СКЗИ для легитимной работы с ЕСИА, СМЭВ и ЦП

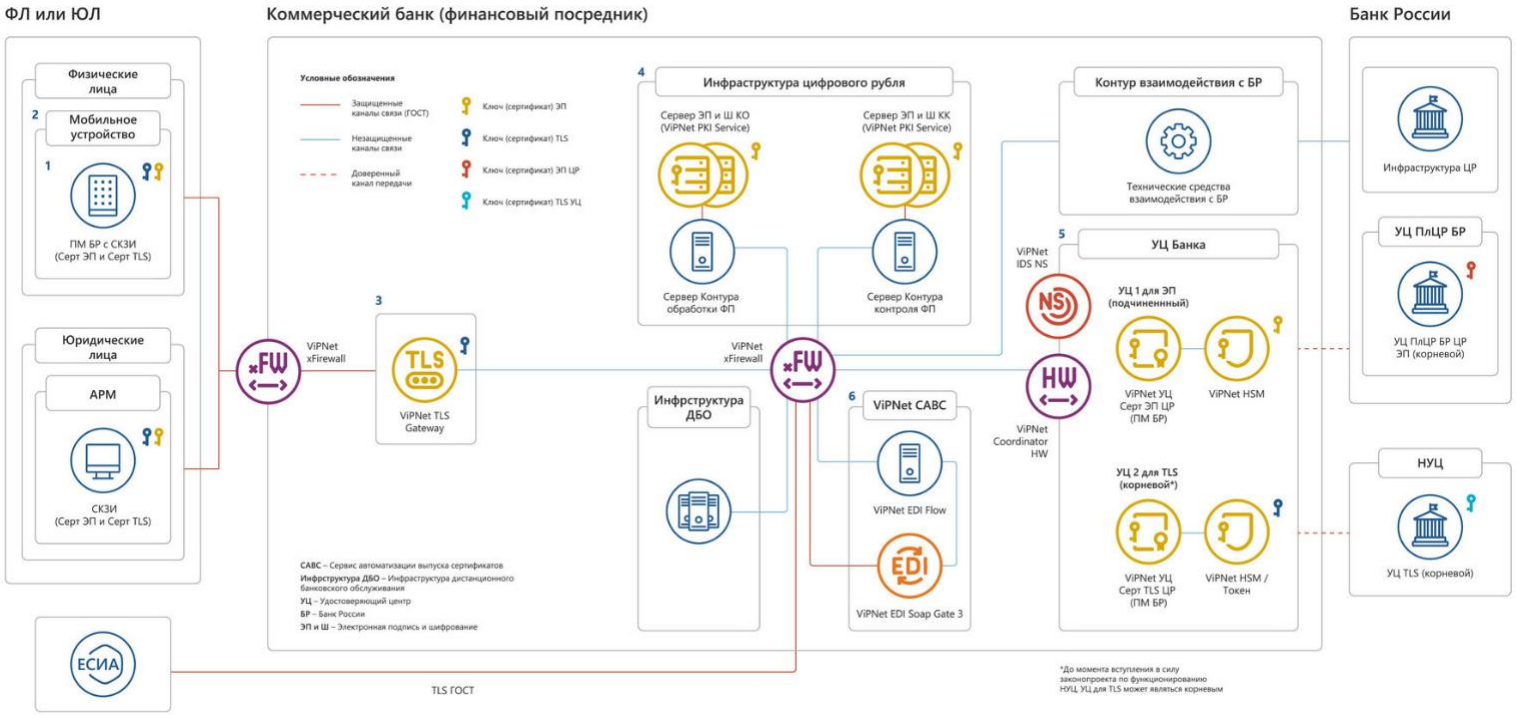
Елена Новикова

Руководитель продуктового направления

инфотекс ТЕХНОДЕСТ

Белый поток

Общая схема инфраструктуры ЦР



ViPNet САВС

Автоматизация процесса выпуска сертификатов

Безопасность данных:

- Обеспечение криптографической защиты информации
- Идентификация пользователя ПлЦР (ФЛ, ЮЛ и ИП)
  - проверки запросов пользователей ПлЦР на создание сертификатов (первичный/повторный)
  - проверки изданных сертификатов

Интеграция с существующими системами:

- Единой Системой Идентификации и Аутентификации (ЕСИА)
- Автоматизированными системами дистанционного банковского обслуживания (АС ДБО) банков
- Удостоверяющими центрами (ViPNet УЦ 4/5.x, УЦ КриптоПро 2.0)

Актуальность сертификатов:

- получение списков отозванных сертификатов и направление их в ПлЦР

Соблюдение нормативных требований:

- соответствие требованиям нормативных документов регуляторов – ЦБ России и ФСБ России

Состав ViPNet CABC 1.0

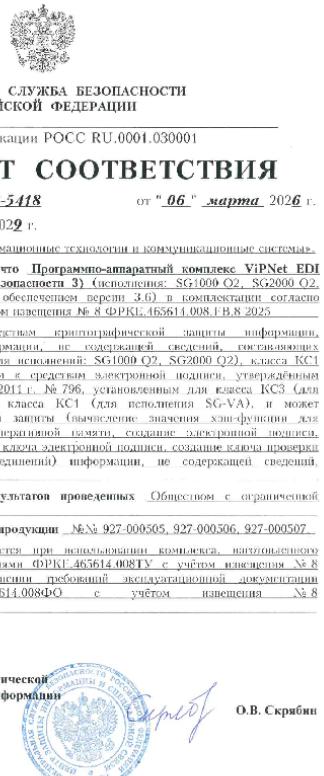
ViPNet EDI Soap Gate 3

ПАК СКЗИ и средство ЭП для взаимодействия с ЕСИА по OpenID Connect в части идентификации пользователей ПлЦР, проставления и проверки ЭП

ViPNet EDI Flow

ПК управления ViPNet CABC и выполнения процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователей платформы ЦР

ViPNet EDI Soap Gate



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер *СФ/124-5418* от "*06*" *марта* 2026 г.

Действителен до "*06*" *марта* 2029 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программно-аппаратный комплекс ViPNet EDI Soap Gate 3 (ViPNet ЭДО Шлюз Безопасности 3) (исполнения: SG1000 Q2, SG2000 Q2, SG-VA со специальным программным обеспечением версии 3.6) в комплектации согласно формуляру ФРКЕ.465614.008ФО с учётом извещения № 8 ФРКЕ.465614.008 РВ.8 2025

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС3 (для исполнений: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VA), Требованиям к средствам электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС3 (для исполнений: SG1000 Q2, SG2000 Q2), класса КС1 (для исполнения SG-VA), и может использоваться для криптографической защиты (вычисление значения хэш-функции для данных, содержащихся в областях оперативной памяти, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория»

сертификационных испытаний образцов продукции №№ 927-000505, 927-000506, 927-000507.

Безопасность информации обеспечивается при использовании комплекса, изготовленного в соответствии с техническими условиями ФРКЕ.465614.008ТУ с учётом извещения № 8 ФРКЕ.465614.008.РВ.8 2025, и выполнении требований эксплуатационной документации согласно формуляру ФРКЕ.465614.008ФО с учётом извещения № 8 ФРКЕ 465614.008 РВ.8-2025.

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России **О.В. Скрябин**

- 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 6 марта 2029 года (СМЭВ3)
- **Заключение от 26 декабря 2025 года** о соответствии требованиям ФСБ России 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

ViPNet EDI Soap Gate

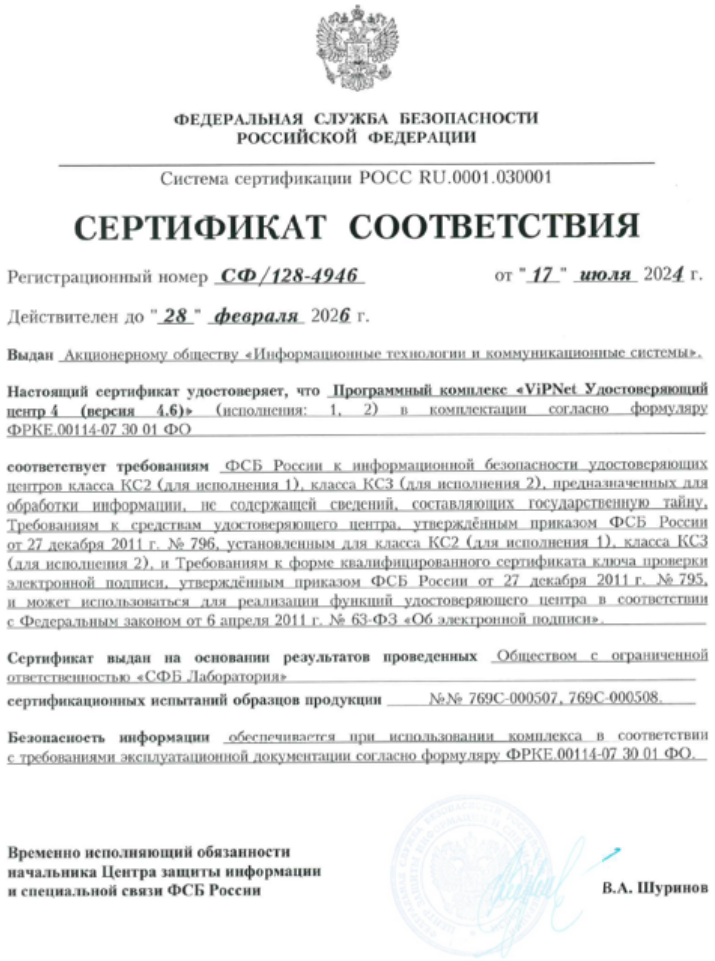
Криптошлюз для обмена электронными сведениями с применением электронной подписи

- 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 Flow

Программный комплекс управления ViPNet CABC

- Контроль и выполнение процессов, связанных с выпуском сертификатов безопасности и сертификатов ЭП пользователям ПлЦР
- Обеспечивает взаимодействие между АС ДБО, ViPNet EDI Soap Gate и УЦ. Для интеграции АС ДБО с ViPNet EDI Flow предоставляется REST API (Справочник разработчика)
- Идентифицирует пользователя ПлЦР в ЕСИА
- Отправляет запросы в УЦ на выпуск сертификатов безопасности и сертификатов ЭП для пользователей ПлЦР
- Получает и распространяет списки отозванных сертификатов



ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/128-4946 от "17" июля 2024 г.

Действителен до "28" февраля 2026 г.

Выдан Акционерному обществу «Информационные технологии и коммуникационные системы».

Настоящий сертификат удостоверяет, что Программный комплекс «ViPNet Удостоверяющий центр 4 (версия 4.6)» (исполнения: 1, 2) в комплектации согласно формуляру ФРКЕ.00114-07 30 01 ФО

соответствует требованиям ФСБ России к информационной безопасности удостоверяющих центров класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), предназначенных для обработки информации, не содержащей сведений, составляющих государственную тайну. Требованиям к средствам удостоверяющего центра, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС2 (для исполнения 1), класса КС3 (для исполнения 2), и Требованиям к форме квалифицированного сертификата ключа проверки электронной подписи, утверждённым приказом ФСБ России от 27 декабря 2011 г. № 795, и может использоваться для реализации функций удостоверяющего центра в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи».

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «СФБ Лаборатория» сертификационных испытаний образцов продукции №№ 769С-000507, 769С-000508.

Безопасность информации обеспечивается при использовании комплекса в соответствии с требованиями эксплуатационной документации согласно формуляру ФРКЕ.00114-07 30 01 ФО.

Временно исполняющий обязанности
начальника Центра защиты информации
и специальной связи ФСБ России В.А. Шуринов

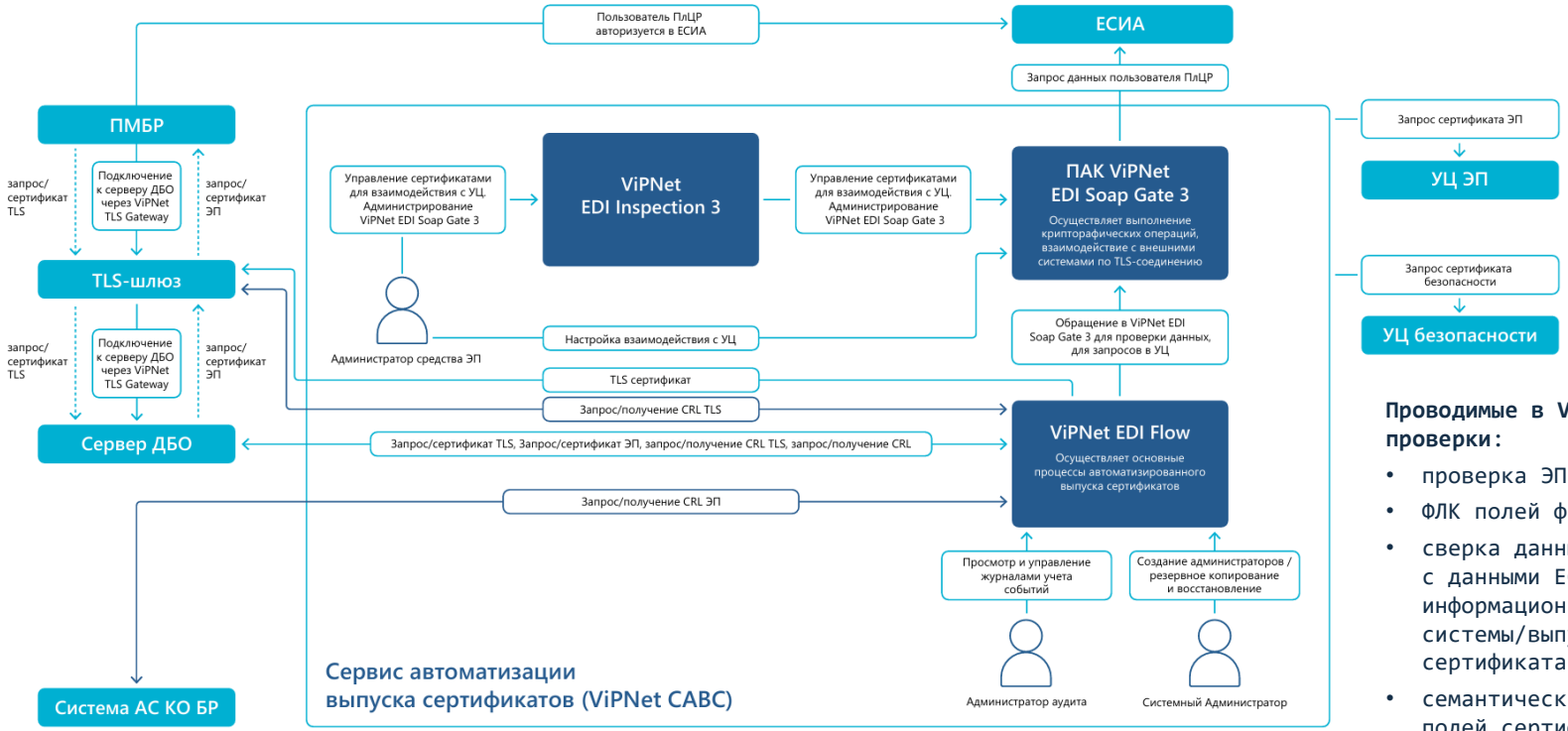
Сертификация: ViPNet УЦ 4.6

- Два исполнения: средство УЦ КС2 и КС3 для ОС Windows
- Текущий сертификат действует до 28.02.2026
- *Новый сертификат **СФ/128-5392** **получен 27 января 2026 года** действует до 31 декабря 2026*

ViPNet УЦ 5

- ***Сертификат до конца 2026 года***

Схема работы ViPNet CABC



Проводимые в ViPNet CABC проверки:

- проверка ЭП файла запроса,
- ФЛК полей файла запроса,
- сверка данных файла запроса с данными ЕСИА/внешней информационной системы/выпущенного сертификата
- семантическая проверка полей сертификата

Роли администраторов ViPNet САВС

Системный администратор (совмещает роль администратора резервного копирования и восстановления)

- создание, удаление, настройка прав и редактирование учетных записей администраторов
- настройка параметров журнала аудита
- запрет на изменение журнала аудита

Администратор аудита

- просмотр журнала аудита
- копирование журналов аудита
- полная очистка журналов

Администратор средства ЭП

Проверки в ViPNet САВС

Первичный выпуск сертификата

- проверка ЭП файла запроса
- форматно-логический контроль файла запроса
- проверка соответствия данных пользователя ПлЦР из файла запроса и информации, полученной из ЕСИА

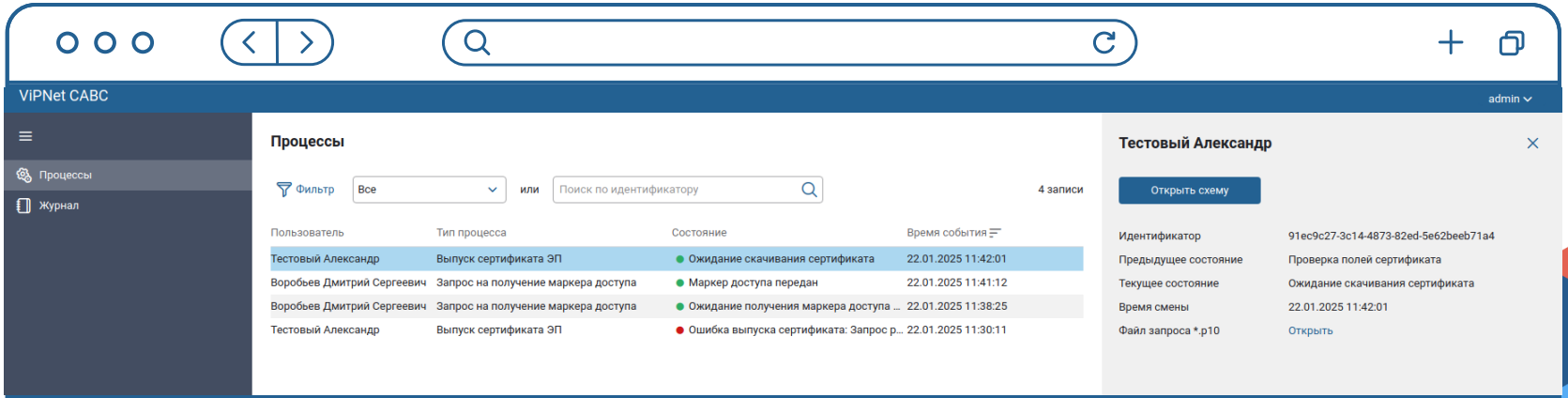
Повторный выпуск сертификата

- проверка ЭП файла запроса
- форматно-логический контроль файла запроса
- проверка идентификационных данных пользователя ПлЦР из файла запроса с использованием внутренних систем участника ПлЦР (АС ДБО)
- проверка соответствия данных из файла запроса с данными из действующего сертификата

Отслеживание и управление процессом выпуска сертификатов

Виды процессов

- Обработка запроса на сертификат безопасности
- Обработка запроса на сертификат подписи
- Обмен авторизационного кода на маркер доступа в ЕСИА
- Обновление списка отозванных сертификатов безопасности
- Обновление списка отозванных сертификатов подписи



Регистрация событий в журнале событий

Фиксация событий:

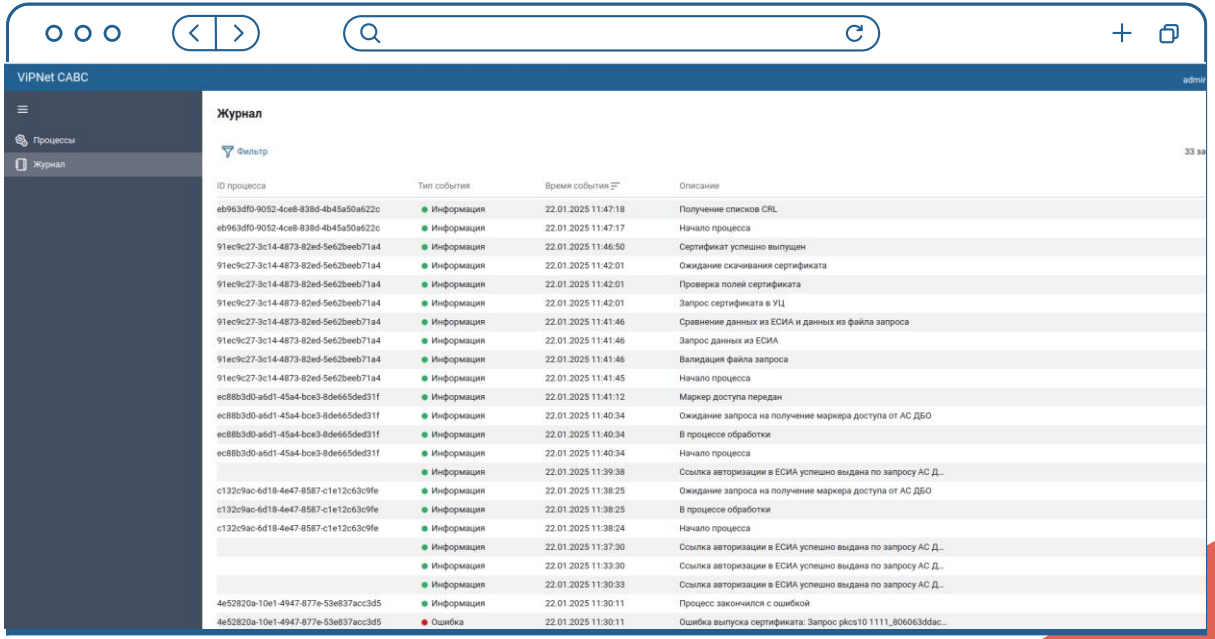
- каждого этапа обработки запросов на выпуск сертификата
- этапов работы с CRL
- этапов взаимодействия с ЕСИА

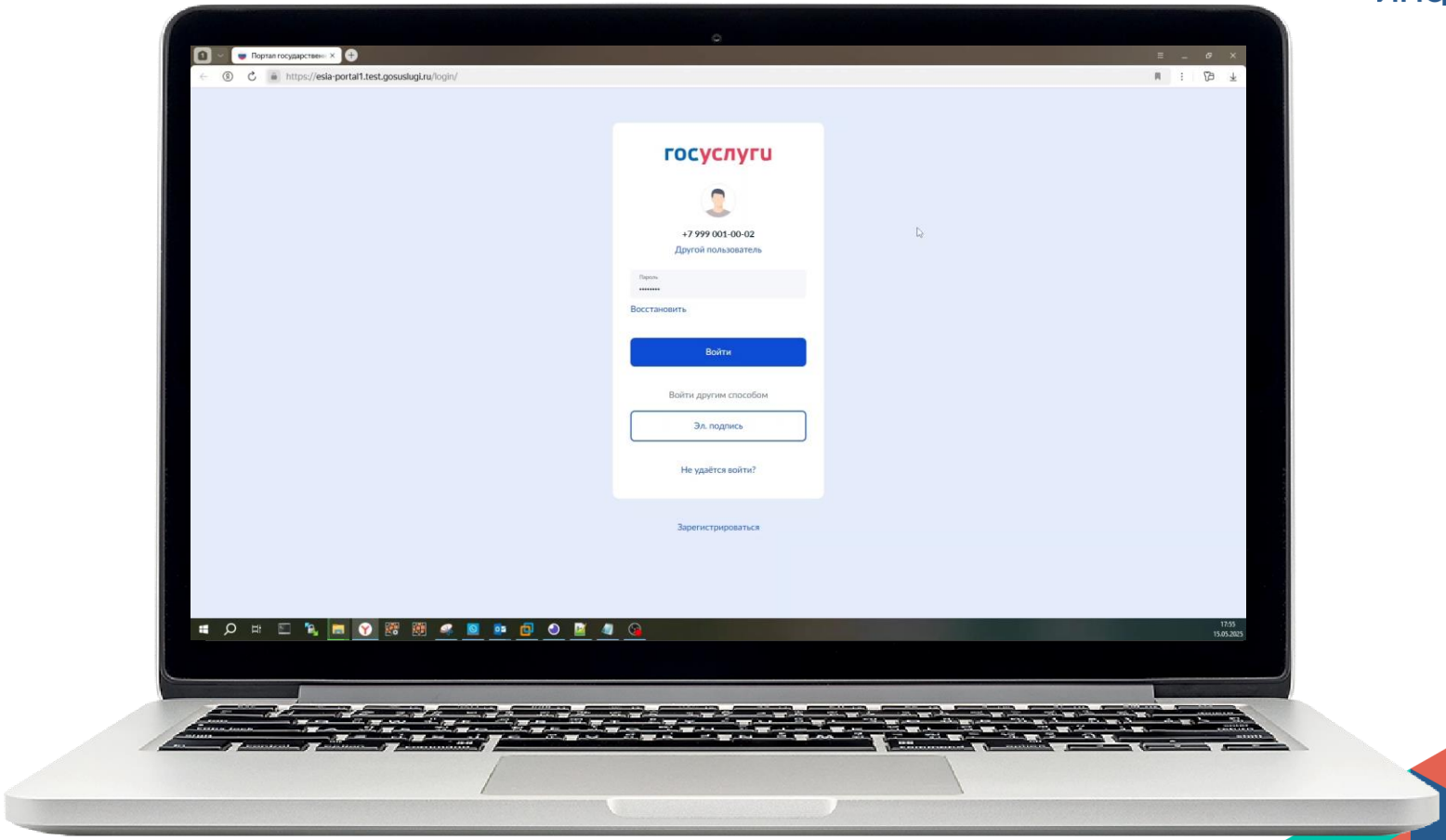
Системный администратор:

- механизмы по обнаружению несанкционированных изменений журналов аудита

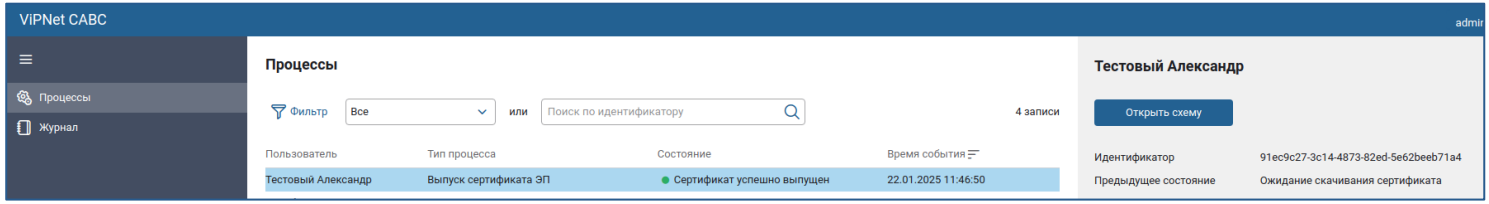
Администратор аудита:

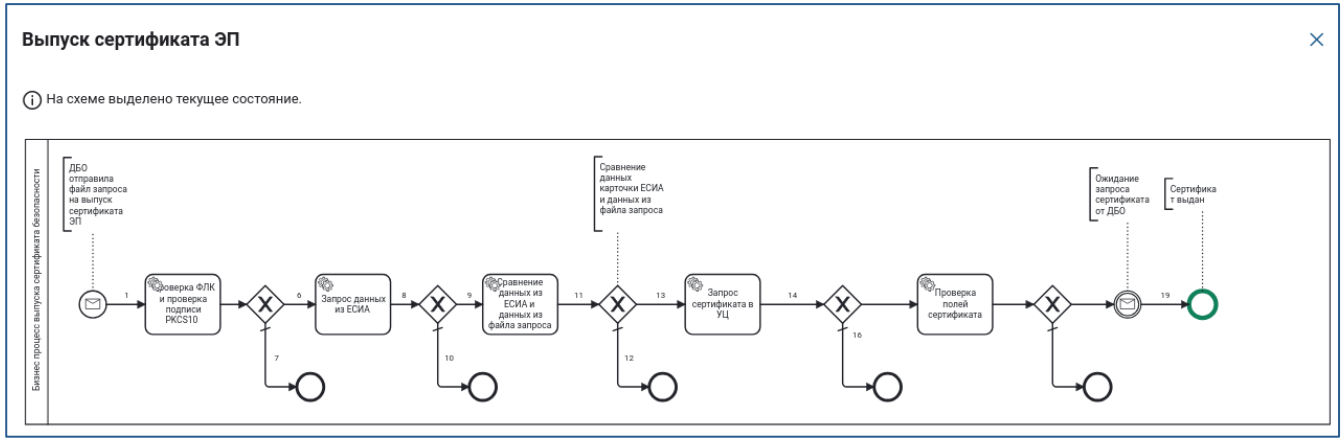
- просмотр журналов аудита
- копирование журналов аудита
- полная очистка журналов аудита

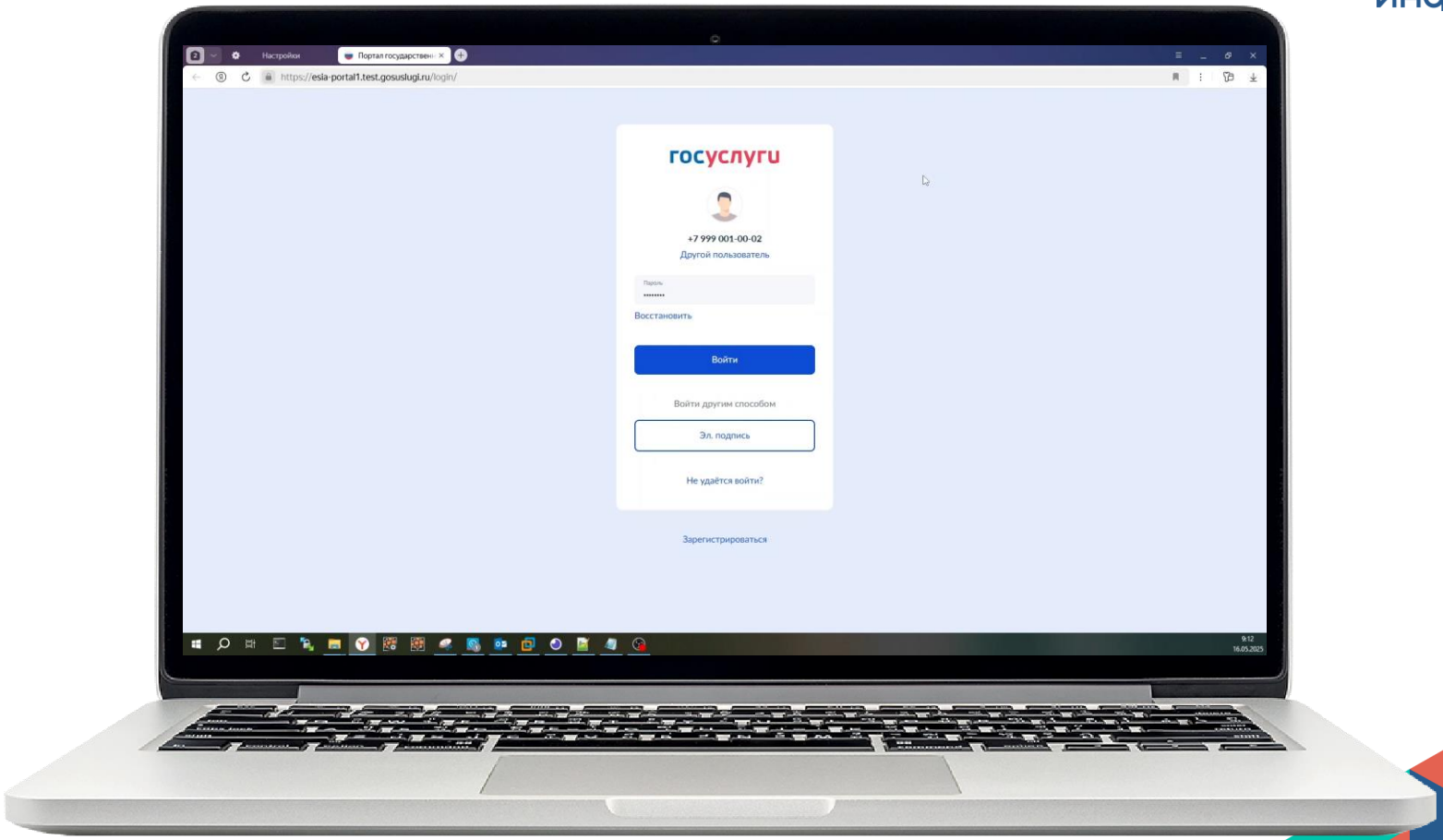



https://esia-portal1.test.gosuslugi.ru/login/
госуслуги
+7 999 001-00-02
Другой пользователь
Восстановить
Войти
Войти другим способом
Эл. подпись
Не удаётся войти?
Зарегистрироваться

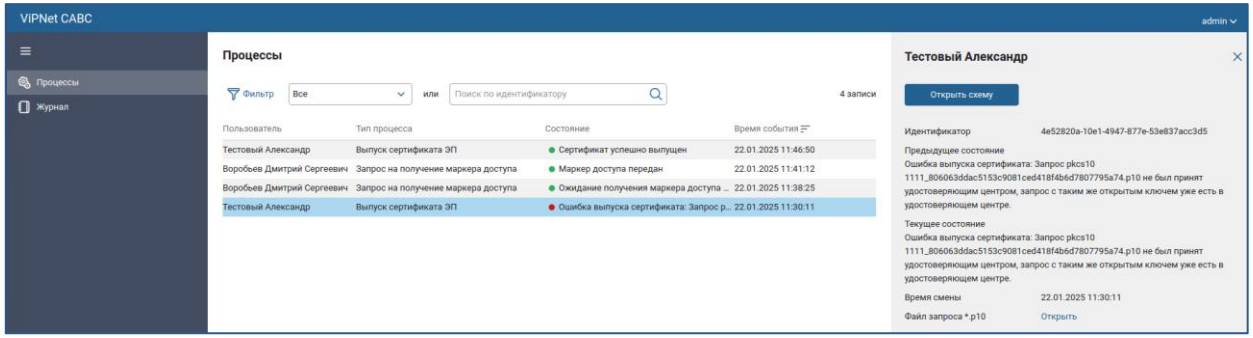
Пример для успешно выпущенного сертификата

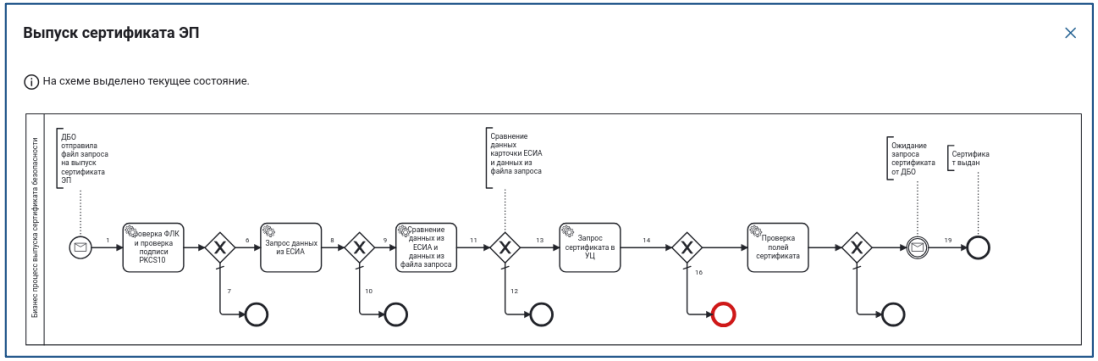





Настройки
Портал государственн
https://esia-portal1.test.gosuslugi.ru/login/
госуслуги
+7 999 001-00-02
Другой пользователь
Восстановить
Войти
Войти другим способом
Эл. подпись
Не удаётся войти?
Зарегистрироваться

Пример неудачного выпуска





САНКТ ПЕТЕРБУРГ

инфотекс

ТЕХНОФЕСТ

Академия инфотекс · Учебный центр инфотекс · AMPIRE · TELEOFIS · КОМФОРТЕЛ оператор связи бизнес-класса · РУТОКЕН компания ИНФОТЕКС · TS Solution · AXOFT

Подписывайтесь на наши соцсети