Защита инфраструктуры Цифрового Рубля для коммерческих банков под «ключ»

Бадмаева Римма

Назначение, возможности ЦР

Формы национальной валюты:

- Наличная
- Безналичная
- Цифровая

Цифровой рубль – цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег

Источник: официальный сайт Банка России

Назначение, возможности ЦР

Цифровой рубль - еще одно средство для платежей и переводов

Операции для граждан будут бесплатными до 100 тыс.р, далее см. тарифы http://www.cbr.ru/fintech/dr/doc_dr/tarif/

Операции для бизнеса – с минимальной комиссией

Цифровые рубли эквивалентны наличным и безналичным

Нормативные документы по Цифровому Рублю

Положения Банка России:

- «О платформе цифрового рубля» **№820-П** от 03.08.2023
- «О требованиях к обеспечению защиты информации для участников платформы цифрового рубля» **№833-П** от 07.12.2023

Стандарты платформы цифрового рубля:

- Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля. Версия 1.2
- ЦВЦБ. Требования по обеспечению информационной безопасности для Финансового посредника
- и другие, см. http://www.cbr.ru/fintech/dr/doc_dr/standarts/

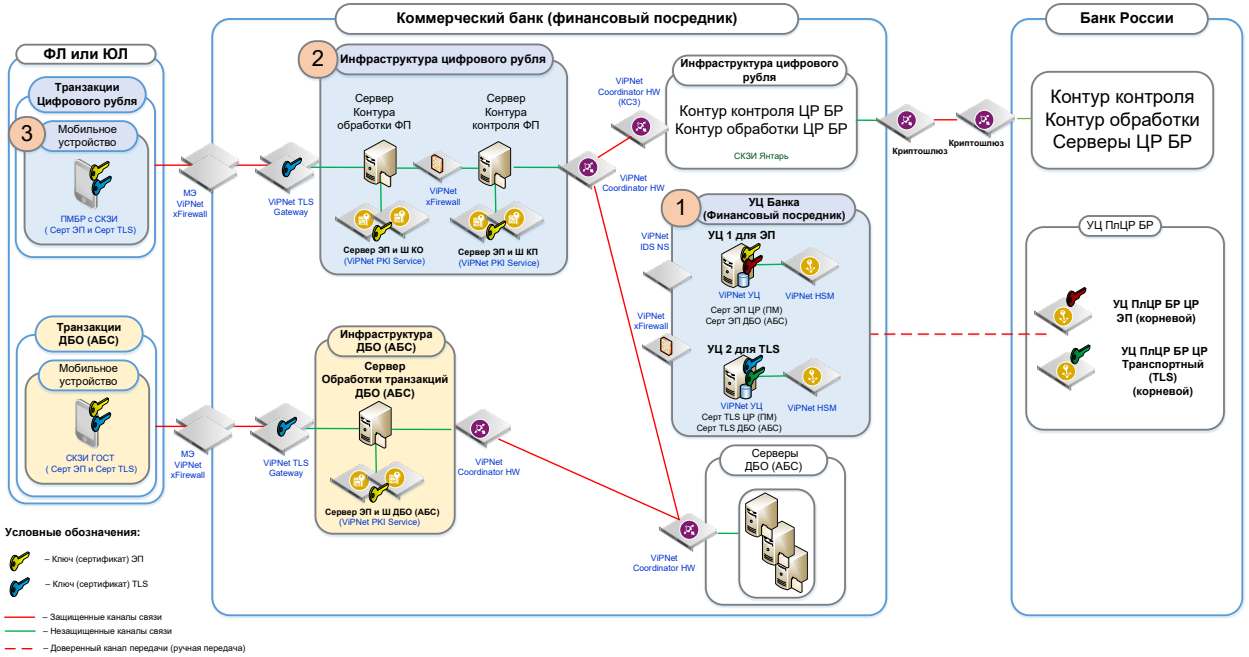
Роли сторон в платформе ЦР

Оператор платформы	Участники платформы (Финансовые посредники)	Пользователи платформы (физ и юр лица)

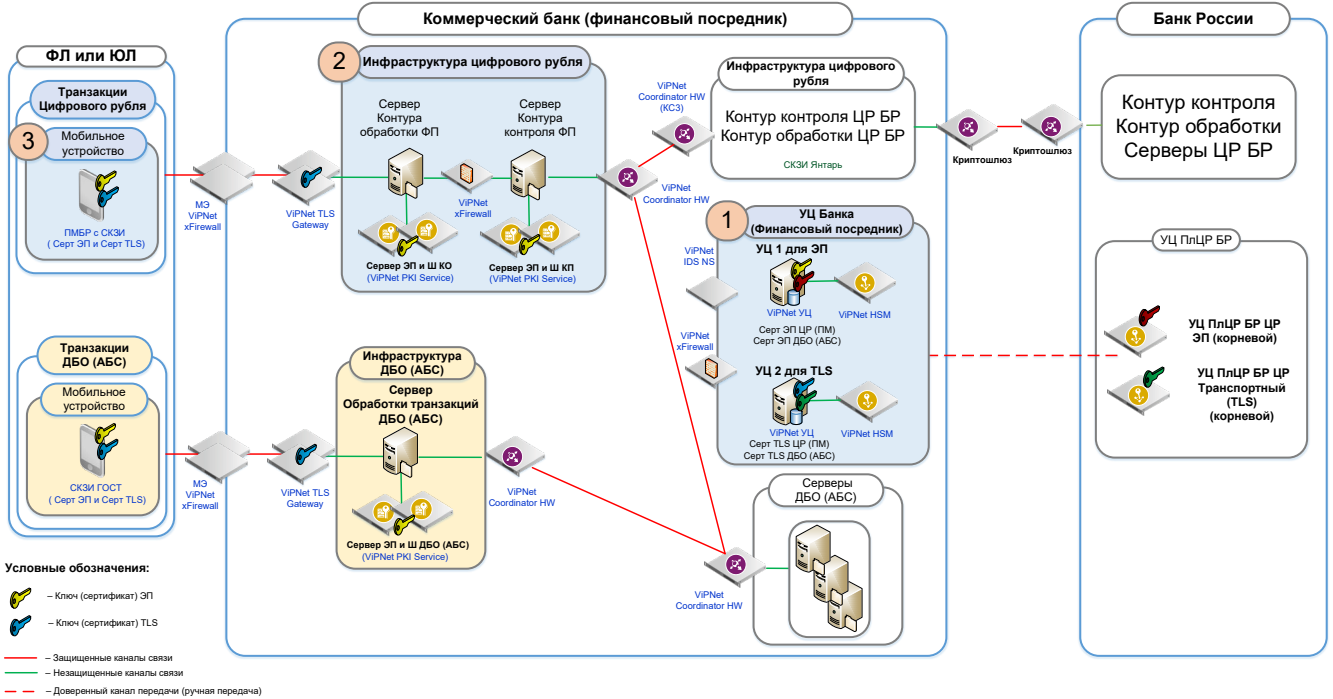
ТЕХНО infotecs 2024 ФЕСТ

Продукты ViPNet для защищенного взаимодействия участников платформы Цифрового рубля

Продукты ViPNet для защищенного взаимодействия участников платформы Цифрового рубля



Сегмент Пользователь – финансовый посредник



ПМ БР – программный модуль Банка России

Основа:

- Ядро - СКЗИ ГОСТ (ViPNet OSSL, КриптоПро CSP, Валидата CSP)
- «Надстройка» в виде API для работы СКЗИ с мобильным приложением банка

Функции:

- Двусторонний TLS
- Подпись сообщений (транзакций)
- Шифрование/расшифрование сообщений (транзакций)

ПМ БР – программный модуль Банка России

ПМ БР (с ViPNet OSSL) – разработка АО «ИнфоТеКС» по заданию Банка России

ПМ БР - Исключительные права принадлежат Банку России

В 2023г. 9 из 13 банков выбрали ПМ БР с ViPNet OSSL

Где взять ПМ БР: обратиться в Банк России с заявкой

Сегмент Пользователь – Банк

На стороне банка:

- Двусторонний TLS
- TLS шлюз класса КС2 (п.14.2, абз 6, 833-П, вступают в силу с.1.01.2025)

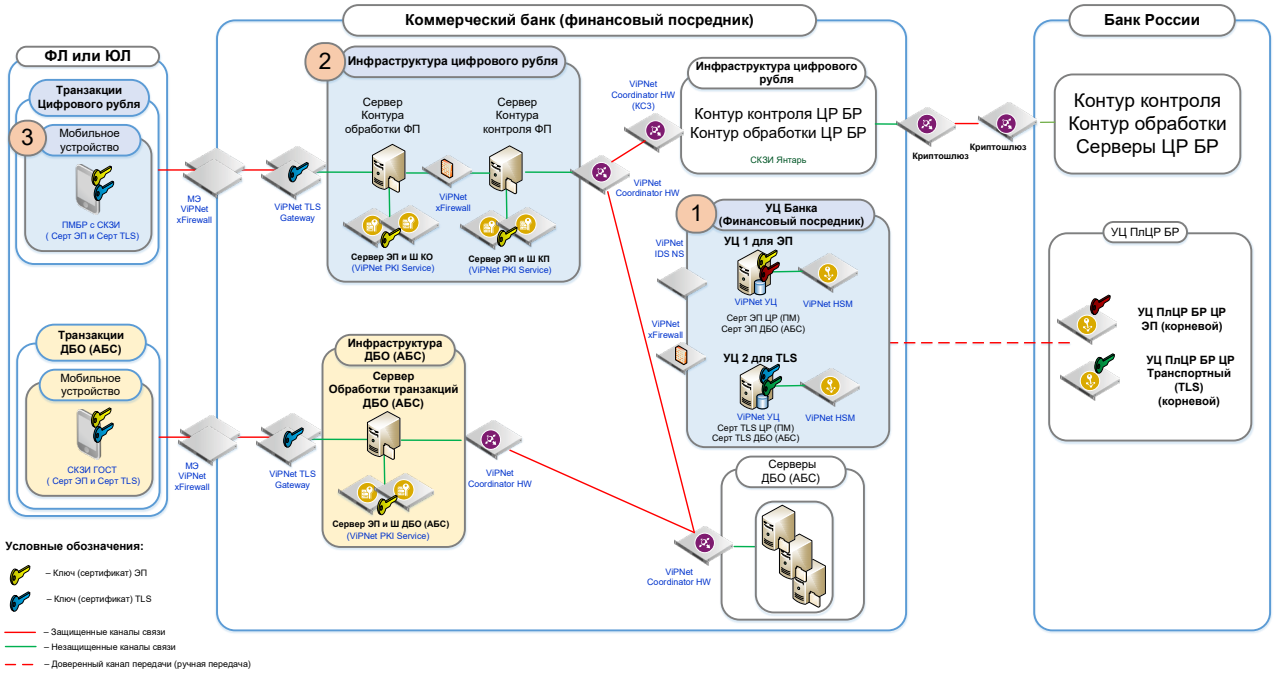
На устройстве пользователя:

- Двусторонний TLS КС1 (п.14.2, абз.6, 833-П, вступают в силу с.1.01.2025)
- СКЗИ класса КС1 (п.14.2, абз.3, 833-П, вступают в силу с.1.01.2025)

Ключевые преимущества ViPNet TLS Gateway

- Легитимная работа с любым СКЗИ на стороне пользователя (ViPNet, КриптоПро, Валидата)
- Легитимная одновременная работа с ГОСТ-шифрованием и RSA шифрованием, т.е. возможность работы с другими банковскими приложениями по иностранным криптоалгоритмам
- Высокая производительность по кол-ву одновременных подключений – гарантировано до 65 000
- Полная линейка продуктов PKI в отличие от других вендоров

Контур обработки.
Контур контроля



Контур обработки.
Контур контроля

Важные Нюансы

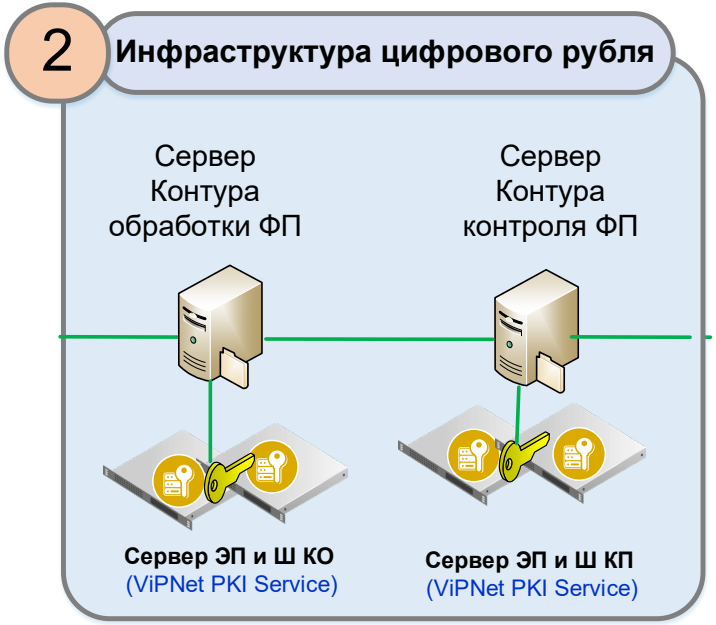
- две отдельных ЭП для контура обработки (КО) и контура контроля (КК) (п.4.1.2 порядка подключения)
- СКЗИ класса КС3 для проверки/простановки подписи и шифрования/расшифровки сообщений (транзакций)
- используется УНЭП (не нужна аккредитация УЦ)
- требуется оценка влияния (информация, защищаемая по закону)
- рассчитать производительность серверов подписи и шифрования

Контур обработки. Контур контроля

СЗИ:
- ViPNet PKI Service
- ViPNet PKI Client для АРМ Администратора

Решаемые в КО и КК задачи:
- Проверка/простановка ЭП
- Шифрование/расшифрование сообщений (транзакций)

Требования к серверу ЭП и Ш:
- УНЭП средствами ЭП не ниже КС3 (п.14.1, 833-П, вступают в силу с 1.01.2025)
- СКЗИ не ниже КС3 (п.14.1, 833-П, вступают в силу с 1.01.2025)



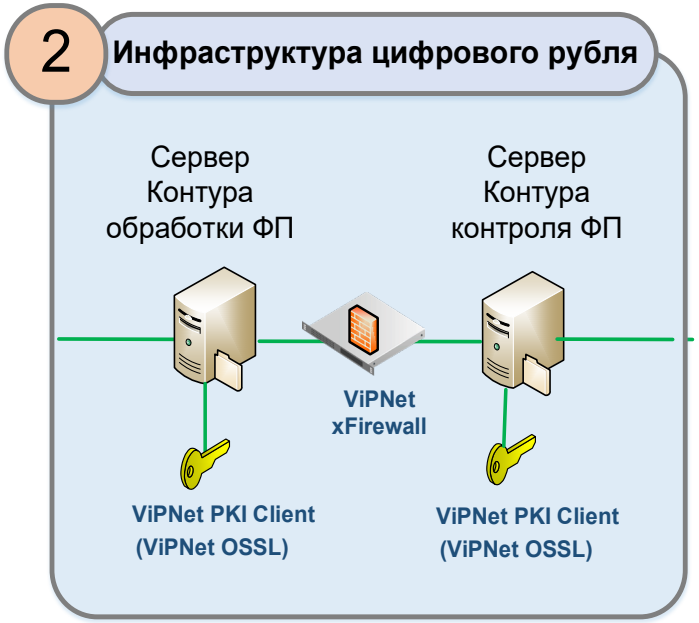
Ключевые преимущества ViPNet PKI Service

- Высокая производительность в сравнении с конкурентами
- Высокая надежность (СКЗИ от КС1 до КВ)
- Легитимная возможность использования неограниченного кол-ва сертификатов разных внешних систем (например, сертификата КО и сертификата КК на 1-ом PKI Service)
- Простота внедрения за счет наличия REST API для взаимодействия с сегментами КО и КК в отличие от сложного PKCS#11 в классическом HSM
- Существенная экономия за счет использования единой аппаратной платформы в сравнении с конкурентами, где надо использовать HSM в связке с доп приложением (например, КриптоПро HSM + КриптоПро DSS)
- ДСДР не нужны

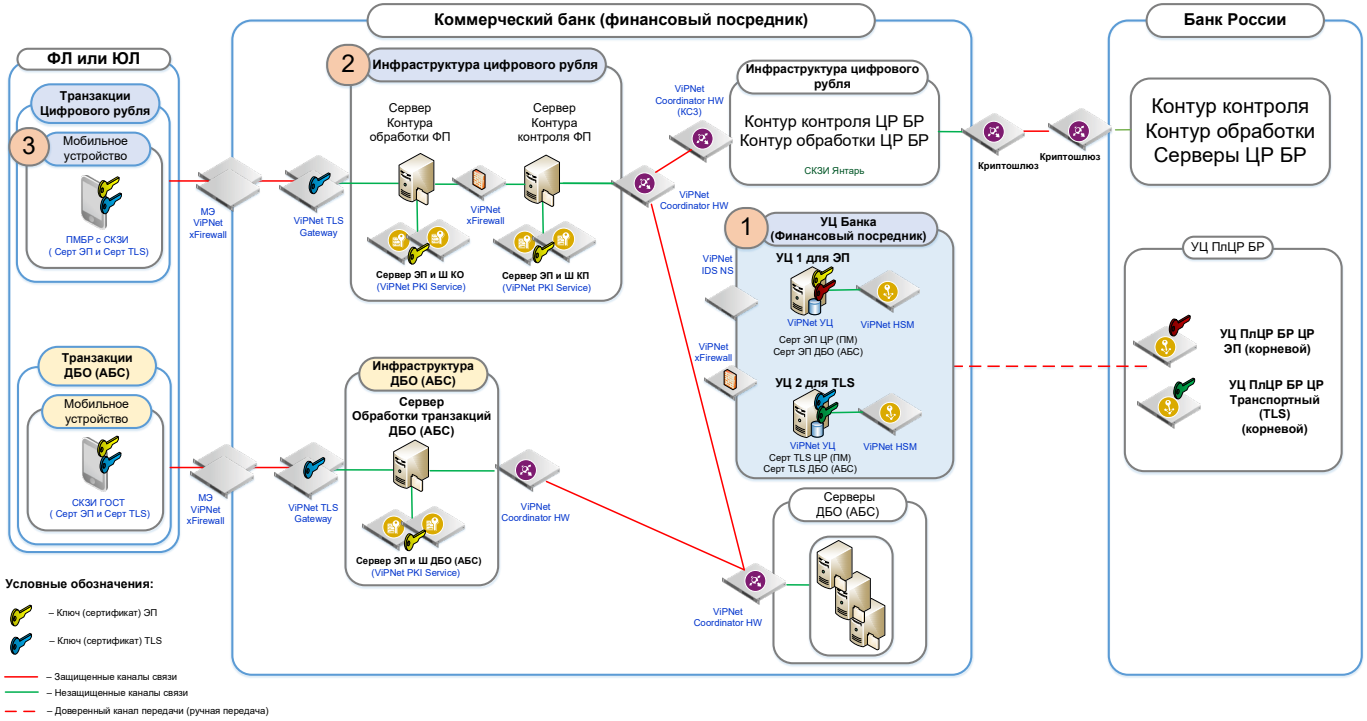
Контур обработки. Контур контроля

Комплектация ЭкстраЭконом:

- PKI Client или OSSL вместо PKI Service



Удостоверяющие центры



Удостоверяющие центры

Важные нюансы

- Два отдельных УЦ для сертификатов ЭП и сертификатов TLS
- Ключ УЦ должен хранится на внешнем носителе в неизвлекаемом виде (HSM, Токен)
- УЦ – класса КС3
- Аккредитация обоих УЦ не требуется

Удостоверяющие центры

СЗИ:

УЦ класса не ниже КС3 (п. 13.4, П-833)

Наличие HSM или токена для хранения ключа ЭП

Решаемые задачи:

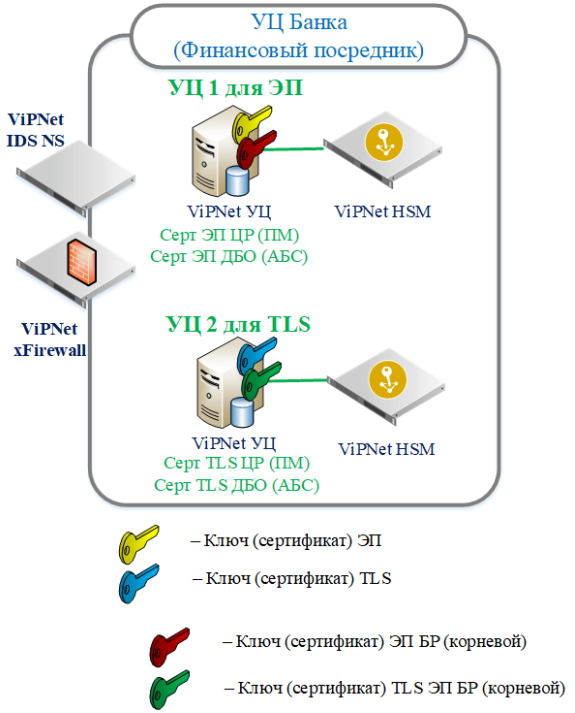
УЦ 1 - Выпуск сертификатов ЭП

УЦ 2 – Выпуск сертификатов TLS

Опционально:

IDS (СОА с сертификатом ФСБ)

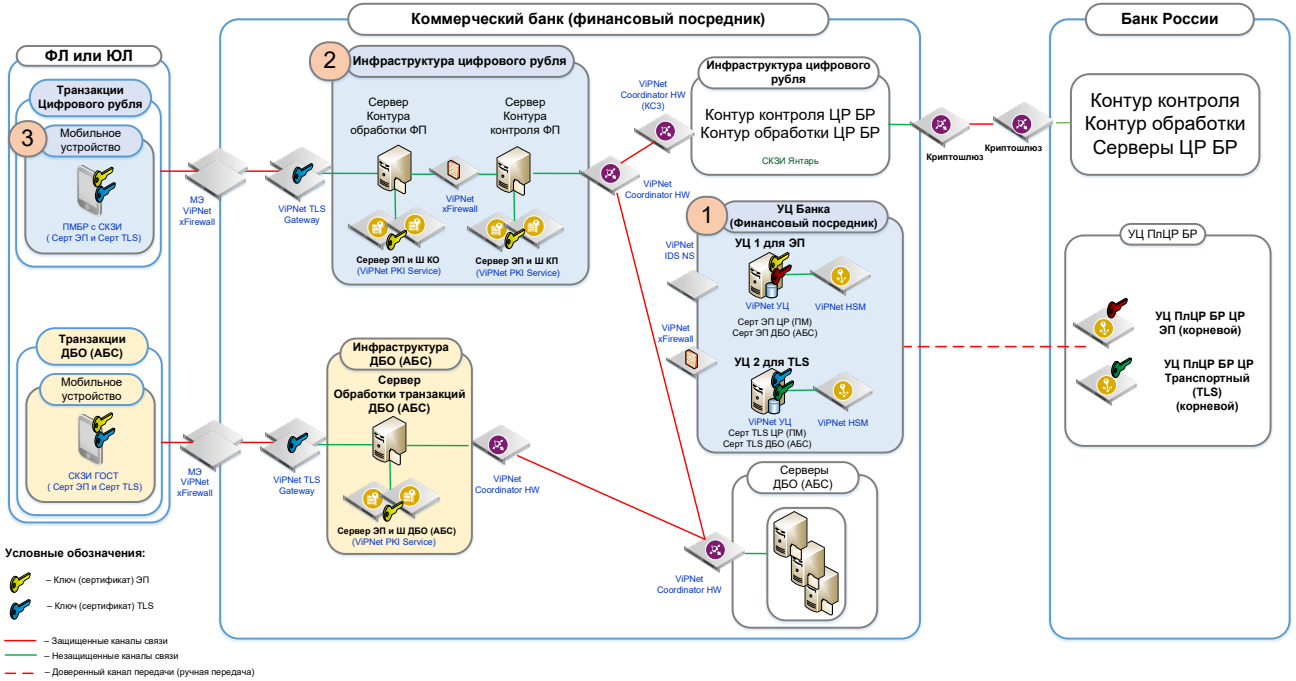
МЭ (класса не ниже 4 класса, ФСТЭК)



Ключевые преимущества УЦ ViPNet

- Низкая стоимость ядра УЦ – от 345 000 рублей
- Низкая стоимость владения УЦ, стоимость лицензии на 1 ЭП – 10 рублей
- Возможность работы с HSM и ТОКЕНОМ

Дополнительные СЗИ для инфраструктуры ЦР банка



Дополнительные СЗИ для инфраструктуры ЦР банка

СЗИ и решаемые задачи:

- ViPNet IDS – СОВ и/или СОА (для УЦ)
- ViPNet xFirewall – межсетевой экран для разделения выделения сегментов ЦР внутри инфраструктуры банка
- ViPNet Coordinator HW – для защиты трафика ЦР в инфраструктуре банка

Coordinator HW VA

xFirewall VA

* Требования к СЗИ определяется в соответствии с моделью угроз и нарушителя безопасности информации для АС банка

Работы встраиванию и оценки влияния ПМ БР в МП ФП, КО и КК

Стандарт. Порядок подключения Финансового посредника к Платформе Цифрового Рубля.

- Получить ПМ БР и выполнить **встраивание ПМ БР в Мобильное приложение ФП** в соответствии с порядком и требованиями на встраиваемый ПМ БР (П.3.4.2 Порядка подключения ФП)
- Проведение исследований по оценке влияния Мобильного приложения Финансового посредника на штатное функционирование ПМБР и СКЗИ

Требования по обеспечению информационной безопасности для Финансового посредника.

- **Требования к АС ФП** - Для реализации бизнес-процессов ЦР во внутренних АС ФП требуется проведение **оценки влияния среды функционирования СКЗИ** в соответствии с требованиями документации на используемое СКЗИ и (7) (п.3.2.3 Мероприятий ИБ к Требованиям). Заключение по результатам оценке влияния среды функционирования СКЗИ

Требования к Мобильному приложению ФП

- **Оценка влияния среды функционирования ПМ БР** на выполнение предъявленных к СКЗИ требований в соответствии с документом (п.3.2.7 Мероприятий ИБ к Требованиям)

Работы встраивания и оценки влияния ПМ БР в МП ФП, КО и КК

Аккредитованная испытательная лабораторией в системах сертификации ФСБ России и ФСТЭК России, имеющая право и опыт проведения тематических исследований (сертификационных испытаний) программных и программно-аппаратных средств на соответствие требованиям ФСБ России к средствам криптографической защиты информации

Варианты поставки

УЦ другого вендора в банке может работать с:

- ПМ БР с ViPNet OSSL
- ViPNet TLS Gateway
- ViPNet PKI Service

ПМБР с СКЗИ другого вендора в банке может работать с:

- ViPNet УЦ
- ViPNet TLS Gateway
- ViPNet PKI Service

УЦ, ПМБР, TLS GW другого вендора в банке может работать с:

- ViPNet PKI Service (!)

ТЕХНО 2024 infotecs ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети

vk.com/infotecs_news

https://t.me/infotecs_official

rutube.ru/channel/24686363