Платформа цифрового доверия для подтверждения персональных данных (ПЦД ПД)

Участники проекта

НАЦИОНАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР ЦИФРОВОЙ КРИПТОГРАФИИ

- Автономная некоммерческая организация «Национальный технологический центр цифровой криптографии» (АНО НТЦ ЦК) создана для обеспечения частно-государственного взаимодействия и развития технологий криптографии. https://digitalcryptography.ru

IDX

- ООО «Системы управления идентификацией» (IDX) – российский провайдер услуг удаленного удостоверения личности, верификации персональных данных и эксперт в сфере доверенного онлайн-взаимодействия, созданный Фондом развития интернет-инициатив (ФРИИ). https://iidx.ru

КРИПТОНИТ

- АО «НПК «Криптонит» — российская технологическая и научно-исследовательская группа компаний в составе холдинга «ИКС». Мы разрабатываем ПО и ПАК для хранения и анализа больших данных с помощью ML-моделей. «Криптонит» также проводит научные исследования в области ИИ, криптографии, информационной безопасности. https://kryptonite.ru

Причина уязвимости персональных данных

1. **Интернет-сервисы собирают избыточные данные о гражданах** (Браузеры, Сервисы доставки, Каршеринг и х-шеринг, E-commerce, Турагентства и пр.)

Ни один онлайн-сервис не может оправдать избыточный сбор данных операционной необходимостью

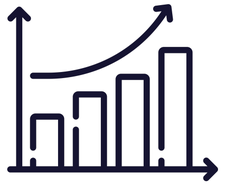
2. **Большинство операторов ПДн не выполняют требования безопасности и защищенности ИСПДн**

3. **Субъекты ПДн не контролируют оборот своих данных**

Утечки персональных данных

- **Ритейл**
- **ИТ**
- **Финансы**

чаще всего сталкиваются с утечками данных*



Рост <u>объема</u> утечек данных

- **на 72%** в H1**
- **двукратный** в Q1 2023

по сравнению с Q1, 2022***

* Агрегированные данные ГК InfoWatch, «Солар», Innostage и др.
** Данные InfoWatch
*** Данные Kaspersky

Проблемы участников рынка

Зачем сервисы собирают ПДн

- **Удостоверить данные пользователя**
- **Знать, кому предъявить претензии, если что-то пошло не так**
- **Обогатить данные для маркетинговой кампании**
- **Выполнить обязательные требования регуляторов** (подтвердить возраст, информировать МВД, подтвердить состояния здоровья и т.д.).

Забота Государства

- **Защитить интересы субъектов ПДн и предоставить им реальный механизм контроля личных данных**
- **Обеспечить цифровым сервисам условия поддержки роста в действующих условиях регулирования оборота ПДн**
- **Обеспечить контроль соблюдения норм регулирования ПДн**

Интересы субъекта ПДн

- **Контролировать передачу и использование личных данных**

Как решить проблемы участников рынка

1. Использовать ЕСИА+ЕБС для идентификации и аутентификации

ЕСИА+ЕБС содержат ограниченный набор данных, которые туда загружены исключительно в целях предоставления госуслуг

к ЕСИА+ЕБС имеют доступ только «избранные» сервисы

ЕСИА раскрывает данные сервису

2. Использовать ПЦД ПД

— информационную систему для предоставления физическим лицам (гражданам) возможности безопасного подтверждения своих ПД при обращении к различным сервисам без раскрытия содержания этих ПД.

Персональные данные гражданина хранятся только у гражданина и инспектора персональных данных (паспортные данные — МВД РФ, СНИЛС — ПФР, ИНН — ФНС)

Для получения цифровых сервисов и услуг гражданин, используя индивидуальный модуль доверия (ИМД), предоставляет свои данные поставщику сервисов и услуг в виде зашифрованного блока данных, при этом поставщик сервисов и услуг не имеет доступа к содержанию этих данных

Поставщик сервисов и услуг имеет возможность передать зашифрованный блок данных инспектору персональных данных и получить от него заключение о соответствии этих данных хранящимся у инспектора

Как работает ПЦД ПД: Участники

Пользователь — Пользователь Сервиса, субъект персональных данных.

Приложение пользователя: — Агент Пользователя — программа или устройство, посредством которой Пользователь взаимодействует с участниками протокола.

Сервис: — Сервис-информационная система бизнеса, запрашивающая у Пользователя информацию о персональных данных в интересах бизнеса.

Инспектор: — Инспектор персональных данных. Доверенная служба, которая подтверждает сервису соответствие предъявляемых персональных данных, идентификатору Пользователя. Например, МВД, ФНС, ПФР.

УЦ: — Удостоверяющий центр.

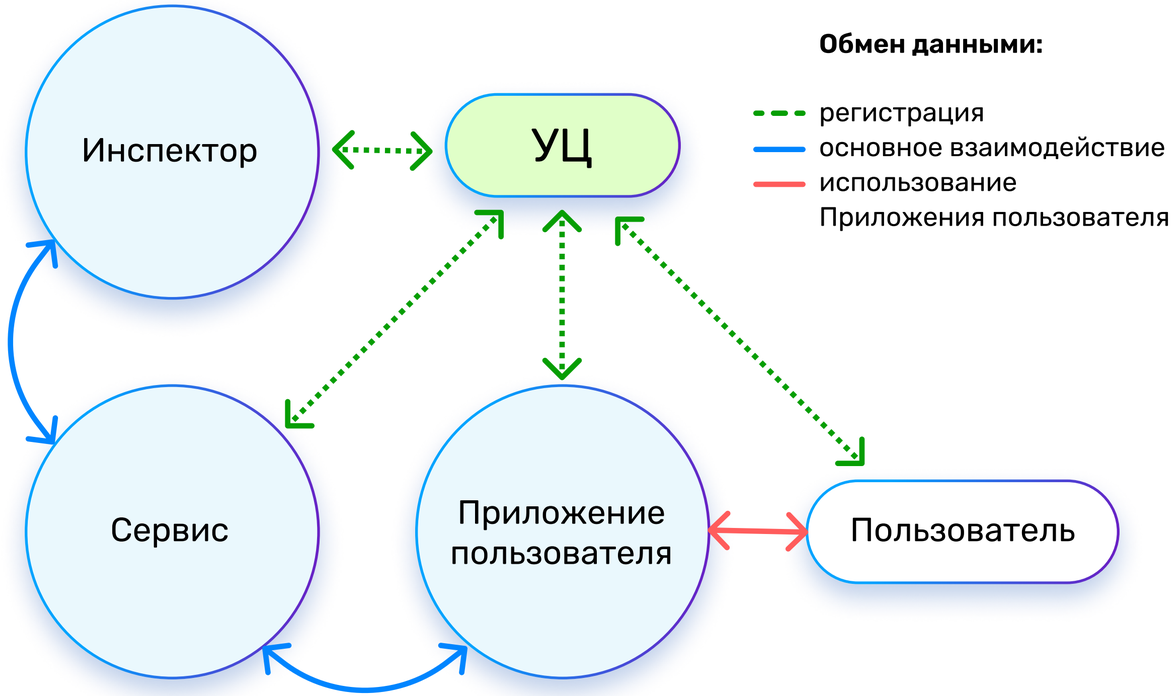


Схема ПЦД ПД

Элементы Платформы цифрового доверия

Государственные информационные системы, ФОИВ
МВД, ФНС, ПФР — **Инспектор**

Проверка шифрованного подтверждения ПДн

Подтверждение ПДн

Бизнес
Магазины, коммерческие компании, гостиницы — **Сервис**

Передача шифрованного подтверждения ПДн

Агент (приложение)

Индивидуальный модуль доверия (ИМД)

Регистрация

Регистрация

Центр Управления

- Служба регистрации
- УЦ
- Служба протоколирования

Получение и проверка идентификаторов участников

Регистрация участников | ИКС-протокол | Защищенное соединение | Открытые ПДн | Шифрованные ПДн

Информация об участниках и транзакциях

Пользователь:

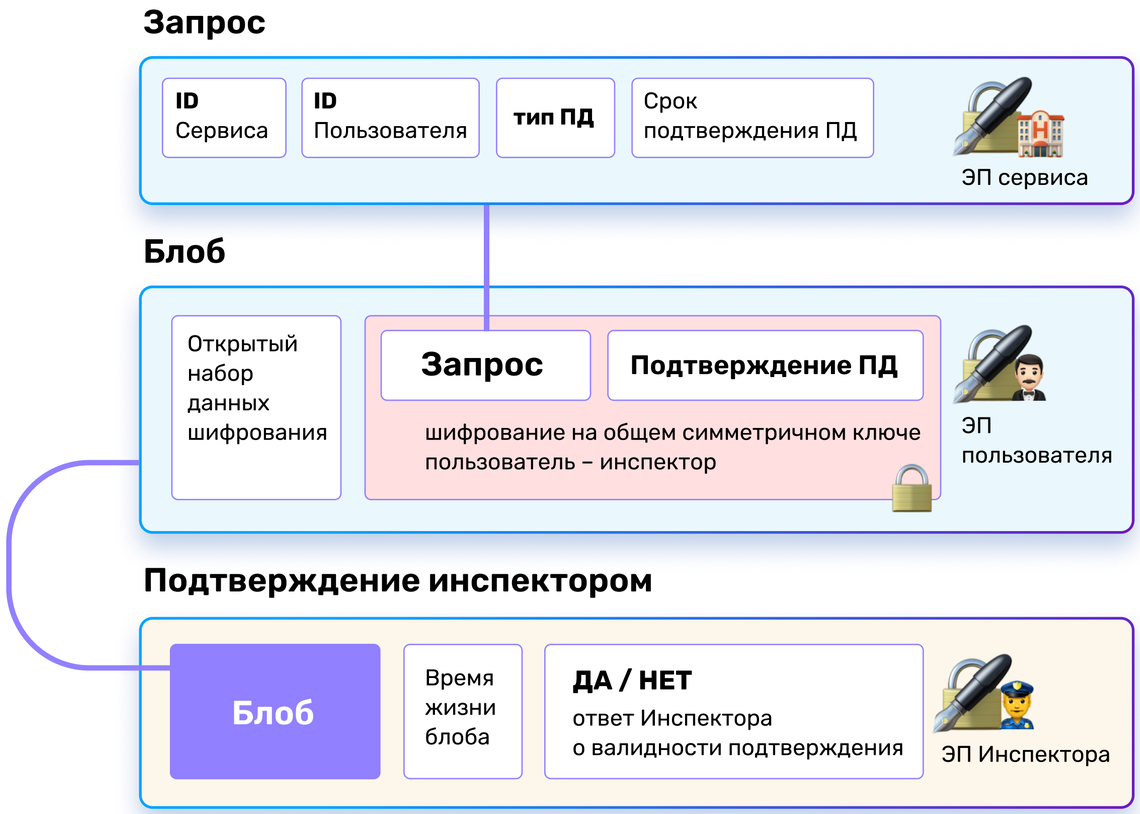
Видит какому сервису и какие ПД он подтверждал (всю свою историю подтверждений).

Сервис:

Доступны только идентификаторы пользователей, которые воспользовались его услугами и подтвердили ПД.

Инспектор:

В онлайн режиме доступна информация когда, какие ПД и какому сервису пользователь с определенным идентификатором подтверждал.



Криптографические механизмы ПЦД ПД

В рамках протокола используются следующие криптографические механизмы:

- вычисление значения хэш-функции в соответствии с ГОСТ 34.11–2018;
- генерация случайного значения и ключевой пары в группе точек эллиптической кривой, удовлетворяющей стандарту ГОСТ 34.10–2018;
- формирование и проверка электронной подписи в соответствии с ГОСТ 34.10–2018.
- Алгоритм согласования ключей VKO P 50.1.113-2016;
- Алгоритм блочного шифрования «Кузнечик» ГОСТ 34.12–2018 в режиме гаммирования ГОСТ 34.13-2018.

Выполнение перечисленного выше функционала осуществляется участниками с помощью отдельного элемента – модуля доверия.

Функционал модулей доверия каждого из участников:

Индивидуальный модуль доверия (ИМД) пользователя

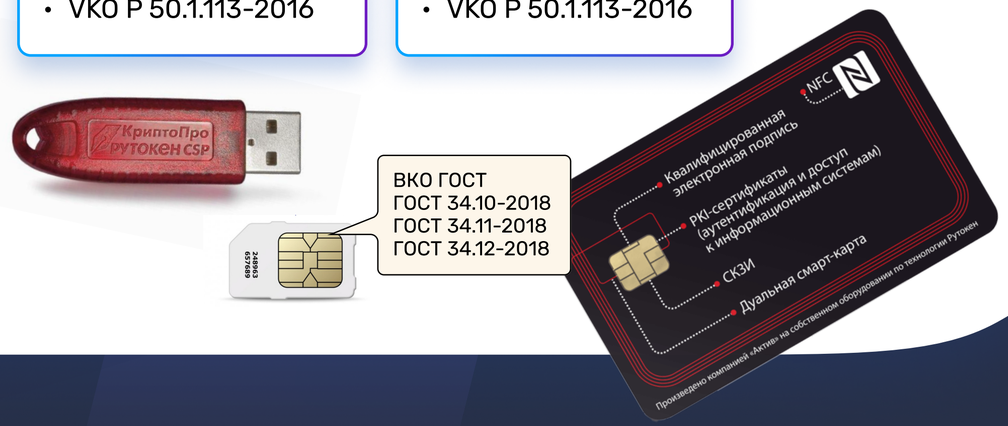
- ГОСТ 34.10-2018
- ГОСТ 34.11-2018
- ГОСТ 34.12-2018
- ГОСТ 34.13-2018
- VKO P 50.1.113-2016

Модуль доверия инспектора (МДИ)

- ГОСТ 34.10-2018
- ГОСТ 34.11-2018
- ГОСТ 34.12-2018
- ГОСТ 34.13-2018
- VKO P 50.1.113-2016

Модуль доверия сервиса (МДС)

- ГОСТ 34.10-2018
- ГОСТ 34.11-2018



Как использование ПЦД ПД защитит ПДн и удовлетворит потребности участников рынка

Для граждан

- Предотвращение утечек ПД и риска их неправомерного использования
- Обеспечение механизма контроля над своими ПД

Для бизнеса

- Уменьшение количества ПД для обработки, а также финансовых затрат на хранение и обработку ПД
- Снижение риска утечки ПД и, как следствие, оборотных штрафов (будут введены, скорее всего, в 2024 году)
- Повышение доверия клиентов
- Возможность создания новых сервисов, исключающих затраты на обработку ПД (работа с обезличенными данными)

Для государства

- Реальный механизм контролируемого оборота ПД
- Безопасность цифровых сервисов и доверие граждан
- Активное использование инфраструктуры электронного правительства