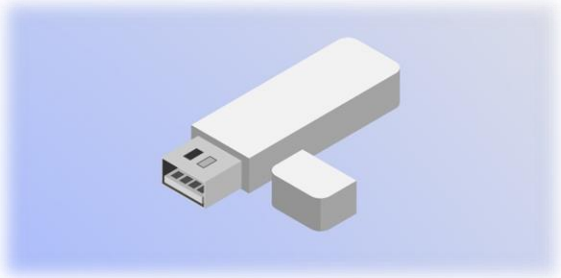
Итоги проекта «Система облачной подписи» в Республике Беларусь

Государственное предприятие "НИИ ТЗИ"

Докладчик: заместитель директора
по научной работе,
к.т.н., **Арестович Дмитрий Николаевич**

АКТУАЛЬНОСТЬ

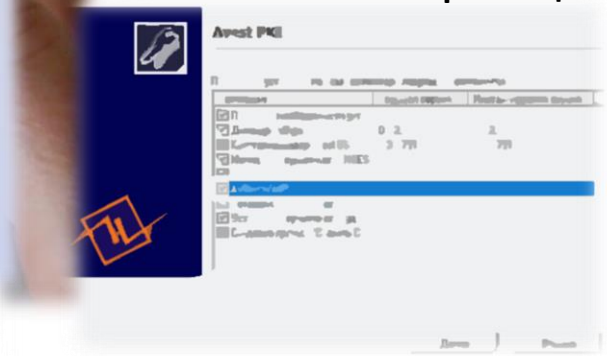
- Отказ от физических носителей ключевой информации, считывателей ID-карт, криптопровайдеров;
- Хранение личных ключей пользователей не на физическом носителе, а на удаленном программно-аппаратном криптографической защиты информации NT HSM;
- Широкий охват операционных систем для работы с личным ключом, будь то персональный компьютер или смартфон;
- Переход на «облачные» сервисы позволит повысить гибкость, более рациональную организацию работы сотрудников и сократить расходы на поддержание собственных серверов.



Носитель ключевой информации
Стоимость от 40 до 90 BYN

ID-карта

Считыватель ID-карт
Стоимость от 15 BYN в рознице



Криптопровайдер
и клиентское ПО

ОКР «Доступность»

Мероприятие 2 программы Союзного государства «**Совершенствование системы защиты информационных ресурсов Союзного государства и государств-участников** Договора о создании Союзного государства в условиях нарастания угроз в информационной сфере» («Паритет»), утвержденной постановлением Совета Министров Союзного государства от 11.06.2018 № 5

Аналитический обзор основных публикаций

- EN 419241-1:2018
- EN 419241-2:2019
- ETSI TS 119 431-1 V.1.1.1
- ETSI TS 119 431-2:2018
- ETSI TS 119 432:2019
- ГОСТ Р 56938-2016
- NIST SP 800-63A
- ISO/IEC 27018:2019
- Cloud Signature Consortium

- Выделены основные компоненты СОП (СД, СП, СР, КП);
- Проведен анализ уже существующих мировых решений (Google Cloud, SigningHub, DocuSign, Adobe Sign Cloud Signature, Cryptomathic Signer);
- Разработан проект ТНПА, определяющий общие правила построения систем облачной подписи и устанавливающий требования и рекомендации к компонентам таких систем и их взаимодействию при реализации технологии облачной подписи;
- Разработан макет программного комплекса, реализующий сервис облачной ЭЦП.

проект ТНПА «Информационные технологии и безопасность. Требования безопасности к системам облачной подписи»

Общие положения:

- Область применения;
- Назначение;
- Уровни гарантий контроля;
- Структура системы;
- Аутентификация подписанта;
- Подписываемый документ;
- Личный ключ подписанта;
- Подпись документа;
- Данные и протокол активации подписи;
- Служба документов;
- Служба подписи;
- Компонент взаимодействия подписанта;
- Оформление требований.

Требования безопасности:

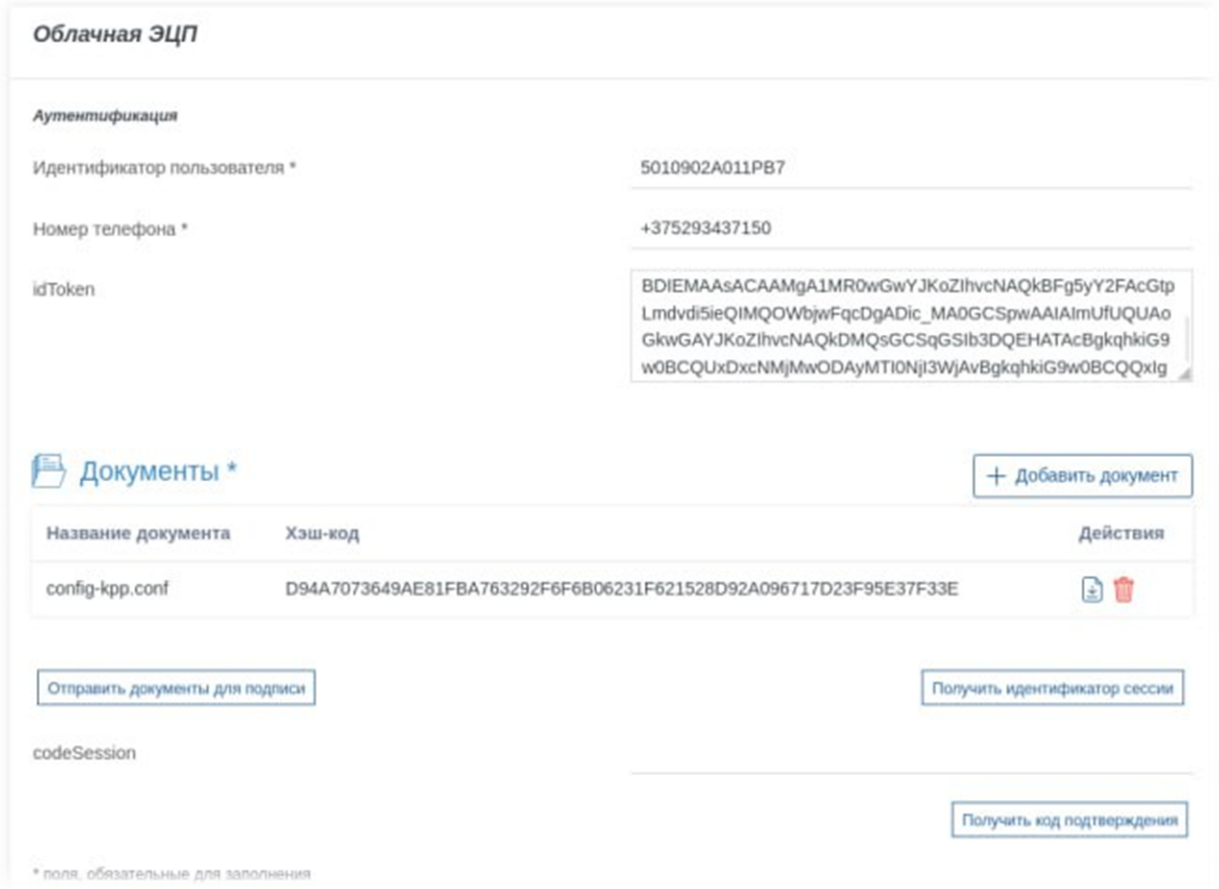
- Система;
- Управление доступом;
- Криптографические алгоритмы;
- Управление ключами;
- Идентификация и аутентификация оператора и подписанта;
- Архивирование;
- Резервное копирование и восстановление;
- Аудит;
- Формирование и проверка электронных документов.

Схема программного комплекса

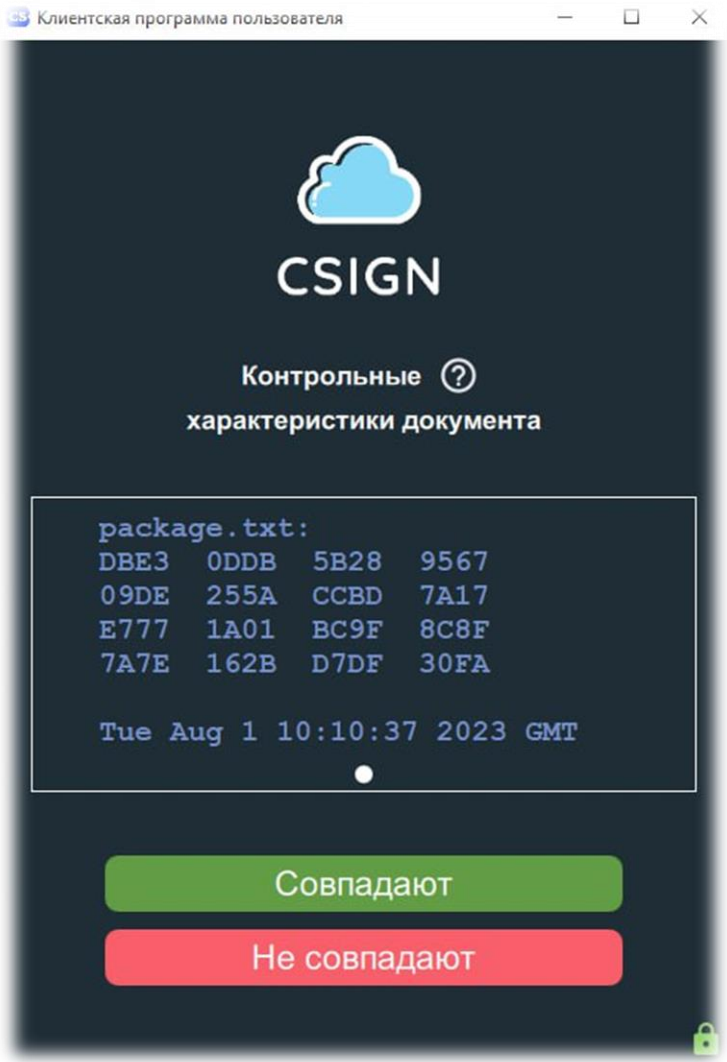
NT HSM основные характеристики:

- Генерация личных или открытых ключей ЭЦП, реализованная в соответствии с требованиями СТБ 34.101.45 с использованием генератора случайных чисел на основе физического источника шума в соответствии с СТБ 34.101.27;
- Выработка и проверка ЭЦП, реализованная в соответствии с требованиями СТБ 34.101.45;
- Шифрование данных с применением криптографических групп алгоритмов шифрования в соответствии с требованиями СТБ 34.101.31;
- Импорт и экспорт репликации резервной копии файловой системы по интерфейсу Ethernet;
- Импорт и экспорт резервной копии файловой системы по интерфейсу USB;
- Горячее резервирование устройства;
- Инициализация и создание токенов не менее 100 000 операторов;
- Создание защищенного канала связи с использованием криптографического протокола BPACE, реализованного в соответствии с требованиями СТБ 34.101.66 и СТБ 34.101.79;
- Аутентификация администраторов и пользователей устройства, с разграничением прав доступа по идентификатору и роли;
- Одновременное предоставление сессий работы с токенами для 1000 операторов.

Программный комплекс

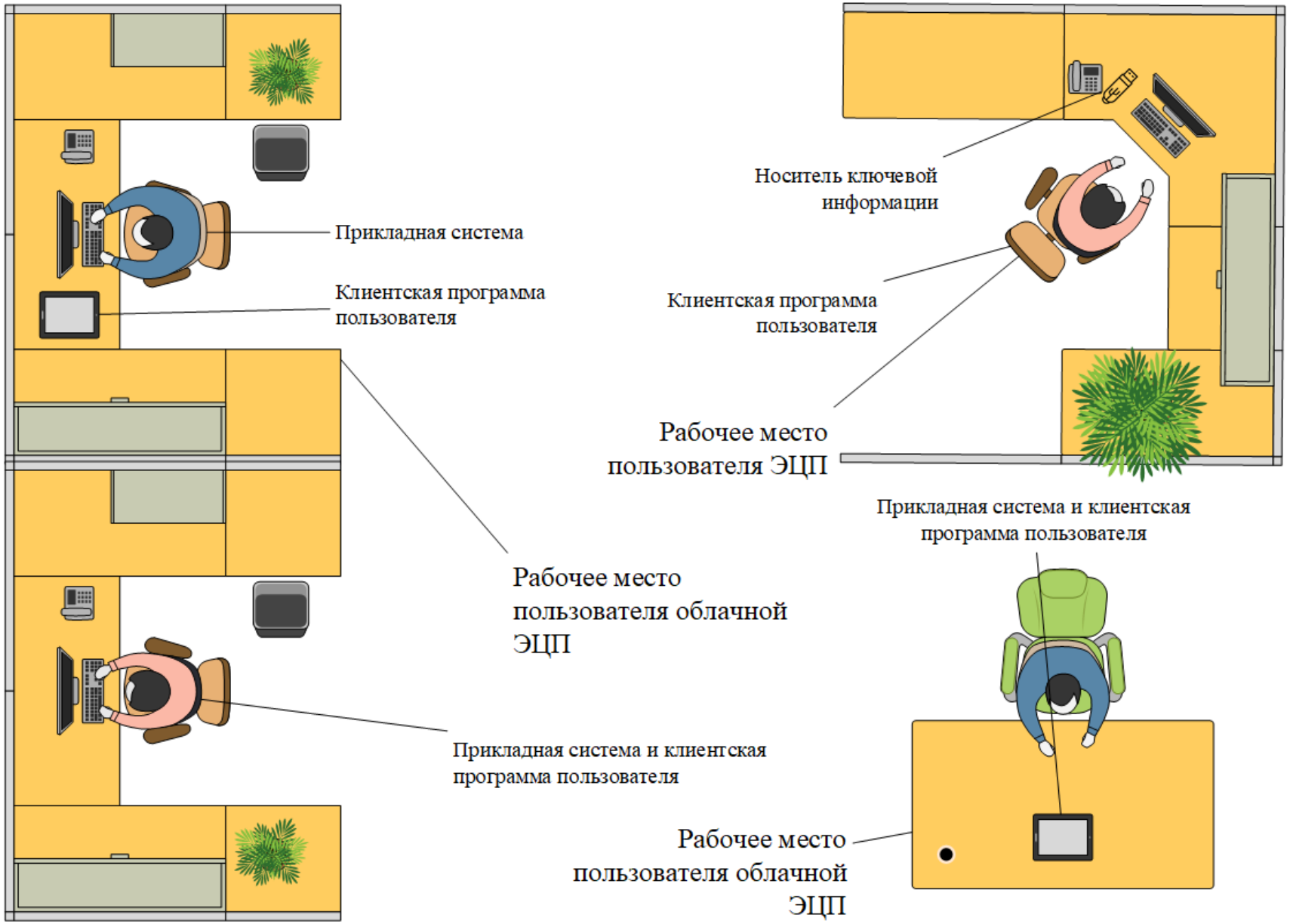


Прикладная система (веб-браузер)

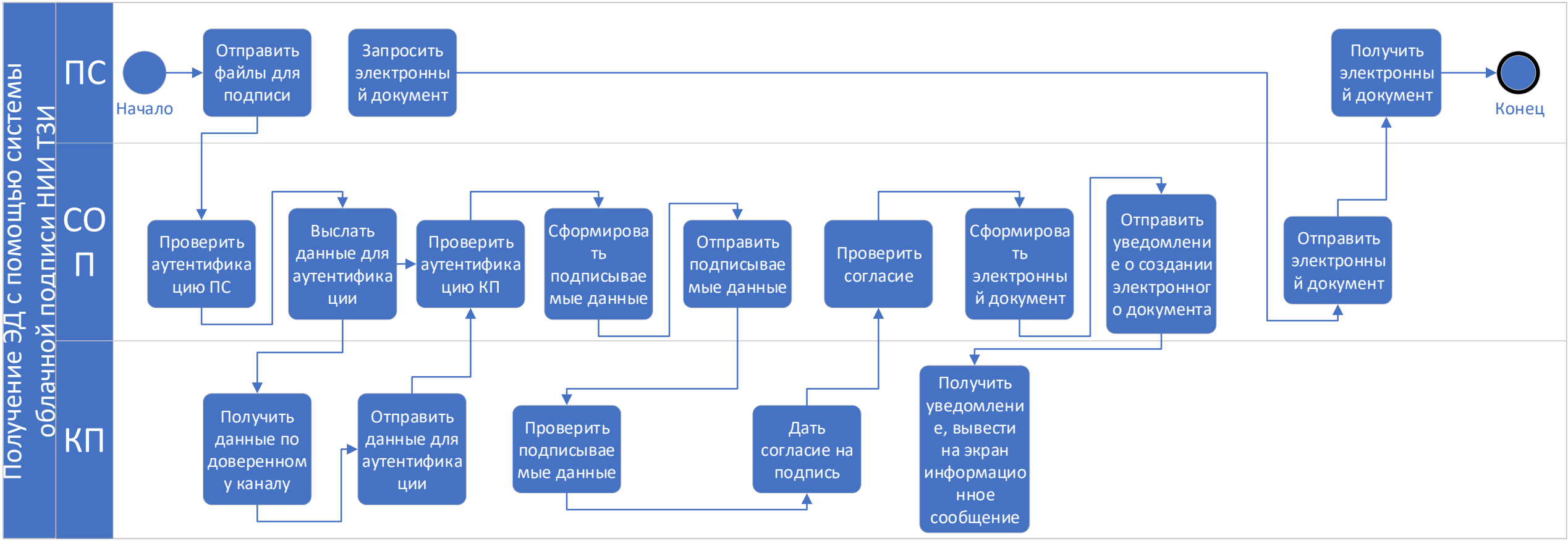


Клиентская программа пользователя (ОС Windows, Linux, Android, MacOS)

Использование программного комплекса



Получение электронного документа



ПОДХОДЫ К ИСПОЛЬЗОВАНИЮ СОП В РЕСПУБЛИКЕ БЕЛАРУСЬ

Апробации возможностей разработанной системы в соответствии с планом действий по оперативному решению проблемных вопросов, связанных с использованием биометрических документов, удостоверяющих личность, была проведена с помощью закрытого бета-тестирования в инфраструктуре единого портала электронных услуг «Е-Паслуга», функционирующего в Республике Беларусь.

ПОДХОДЫ К ИСПОЛЬЗОВАНИЮ СОП В РЕСПУБЛИКЕ БЕЛАРУСЬ[1]

- Использование системы облачной электронной цифровой подписи в **системе электронного голосования**;
- Использование системы облачной электронной цифровой подписи в **интегрированной информационной системе Министерства Образования РБ**;
- Использование системы облачной электронной цифровой подписи в **автоматизированной информационной системе «электронный рецепт»**.

1 - Герасимов В.А. - Подходы к использованию системы облачной электронной цифровой подписи в Республике Беларусь

Итоги проекта «Система облачной подписи» в Республике Беларусь

Государственное предприятие "НИИ ТЗИ"

Докладчик: заместитель директора
по научной работе,
к.т.н., **Арестович Дмитрий Николаевич**