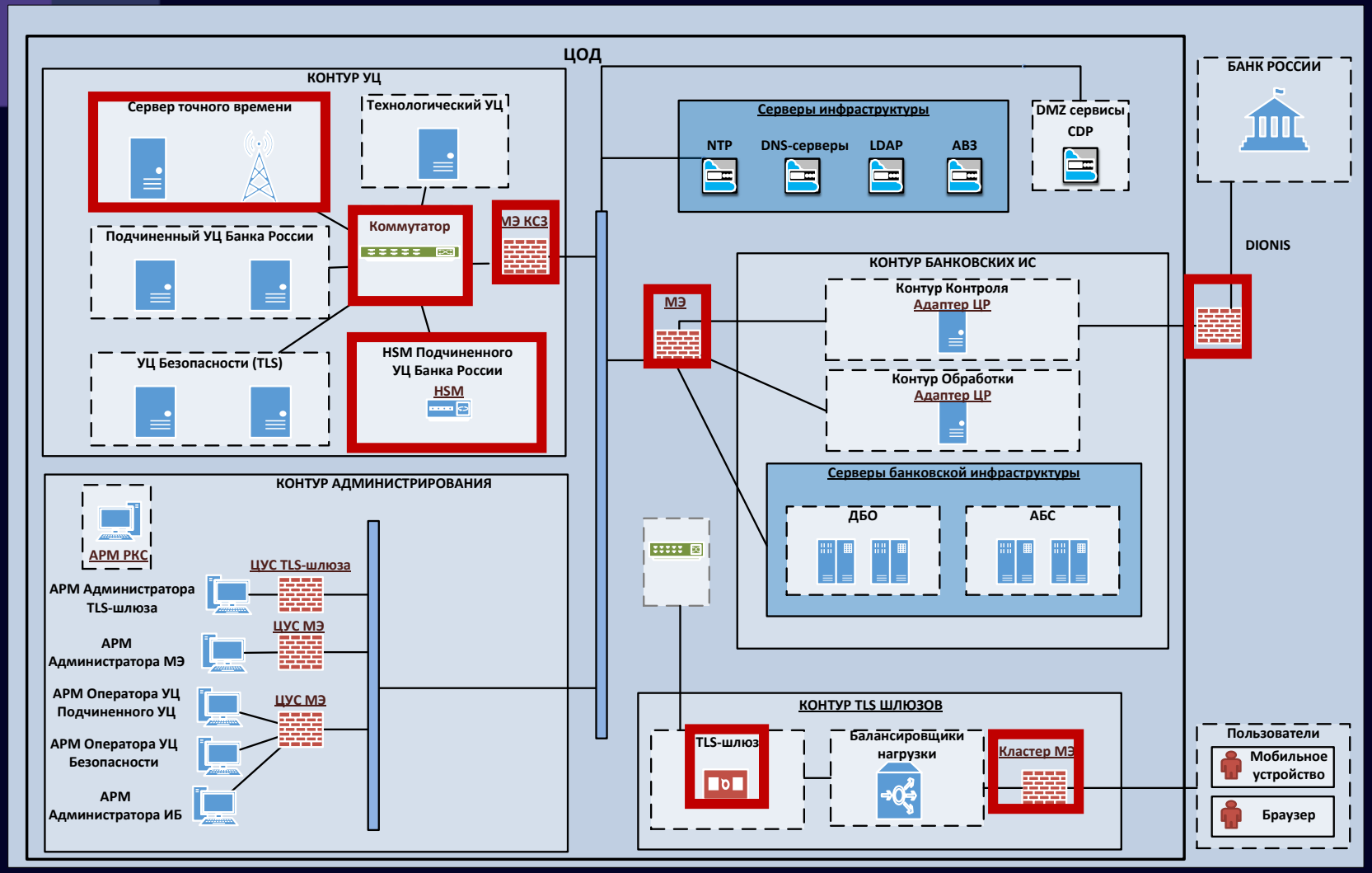
Драйверы изменений:

- Большая вариативность используемых СКЗИ
- Распределение контуров по различным локациям
- Требования к отказоустойчивости
- Различные продукты для бизнес-логики
- Требования к автоматизации выпуска сертификатов
- Требования к методам идентификации клиентов
- Различные варианты мониторинга компонентов

Этапы и длительность указаны для работ в области ИБ. Работы по развертыванию и интеграции ПО для обеспечения работоспособности бизнес-функционала ЦР идут параллельно и взаимно зависимы.

		месяцы											
Этап	Краткое описание этапа	1	2	3	4	5	6	7	8	9	10	11	12
1	Формирование требований к системе												
2	Проектирование и разработка техно-рабочей, эксплуатационной и организационно-распорядительной документации												
3	Получение счета ЦР ФП и подписание договора с ЦБ РФ - Заяление на пилот и подготовка документов - Заключение Договора счета ЦР с ЦБ РФ и получение и получение идентификаторов												
4.1.	Поставка оборудования												
4.2.	Поставка лицензий												
5	Тестовые испытания взаимодействия (ТИВ)												
5.1.	Подготовка макетов и встраивание в ДБО												
5.2.	Развертывания адаптера и доработка АБС												
5.3.	Подготовка инфраструктуры и выполнение настроек												
5.4.	ТИВ												
6	Ввод в действие												
6.1.	Ввод в действие контура в ЦОД												
6.2.	Опытная эксплуатация и проведение пользовательского тестирования												
6.3.	Кластеризация												
6.4.	Проведение приемо-сдаточных испытаний												
7	Опционально: Итоговая оценка соответствия требованиям ГОСТ Р 57580.1 Проводится отдельно по итогам работ												

Переиспользование узлов



Принципы переиспользования:

- Большая часть оборудования для контура ЦР может быть использована только для целей ЦР
- Переиспользование подразумевает переформатирование / очистку устройства
- Следует внимательно отнестись к версии и актуальности прошивок, сертификатам устройств
- Имеющиеся каналы к СМЭВ / ЕБС / ЕСИА требуется оценить с точки зрения повышения нагрузки

Общие ошибки

1. Построение инфраструктуры ЦР в банке без обеспечения отказоустойчивости, в том числе для балансировки запросов

2. Неполное понимание регуляторных требований, что приводит к применению неподходящих классов СЗИ (КС2 вместо КС3 или КВ)

3. Отсутствие тестирования компонентов инфраструктуры ЦР на совместимость друг с другом. Наиболее яркий пример: несовместимость АПМДЗ с рядом моделей серверов.

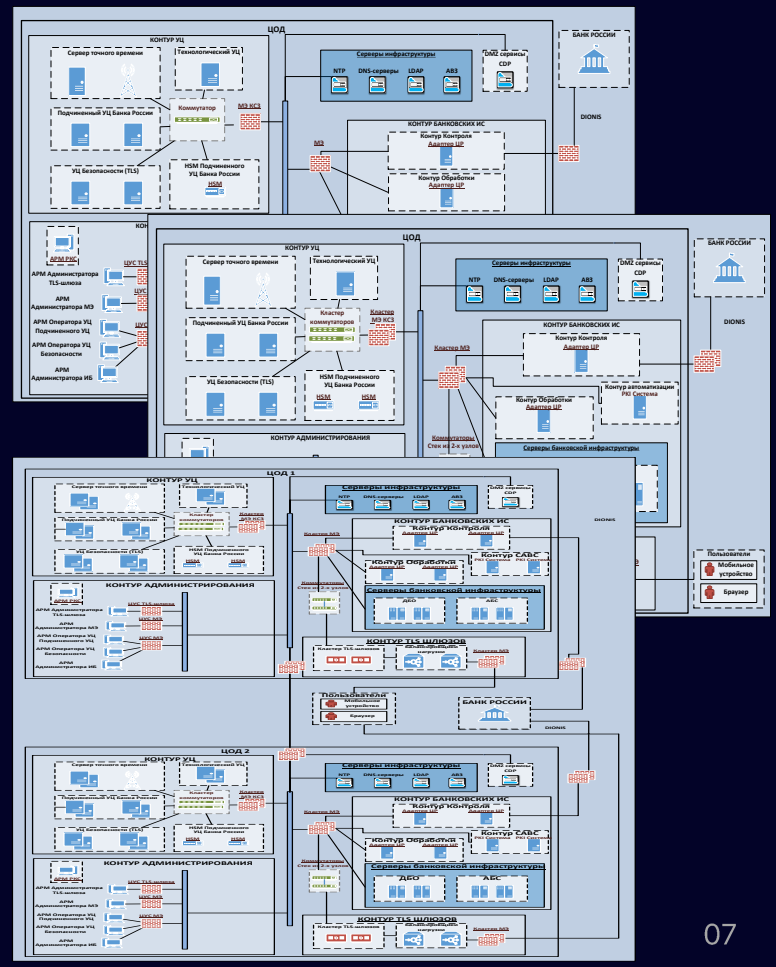
Построение инфраструктуры ЦР в банке

Общие тезисы:

1. Требования к операционной надежности контура ЦР как ЗОКИИ не указаны. **Это не значит, что они не появятся.**

2. При проектировании необходимо учитывать возможности масштабирования инфраструктуры и перспективы роста количества клиентов, совершающих транзакции в Цифровом рубле

3. Реализация функций ИБ, не указанных в требованиях к контуру Цифрового рубля, как правило, не входит в состав работ. Их необходимость нужно учитывать при проектировании архитектуры



Регуляторные требования и тестирование

1. Отсутствие требований / мероприятий по интеграции системы ПлЦР в имеющуюся инфраструктуру банка для соответствия ГОСТ Р 57580.1
2. Банк не учитывает требования по корректности встраивания в ДБО криптопровайдера
3. Попытки переиспользовать имеющиеся HSM / УЦ / МЭ, уже применяющиеся для других целей (СМЭВ /ЕБС, СБП)
4. Отсутствие защиты канала между ЦОД и АРМ администраторов / операторов УЦ, подключаемого к сетям общего пользования
5. Временное отсутствие нормативного регулирования по автоматизированному выпуску сертификатов для ЮЛ
6. Необходимость тестирования оборудования с помощью выбранного интегратора ДО закупки на отдельных образцах из партии (несколько экземпляров). Пример: АПМДЗ могут по разному вести себя с матплатами серверов из одной партии.

Контакты

Марат Цихмистров

Руководитель направления

+7 985 614 1721

m.tsikhmistrov@infosec.ru