DATA FUSION

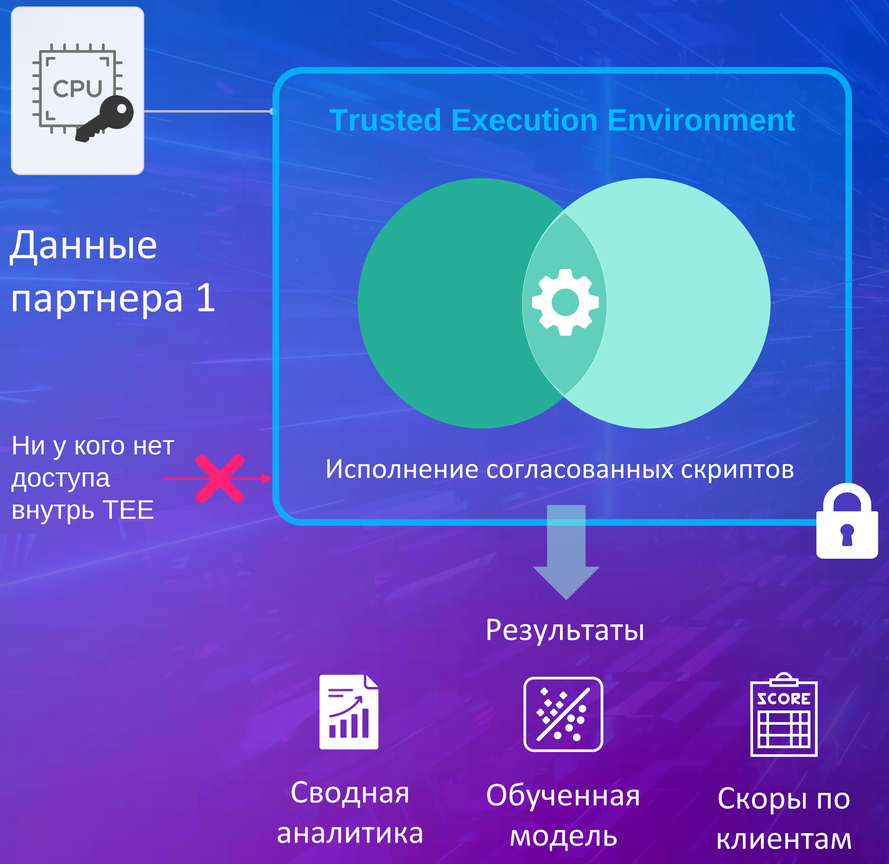
FIRST RUSSIAN DATA FORUM

ДОВЕРЕННЫЕ СРЕДЫ ИСПОЛНЕНИЯ ДЛЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Артём Алексеев

Управляющий партнер Aggregion

Технология Доверенных сред исполнения (TEE)



ОБЕСПЕЧИВАЮТ СКВОЗНУЮ ЗАЩИТУ ДАННЫХ

Хранение

Передача

Обработка

МОГУТ БЫТЬ РАЗНЫЕ КОМБИНАЦИИ:

1. TEE у каждого партнера, соединенные в конфиденциальный кластер
2. TEE у одного из партнеров
3. TEE у стороннего обработчика

Поддерживается основными производителями процессоров и доступна автономно

intel. HUAWEI NVIDIA AMD arm

Практика внедрения

БИЗНЕС

Развитие бизнеса с использованием данных партнеров: допродажи, новые клиенты, точнее оценка рисков и пр.

ИБ

Ок: надежная хоть и новая технология. Лучше других доморощенных решений.

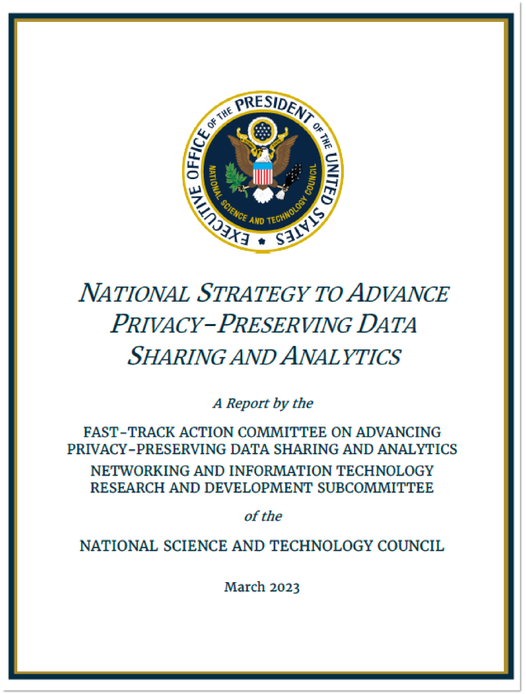
ЮРИСТЫ

Нет понятия конфиденциальная обработка/TEE в законодательстве

Ключевой вопрос – является ли такая обработка передачей данных и соответственно, требует ли согласий?

На сегодня ответ зависит от риск-аппетита компаний.

Регуляторные документы



Решение для совместной обработки данных в соответствие с законодательством о ПД

Input privacy - ✓

Обработчик и другая сторона не получают доступа к передаваемым на обработку данным – раскрытия нет

Confidential data processing - ✓

Нет доступа во время обработки данных-

Output privacy - ?

Выходные данные не содержат данных по отдельным субъектам ПД?

Output privacy может быть обеспечена обязательным контролем выходных данных.

Дополнительные инструменты снижения рисков:

1. **Фильтры Блума** (вероятностные отпечатки данных) для пересечения данных – другая сторона не сможет найти не своих клиентов, без ПД
2. **Блокчейн для подписания скриптов.** Внутри TEE могут быть запущены только согласованные скрипты. Скрипт контроля выходных данных обязателен.
3. **Аудиторский след** всех операций в неизменяемом реестре
4. **Использование единого TEE-обработчика** (формально нет передачи данных между партнерами)

Конфиденциальные вычисления открывают беспрецендентные новые возможности

Конфиденциальное облако

Confidential AI

Аналитика на чувствительных данных

CONFIDENTIAL DATA COLLABORATION

Банки и финтех

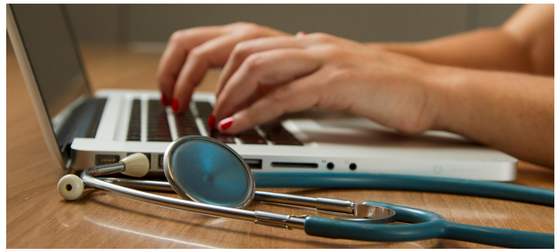
- Партнерства и экосистемы
- Кросс-продажи с использованием данных партнеров
- Улучшение рисковых моделей
- Антифрод

Телеком и медиа

- Работа без кук
- Развитие Adtech/martech решений с использованием data cleanrooms
- Отраслевые дата-платформы: туризм, умные города и пр.

Гос. сектор

- Обмен данными между учреждениями
- Аналитика граждан 360 совместно с бизнесом
- Отраслевые дата-платформы
- Digital identity
- Анонимные опросы



Медицина

- Интеграция мед. данных
- Отбор пациентов для клинических исследований
- Безопасный AI над мед. данными