

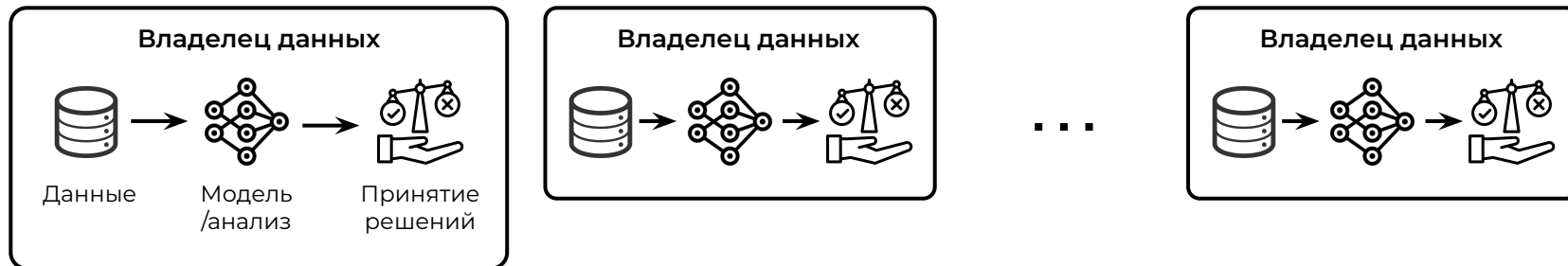
Массовые конфиденциальные вычисления Почему их нет?

П.В. Снурницын (ВМК МГУ)

5 июня 2025 г.

CTCrypt 2025, Круглый стол “На пути к экономике данных без
экономии данных. Практические наблюдения о протоколах
конфиденциальных вычислений”

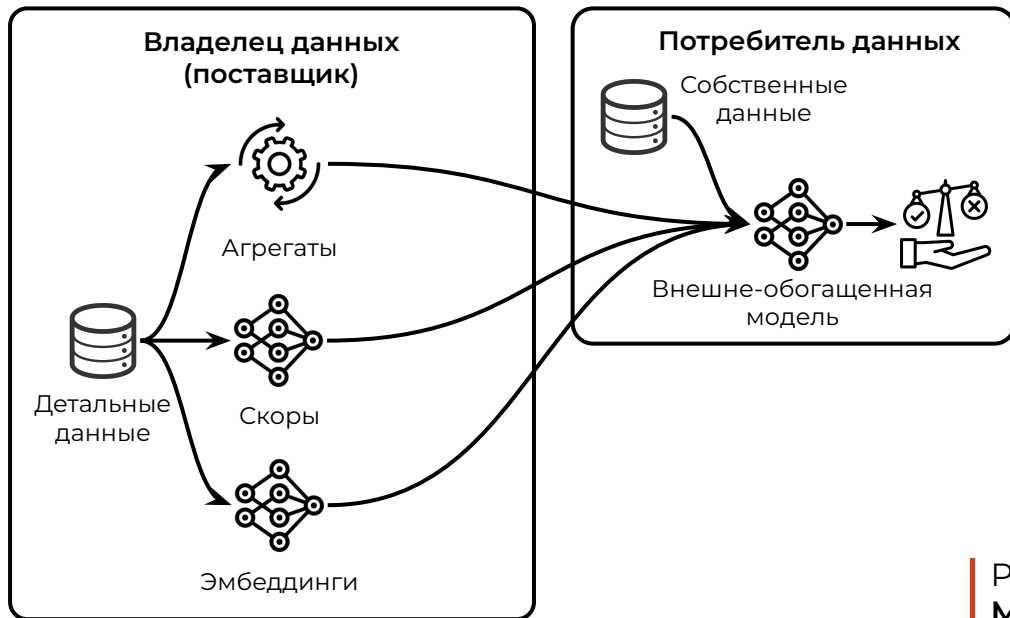
Обогащение данных: задача



Базовое допущение:

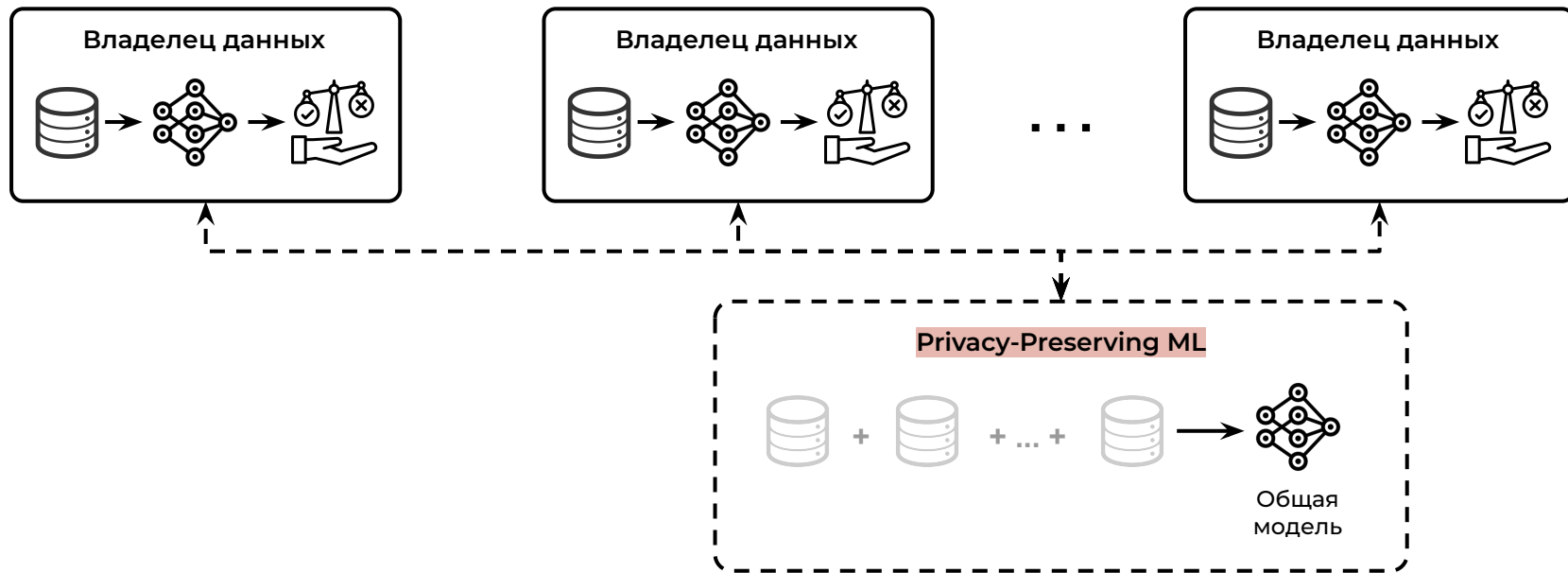
Чем больше данных тем лучше модель/аналитика

Обогащение данных: data-сервисы



Развитие подхода:
Маркетплейсы данных

Обогащение данных: конф. вычисления & PPML

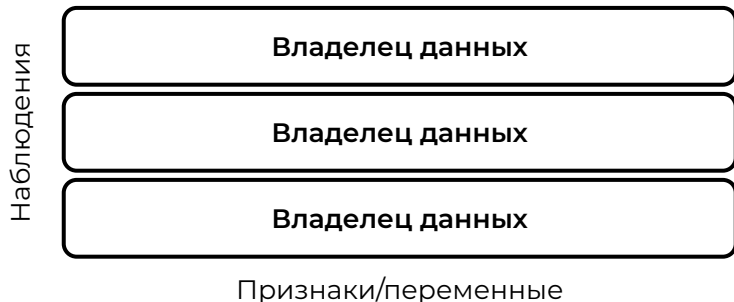


Другое допущение:

Прямое использование признаков лучше, чем скоры и агрегаты

Виды обогащения данных

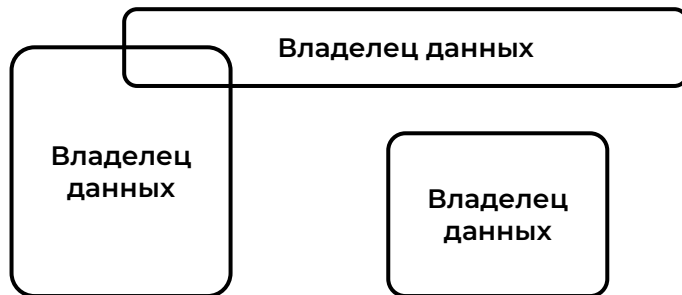
Горизонтальное



Вертикальное



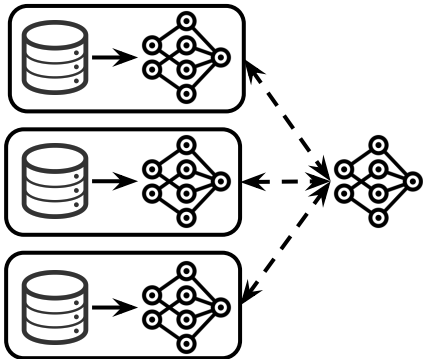
Агрегированное/трансферное/метаданные



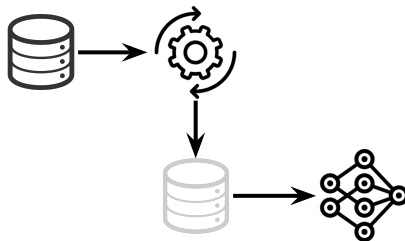
Интересный кейс:
валидация моделей

Конфиденциальные вычисления & PPML

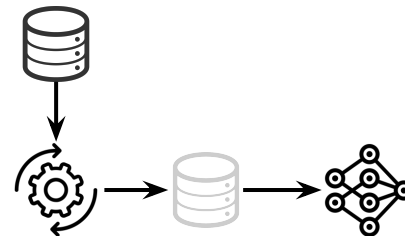
Федеративное обучение (FL)



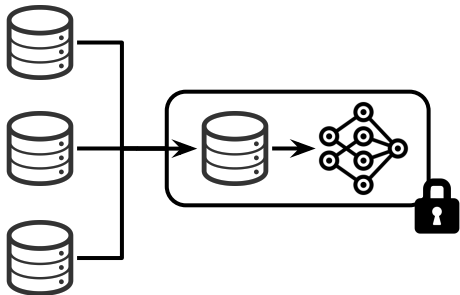
Синтетические данные
сохраняющие структуру



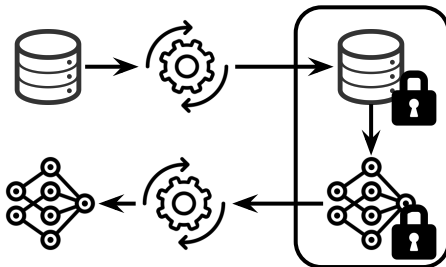
Дифференциальная
приватность



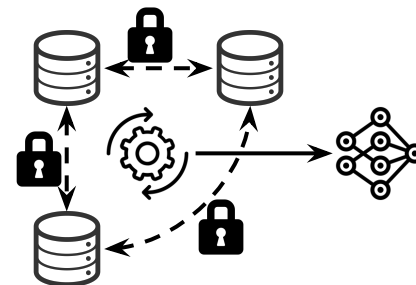
Доверенные среды
/криптоанклавы (TEE)



(Полностью) гомоморфное
шифрование (FHE)



Совместные конф.
вычисления (SMPC)



Обогащение данных & PPML: основные вызовы

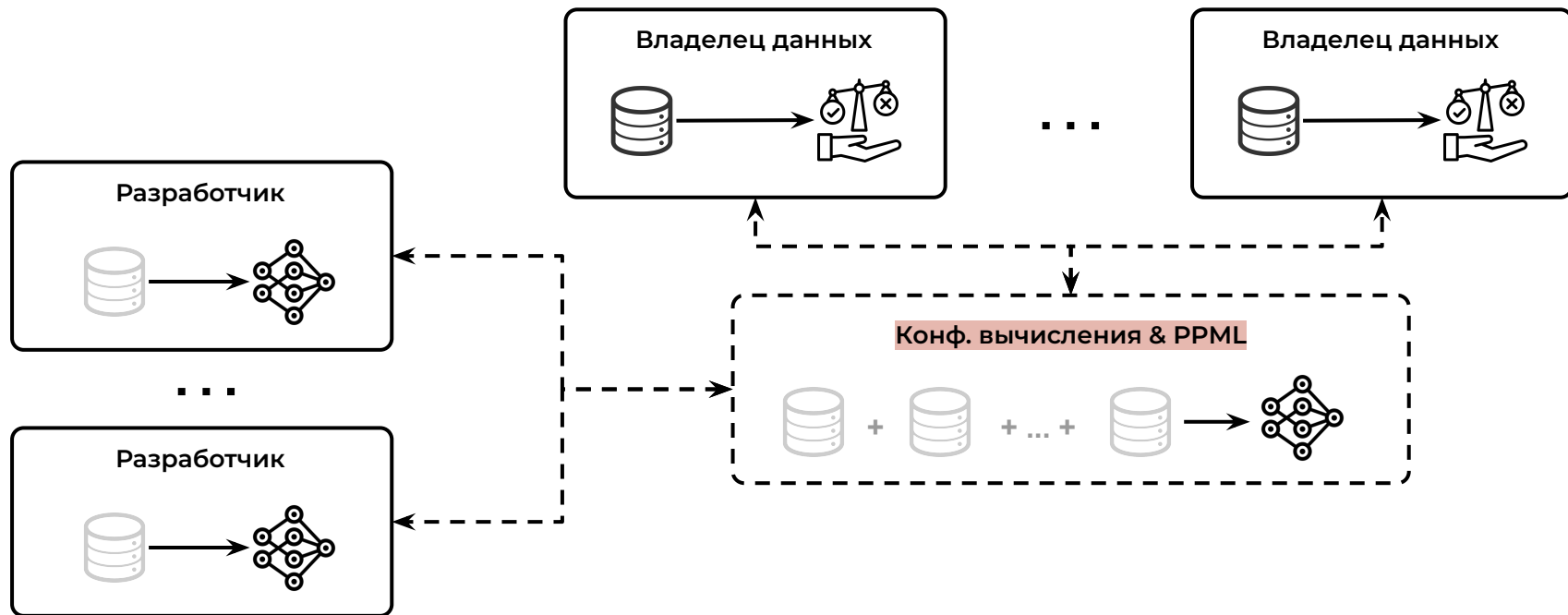
Базовое допущение Чем больше данных тем лучше модель/аналитика
часто не выполняется на практике

Feature Engineering никуда не девается, а становится сложнее

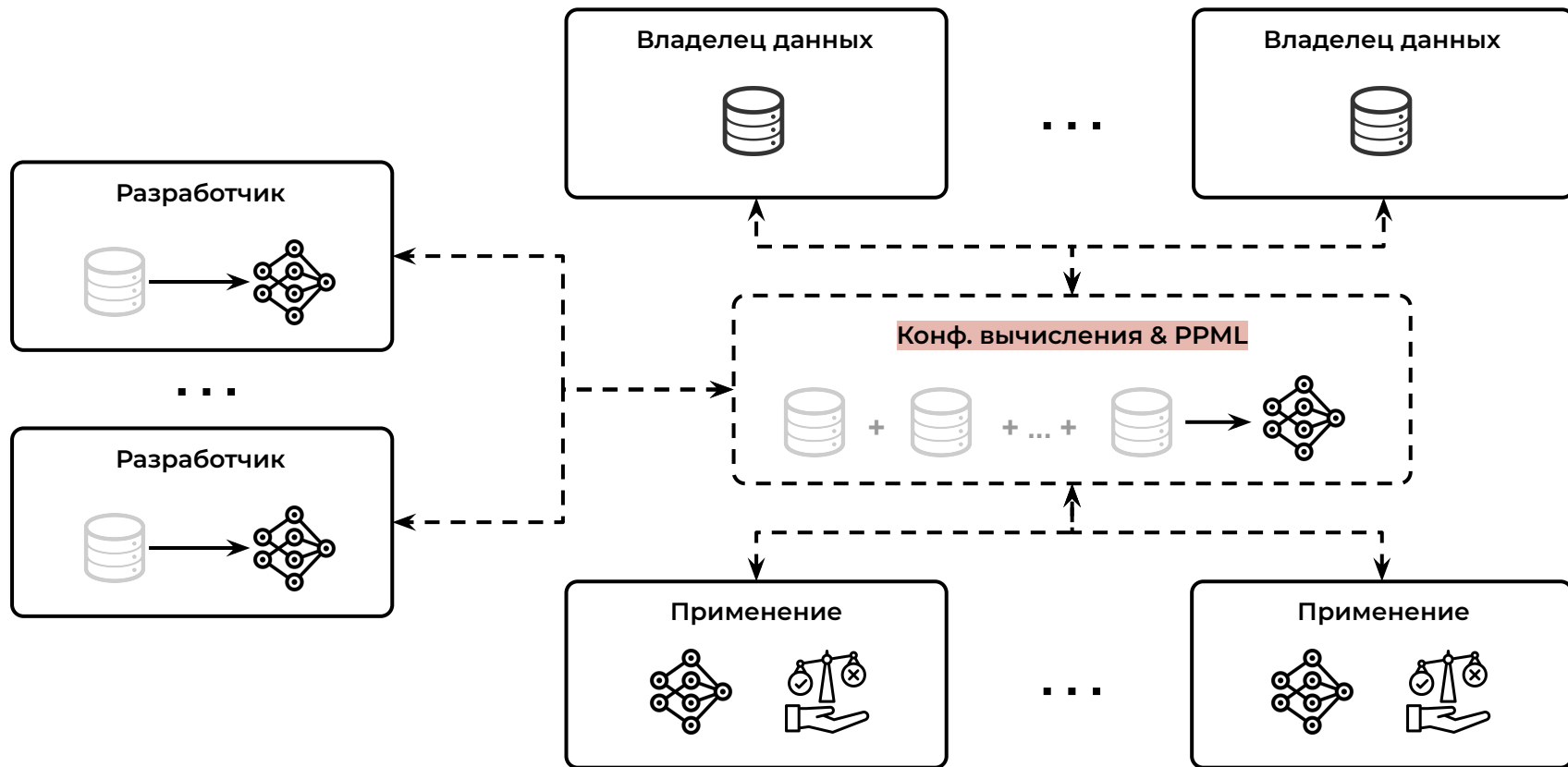
Для бизнеса – пилот, а для IT – полноценный проект (инфраструктура, ИБ, ...)

Ценообразование: чьи данные приносят большую ценность?

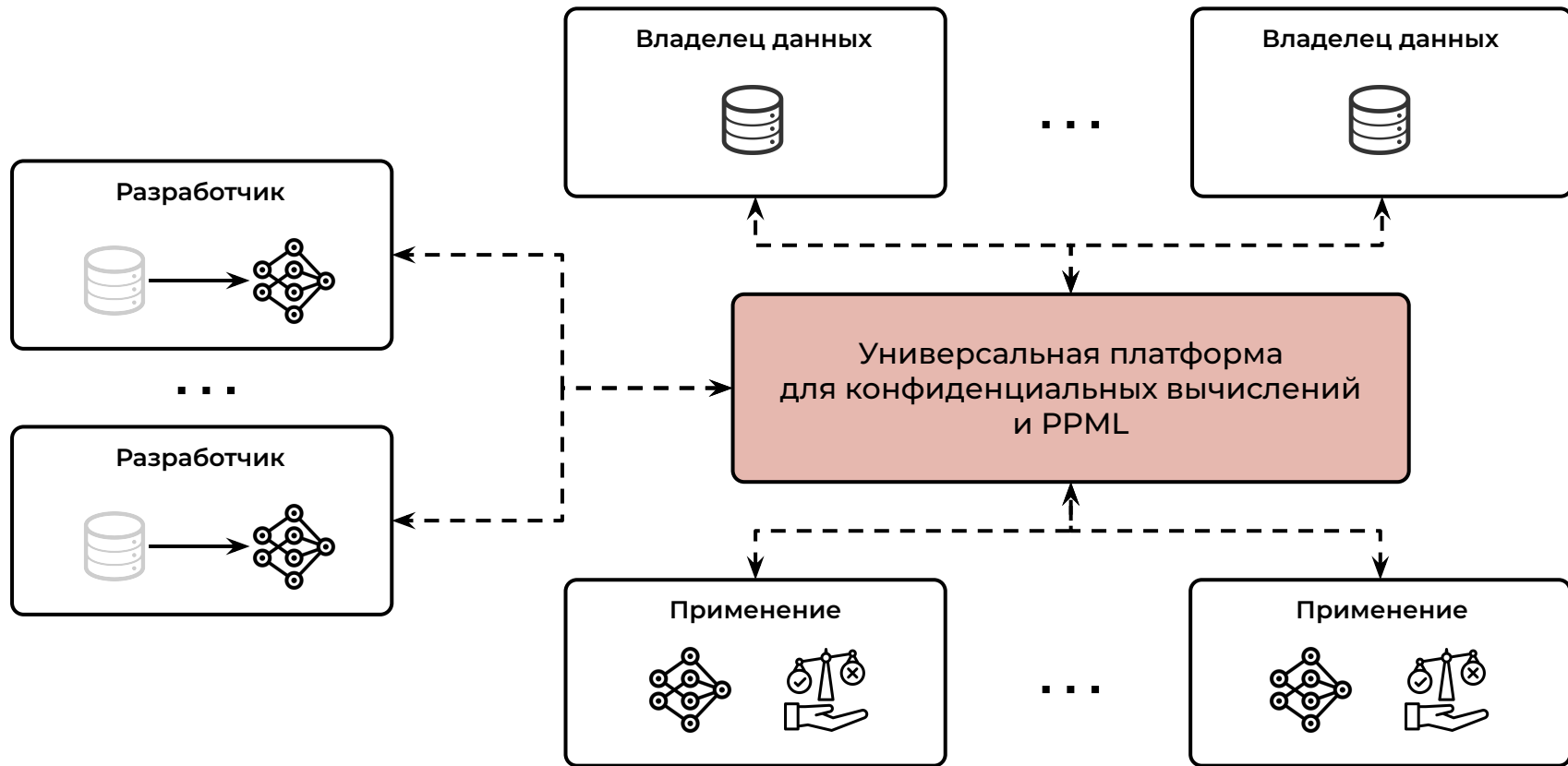
Другие задачи: доступ к данным



Другие задачи: недоверенные среды



Идеальный мир



Вызовы и открытые вопросы

Производительность

Свойства безопасности, в том числе
для не-СКЗИ (например, FL)

Стандартизация и сертификация

Правовое поле

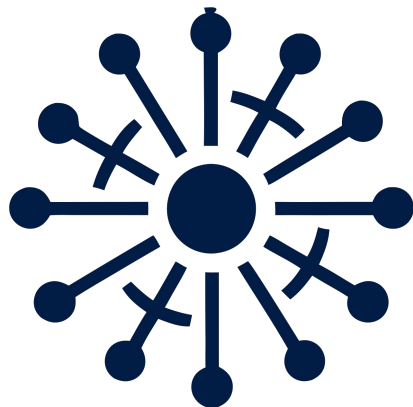
Ценообразование

...

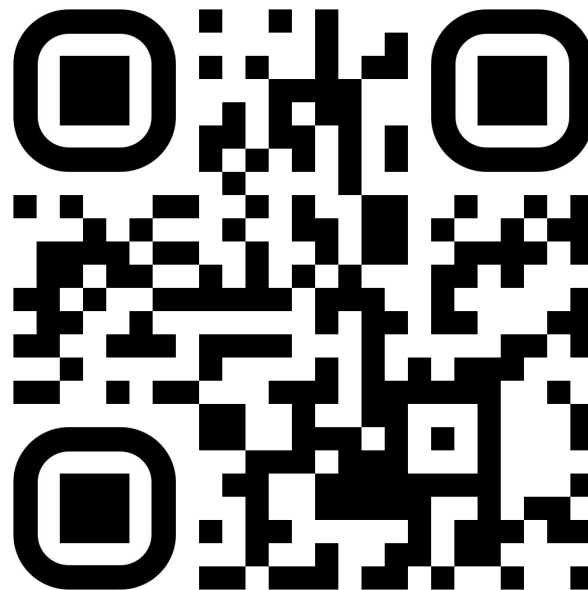
Универсальная платформа
для конфиденциальных вычислений
и PPML

Семинар СПАА

Современная Прикладная Алгебра и Арифметика, ИБ ВМК МГУ
Telegram: **@spaasem**



СПАА



Сообщество NoML

| Not Only ML: анализ данных, интеллект принятия решений и связанные вопросы
Telegram: **@noml_digest**

