АССОЦИАЦИЯ БОЛЬШИХ ДАННЫХ

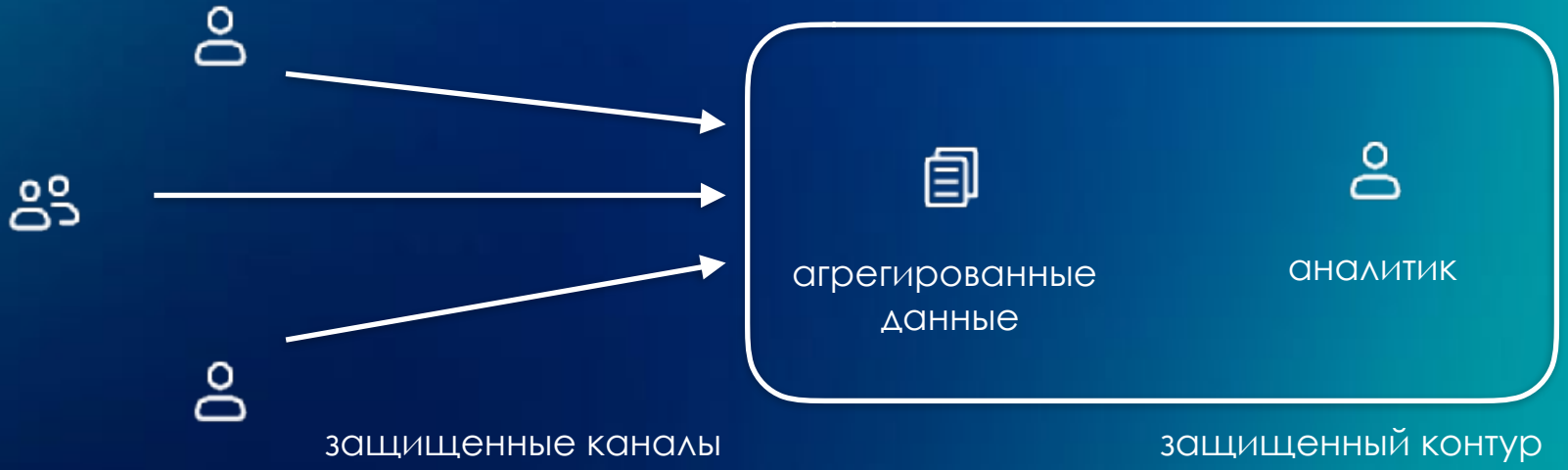
ЭКОНОМИКА

FIRST RUSSIAN DATA FORUM

Защищенная обработка данных

АК РФ/ Г. Маршалко

Анализ данных (классический подход)



Анализ данных (проблема)

Анализ данных (возможное решение)

Анализ данных (вопросы)

* Цель нарушителя

  Возможности нарушителя

  Методы противодействия нарушителю

  Оценки безопасности методов

  Архитектура системы анализа данных

  Качество анализа данных

  Удобство эксплуатации

Новая информация о защищаемых данных

Анализ данных (вопросы)

Цель нарушителя

* Возможности нарушителя

Методы противодействия нарушителю

Оценки безопасности методов

Архитектура системы анализа данных

Качество анализа данных

Удобство эксплуатации

Честный, но любознательный: формирует запросы к базе данных

Анализ данных (вопросы)

Цель нарушителя

Возможности нарушителя

* Методы противодействия нарушителю

Оценки безопасности методов

Архитектура системы анализа данных

Качество анализа данных

Удобство эксплуатации

организационно-технические: федеративное обучение

алгоритмические: обезличивание, синтетические данные

криптографические: MPC, гомоморфное шифрование

Анализ данных (вопросы)

Цель нарушителя

Возможности нарушителя

Методы противодействия нарушителю

* Оценки безопасности методов

Архитектура системы анализа данных

Качество анализа данных

Удобство эксплуатации

организационно-технические: слабые оценки

алгоритмические: гарантированные при определенных условиях

криптографические: гарантированные

Анализ данных (вопросы)

Цель нарушителя

Возможности нарушителя

Методы противодействия нарушителю

Критерии эффективности методов

* Архитектура системы анализа данных

Качество анализа данных

Удобство эксплуатации

Зависит от используемого метода. Общее свойство - аналитик не имеет прямого доступа к данным

Анализ данных (вопросы)

FIRST RUSSIAN DATA FORUM

Цель нарушителя

Возможности нарушителя

Методы противодействия нарушителю

Критерии эффективности методов

Архитектура системы анализа данных

* Качество анализа данных

Удобство эксплуатации

Такое же, или несколько хуже снижаться. Можно оценивать ошибки

Анализ данных (вопросы)

Цель нарушителя

Возможности нарушителя

Методы противодействия нарушителю

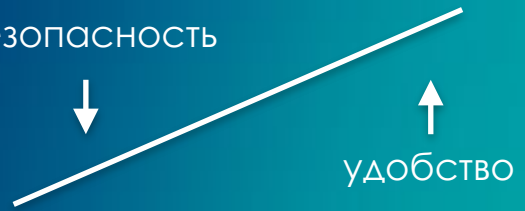
Критерии эффективности методов

Архитектура системы анализа данных

Качество анализа данных

* Удобство эксплуатации

Изменение принципов работы аналитика



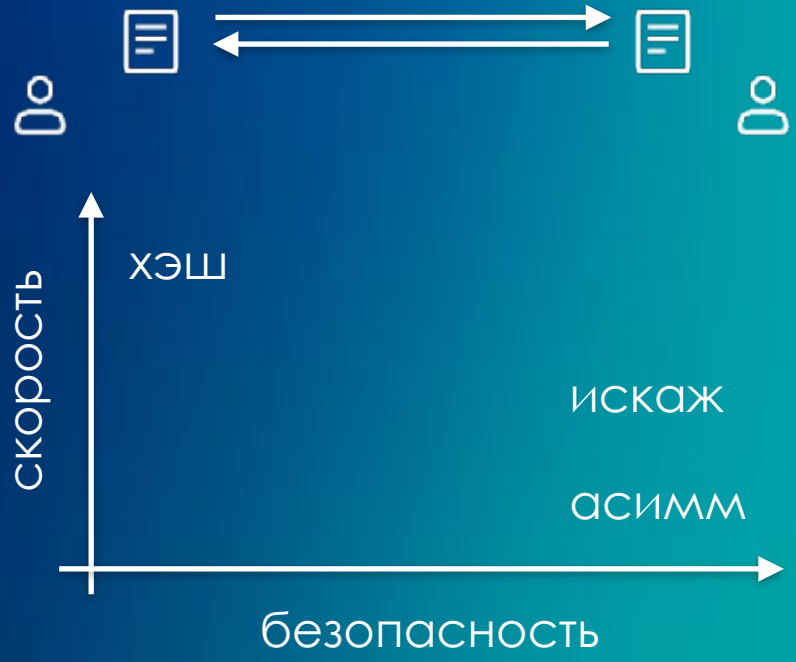
Конфиденциальное сравнение множеств (private set intersection)

Два абонента должны определить общие элементы своих списков без раскрытия различных

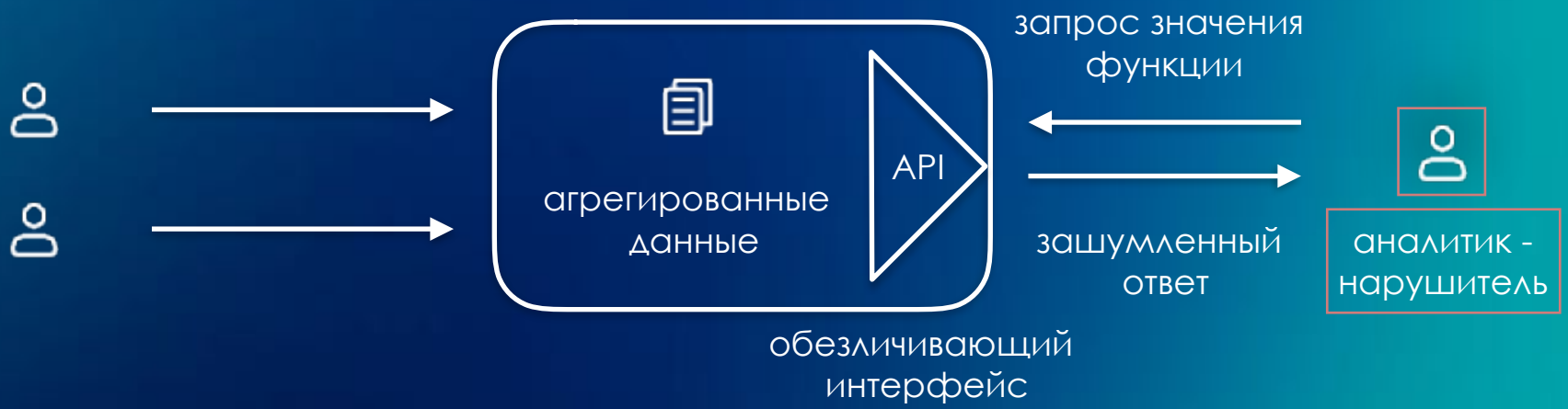
~~сравнить хэш-значения -~~ небезопасно!

использование асимметричных криптографических механизмов, искаженных схем, передачи с забыванием и тп

гарантированная безопасность



Статистическое обезличивание (differential privacy)



сервисная архитектура

гарантированное обезличивание при контроле количества запросов

гарантированное качество данных

требует реализации функций в API

требует контроля количества запросов

применимо к числовым данным