

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



Цифровой рубль сегодня



25 банков – участники пилота с реальными цифровыми рублями



+30 банков заключили договор с Банком России и настраивают свои системы для участия в пилоте

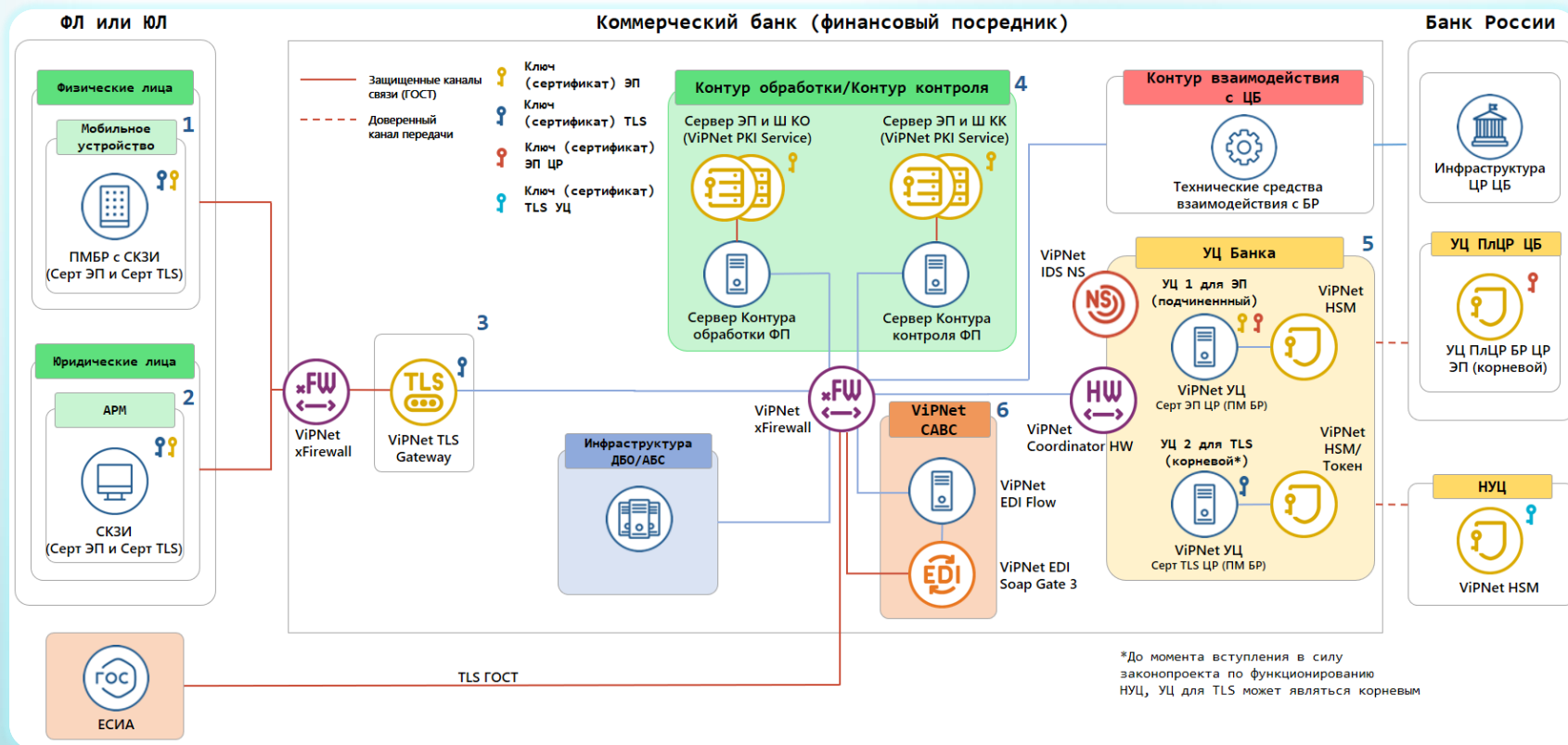


25 банков – участники проекта, выбрали ПМ БР с ViPNet OSSL



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

Общая схема инфраструктуры ЦР





ПМ БР: опыт ИнфоТеКС

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

**исключительные права принадлежат Банку России*

Функции:

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

Важно:

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



Основа:

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



VIPNet OSSSL – универсальная криптобиблиотека для финтеха

Сценарии применения:

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



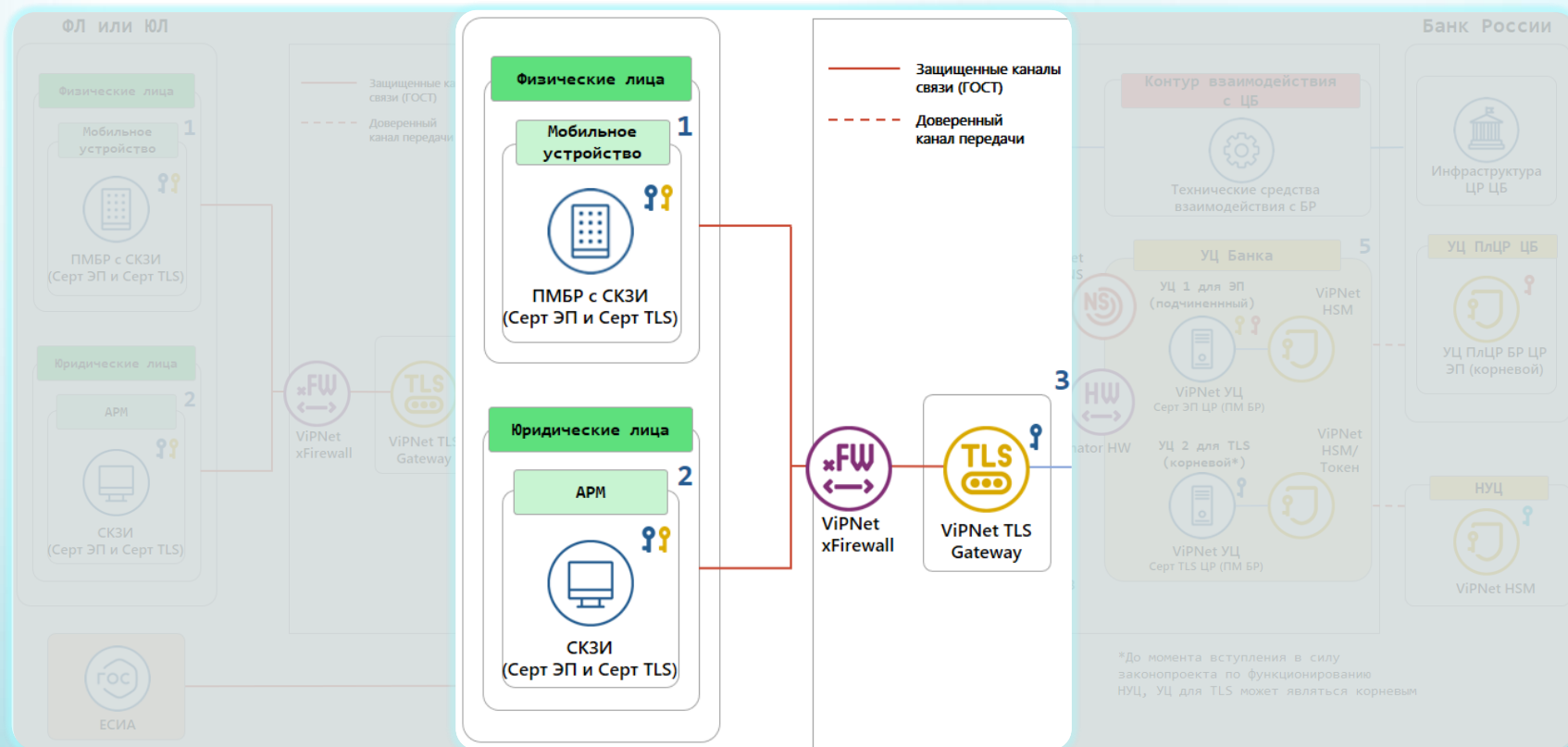
VIPNet OSSSL – ЭКСКЛЮЗИВНАЯ СТОИМОСТЬ

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



Цена комплекта – 4,8 млн рублей, в том числе:

- ✓ ПАК VIPNet TLS Gateway 550 – 0,62 млн рублей
- ✓ Лицензия 5000 пользователей – 4,18 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 + 2 штуки
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/простоявка ЭП
- Шифрование/расшифрование сообщений (транзакций)

Требования к серверу ЭП и Ш:

- УНЭП средствами ЭП не ниже КСЗ (п.14.1, 833-П)
- СКЗИ не ниже КСЗ (п.14.1, 833-П)

Оценка влияния СКЗИ в КО и КК



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 КСЗ)
- ДСДР не нужны

**Оценка влияния на СКЗИ в КО и КК*



Цена ПАК ViPNet PKI Service – 3,62 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)

Кластеризация:

Кластеризация	до 10 шт.
---------------	-----------

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



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)



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



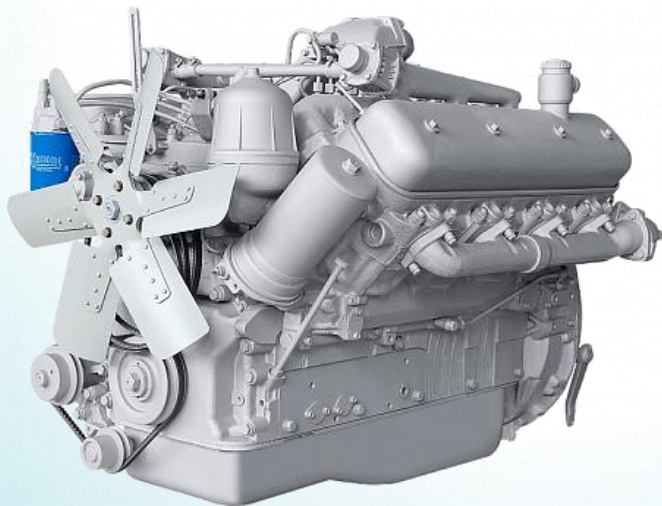
СКЗИ для КО и КК

Комплектация решения для соответствия классу КСЗ

	Единый ПАК ViPNet PKI Service	Альтернативные решения на базе программных СКЗИ
СКЗИ класс КСЗ (сертификат ФСБ России)	Да (КВ)	Да (КСЗ)
Наличие сервера	Не требуется	Требуется
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



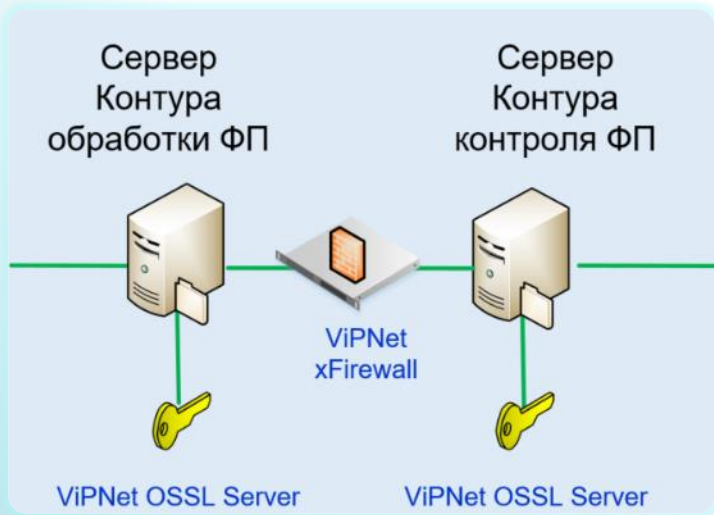
**ViPNet PKI Service
Работает сразу!**



**Криптобиблиотеки
(например, ViPNet OSSL)
организовать сервер,
собрать и доработать**



ViPNet OSSL Server (КСЗ) для КО и КК



ПО ViPNet OSSL Server (КСЗ)*

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

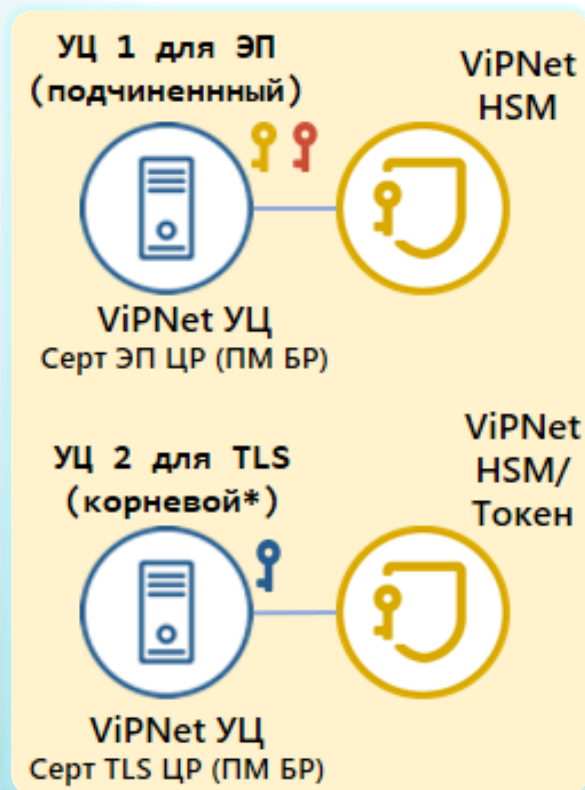


**Оценка влияния на СКЗИ в КО и КК*



ViPNet OSSL Server – 0,055 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 (COA 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 31.12.2026

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



*Продлили действие сертификата ФСБ
России до декабря 2026!!!*



ПК ViPNet УЦ 4 – 0,2 млн рублей

ViPNet HSM



ПАК ViPNet HSM

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



ПАК ViPNet HSM – 2,96 млн рублей

0 смене поколений ViPNet УЦ ViPNet УЦ 5

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



Получение сертификата
ФСБ России ~ Q3 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 – **3,1 млн рублей**

Upgrade с ПК УЦ 4 до ПАК УЦ 5 – **2,7 млн рублей**

VIPNet УЦ, VIPNet HSM, VIPNet PKI Service

Примеры внедрения для УЦ



УЦ ИнфоТекС Интернет
Траст (Госключ)

- 3,3 млн сертификатов*
за 2025г.



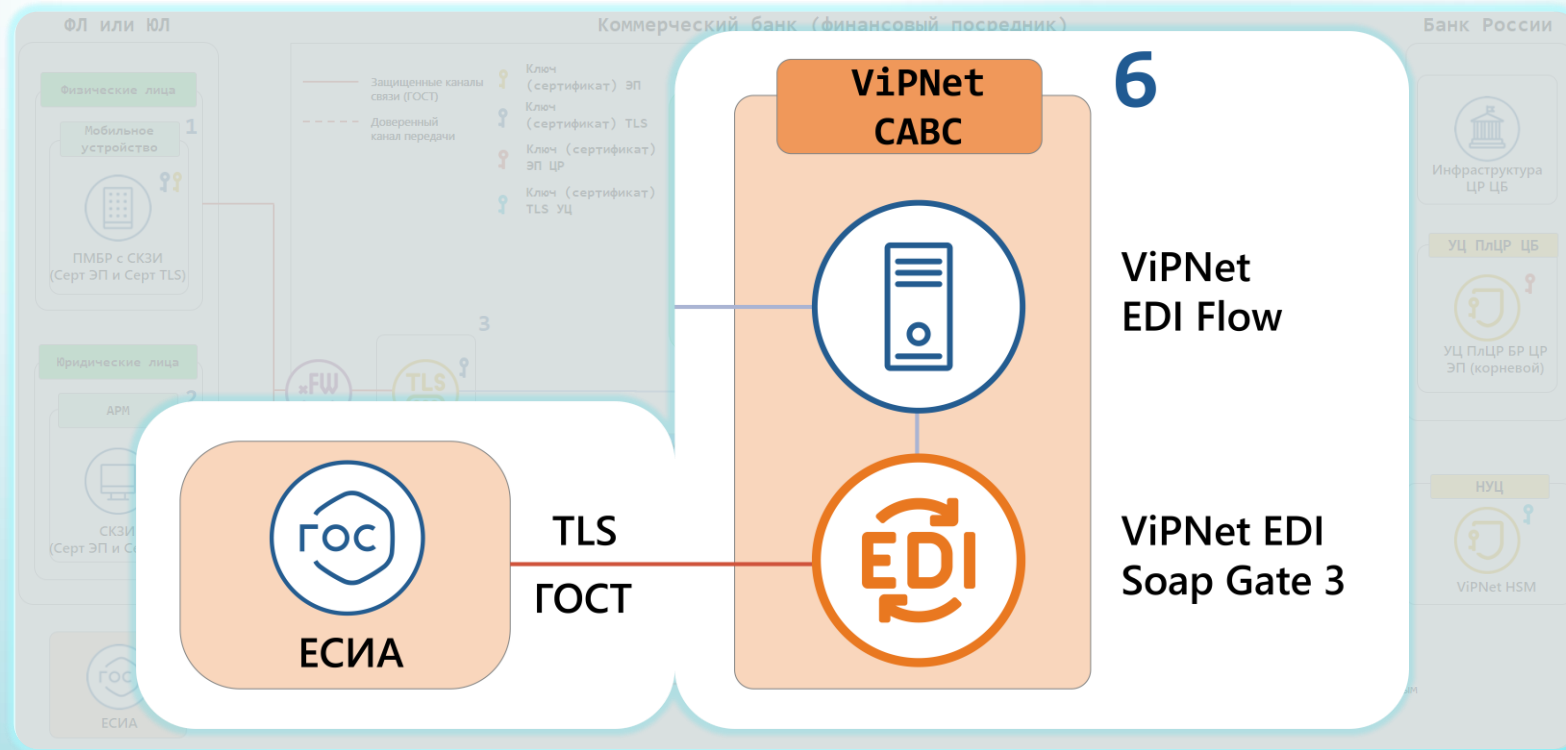
УЦ Федерального
Казначейства

- 2,6 млн сертификатов*
за 2025г.



УЦ инфраструктуры
цифрового рубля

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

инфотекс

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 – 2,3 млн рублей

VIPNet EDI Soap Gate

ПАК для обмена электронными сведениями с применением электронной подписи



- СКЗИ КСЗ и средство ЭП КСЗ (для СМЭВ)
- 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



Кластеризация (опыт СФР):

Кластеризация	10 шт.
---------------	--------

Производительность SG2000 (САВС)

на 1 ПАК

100 сертификатов /секунду

Производительность SG2000 (ProхуSMEV)

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

Положение Банка России №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 (с 3 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)

ИнфоТеКС – надежный производитель

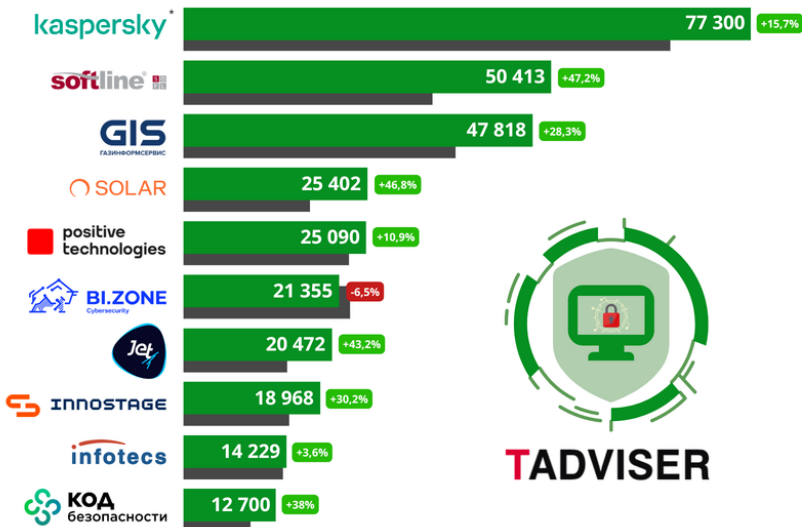
Крупнейшие поставщики решений в сфере информационной безопасности в России

по выручке за 2024 год (в млн рублей)

Динамика выручки 2024/2023

2024 год 2023 год

* - Глобальная выручка



TADVISER

ИнфоТекс – надежный производитель



>30

лет работы
на рынке



12

филиалов по
всей стране



>2000

сотрудников



>60

продуктов
для защиты
информации

> 400

партнеров
в регионах



Топ-10

крупнейших компаний
в сфере защиты
информации



>10 млн

рабочих станций,
защищенных
продуктами ViPNet



Топ-5

компаний по количеству
патентов в области
цифровых технологий

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 финтехе.



Подписывайтесь
на наши соцсети,
там много интересного




инфотекс



Самыловский
Александр

san@infotecs.ru
+7(915)315-56-08



Спасибо за внимание!

