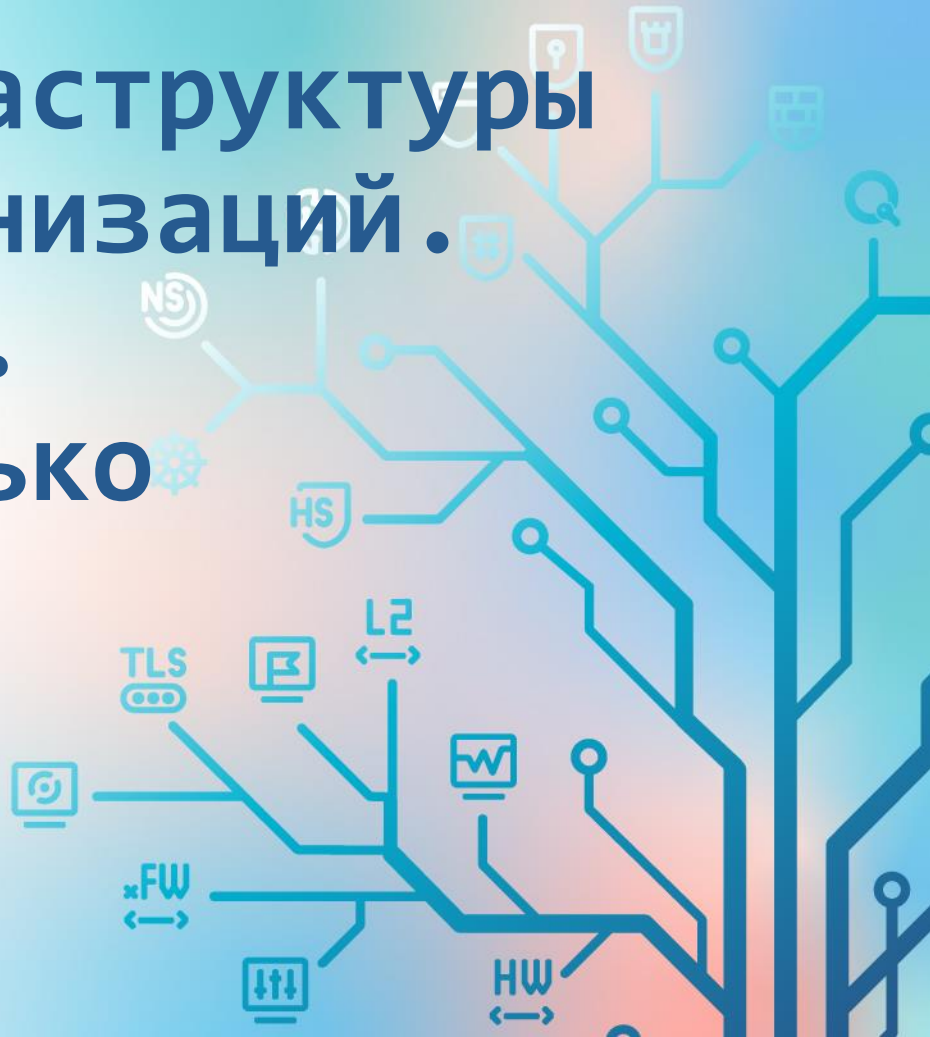
Защита ИТ-инфраструктуры кредитных организаций. Цифровой рубль. 851-П и не только

Сергей Дурягин
вице-президент ИнфоТеКС

infotecs



Цифровой Рубль

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

Схема двухуровневой розничной модели цифрового рубля

*https://cbr.ru/fintech/dr/

Этапы реализации проекта

2021
Декабрь

Создание прототипа платформы цифрового рубля

2022

Тестирование прототипа платформы цифрового рубля и разработка дорожной карты по внедрению с учетом результатов тестирования

Разработка законодательства для внедрения цифрового рубля

2023
Август

Старт пилотирования операций с реальными цифровыми рублями с привлечением узкого круга клиентов 13 банков
9 банков выбрали ПМ БР производства ИнфоТеКС

2024
Сентябрь

Расширение параметров пилота с возможностью подключения до 9 тысяч человек и до 1200 компаний

Этапы реализации проекта

2025
Июль

Госдумой принят закон о поэтапном запуске банками и торговыми компаниями возможности оплаты цифровым рублем:

- ***с 1 сентября 2026 года*** – крупнейшие банки (18 банков) и торговые компании, которые являются клиентами крупнейших банков и выручка которых за прошедший год превышает 120 млн рублей
- ***с 1 сентября 2027 года*** – банки с универсальной лицензией и их клиенты – торговые компании с годовой выручкой свыше 30 млн рублей
- ***с 1 сентября 2028 года*** – остальные банки и продавцы с выручкой менее 30 млн рублей в год*

**Обязанность принимать оплату цифровыми рублями не будет распространяться на торговые точки, чья выручка за год составляет менее 5 млн рублей*

Цифровой рубль сегодня

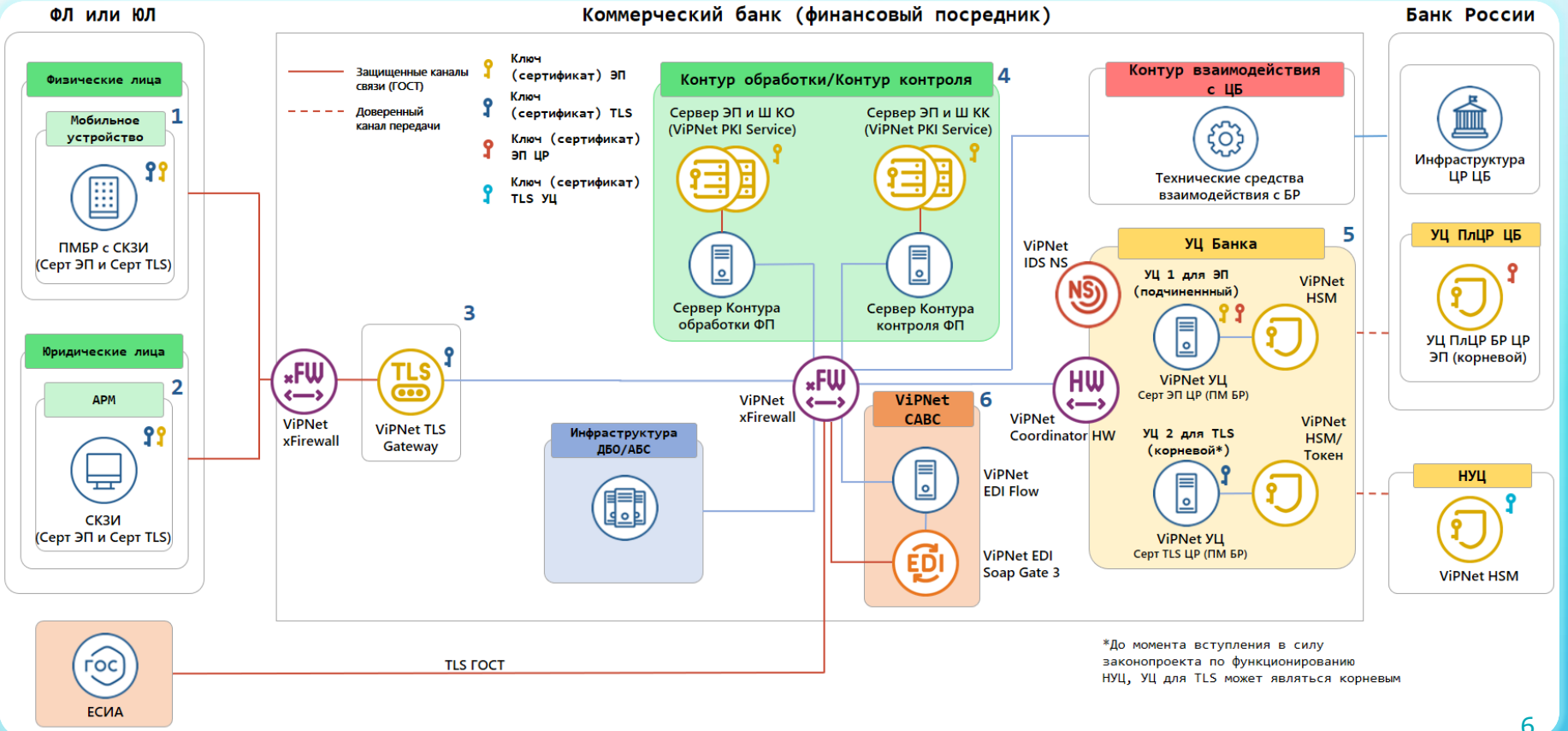
15 банков – участники пилота с реальными цифровыми рублями

+27 банков заключили договор с Банком России и настраивают свои системы для участия в пилоте

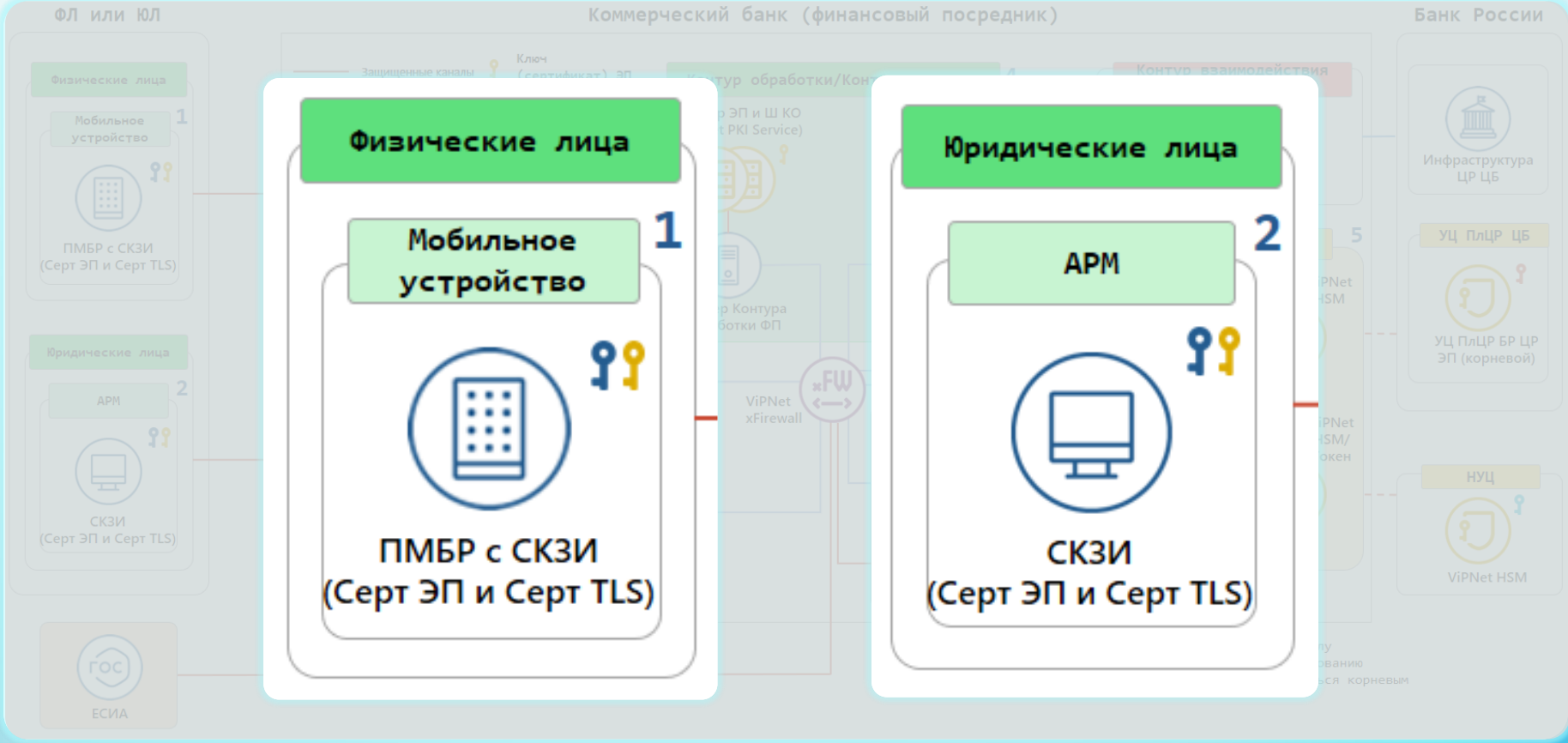
19 банков – участники проекта, выбрали ПМ БР с ViPNet OSSL

7 банков уже выбрали СФБ Лаб для проведения ОВ (5 банков планируют обратиться в нашу ИЛ)

Общая схема инфраструктуры ЦР



1.Сегмент Пользователя



ПМ БР: опыт ИнфоТеКС

ПМ БР (с ViPNet OSSL) – разработка ИнфоТеКС по заданию Банка России*

**исключительные права принадлежат Банку России*

Важно:

Требуется проведение оценки влияния мобильного приложения банка в составе с ПМ БР на СКЗИ ViPNet OSSL

Функции:

- Создание запросов на сертификат
- Организация TLS-соединений
- Подпись сообщений
- Шифрование/расшифрование сообщений

Основа:

- Ядро – сертифицированное СКЗИ ГОСТ **ViPNet OSSL**
- «Надстройка», реализующая API для работы СКЗИ с мобильным приложением банка

ViPNet OSSL – универсальная криптобиблиотека

Сценарии применения:

- Одно банковское приложение с интегрированным ПМ БР с одним СКЗИ:
  - ✓ для защиты операций с цифровым рублем
  - ✓ для защиты финансовых операций (851-П) NEW
  - ✓ для защиты операций с биометрией (ЕБС) NEW
- Защита открытых API (открытых банковских интерфейсов)
- Произвольные сценарии криптографической защиты

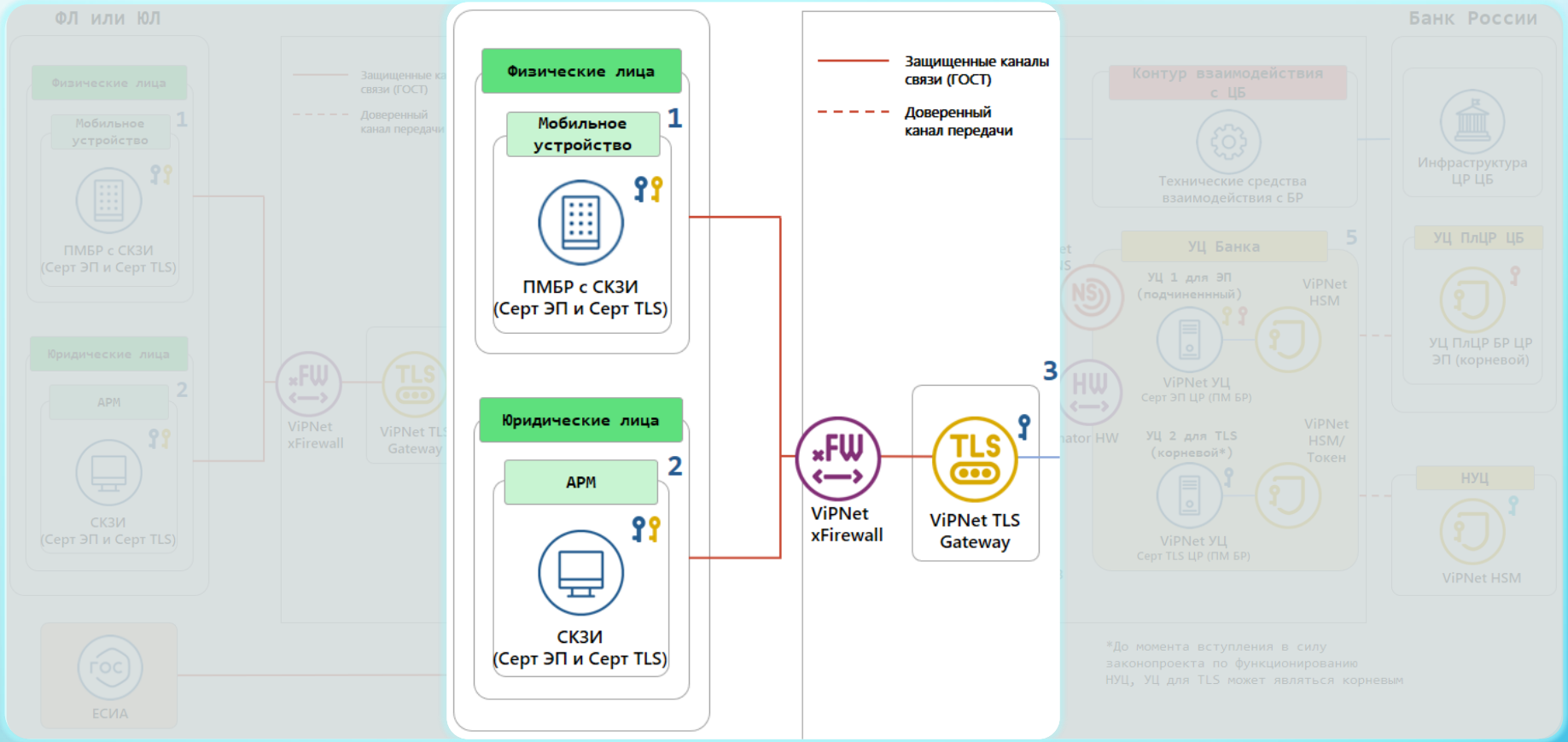
ViPNet OSSL – эксклюзивная стоимость

Количество	Цена, руб.	Стоимость, руб.	Тип
40 000 000	1,00	40 000 000,00	1 год
20 000 000	1,80	36 000 000,00	1 год
10 000 000	3,00	30 000 000,00	1 год
5 000 000	5,00	25 000 000,00	1 год
2 000 000	8,00	16 000 000,00	1 год
1 000 000	12,50	12 500 000,00	1 год
500 000	20,00	10 000 000,00	1 год
100 000	55,00	5 500 000,00	1 год
50 000	95,00	4 750 000,00	1 год

В реестре российского ПО!!!

Сертификация ФСБ России по классам: КС1, КС2, КС3

1-2-3.Сегмент Пользователь – Банк



ViPNet TLS Gateway

Шлюз безопасности для организации TLS-соединений

Функции:

- Поддержка отечественных и иностранных криптоалгоритмов (ГОСТ, RSA, ECDSA)
- Односторонние и двухсторонние ГОСТ TLS-соединения
- Легитимная работа с любым СКЗИ у пользователя (ViPNet, КриптоПро, Валидата)
- Автоматическое поддержание списков аннулированных сертификатов (CRL), поддержка OCSP

Смотрите реестр Минпромторга при выборе решения (ПАКов)

ViPNet TLS Gateway Характеристики

Рекомендации:

- выбирать ПАК из расчета перспективной нагрузки, а не тестовой
- использовать горячий резерв с возможностью балансировки нагрузки

Характеристика	Значение
Количество единовременных соединений, ГОСТ	до 155 000
Возможность кластеризации	до 64 нод в кластере
Варианты исполнения	ПАК (СКЗИ КС3) VA (СКЗИ КС1)

Цена комплекта – 4,18 млн рублей, в том числе:

- ✓ ПАК ViPNet TLS Gateway 550 – 0,54 млн рублей
- ✓ Лицензия 5000 пользователей – 3,64 млн рублей

ViPNet TLS Gateway
Пример внедрения

Расчет количества ViPNet TLS Gateway для 1-го из банков в топ-2:

- Пиковая нагрузка в пилотном проекте – 65 000 соединений / в секунду
- ViPNet TLS Gateway – 155 000 соединений / в секунду

65 000 Соединений в секунду (пиковая нагрузка) / 155 000 Соединений в секунду (производительность TLS Gateway) = 1 штука + 1 штука в кластер ViPNet TLS Gateway

Возможности масштабирования и резервирования:

- геораспределенное резервирование ЦОД – РЦОД
- кластер в ЦОД и РЦОД
- контур для тестирования

4. Контур обработки/ Контур контроля

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)
- СКЗИ не ниже КС3 (п.14.1, 833-П)

Оценка влияния СКЗИ в КО и КК

4. Контур обработки/ Контур контроля

Новости облачных сервисов:

Dropbox ограничила безлимитное **облачное** хранилище из-за...
3dnews.ru › 1092038/dropbox-ogranichila-bezlimitnoe...
Служба **облачного** хранения данных Dropbox решила из-за злоупотреблений ввести ограничения на свой безлимитный тарифный план: вместо того, чтобы предоставлять пользователям «столько места, сколько необходимо», компания примет меры к...
Не найдено: уменьшение, бесплатного

Храните, сколько хотите: Google отменила спорный л...
dzen.ru › a/ZCxBu4293D164kZI
Подписчиков: 181,2 тыс.
Компания Google изменила ограничения, которые действуют для пользователей фирменного...
Не найдено: уменьшение, бесплатного

Microsoft в три раза **уменьшила размер облачного** хранилища...
ixbt.com › news/2016/05/07/microsoft-v-tri-raza-...
Бесплатно в OneDrive теперь можно получить лишь 5 ГБ. Среди самых популярных **облачных** сервисов для хранения данных самым «жадным» всегда был Dropbox. Пользователям, которые не желают платить за использование сервиса, доступно лишь 2 ГБ.
Не найдено: диска

Внимание! «Подмоченная» репутация облачных сервисов

ViPNet PKI Service

Сервер подписи, разработанный на базе ViPNet HSM

Особенности ViPNet PKI Service:

- Шифрование/расшифрование
- Простановка/проверка ЭП
- Высокая надежность (хранение ключей в неизвлекаемом виде)
- СКЗИ класса КВ, средство ЭП класса КВ2 (перекрывает класс КС3)
- ДСДР не нужны

**Оценка влияния на СКЗИ в КО и КК*

Цена ПАК ViPNet PKI Service – 3,15 млн рублей

ViPNet PKI Service
Характеристики

Ключевые особенности:

- Экономия – реализация всех функций в едином ПАК
- REST API – простота внедрения и последующего проведения оценки влияния
- Легитимная возможность работы с неограниченным количеством сертификатов разных внешних систем и пользователей (не применимо для КК и КО)

Производительность:

Размер сообщения/файла	Производительность на 1 ПАК
до 2 Кб	> 10 000 сообщений /секунду
до 100 Кб	> 4 000 файлов/секунду
до 1 Мб	> 700 файлов/секунду

Кластеризация:

Кластеризация	до 10 шт.

ViPNet PKI Service
Пример внедрения для КО и КК

Расчет количества ViPNet PKI Service для 2-х банков из топ-2:

- Пиковая нагрузка – 2700 транзакций / в секунду
- ViPNet PKI Service – 700 транзакций / в секунду

Важно: нагрузку по производительности на ViPNet PKI Service можно линейно увеличивать добавлением новых нод (по аналогии с ViPNet TLS Gateway)

2700
Транзакций в секунду
(пиковая нагрузка)

/

700
Транзакций в секунду
(производительность ViPNet PKI Service)

=

3,71 штуки
ViPNet PKI Service

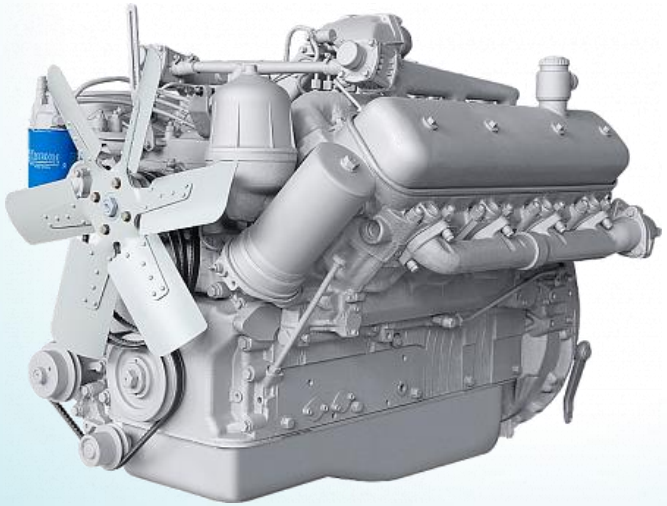
4 шт.(округляем 3.71) X 2 (КО+КК) X 2 ЦОДа = 16 шт. ViPNet PKI Service

СКЗИ для КО и КК

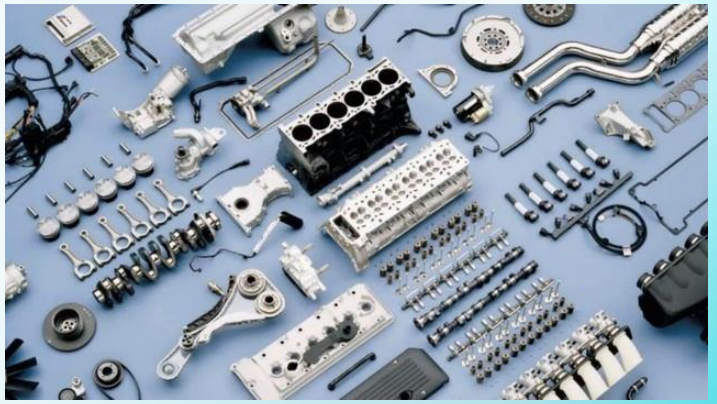
Комплектация решения для соответствия классу КС3

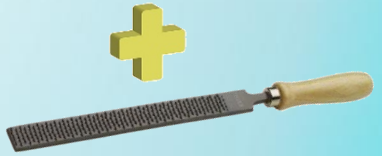
	Единый ПАК ViPNet PKI Service	Альтернативные решения на базе программных СКЗИ
СКЗИ класс КС3 (сертификат ФСБ России)	Да (КВ)	Да (КС3)
Операционная система с замкнутой программной средой (сертификат ФСБ России)	Не требуется	Требуется
Наличие АПМДЗ (сертификат ФСБ России)	Не требуется	Требуется
REST API	Есть	Отсутствует
Синхронизация версий и сроков сертификатов всех компонентов	Не требуется	Требуется

СКЗИ для КО и КК



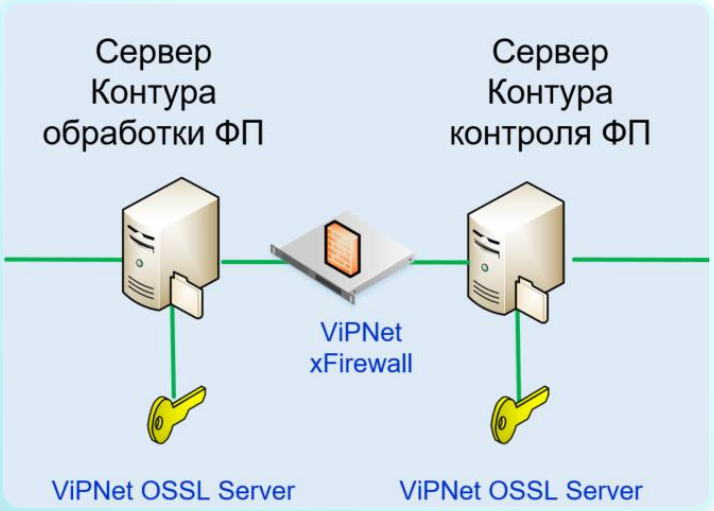
ViPNet PKI Service
Работает сразу!





Альтернатива.
Собрать и доработать
«напильником»

ViPNet OSSL Server (КС3) для КО и КК



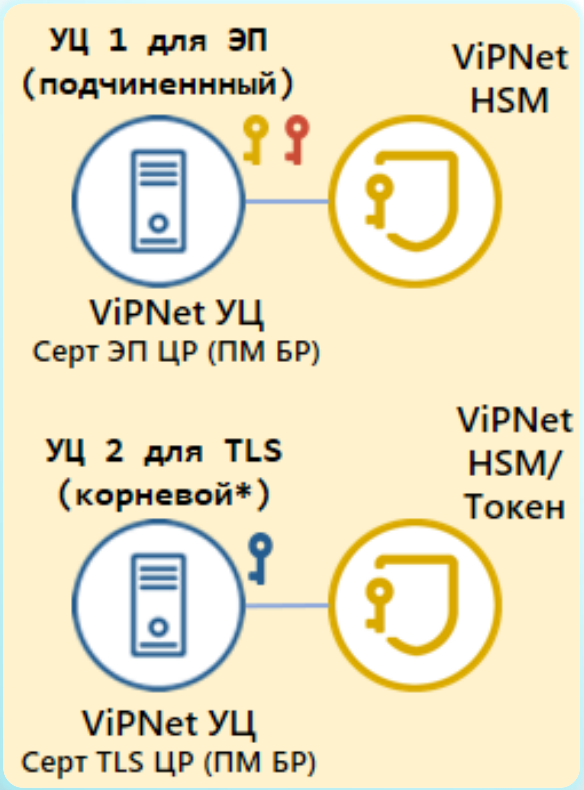
ПО ViPNet OSSL Server (КС3)*

- API со списком «белых» функций
- Требуются дополнительные СЗИ для защиты инфраструктуры

**Оценка влияния на СКЗИ в КО и КК*

ViPNet OSSL Server – 0,047 млн рублей

5. Удостоверяющие центры



Решаемые задачи:

- УЦ 1 – Выпуск сертификатов ЭП
- УЦ 2 – Выпуск сертификатов TLS

Опционально:

- HSM (хранение ключей на внешнем носителе в не извлекаемом виде)
- IDS (СОА с сертификатом ФСБ России)
- МЭ (класса не ниже 4 класса, ФСБ России)

ViPNet УЦ 4

Программный комплекс – ViPNet Удостоверяющий центр 4

В реестре российского ПО

Класс защиты КС2, КС3

Сертификат ФСБ России
до 28.02.2026

ViPNet УЦ 4

- выпуск сертификатов УКЭП
- выпуск сертификатов УНЭП ЦР
- выпуск сертификатов УНЭП (851-П)
- выпуск сертификатов безопасности (TLS)
- API для работы с внешними системами

Ведем работу по продлению сертификата ФСБ России до декабря 2026!!!

ПК ViPNet УЦ 4 – 0,174 млн рублей

Продления сертификатов на УЦ для Windows

Продление сертификатов на «КриптоПро УЦ» версии 2.0 (исполнения 5, 6, 9, 10)

Главная

Публикация: 11 Июль 2025 - 09:01

Мы получили новые сертификаты соответствия ФСБ России на программно-аппаратный комплекс «КриптоПро УЦ» версии 2.0 (исполнения 5, 6, 9, 10). Сертификаты действительны до 15.01.2026.

С полным перечнем сертификатов соответствия на наши продукты вы можете ознакомиться в соответствующем разделе нашего сайта.

ViPNet HSM

ПАК ViPNet HSM

- СКЗИ, класс КВ
- работа в кластере
- работа с ViPNet УЦ «из коробки»
- поддержка иностранной криптографии

ПАК ViPNet HSM – 2,58 млн рублей

О смене поколений ViPNet УЦ

Эпизод 4: ViPNet УЦ 4

Эпизод 5: ViPNet УЦ 5

ViPNet УЦ 5

Программно-аппаратный комплекс (ПАК) – ViPNet Удостоверяющий центр 5

Получение сертификата
ФСБ России ~ Q1 2026 года

ПАК ViPNet Удостоверяющий центр 5

- HSM – ядро ПАКа УЦ 5
- выпуск сертификатов ЭП
- выпуск сертификатов безопасности (TLS)
- REST API для работы с внешними системами

ПАК ViPNet УЦ 5 – 2,8 млн рублей

Upgrade с ПК УЦ 4 до ПАК УЦ 5 – 2,4 млн рублей

ViPNet УЦ, ViPNet HSM, ViPNet PKI Service Примеры внедрения для УЦ

УЦ ИнфоТеКС Интернет Траст (Госключ)

- 1,45 млн сертификатов* за 7 месяцев 2025

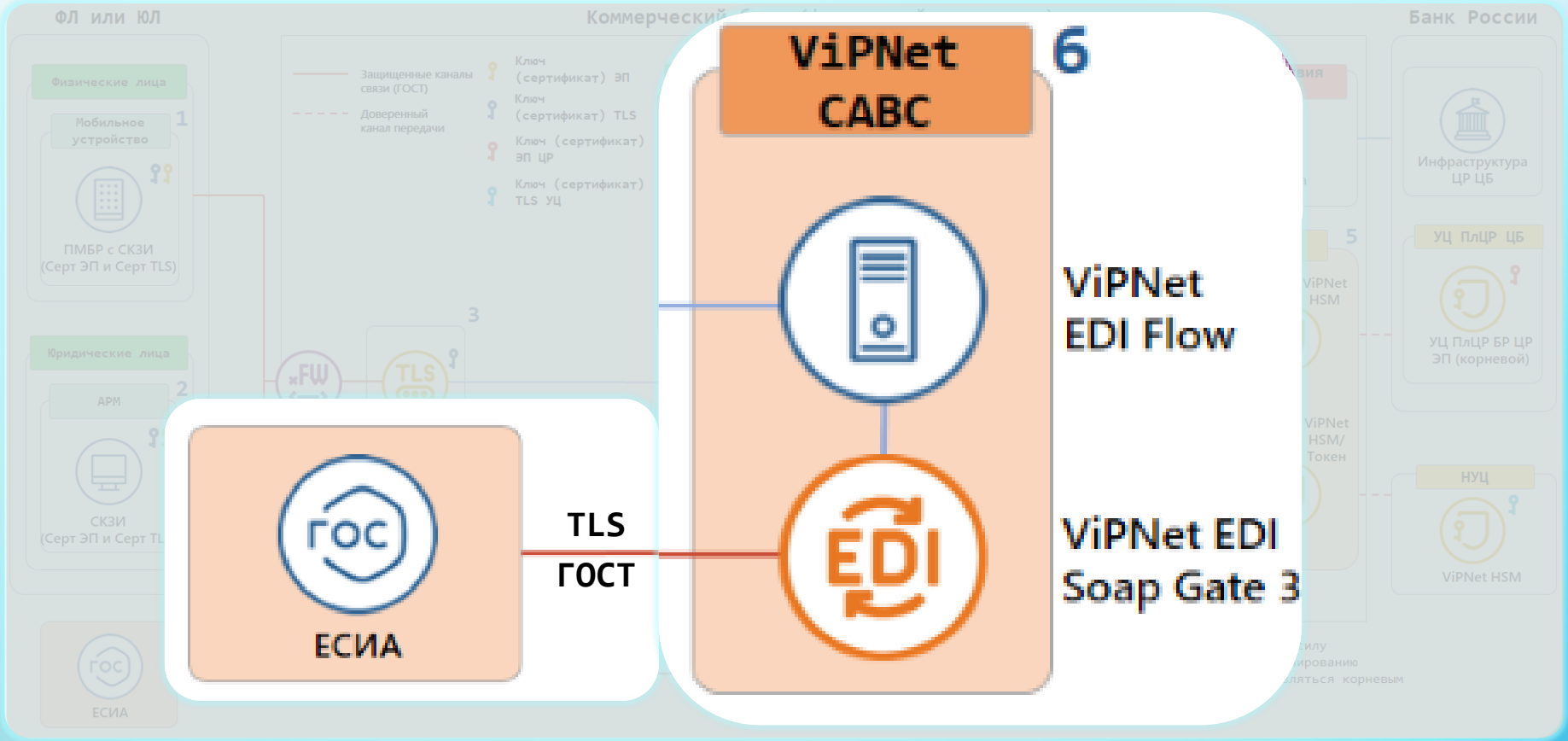
УЦ Федерального Казначейства

- 1,41 млн сертификатов* за 7 месяцев 2025

УЦ инфраструктуры цифрового рубля

** Данные телеграм-канала «Об ЭП и УЦ»*

6. Сервис автоматизации выпуска сертификатов (САВС)



6. Сервис автоматизации выпуска сертификатов (САВС)

ViPNet САВС

ПК ViPNet EDI Flow

Управление системой автоматизации выпуска сертификатов

ПАК ViPNet EDI Soap Gate 3

ПАК для взаимодействия с ЕСИА, СМЭВ, ЦПГ, ЕБС (1 кв. 2026)

Важно:

- Интеграция с ViPNet УЦ 4/УЦ 5
- Интеграция с КриптоПро УЦ
- Соответствует требованиям Банка России

ПК ViPNet EDI Flow

Программный комплекс для взаимодействия с ViPNet EDI Soap Gate, УЦ и ДБО

Выполнение процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователя ПлЦР

- Получение списков отозванных сертификатов и направление их в ПлЦР
- Интеграция с АС ДБО
- Форматно-логический контроль
- Регистрация событий
- Взаимодействие с ПАК ViPNet EDI Soap Gate

ViPNet EDI Soap Gate

ПАК для обмена электронными сведениями с применением электронной подписи

Функционал:

- Авторизация пользователей в ЕСИА
- Получение данных из ЕСИА
- Проставление и проверка подписи ГОСТ
- Построение TLS ГОСТ 1.2, 1.3
- Соответствует Регламенту ЕСИА 2.47 и Методическим рекомендациям ЕСИА 3.48

ПАК ViPNet EDI Soap Gate 1000 – 2,1 млн рублей

ViPNet EDI Soap Gate

ПАК для обмена электронными сведениями с применением электронной подписи

- СКЗИ КС3 и средство ЭП КС3 (для СМЭВ)
- Регистрация в Едином реестре российских программ для ЭВМ и баз данных №3276
- Зарегистрирован в реестре Минпромторга и реестре Минцифры
- Возможность интеграции с ИС без оценки влияния

ViPNet EDI Soap Gate

ViPNet EDI SOAP Gate – один ПАК и для САВС, и для СМЭВ, и для ЦПГ

Производительность SG2000 (САВС)

на 1 ПАК
100 сертификатов /секунду

Производительность SG2000 (ProxySMEV)

Размер сообщения	на 1 ПАК
до 1 Кб	900 запросов /секунду
до 100 Кб	200 запросов/секунду
до 1 Мб	35 запросов/секунду

Кластеризация (опыт СФР):

Кластеризация	10 шт.

Положение Банка России №851-П Страшное и ужасное в части СКЗИ?

Положение Банка России №851-П
29 марта 2025 вступило в силу
«Об установлении обязательных для кредитных организаций, иностранных банков, … требований к обеспечению защиты информации при осуществлении банковской деятельности…»

- Пришло на смену 683-П, обновляет и устанавливает новые требования к СКЗИ при осуществлении банковской деятельности

- **П.5.1**

При использовании УНЭП, в целях обеспечения целостности электронных сообщений, необходимо использовать сертифицированные ФСБ России средства ЭП и средства УЦ

Срок вступления в силу п.5.1 ***1 октября 2025 года***

Положение Банка России №851-П
Обзор от Владимира Голованова

Для поиска набрать «851»

В телеграм-канале «Криптография в финтехе»

851-П. На что стоит обратить внимание

- **П.5.2.1**

В случае использования ЕСИА необходимо соблюдать требования к обеспечению защиты информации при работе со СМЭВ и ЕСИА (572 ФЗ, приказ Минсвязи № 210, требования по подключению к ЕСИА)

- **П.5.3**

При использовании УНЭП, в целях подтверждения составления электронных сообщений, необходимо использовать сертифицированные ФСБ России средства ЭП и средства УЦ

- **П.6**

При осуществлении банковских операций необходимо обеспечивать защиту информации в соответствии:

- 152 ФЗ «О персональных данных»
- Постановлением Правительства РФ № 1119
- Положение ПКЗ-2005
- Приказом ФСБ России № 378
- Технической документацией на СКЗИ (в т.ч. о необходимости проведения оценки влияния)

851-П. Продукты ViPNet

Серверные компоненты ViPNet для выполнения требований 851-П:

- ПК ViPNet УЦ 4 (до декабря 2026)
- ПАК ViPNet УЦ 5 (со 2 квартала 2026)
- ПАК ViPNet PKI Service
- ПАК ViPNet TLS Gateway
- ПАК ViPNet EDI Soap Gate (СМЭВ, ЕСИА)
- ПО ViPNet OSSL Server

851-П. Продукты ViPNet

Клиентские компоненты ViPNet для выполнения требований 851-П:

- ПО ViPNet OSSL (мобильные устройства)
- ПО ViPNet PKI Client (мобильные устройства, АРМ для физических и юридических лиц)

851-П. Продукты ViPNet

Дополнительные продукты ViPNet для выполнения требований 851-П:

- ПАК ViPNet Coordinator HW 5 (VPN + NGFW)
- ПАК ViPNet xFirewall (NGFW)

Официальный канал ИнфоТеКС

Криптография в финтехе

Официальный канал ИнфоТеКС, посвященный защите информации в банковской сфере. Мы рассказываем о том, как с помощью криптографических операций, например, шифрования, электронной подписи, обеспечивается информационная безопасность современного финтеха.

Подписывайтесь
на наши соцсети,
там много интересного

infotecs

Дурягин Сергей