

Новые требования ЕСИА и ЦПГ*

с 01.07.2025

для вновь подключаемых ИС

с 01.01.2027

для ранее подключенных ИС

с 01.04.2026

Данные ЦП через СМЭВЗ**

**Приняты Протоколом Президиума Правкомиссии от 18.07.2024 № 26пр утвержден действующий Регламент подключения к Инфраструктуре электронного правительства и Методические рекомендации ЕСИА.*

*** Письмо Минцифры России от 01.12.2025 N МШ-П24-117737 "О взаимодействии с инфраструктурой цифрового профиля"*

Регламент подключения к ИЭП 2.47 и Методические рекомендации ЕСИА 3.48 поэтапно вводят новые требования к подключению информационных систем к федеральной инфраструктуре электронного правительства и ЕСИА

1. Требования к используемым средствам СКЗИ
2. Требования к подключаемой информационной системе
3. Требования к реализации взаимодействия с ЕСИА
4. Организационные требования

1. Требования к используемым СКЗИ

Для формирования ЭП должно применяться СКЗИ класса КСЗ

Пункт 9.1 Регламента:

«Критериями принятия решения о корректности выбора СКЗИ, включая средства ЭП, применяемых для организации взаимодействия с ФГИС ЕСИА, являются:

- *наличие действующего сертификата ФСБ России у средства ЭП (название в соответствии с эксплуатационной документацией (формуляром) на изделие, номер сертификата, его срок действия и класс СКЗИ указываются заявителем);*
- *класс средства ЭП не ниже КСЗ. "*

Канал взаимодействия с тестовой ЕСИА должен быть защищен по протоколу TLS, а с промышленной ЕСИА — с использованием СКЗИ класса КСЗ

- **Пункт 9.1 Регламента:** *«При организации канала связи до тестовой среды ЕСИА должен применяться канал, защищенный с использованием протокола TLS».*
- **Пункт 10.1 Регламента:** *«Подключение к промышленной среде ЕСИА допускается только с использованием сертифицированных ФСБ России средств защиты канала связи класса не ниже КСЗ».*

2. Требования к ИС организации

Защищенность ИС должна быть уровня УЗ.3+

Пункт 9.1 Регламента: «При необходимости получения персональных данных уровень защищенности персональных данных подключаемой системы должен быть УЗ.3 и выше».

Канал работы ИС с ЕСИА и с пользователями должен быть защищен с использованием СКЗИ класса КСЗ

Пункт Д1.6 МР: «Все каналы связи на участке взаимодействия «ЕСИА-ВИС», выходящие за пределы контролируемых зон участников взаимодействия, должны быть защищены с помощью сертифицированных средств криптографической защиты информации, удовлетворяющих установленным требованиям к средствам криптографической защиты информации класса не ниже КСЗ».

Серверная часть ВИС должна поддерживать возможность взаимодействия с пользователями по протоколу TLS, реализованному с использованием СКЗИ, сертифицированных ФСБ России по классу не ниже КСЗ на стороне ВИС (сервера) и КС1 на стороне пользователя (клиента)".

Используемые в ИС СЗИ должны быть уровня доверия 5+

Пункт Д1.5 МР: «Все используемые средства защиты информации должны быть сертифицированы ФСТЭК России и соответствовать уровню доверия не ниже 5 или должны быть сертифицированы ФСБ России».

ИС должна быть аттестована по требованиям ИБ

Пункт 10.1 Регламента: «Решение о подключении ИС к промышленной среде ЕСИА принимается Минцифры России, в том числе, на основании следующих сведений:

сведения об оценке эффективности реализованных мер по обеспечению безопасности информации подключаемой информационной системы, осуществленной в порядке, установленном законодательством Российской Федерации, и проведенной с привлечением организации, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации".

3. Требования к реализации взаимодействия с ЕСИА

Реализация интеграции с ЕСИА должна пройти оценку влияния на СКЗИ

Пункт 10.1 Регламента: «В случае выбора заявителем варианта реализации подсистемы идентификации, аутентификации OpenID Connect с использованием собственного технического решения <...> заявитель должен провести процедуру оценки влияния на СКЗИ, применяемое в составе технического решения, согласно требованиям (или положениям) эксплуатационной документации на СКЗИ с привлечением испытательных лабораторий, аккредитованных ФСБ России, в соответствии с требованиями действующего законодательства».

Реализация OpenID Connect должна быть согласована с Минцифры и проверена на корректность реализации в ФСБ России

Пункт 10.1 Регламента: «Техническое задание на создание такого технического решения в части реализации протокола OpenID Connect при взаимодействии с ЕСИА должно быть согласовано Минцифры России».

Пункт Д1.3 МР: «Реализуемый в собственном техническом решении протокол на базе OpenID Connect 1.0 и OAuth2.0, должен соответствовать описанию и схемам, приведенным в Приложение Б (за исключением разделов, рекомендованных к выводу из эксплуатации). Безопасность реализации протокола должна быть подтверждена в установленном порядке в соответствии с действующими нормативно-правовыми актами».

4. Организационные требования

В соответствии с действующей редакцией документа “РЕГЛАМЕНТ ЕДИНОЙ СИСТЕМЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ” версия 2.47, раздел “Обозначения и сокращения” содержит следующую информация: “Шлюзовой модуль (API Gateway) Компонент, обеспечивающий взаимодействие ИС коммерческой организации с ЕСИА и ЕПГУ, прошедший сертификационные исследования по требованиям информационной безопасности ФСТЭК России в соответствии с Положением о системе сертификации средств защиты информации, утвержденным приказом ФСТЭК России от 03.04.2018 № 55”

Соответственно, необходимо сертифицировать ИС в соответствии с этими требованиями.

Так как в ИС применяется средства контейнеризации, то необходимо привести системное окружение в соответствие с требованиями приказа №118 ФСТЭК России, информационных сообщений ФСТЭК России от 10 января 2025 г. № 240_24_39 и от 13 января 2025 года № 240_24_38.

В случае неисполнения данных требований, появляется риск отключения от ЕСИА в соответствии с нормами содержащимися в указанных документах. Например пункт 2, раздела I. Права и обязанности участника информационного взаимодействия, документа “Права и обязанности участника информационного взаимодействия” гласит: “Участник осознает, что нарушение требований и условий, содержащихся в настоящем разделе, повлечет отключение от сервисов и интерфейсов ЕСИА;”

Три варианта решения для работы с ЕСИА, ЦПГ и даже СМЭВ

1



Собрать самим: провести ОВ на СЭП КСЗ, доказать корректность встраивание ОИС, докупить оборудование, АПМЗ, ОС и пр.

2



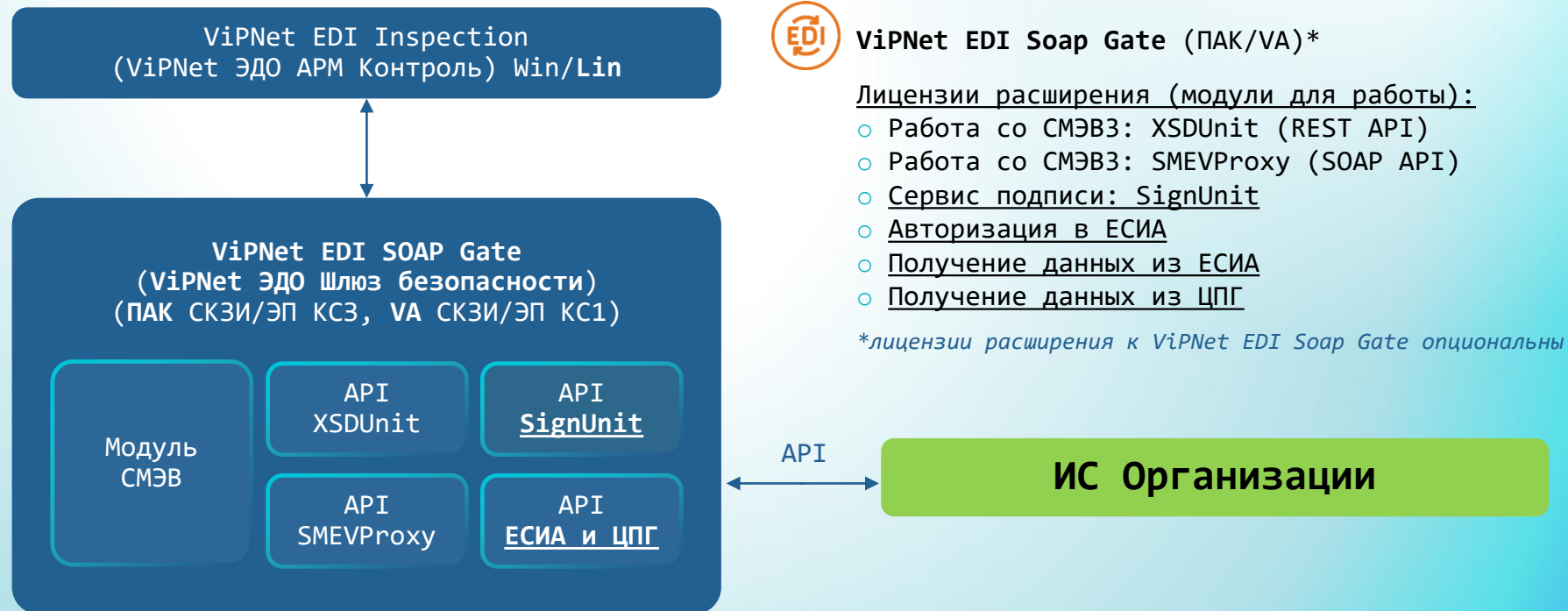
Купить готовое с проведенной ОВ и встроенным ОИС: докупить СЭП КСЗ, оборудование, АПМЗ, ОС и пр.

3



Купить готовое сертифицированное решение

ViPNet EDI Единое решение для всех участников взаимодействия





VipNet EDI Soap Gate

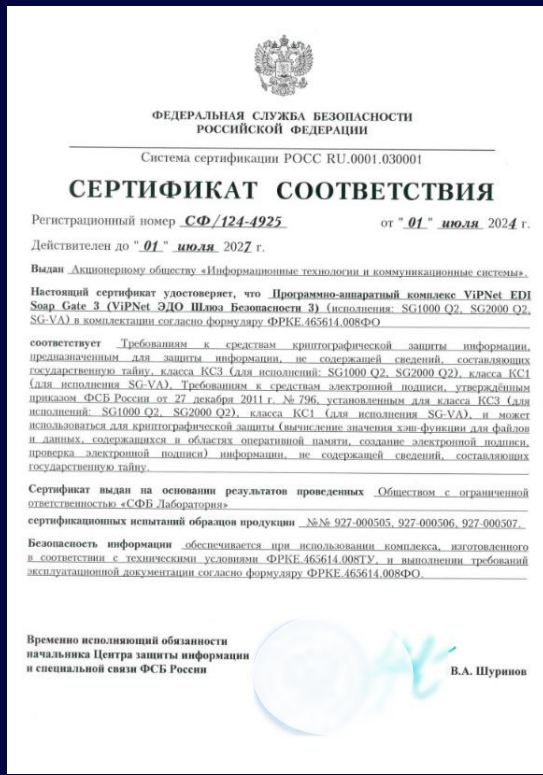
Криптошлюз для обмена
электронными сведениями
с применением электронной
подписи



- Соответствует Регламенту ЕСИА 2.47+ и Методическим рекомендациям ЕСИА 3.48+
- Авторизация и аутентификация пользователей в ЕСИА с помощью протокола авторизации OAuth 2.0 и расширения OpenID Connect
- Построение защищенного канала связи по протоколу TLS ГОСТ 1.2, 1.3
- Заверение данных ЭП определенного формата и ее проверка, включая проверку действительности сертификата ключа проверки ЭП, списка аннулированных сертификатов и цепочки сертификатов
- Формирование, заверение и проверка ЭП хэша данных
- Получение информации о владельцах ЭП и наличии в хранилищах сертификатов и CRL

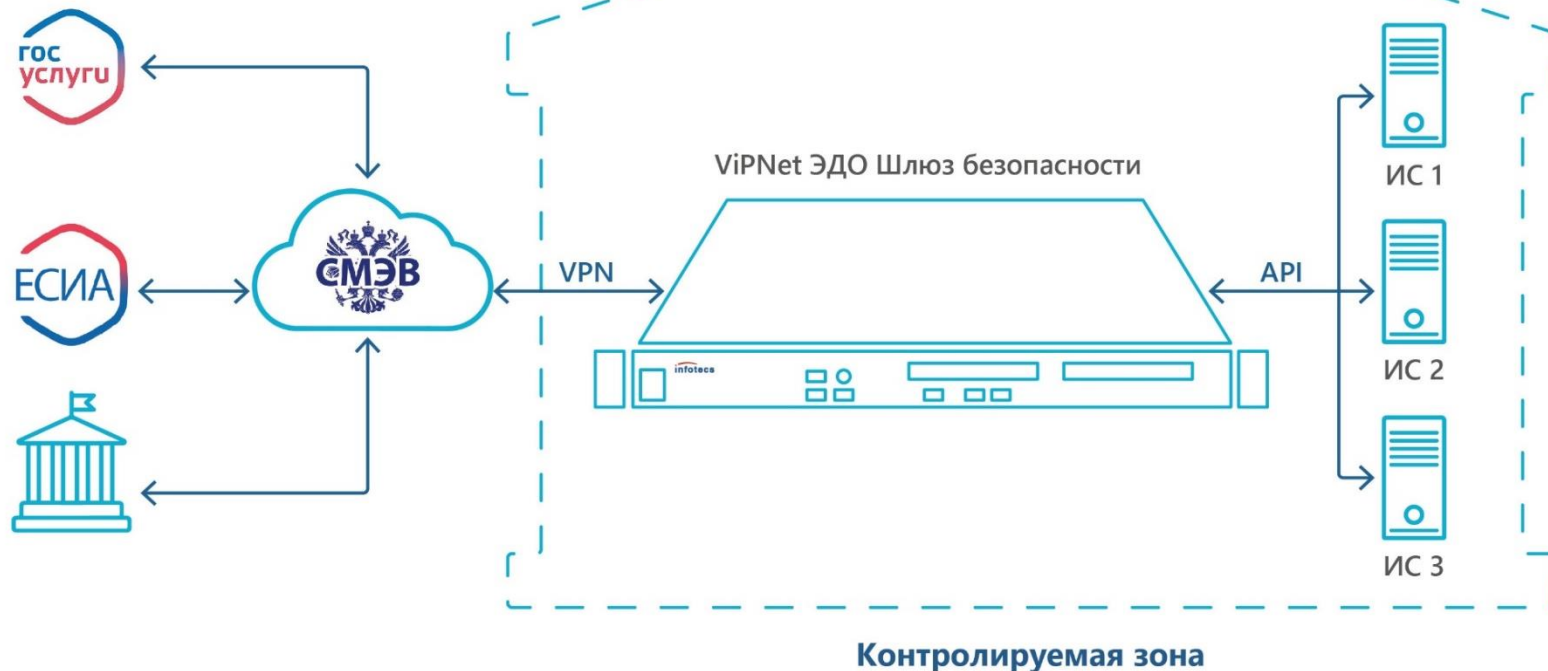


VIPNet EDI Soap Gate



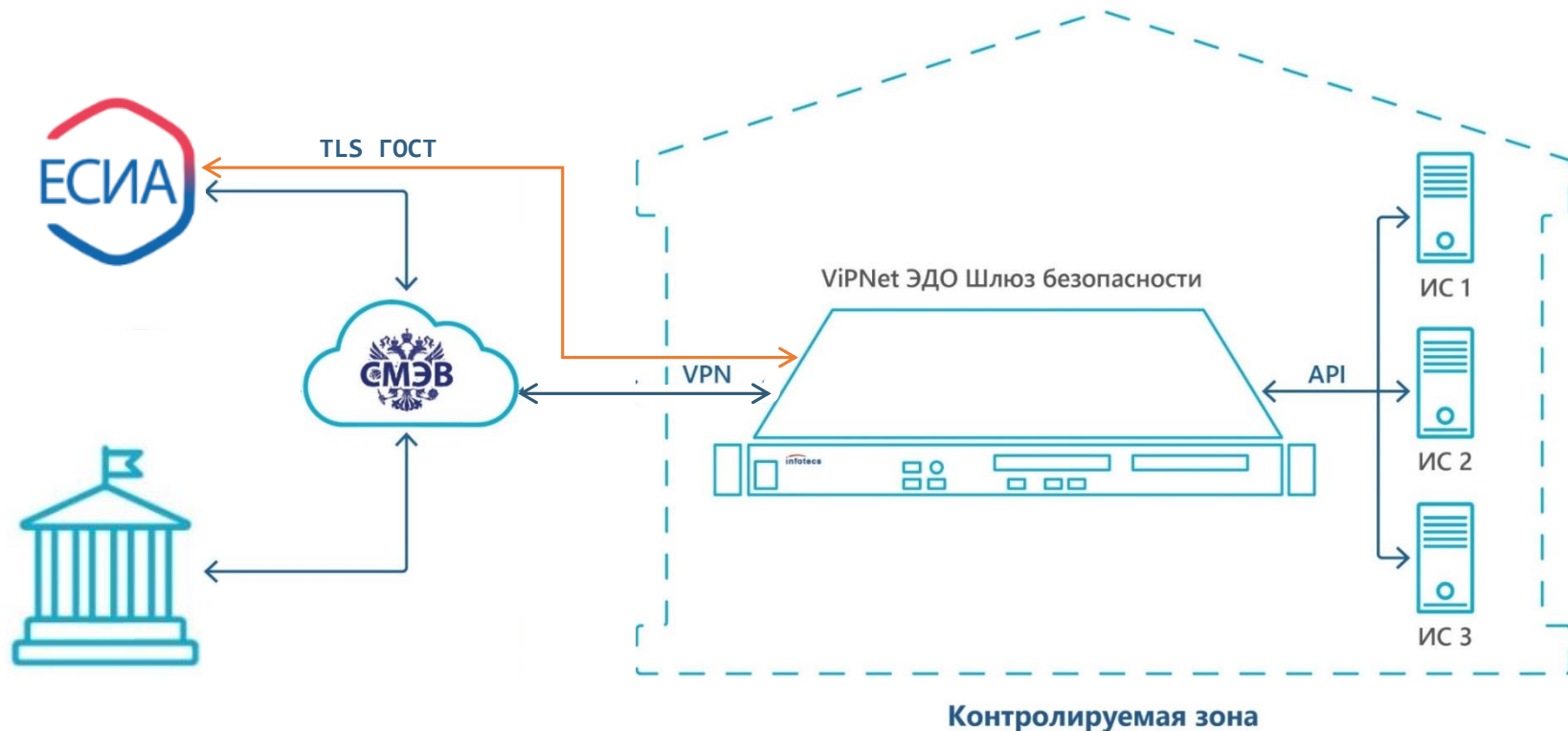
- Соответствует требованиям ФСБ России к СКЗИ и ЭП по классу КС3 и КС1 (нет требования о проведении ОВ при подключении ИС организации)
- Действующий сертификат до 1 июля 2027 года (СМЭВ3)
- Заключение от 26 декабря 2025 года о соответствии требованиям ФСБ к СКЗИ КС3 и средство ЭП КС3, в том числе для взаимодействия с ЕСИА, СМЭВ3
- Регистрация в Едином реестре российского ПО №3276 и в реестре Минпромторга

Единое решение для интеграции ИС УВ со СМЭВ/ЕСИА/ЦП



ViPNet EDI (заклучение получено)

Работа со СМЭВ, ЕСИА, ЦПГ



API для взаимодействия с ЕСИА и ЦПГ

Возможность авторизовать пользователя через ЕСИА

Запросить у пользователя доступ к персональным данным, получить ПД пользователя из ЕСИА

Авторизация пользователя через ЕСИА для получения данных пользователя из ЦПГ

Запрос в ЕСИА данные о самозанятых пользователях, организациях пользователя, категориях организации пользователя и список участников организации пользователя

Для интеграции предоставляется Справочник разработчика с описанием методов API



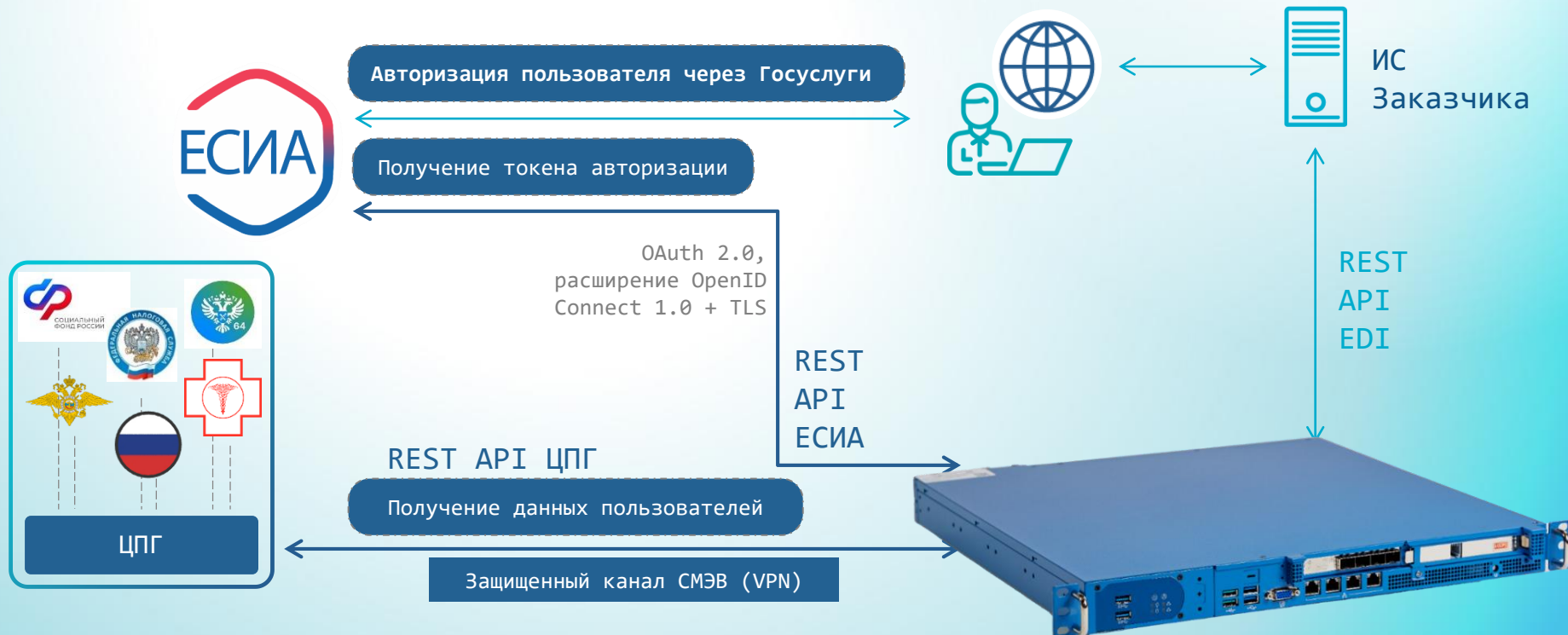
Интеграция с ЕСИА с помощью ViPNet EDI Soap Gate



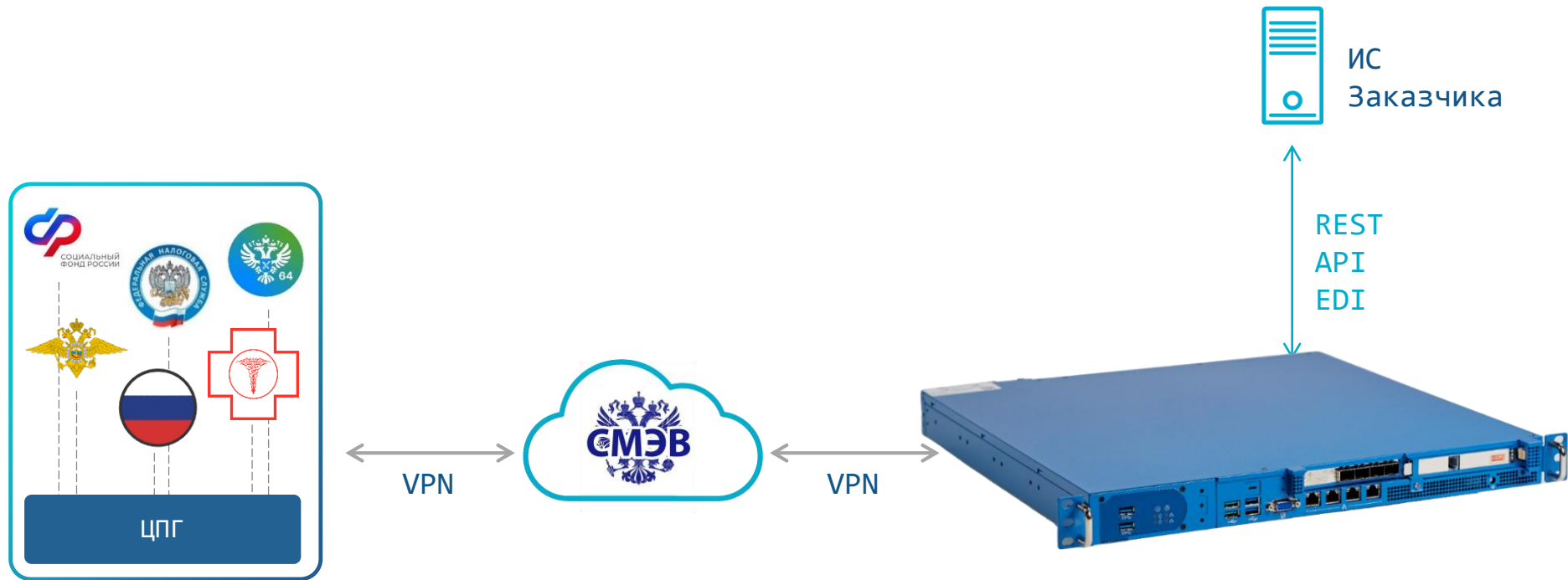
Производительность API ESIA в ViPNet EDI Soap Gate

ESIA	
SG 2000 Q2	SG 1000 Q2
400 запросов в секунду - получение маркера доступа	200 запросов в секунду - получение маркера доступа
700 запросов в секунду - запрос на получение данных пользователя	430 запросов в секунду - запрос на получение данных пользователя

Интеграция с ЦПГ с помощью ViPNet EDI (online-режим)



Интеграция с ЦПГ с помощью ViPNet EDI (offline-режим)



*Взаимодействие с ЦПГ
через СМЭВ*

**Настройка получения
«Запроса согласий
пользователя ЕСИА от
организации»**

Личный кабинет участника

lkuv.gosuslugi.ru/paip-portal/#/main

lkuv Войти

Используйте обновленную "Судьбу сообщений"

Отслеживайте статус своих обменов в СМЭВ3 с помощью Telegram-бота или функционала в ЛК УВ

[Перейти](#)

Виды сведений

[Посмотреть все](#)

Поиск по наименованию, описанию, URI (name=расе)

Запрос согласий пользователя ЕСИА от организации

Быстрые действия

Судьба сообщения СМЭВ3

Посмотрите судьбу сообщения СМЭВ3

Все виды сведений

Посмотрите все виды сведений в СМЭВ

Все запросы (SQL-запрос)

Посмотрите все регламентированные запросы типа SQL

Все запросы (REST-сервис)

Посмотрите все регламентированные запросы типа REST-сервис

Настройка учетной записи ИС и настройка полномочий ИС

Создание учетной записи информационной системы

Настройка параметров учетной записи

Учетная запись | Полномочия

Учетная запись


Наименование информационной системы*: Информационная система №6

Имя учетной записи*: inf_system_6

Пароль*: ●●●●●●●●

Уровень полномочий: Информационная система

Авторизация по ГОСТ

Сертификат для работы по TLS: 

Создание учетной записи информационной системы

Настройка параметров учетной записи

Учетная запись | Полномочия

Выбрать все полномочия

С правом на взаимодействие со СМЭВ

С правом на использование сервиса подписи

С правом на использование сервиса по работе с УЦ

ЕСИА и ЦПГ

С правом на авторизацию пользователей в ЕСИА

С правом на получение данных пользователя и его организации из ЕСИА

С правом на получение данных пользователей из ЦПГ

Преимущества ViPNet EDI



Соответствует требованиям регулятора за счет применения сертифицированных СКЗИ и средств ЭП по классу КСЗ



Подходит для внедрения в рамках программы импортозамещения



Не требует знаний, опыта работы с протоколами СМЭВЗ, отслеживания изменений в СМЭВ



Обеспечивает уровень защищенности обрабатываемой информации по классу КСЗ



Автоматизирует процесс запроса и предоставления сведений из БД государственных органов



Взаимодействие с ЕСИА по протоколу OpenID Connect в соответствии с Регламентом 2.47

Подписывайтесь
на наши соцсети,
там много интересного



инфотекс

Приглашаем на стенд № 12.

В начале каждого часа
демонстрация:

- ViPNet CABCS
- ViPNet EDI Soap Gate с ЕСИА
и СМЭВЗ



Спасибо за внимание!

