



АССОЦИАЦИЯ
БОЛЬШИХ ДАННЫХ

ЭКОНОМИКА
АНО «Цифровая экономика»

FIRST RUSSIAN DATA FORUM

Доверенный посредник на рынке данных

Ассоциация больших данных, Марат Тахавиев,
руководитель GR-проектов

Доверенный посредник удовлетворит потребности всех участников рынка больших данных

Потребности

Решения в рамках Доверенного посредника



Владельцы данных и разработчики

- Разработка инструментов для **безопасной совместной** работы с данными
- Повышение **доступности данных** для развития технологий ИИ и БД

- Создание технологической **инфраструктуры**, организационной и договорной **обязки**, обеспечивающей целевое и безопасное использование данных с **быстрым и не затратным** подключением
- Достижение **нормативной определенности**, предоставление **возможности** для обезличивания и обработки данных



Общество и потребители

- **Защита прав**, включая безопасность данных и минимизацию рисков при обработке данных
- Внедрение более безопасных продуктов и **повышение их качества** для потребителей

- Использование **обезличенных** данных и оценка **уровня риска** их деобезличивания, **контроль целей** использования данных и расширенные **меры и гарантии их безопасности**
- Повышение **прозрачности** процессов обработки данных и дополнительные **инструменты государственного контроля** над обработкой данных



Государство

- Снижение **зависимости от иностранных** решений и технологий
- Обеспечение налоговых **доходов бюджета** за счет развития рынка ИИ и БД

- Поддержка **отечественных новаторов** путем предоставления доступа к данным
- **Активизация бизнеса** за счет **нормативной определенности** и **сокращение его затрат** на инфраструктуру

Организационная структура: управление и контроль

ПОЛНОМОЧИЯ ОПЕРАТОРА ПЛАТФОРМЫ

- Осуществляет методическую поддержку Поставщиков по обезличиванию данных
- Обеспечивает работу Платформы, вкл. контроль доступов и обеспечение безопасности данных, мониторинг использования данных
- Готовит датасеты для разработчиков в сфере БД и ИИ

ПОЛНОМОЧИЯ РАБОЧЕЙ ГРУППЫ

- Оценивает данные на соответствие допустимому риску деобезличивания
- Готовит рекомендации для поставщиков данных по снижению риска деобезличивания

Состав

- Академия криптографии РФ
- Ассоциация Больших Данных
- Роскомнадзор
- Индустрия (банкинг, телеком, ритейл, медицина)
- АНО «Цифровая экономика»



Права и обязанности Поставщика данных

- Обезличивает персональные данные и загружает их на платформу
- Вправе получить доступ к лог-файлам по запросу Оператору Платформы
- Вправе требовать изменения паспорта Проекта

Права и обязанности Разработчика

- Осуществляет работу с обезличенными данными на Платформе, в т.ч. создает модели
- Обязан прекратить обработку, если был реализован риск деобезличивания данных

Безопасность данных на Платформе

- Платформа соответствует 152-ФЗ и подзаконным актам, сертифицирована ФСТЭК
- Выгрузка данных с Платформы в каком-либо виде технически невозможна
- Данные на Платформе хранятся отдельно и могут быть объединены только в рамках интерактивной среды, если это предусмотрено проектом
- На Платформе возможна работа исключительно с преобразованными (обезличенными, синтезированными или санитизированными) данными
- Все действия на Платформы логируются и отслеживаются Оператором Платформы и Поставщиком данных
- Поставщик данных и Разработчик реализуют меры безопасности, предусмотренные паспортом Проекта и договором с Оператором Платформы

Обезличивание, синтезирование или санитизация данных осуществляется **Оператором Платформы или Поставщиком данных** в зависимости от условий Проекта.

Они самостоятельно определяют метод обезличивания, в т.ч. из утвержденных Приказом Роскомнадзора № 996.

Риск деобезличивания (P_o) – риск реидентификации субъекта персональных данных.

Если набор данных не соответствует допустимому риску, допуск Разработчика запрещен.

Для разных сценариев использования данных устанавливаются разные пороги риска реидентификации.

Оценка риска деобезличивания учитывает контекстный риск и риск данных.

$$P_o = P_k \times P_d$$

Контекстный риск (P_k)

Политики безопасности, безопасность IT серверов, внешние факторы

Риск данных (P_d)

Чувствительность данных, сценарий публикации, профиль атаки

Апробация подходов к регулированию Доверенных посредников в рамках экспериментального правового режима



Алгоритмы преобразования данных, обеспечивающие их защиту и доступность для разработчиков в сфере ИИ и БД

1

Разработать и подтвердить **требования к обезличиванию** данных, при котором гарантируется и безопасность, и полезность использования данных путем апробации **методики** оценки рисков деобезличивания

2

На основании разработанной методики оценки рисков установить **значение рисков для (не)отнесения** получаемых в результате обезличивания, санитизации, синтезирования данных к персональным

3

Подтвердить востребованность **института доверенного посредника** в сфере данных и разработать **требования** к организационной, технологической и правовой моделям его функционирования



Технологическая инфраструктура и организация доступа к ней для безопасной работы с данными

По результатам ЭПР станет возможно установить:

- **критерии разграничения** персональных и неперсональных данных
- **требования к обезличиванию и иному преобразованию данных** на основе модели оценки риска, создать **библиотеки** методик обезличивания и рисков деобезличивания
- **требования к институту** доверенного посредника, включая распределение ответственности, требования к его деятельности, информационной безопасности и т.д.