Цифровой рубль после вступления в силу закона. Только практика

Елена Смышляева,
заместитель генерального директора
АО «Современные системы»

современные системы

О компании. Реализованные проекты

ЕБС и УБИ
> 100 банков
в облаке

Цифровой профиль ФЛ
> 30 банков

Криптомодули и криптоадаптеры
> 100 клиентов

Маркетплейсы
> 15 клиентов

Адаптер СМЭВ
> 100 банков

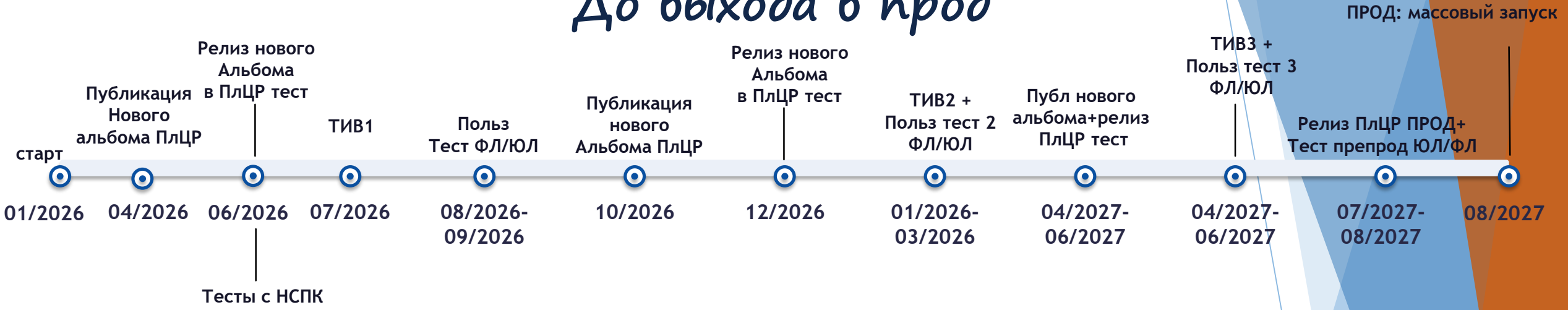
Цифровой рубль
10 проектов и растем

> 50 проектов
в пике делали одновременно

ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Дорожная карта. Бизнес процессы

До выхода в прод

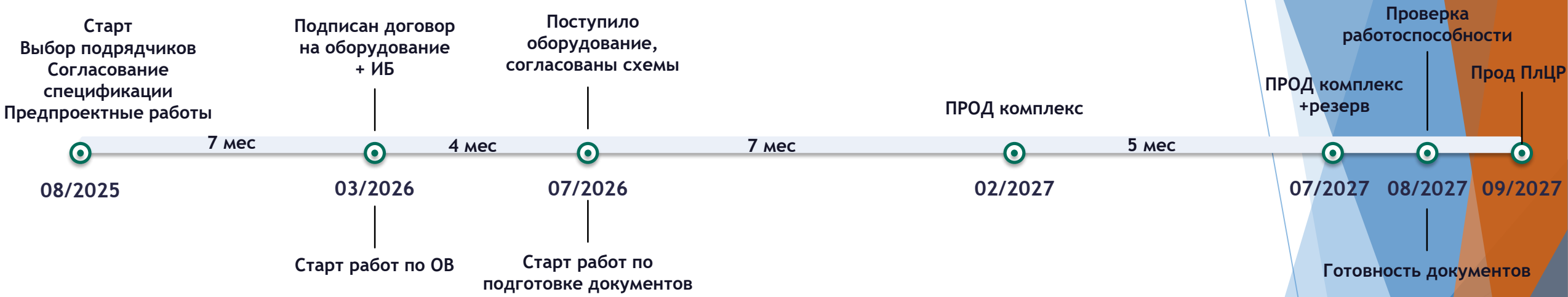


После выхода в прод

современные системы

Дорожная карта

Инфраструктура + ИБ + ИТ



современные системы

Группировка сценариев для упрощения процессов

КЛИЕНТСКИЕ СЦЕНАРИИ:

1. Регистрация клиента ЮЛ и ФЛ
2. Выпуск/Перевыпуск сертификатов ФЛ и ЮЛ (Построение ГОСТ-TLS с клиентского устройства). Управление сертификатами ФЛ, ЮЛ, ФП и САС
3. Операции по покупке и продаже ЦР клиентами (списание/зачисление на рублевый счет)
4. Получение фоновых уведомлений со стороны ПлЦР для ФП и клиента
5. Клиентские платежи: C2C, B2B

- *Запрос возможности*
- *Подписание дайджеста*

6. Клиентские платежи: C2B (универсальный QR)

- *Статическая ссылка. Срок действия всегда 1 год.*
- *Динамическая ссылка. Срок действия от 5 минут до 3 месяцев. По умолчанию 72 часа.*
- *Кассовая ссылка. Срок действия от 5 минут до 3 месяцев. По умолчанию 72 часа.*

В запросе возможности к нам приходит тип ссылки, но не приходит срок действия – додумываем сами.

7. СиС (самоисполняемые сделки)
8. Другие операции (изменение реквизитов, отмена СиС), где есть дайджест

ОПЕРАЦИИ ФП: …

современные системы

C2C. Пример платежа

Особенности. Актуальные вопросы

1. Постконтроль ПОД/ФТ по всем клиентам?

- При выявлении признаков ПОД/ФТ ФП отправляет по клиенту спец уведомление cbdc 070 в ПлЦР (без привязки операции). В ответ cbdc 071 + может быть со стороны ПлЦР изменение статуса на «заблокировать» или «закрыть» cbdc 023).

2. Что может делать ФП самостоятельно в отношении клиента?

- Изменение ФП статуса СЦР cbdc 012 (заблокировать или разблокировать) – ПлЦР в ответ cbdc 023 всем ФП
- Запрос на изменение реквизитов клиента по инициативе ФП cbdc 020, в ответ от ПлЦР cbdc 021 от ПлЦР всем.
- Если клиент найден в черных списках, то банк инициирует отмену СиС cbdc 108. Отмена Сис по основаниям ПОД/ФТ, ПлЦР присылает 111 уведомление только отправителю.

3. Клиент может закрыть доступ к кошельку конкретному ФП?

3. По всем фоновым сценариям ПлЦР отправляет уведомление во все ФП (где ФП не был отправителем).

современные системы

Ограничения/новости/предложения

1. B2C не в части возврата (зимний релиз)

2. Как банку платить в ЦР? Операции для банков Fi2…

3. Добавление в 111 уведомление идентификаторов клиента и Сис.
4. Уведомления для касс в ТСП. В случае негативного сценария на кассе: уведомления по негативному сценарию нет. Будут доработки на стороне ПлЦР по запросу статуса этого перевода
5. ПОД/ФТ связка операций при ручном контроле

6. Неограниченное количество сертификатов для КО…

7. 851-п для всех операций

8. КСЗ на Java. Согласовано ТЗ со стороны Axiom JDK/КриптоПро.

9. ЗО КИИ для ЦР

современные системы

Ограничения/новости/предложения

ТР ЕСИА для ЮЛ?

Для однозначной идентификации ФЛ, действующего от имени ЮЛ:

- следующий набор информации:
  - Наименование ЮЛ – уже есть для ЮЛ в структуре сертификата
  - Юридический адрес ЮЛ – уже есть для ЮЛ в структуре сертификата
  - ОГРН ЮЛ
  - ФИО ФЛ, уполномоченного действовать от имени ЮЛ – уже есть для ЮЛ в структуре сертификата
  - СНИЛС ФЛ, уполномоченного действовать от имени ЮЛ

- участник ПлЦР должен проверить полномочия представителя, в т.ч. проверку наличия полномочий на совершение действий, связанных со счетом ЦР (для представителей пользователя ПлЦР, не имеющих право действовать от имени ЮЛ без доверенности, в соответствии с принятыми у участника ПлЦР процедурами)

Документ «Временные требования по обеспечению информационной безопасности для автоматизации выпуска сертификатов пользователя платформы цифрового рубля» распространяются на пользователей-ФЛ. Для пользователей-ЮЛ сертификаты ключа проверки ЭП и сертификаты ключей безопасности должны выпускаться в соответствии с требованиями ФЗ от 06.04.2011 № 63-ФЗ «Об электронной подписи».

Сертификаты и CAC для серверного сегмента

Контур	Компонент	Ключи/Сертификаты/CAC, необходимые для работы
Контур Обработки (КО)	**Бэкенд КО**	1.1. Сертификат КО ФП (Выдаёт ЦБ)
		1.2. Сертификат КК ФП (Выдаёт ЦБ)
		1.3. Сертификат КО РОРД (Банк передает в ПлЦР CAC ПУЦ Банка, после этого ПлЦР выдает сертификат (КО РОРД, 4 шт.))
		1.4. Сертификат УЦ БР (Выдаёт ЦБ)
		1.5. Сертификат УЦ ФП (Выдаёт ЦБ)
		1.6. Сертификат КК ПлЦР (Выдаёт ЦБ)
		1.7. Сертификат УЦ ПлЦР Банка России (Выдаёт ЦБ)
		1.8. Сертификат Корневого УЦ TLS Банка для пользователей и серверного TLS сертификата Банка (для TLS шлюза) (Выпускает Банк в УЦ Безопасности)
		1.9. CAC Корневого УЦ ПлЦР (Передает ЦБ через ЛК)
		1.10. CAC Подчиненного УЦ Банка (Выпускает Банк в ПУЦ Банка)
		1.11. CAC Корневого УЦ TLS Банка (УЦ Безопасности) для пользователей и серверного TLS сертификата Банка (для TLS шлюза) (Выпускает Банк в УЦ Безопасности)
	КриптоМодуль КО	2.1. Ключ КО ФП (Выдает ЦБ)
		2.2. Цепочки сертификатов (Выдает ЦБ вместе с сертификатом КО ФП): Сертификат УЦ ПлЦР Банка России Сертификат ПУЦ ФП Сертификат КО ФП Сертификат КК ФП Сертификат КО РОРД (4 шт.) Сертификат КК ПлЦР Сертификат Эмитента ПлЦР
		2.3. CAC для вышеуказанных цепочек сертификатов: CAC Корневого УЦ ПлЦР (Передает ЦБ через ЛК) CAC Подчиненного УЦ Банка (Выпускает Банк в ПУЦ Банка)

современные системы

Сертификаты и CAC для серверного сегмента

Контур Контроля (КК)	**Бэкенд КК**	3.1. Сертификат КК ПлЦР (Выдаёт ПлЦР)
	КриптоМодуль КК	4.1. Ключ КК ФП (Выдаёт ПлЦР)
		4.2. Цепочки сертификатов (Выдает ЦБ вместе с сертификатом КК ФП): Сертификат УЦ ПлЦР Банка России Сертификат ПУЦ ФП Сертификат КО ФП Сертификат КК ФП Сертификат КО РОРД (4 шт.) Сертификат КК ПлЦР Сертификат Эмитента ПлЦР
		4.3. CAC для вышеуказанных цепочек сертификатов: CAC Корневого УЦ ПлЦР (Передает ЦБ через ЛК) CAC Подчиненного УЦ Банка (Выпускает Банк в ПУЦ Банка)
Контур Сервиса автоматизации выпуска сертификатов	**Модуль по работе с сертификатами (МС)**	5.1. Ключ и сертификат Оператора ПУЦ и Оператора УЦ Безопасности, для подключения Модуля по работе с сертификатами к УЦ через stunnel (указывается в настройках stunnel) (Выпускает сам Банк в ПУЦ Банка и УЦ Безопасности Банка)
		5.2. Цепочка сертификатов для серверного сертификата ПУЦ Банка и УЦ Безопасности Банка: Сертификат УЦ ПлЦР Банка России (Выдаёт ЦБ) Сертификат ПУЦ ФП (Выдаёт ЦБ)
		5.3. CAC для вышеуказанных цепочек сертификатов: CAC Корневого УЦ ПлЦР (Передает ЦБ через ЛК) CAC Подчиненного УЦ Банка (Выпускает Банк в ПУЦ Банка)
	КриптоМодуль для Модуля по работе с сертификатами (сопряжение с УЦ)	6.1. Ключ Оператора ПУЦ и Оператора УЦ Безопасности (Выдает сам Банк)
	Директория для Модуля по работе с сертификатами (автоматизация работы с CAC и сертификатами)	7.1. Банк обеспечивает размещение и своевременное обновление всех сертифкатов и CAC, перечисленных в п. 1.
Канал с ЦБ	**ПАК "Dionis" или СКЗИ "DiSec-W"**	8.1. Ключи, сертификаты и CAC согласно документации на СКЗИ и Регламенту ЦБ (Выдаёт ЦБ). Запрос на сертификат готовится Банком самостоятельно согласно Регламенту ЦБ.

Сертификаты и CAC для клиентского устройства

Назначение	Список сертифкатов\CAC (CRL)
1. CAC (CRL)	1. CAC Корневого УЦ ПлЦР
	2. CAC Подчиненного УЦ Банка
	3. CAC Корневого УЦ TLS Банка (УЦ Безопасности) для пользователей и серверного TLS сертификата Банка (для TLS шлюза)
	4. CAC Подчиненного УЦ TLS Банка (УЦ Безопасности) для пользователей и серверного TLS сертификата Банка (для TLS шлюза) - при наличии
2. Список сертификатов необходимых для обеспечения возможности загрузки сертификата ЭП пользователя в ключевой контейнер ПМ БР, проверки ЭП на ЭС и шифрования ЭС в МП	1. Сертификат УЦ ПлЦР Банка России (ROOT)
	2. Сертификат подчиненного УЦ Банка (CA)
	3. Сертификат КК ПлЦР
	4. Сертификаты КО РОРД (4 сертификата)
	5. Сертификаты ЭП (основного и резервного) ключа КО Банка
	6. Сертификат ЭП (основного и резервного) ключа КК Банка
3. Список сертификатов необходимых для обеспечения возможности загрузки сертифката TLS пользователя в ключевой контейнер ПМ БР, построения ГОСТ TLS соединения (одностороннего и с взаимной аутентификацией)	1. Сертификат Корневого УЦ TLS Банка для пользователей и серверного TLS сертификата Банка (для TLS шлюза) (ROOT TLS) 2. Сертификат подчиненного УЦ TLS Банка для пользователей и серверного TLS сертификата Банка (для TLS шлюза) (CA TLS) - при его наличии
4. Список сертифкатов клиентов	1. Сертификат УНЭП клиента
	2. ГОСТ TLS-Сертификат Клиента

современные системы

33 ДОКУМЕНТА для АКТА готовности

Техническое задание на создание ИС
Модель угроз и нарушителей безопасности информации в ИС
Технический проект (пояснительная записка) на создание ИС
Проект схемы структурная комплекса технических средств;
Руководство Администратора системы (описание внутреннего администрирования системы);
Руководство Администратора ИБ системы (положение внутреннее для сотрудников ИБ);
Руководство Системного администратора системы (положение внутреннее для СисА);
Инструкция по резервному копированию;
Программа и методика испытаний
Проект Положения по обеспечению защиты информации при обработке и передаче электронных сообщений при осуществлении операций с цифровыми рублями
Проекты Приказов о назначении пользователей, администраторов и АКС СКЗИ
Проект Состава организационных мер защиты информации, а также состав технических средств защиты информации и порядок их использования при взаимодействии Финансового посредника с платформой цифрового рубля
Проект схемы сети с указанием API и Vlan
Проект перечня используемых СКЗИ с заполненными формулярами
Регламент работы с криптографическими ключами и САС для аутсорсинга
Форма для банков эксплуатируемого комплекста ключей и сертификатов. Распечатка всех сертификатов, которые мы используемых на стороне поставщика услуг и согласование с банком
Проект положения об УЦ (Проект положения о подразделении УЦ)
Проект регламента функционирования УЦ
Порядок работы с ключами ЭП и сертификатами ЭП, ключами безопасности выпускаемыми в УЦ
Документ Обеспечение безопасности УЦ
Проект порядка применения СКЗИ и управления ключевой информацией
Документ "Программные и технические средства обеспечения деятельности УЦ"
Описание функциональных ролей УЦ
Проект должностных инструкций работников УЦ
Проект порядка архивного хранения документов УЦ
Проект приказа о назначении работников на роли УЦ
Проект Приказа о вводе в эксплуатацию УЦ
Описание орг мер из СП по УЦ
Функциональные роли УЦ
Спецификация оборудования и ПО
Описание комплекса технических средств
Оценка ГОСТ
Оценка влияния СКЗИ

Подсистемы	Роль	Кол-во	Комментарии
АКС ФП	Администратор ключевой системы	1	Работник, ответственный за генерацию ключей ФП и взаимодействие с АКС ПлЦР ЦБ
КО	Администратор	1	Администратор КО отвечает за настройку программного обеспечения, используемого на КО
	Администратор резевный	1	Резервный администратор КО выполняет роль администратора КО в случае отсутствия основного администратора КО
	Администратор ИБ	1	Отвечает за обеспечение информационной безопасности КО
	Администратор ИБ резервный	1	Резервный администратор ИБ КО выполняет роль администратора ИБ КО в случае отсутствия основного администратора ИБ КО
	Оператор	1	Работник, назначенный пользователем ключа КО
	Оператор резервный	1	Работник, назначенный пользователем резервного ключа КО
КК	Администратор	1	Администратор КК отвечает за настройку программного обеспечения, используемого на КК
	Администратор резервный	1	Резервный администратор КК выполняет роль администратора КК в случае отсутствия основного администратора КО
	Администратор ИБ	1	Отвечает за обеспечение информационной безопасности КК
	Адмнистратор ИБ резервный	1	Резервный администратор ИБ КК выполняет роль администратора ИБ КК в случае отсутствия основного администратора ИБ КК
	Оператор	1	Работник, назначенный пользователем ключа КК
	Оператор резерв	1	Работник, назначенный пользователем резервного ключа КК
УЦ	Руководитель УЦ	1	Руководит подразделение УЦ
	Заместитель руководителя УЦ	1	Замещает руководителя УЦ
	Уполномоченное лицо УЦ *в целях повышения безопасности Уполномоченное ПУЦ и Уполномоченное лицо УЦБ разные работники	2	Выполняет загрузку и использования ключа Центра Сертификации
	Системный администратор УЦ	1	Настраивает и сопровождает общесистемное ПО
	Администратор безопасности УЦ	1	Настраивает СКЗИ и специальное программное обеспечение (компоненты УЦ)
	Администратор аудита УЦ	1	Выполняет аудит
	Администратор УЦ	1	Является администратором Центра Регистрации (настраивает Центр регистрации)
	Оператор ЦР	1	Выполняет проверку данных клиентов при регистрации (при необходимости), направляет запрос на сертификат в Центр регистрации. Сертификаты оператора используются в модуле по работе с сертифкатытами для автоматизации выпуска сертификатов
	Делопроизводитель УЦ	1	Обрабатывает поступающую/исходящую корреспонденцию в/из УЦ. Например, пользователь при утере своего оборудования может обратиться в письменной форме в УЦ для отзыва сертификата
HSM	Работники, назначенные на роль для инициализации HSM	5	Запуск HSM
	Администратор	1	Выполняет настройки HSM, создает пользователей
	Аудитор	1	Выполняет анализ работы пользователей и использования ключей
	Администратор резервного копирования	1	Выпоняет резервное копирование настроек и ключей, находящихся на HSM
	Администратор Статистики *опционально	1	Анализ статистики
	Пользователь*Уполномоченное лицо ПУЦ и Уполномоченное лицо УЦБ	2	Загружает ключ
ТШ КБР	АКС	1	Генерирует и направляет запросы на серфикаты в ЦБ
	Оператор	1	Работник, назначенный пользователем ключа

Необходимое количество персонала

Оценка влияния

1. Клиентское Приложение: Проводить ОВ для МП по упрощенному или стандартному порядку?

2. Клиентское Приложение: Проводить ли оценку влияния для веб-приложения?

3. Серверный сегмент: Проводить ОВ только прикладных компонентов, выполняющих непосредственные вызовы СКЗИ или же выполнять ОВ всей среды функционирования (СФ) СКЗИ, включающей все компоненты системы, участвующие в трассах вызовов СКЗИ?

- Подход к проведению ОВ должен быть комплексным, происследованное решение не должно требовать проведения дополнительных исследований.
- Рекомендации: приобретать решения, гарантирующие проведение исследований всей системы, даже если для запуска будет достаточно мини-исследований

Аутсорсинг

1) *Вступает в силу 01.10.2025* Указание Банка России от 22 октября 2024 года № 6906-У) Положение Банка России от 8 апреля 2020 года о внесении изменений № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе».
Глава 8, Приложение 6 к положению 716-п (управление риском аутсорсинга, включая процедуры организации аутсорсинга)

2) *Письмо Банка России от 19.08.2025* о передаче критически важных процессов на аутсорсинг
https://cbr.ru/Crosscut/LawActs/File/10071

Аутсорсинг (предпосылки)

1) Сложность внедрения криптографических решений в существующую инфраструктуру банка и последующей их эксплуатации

- финансовая.
- кадровый дефицит

Наши рекомендации:

- Размещение компонентов системы у поставщика и передача поставщику функций по эксплуатации и сопровождению данных компонентов не должны снижать уровень защищенности системы по отношению к уровню защищенности этой же системы при ее полноценном размещении в банке.
- Решение поставщика должно обеспечивать соблюдение требований законодательства, требований регуляторов и эксплуатационной документации на компоненты системы.
- Решение поставщика услуг по своей оснащенности, предоставляемому уровню безопасности, доступности и отказоустойчивости должно соответствовать уровню решений крупных банков. При этом использование решения банком не должно требовать увеличения штата сотрудников, отвечающих за информационную безопасность и ИТ-эксплуатацию.
- Использование решения поставщика должно снижать риски, связанные с возможным сговором работников банка или сговором работников поставщика. Не стоит сосредотачивать все значимые компоненты системы на одной стороне, необходимо распределять их между поставщиком решения и банком.
- Между банком и поставщиком должны быть четко определены их зоны ответственности.

2) Основные преимущества использования решений поставщиков для банков:

- Доступ к экспертизе: поставщики специализируются на конкретных областях информационной безопасности, что позволяет банкам получать доступ к экспертным знаниям и опыту, которые могут быть недоступны в штате.
- Снижение рисков: Опытные поставщики имеют отработанные процессы и процедуры, что снижает риски, связанные с информационной безопасностью.
- Экономия на затратах на оборудование и персонал: нет необходимости держать в штате большое количество сотрудников, необходимых для эксплуатации криптографически защищенных систем высоких классов защиты с соблюдением всех требований ЭД и регуляторов.
- Улучшение качества обслуживания клиентов: передача на сторонней организации функций, не связанных с основными направлениями своей деятельности, позволяет банкам сосредоточится на своей ключевой деятельности, уделять большее внимание разработке новых финансовых продуктов и укреплению позиций на рынке.

Стоимость ИБ и инфраструктуры (БЕЗ ПО)

Инхаус	Гибрид (аутсорсинг)	
ЦОД Банка	ЦОД поставщика	ЦОД Банка
Без резерва: от 60 млн	Геокластер + ЗО КИИ: 25 млн	+ Без резерва: от 15 млн
Холодный резерв: от 70 млн	Геокластер + ЗО КИИ: 25 млн	+ Холодный резерв: от 20 млн
Горячий резерв: от 110 млн	Геокластер + ЗО КИИ: 25 млн	+ Горячий резерв: от 35 млн
Кластер в одном ЦОД: от 130 млн	Геокластер + ЗО КИИ: 35 млн	+ Кластер в одном ЦОД: от 40 млн
Геокластер 1N+1N: от 170	Геокластер + ЗО КИИ: 35 млн	+ Геокластер 1N+1N: от 45 млн
Геокластер 2N+2N: от 220	Геокластер + ЗО КИИ: 45 млн	+ Геокластер 2N+2N: от 90 млн

современные системы

Преимущества гибридной модели (Аутсорсинг)

- 80% инфраструктуры размещается в ЦОД поставщика услуг аутсорсинга, что существенно экономит средства банка на закупку оборудования и ПО 3хлиц для выполнения требований по ИБ.
- Экономия банка на сотрудниках и сопровождении (количество сотрудников и их рабочее время, а также ежегодная закупка поддержки оборудования и ПО 3х лиц)
- ГОСТ 57580.1-2017 поставщик проводит аудит части размещаемой в ЦОД поставщика
- Производительное оборудование в георасределенном кластере.
- Доступ к ПлЦР 24/7.
- Реализация инфраструктуры с учетом требований ЗО КИИ
- Можно использовать любой из 4-х доступных стендов: Тест1 с эмуляторами, Тест2 для ТИВ и пользовательского тестирования, Прод, Резерв
- Сокращение сроков проекта в 2 раза
- Масштабируемость без дополнительных затрат (При повышении нагрузки при увеличении количества операций, инфраструктуры реализуется силами Современных Систем, что при размещении в инхаус увеличивает затраты банка)
- Выполнение/Изменение законодательства – включено в поставку и не потребует дополнительных вложений
- Более высокий уровень информационной безопасности в части управления ключевой информации
- Распределенная технологическая инфраструктура позволяет выстроить более безопасную модель. Если злоумышленник атакует одну часть инфраструктуры, то не получит доступ к другой и наоборот, от чего невозможно защититься при размещении в инхаус, если, например, злоумышленник получил доступ к инфраструктуре банка или сотрудники банка вступили в сговор.
- Используется собственная защищенная СУБД (FT-Data) – уровень PostgrePro существенно увеличивает стоимость в Инхаус
- В Контуре Обработки на стороне ЦОД-поставщика добавлен HSM-модуль для работы с ключевой информацией. Прямых требований в 833-П нет
- СКЗИ уровня КВ для защиты каналов связи внутри инфраструктуры и между ЦОД для разных контролируемых зон
- Сокращение нагрузки на сотрудниках ИБ: 833-П требует доступ/эксплуатации в Контуре обработки и контуре контроля разными ответственными лицами на стороне банка, поэтому разные люди должны иметь доступ к Контуру Обработки и Контуру Контроля. Разделение контуров между ЦОД поставщика услуг аутсорсинга (Контур Обработки) и ЦОД банка (Контур Контроля) гарантирует выполнение этого требования как на физическом на и на организационном уровне, а также не требует увеличения штата на стороне банка
- Возможность построения выделенного канала связи между облаком и ЦОД банка (предоставляется на выбор 5 провайдеров) для дополнительной защиты от DDOS-атак.
- Организация канала между ЦОД банка и ЦОД поставщика услуг аутсорсинга (при наличии ЕБС канал уже есть) не ниже класса КС3.
- Сокращение затрат на привлечение сторонней организации по построению защищенной ИБ-инфраструктуры (настройка УЦ в кластерах, настройка МЭ в кластерах, настройка HSM, станции точного времени, др СКЗИ и СЗИ, сокращение затрат на проектирование и документирование. В среднем стоимость построения защищенной инфраструктуры для Инхаус варианта от 20 млн. руб. в кластерной конфигурации)
- Поставщик облака не может себе позволить принятия рисков, которые может принять банк в инхаус и гарантирует банку по договору как выполнение требований законодательства, так и SLA, требуемых со стороны банка
- Банку не требуется экономить на ручном выпуске сертификатов, так как предусмотрена инфраструктура под автоматический выпуск сертификатов (сервис автоматизации выпуска сертификатов)

Преимущества программного обеспечения применимые, как гибридной так и к Инхаус поставке

- Оценка влияния от поставщика контура обработки, контура контроля, а также модулей сервиса автоматизации выпуска сертификатов за свой счет. Банку не придется проходить многолетний дорогостоящий процесс с сертифицированной лабораторией.
- Протокол OpenIDConnect для взаимодействия с ЕСИА (аутентификация через Госуслуги) для выпуска сертификатов - входит в поставку.
- Модуль управления сертификатами и CAC (единственные на рынке).
- АРМ Мониторинга для службы сопровождения банка: Отслеживание рабоспособности каждого модуля, а не только в разбивке на операции разбивка
- На уровне программного кода реализована балансировка запросов в сторону узлов ТШ КБР. Не требуется покупать Nginx платной версии.
- В поставку может быть включена защищенная СУБД по цене в десятки раз ниже рыночной (FT-data)
- ПО для взаимодействия с СКЗИ класса КС3 есть в 2-х поставках: как компилируемые, так и интерпретируемые языки программирования (Java и C++). Банк может выбрать удобный для себя вариант, так как java накладывает необходимость покупки доп. СКЗИ, таких как защита от НСД
- Специализированная архивная БД для обеспечения долговременного хранения (не менее 5 лет) подписанных ЭП электронных сообщений и средств обеспечивающих проверку ЭП (согласно п.10 833-П), в том числе для передачи по запросу в ЦБ РФ
- Дистрибутивная интеграция с АБС ЦФТ-банк и ДБО Фактура. В рамках решения предоставляется API, что позволяет интегрироваться с любыми ИС Банка.
- Система маршрутизации позволяет настроить любое количество внешних систем в разрезе операций ФП/Клиентов, ЮЛ/ФЛ и другие фильтры
- КриптоСДК SDK. ЦР - библиотека для встраивания в МП для ФЛ и веб-приложения для ЮЛ
- Отслеживание таймингов, как на уровне банка, так и на уровне ПлЦР

Вопросы?

Елена Смышляева,
заместитель генерального директора
АО «Современные системы»
e.smyshljaeva@modernsys.ru
+7 925 376 65 27

современные системы