КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

ИИ в R&D: от молекул до процессов

Федеративное обучение в R&D

Промышленность, материалы, биотех: как обучать общие модели, не вывозя данные



Руслан Лукин

Руководитель лаборатории ИИ в новых материалах, Университет Иннополис

О докладчике



Руслан Лукин

Руководитель лаборатории ИИ в новых материалах

Университет Иннополис

10
индекс Хирша

30+
статей и патентов

Специализация

- Оптимизация индустриальных производств
- Активное обучение для R&D
- Генеративные алгоритмы для материалов и молекул

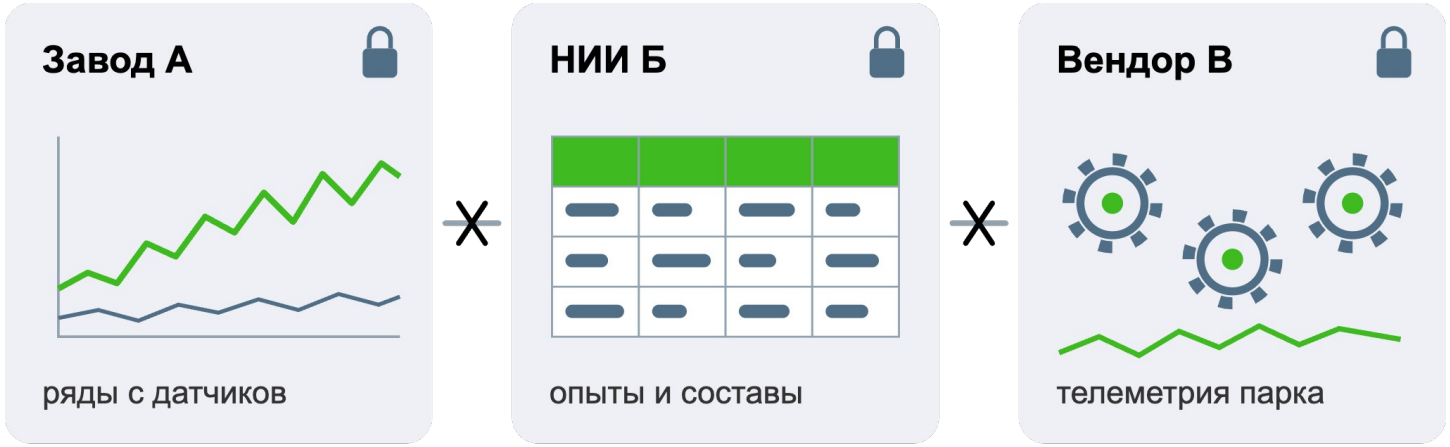
Реализованные проекты

ХимРар	**Сбер**	**Норникель**
СИБУР	**Татнефть**	**Минсельхоз**

и другие индустриальные и государственные заказчики

Данные R&D разложены по закрытым контурам

Три контура — три неполные картины





Почему нельзя просто собрать всё в одном месте

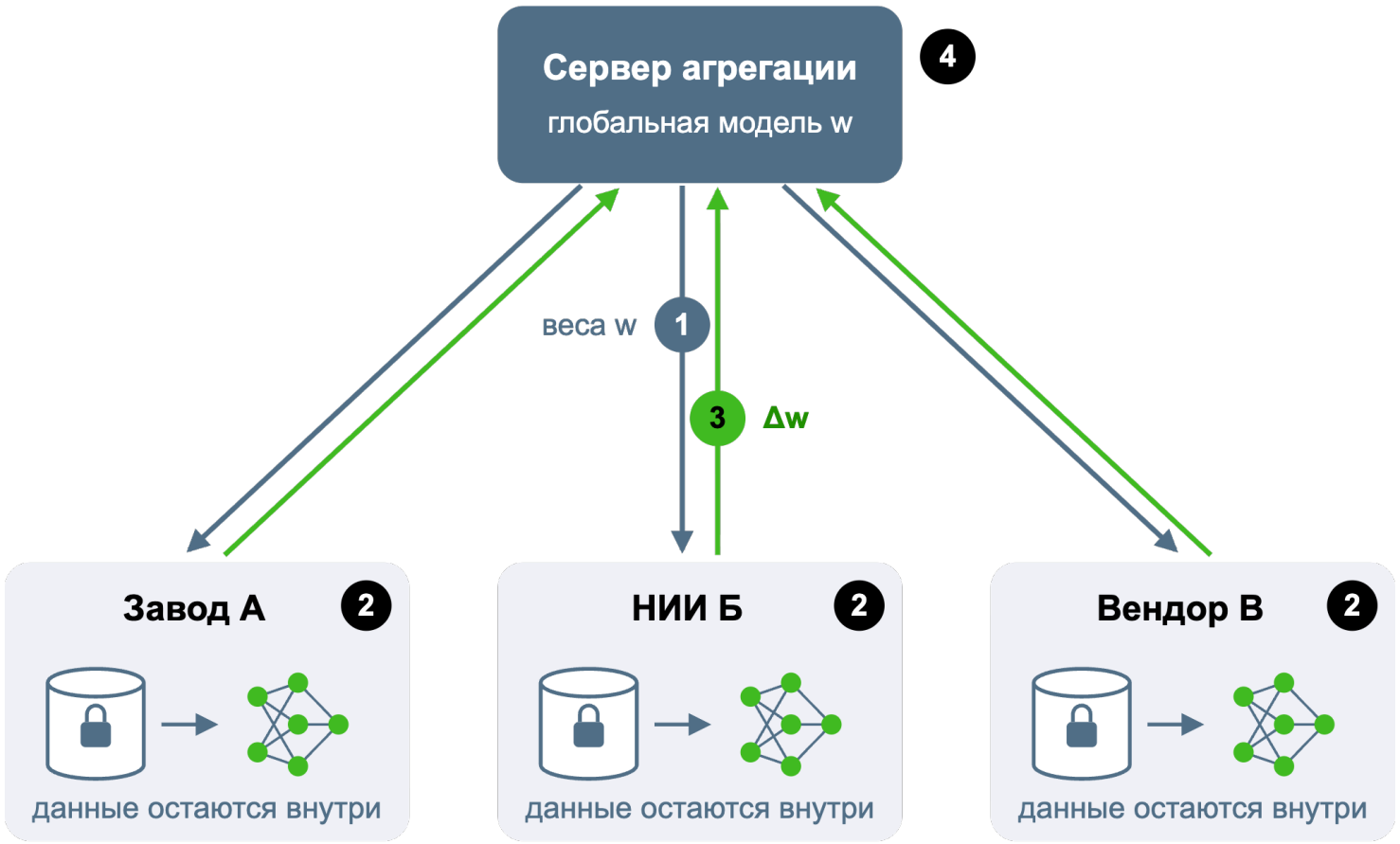
- Коммерческая тайна: рецептуры, режимы, выход годного
- Регуляторика: КИИ, персональные данные
- Объём: сырые ряды АСУ ТП — терабайты
- Доверие: в проекте конкуренты и поставщики

Федеративное обучение: модель едет к данным, а не данные — к модели

2,6 млрд+

точек активности 10 фармкомпаний обучали общую модель, не покидая своих контуров (MELLODDY)

Один раунд федеративного обучения



1. Сервер рассылает участникам текущие веса модели
2. Каждый дообучает модель на своих данных: несколько эпох SGD
3. Наружу уходят только обновления весов, сырые данные — нет
4. Сервер усредняет обновления с весами по объёму данных — и начинается новый раунд

FedAvg

$$w_{t+1} = \Sigma_k \, (n_k / n) \cdot w_k$$

n с индексом k — объём данных участника k

McMahan et al., AISTATS 2017

Дальше — шесть кейсов

№	Кейс	Участники	Что обучают вместе	Статус
1	Сталь: рецептура и режим	Три завода	Суррогат «состав и режим → свойство»	Модельный пример
2	Ветротурбины	Операторы ветропарков	Модель нормального поведения по SCADA-рядам	Публикации 2023 и 2025
3	Батареи	Переработчики ячеек	Классификатор типа катода	Nature Communications, 2023
4	Материалы	30+ институтов	Модели свойств материалов	Nature Communications, 2024
5	Малые молекулы	10 фармкомпаний	Мультизадачную модель активности	Проект MELLODDY, 2019–2022
6	Структуры белков	5 фармкомпаний	Дообучение OpenFold3	Консорциум AISB, 2025

Четыре вопроса к каждому кейсу

Кто участники. Какие у них данные. Что пересекает периметр. Что получили в итоге.

01

Кейсы: промышленность

Рецептура стали, ветротурбины, батареи



КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

Кейс 1. Три завода и новая марка стали

Модельный пример · три металлургических завода · данные: составы и режимы плавок · наружу: только веса суррогата

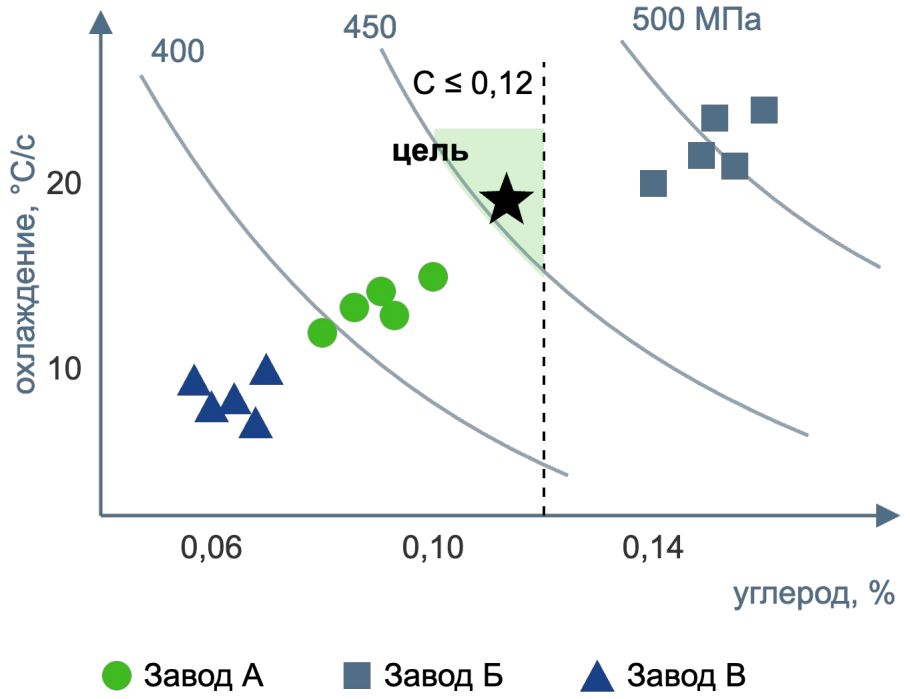
Задача: σт не ниже 450 МПа при углероде до 0,12 %

Завод	C, %	Mn, %	Si, %	T прокатки, °C	Охлажд., °C/с	σт, МПа
А	0,08	1,45	0,25	860	12	412
А	0,10	1,52	0,30	845	15	438
Б	0,14	1,30	0,35	830	20	471
Б	0,16	1,25	0,38	820	24	496
В	0,06	1,60	0,20	880	8	389
В	0,07	1,58	0,22	875	10	401

Условные данные: по две плавки от каждого завода из тысяч.

В чём проблема. У завода А прочности не хватает, у завода Б слишком много углерода. В целевой зоне нет плавок ни у кого, а делиться рецептурами заводы не готовы.

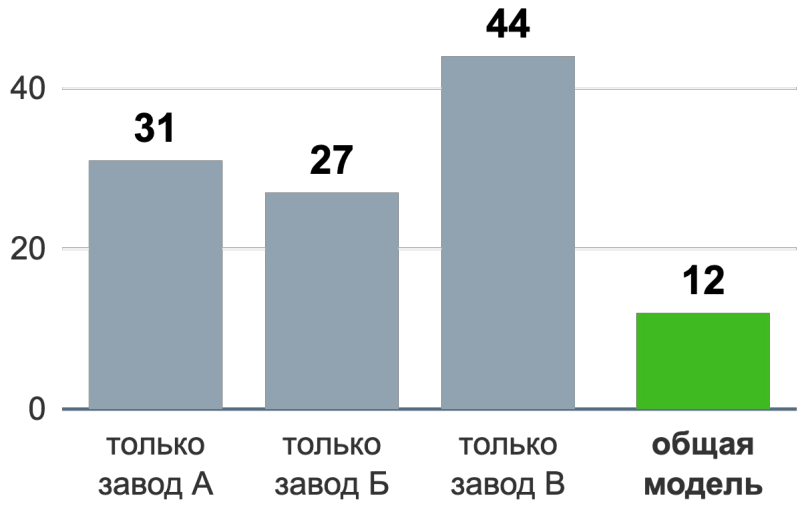
Где лежат данные заводов и где цель



Кейс 1 по шагам: от рецептуры к суррогату и обратно

Модельный пример · числа условные и показывают логику, а не результат эксперимента

Ошибка прогноза σт в целевой зоне, МПа



1 Локальные суррогаты

Каждый завод учит модель «состав и режим → σт» на своих плавках. В целевой зоне ошибка 27–44 МПа: данных там нет.

2 Общий суррогат

Двадцать раундов FedAvg между тремя заводами. Модель интерполирует между областями А и Б: ошибка в целевой зоне 12 МПа.

3 Кандидат рецептуры

Завод А у себя перебирает варианты через общую модель: C 0,11 %, Mn 1,50 %, Si 0,30 %, прокатка 840 °C, охлаждение 18 °C/с.

Прогноз: 452 ± 12 МПа

4 Опытная плавка

Одна плавка вместо серии. Результат остаётся в данных завода А и в следующем раунде уточняет общую модель.

Факт: 447 МПа

Что пересекло периметр

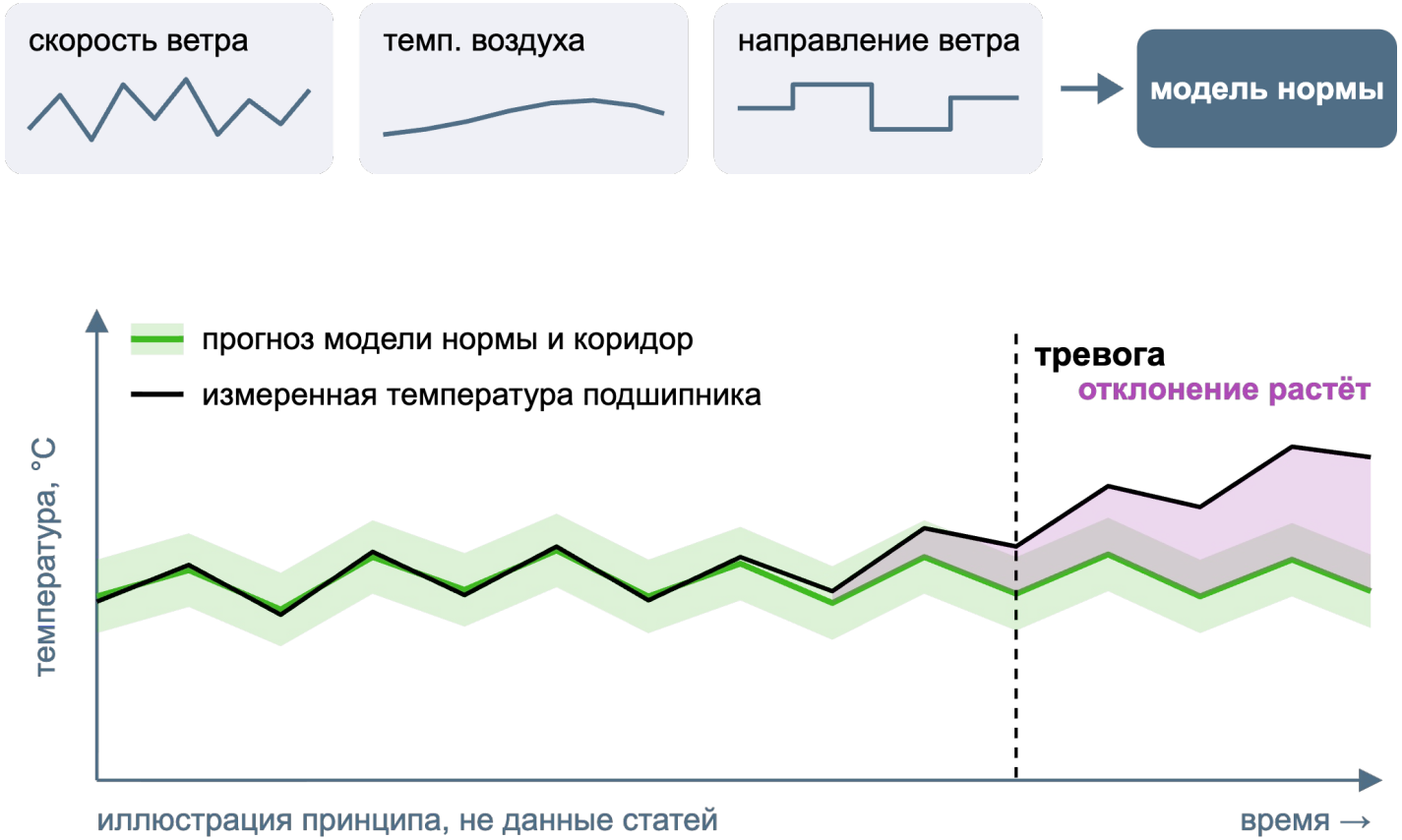
Только веса суррогата. Рецептуры, режимы и результаты плавок остались на заводах, поиск кандидата завод А вёл у себя.

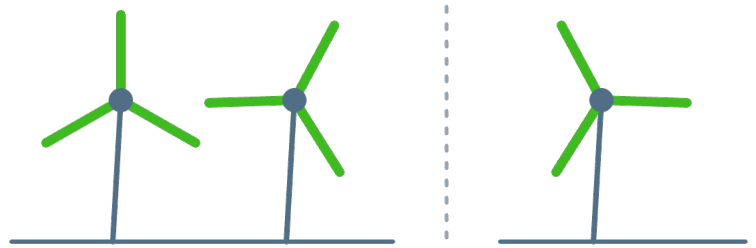
Федеративная байесовская оптимизация: Dai, Low, Jaillet, NeurIPS 2020

Кейс 2. Ветротурбины: общая модель нормы

Кейс 2 · операторы ветропарков · данные: SCADA-ряды турбин · наружу: веса модели · итог: выигрыш при малой истории

Отказ виден как растущее отклонение от прогноза нормы





Два ветропарка, у каждой турбины своя SCADA. Общая модель нормы обучается через FedAvg.

×10 дольше обучение при федерации: связь и медленная сходимость

Что показали работы

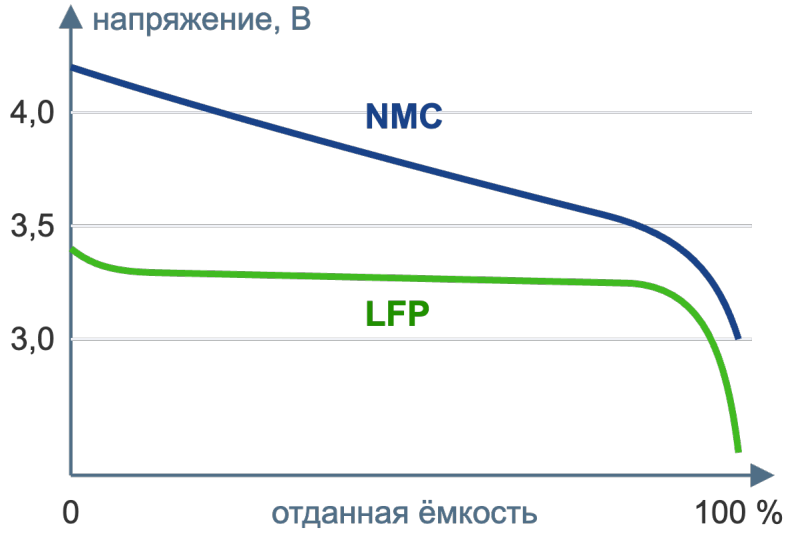
- Турбины с короткой историей выигрывают больше всех
- Между парками общая модель может проиграть внутрипарковой: non-IID
- Лучше всего — дообучить общую модель под каждую турбину

Кейс 3. Батареи: сортировка отслуживших ячеек

Кейс 3 · переработчики батарей · данные: кривые заряда–разряда · наружу: параметры классификатора · итог: ошибка 1–3 %

Вход — одна кривая разряда в конце жизни ячейки





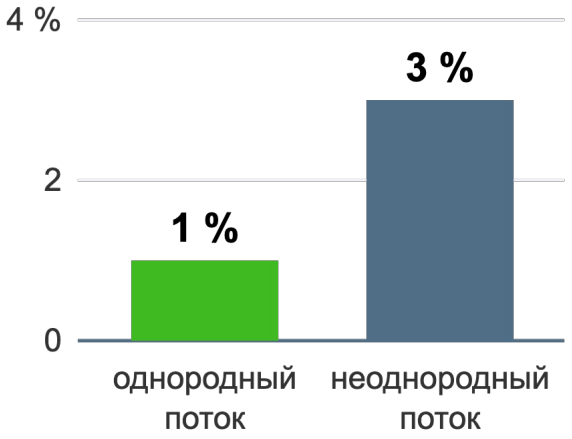
Типичный вид разрядных кривых двух химий. Иллюстрация.

130
ячеек в датасете

5
катодных материалов

7
производителей

Ошибка сортировки по типу катода



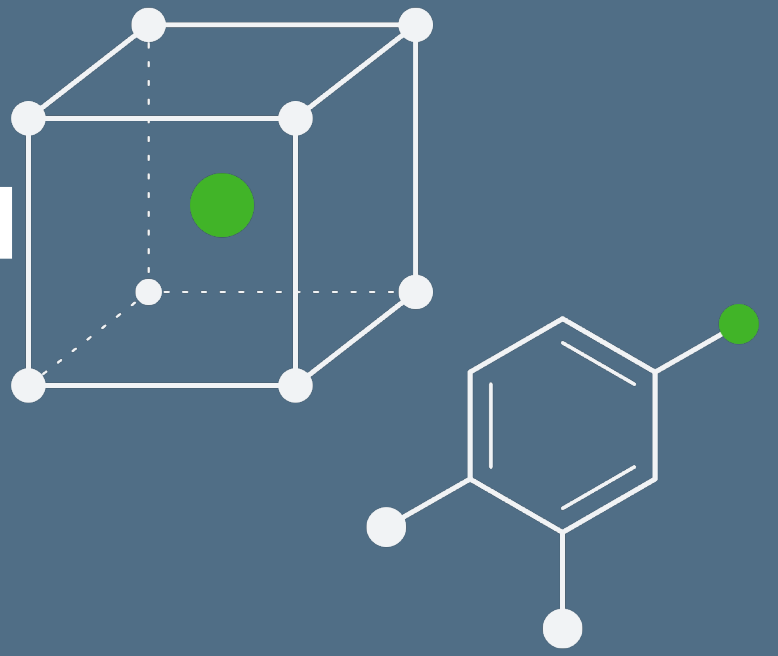
Как это сделано

- Признаки — из одной кривой заряда–разряда, история эксплуатации не нужна
- Переработчики учат общий классификатор федеративно
- Итог — голосование с весами по расстоянию Вассерштейна
- Точная сортировка по катоду нужна для прямой переработки

Tao et al., Nature Communications, 2023

02

Кейсы: материалы и биотех



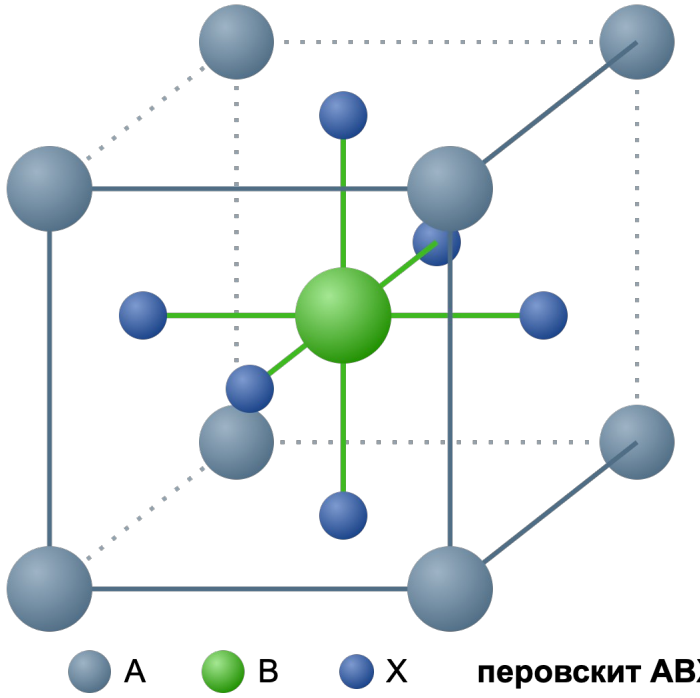
Базы данных материалов, малые молекулы, структуры белков

КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

Кейс 4. Материалы: модель свойств без общей базы данных

Кейс 4 · 30+ институтов Китая · данные: расчёты и эксперименты · наружу: параметры моделей · итог: точнее локальных

Объект данных: кристаллическая структура → свойство

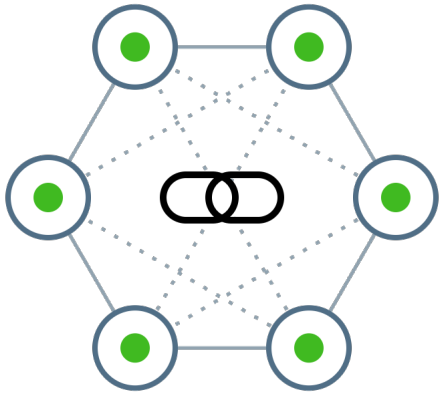


14 млн+

записей о материалах на национальной платформе NMDMS, Китай

30+

исследовательских институтов — источники данных платформы



MatSwarm: рой вместо центрального сервера

- Обмен параметрами моделей, не данными
- Координация через блокчейн Hyperledger Fabric
- Агрегация в доверенной среде Intel SGX
- Регуляризация против non-IID между институтами

Точность и обобщение выше, чем у моделей отдельных институтов

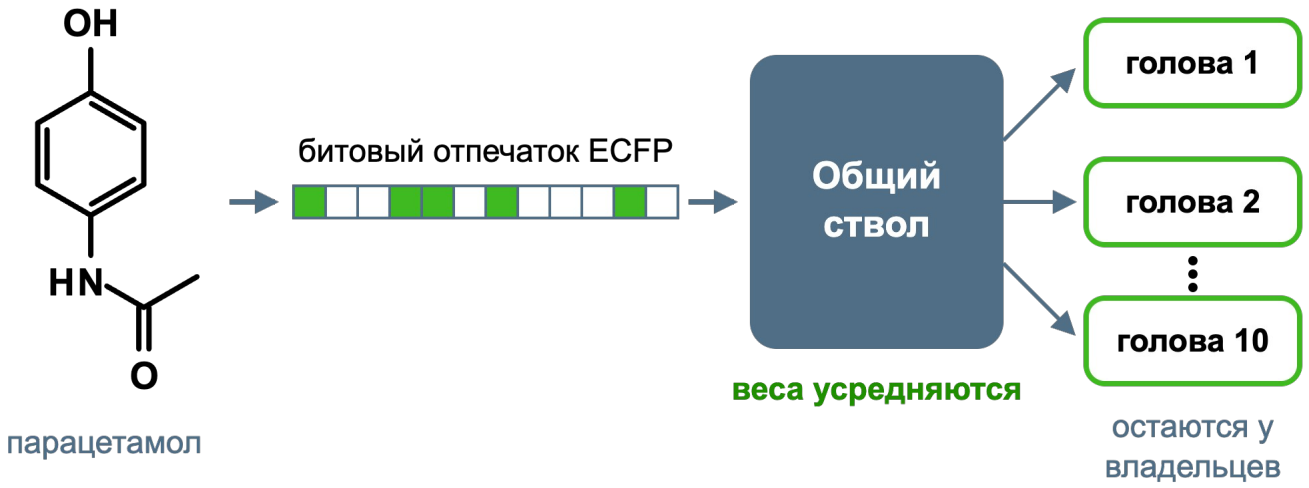
Wang et al., MatSwarm, Nature Communications, 2024

Кейс 5. Малые молекулы: десять конкурентов, одна модель

Кейс 5 · 10 фармкомпаний · данные: активность молекул · наружу: веса общего ствола · итог: выигрыш у всех десяти

10	2,6 млрд+	21 млн+	40 тыс.+
фармкомпаний	точек активности	молекул	ассаев

MELLODDY: общий ствол, частные головы



Что получилось

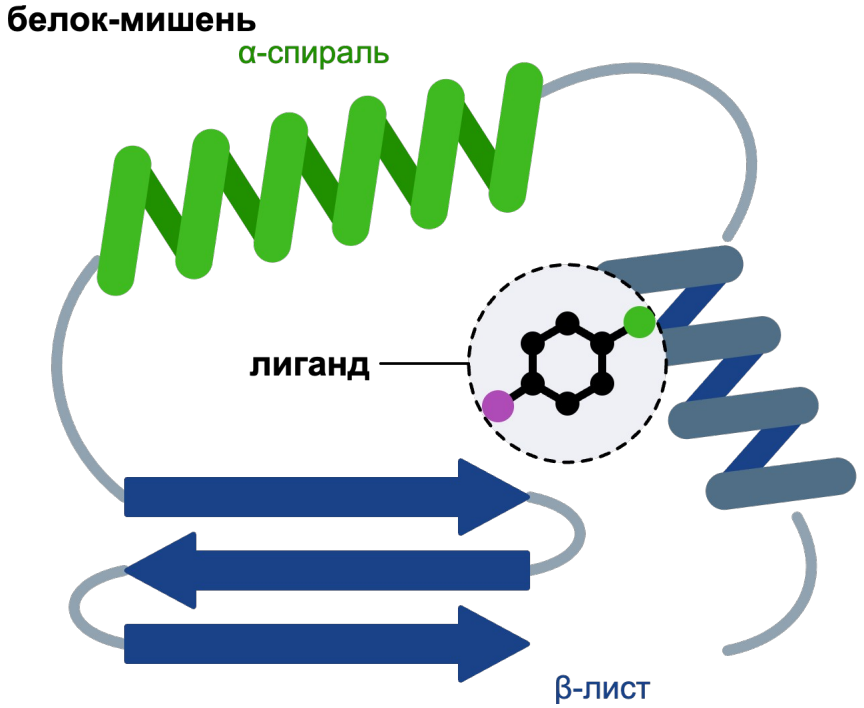
- Выигрыш у всех десяти партнёров — в классификации или регрессии
- Максимум — фармакокинетика и панели безопасности
- Шире область применимости модели
- Наружу уходят только веса ствола; ассаи и головы приватны

Для GNN. Бенчмарк FedChem: при разбиении молекул по каркасам обычный FedAvg заметно теряет; помогает перевзвешивание примеров FLIT.

Кейс 6. Структуры белков: дообучение OpenFold3

Кейс 6 · 5 фармкомпаний · данные: закрытые структуры · наружу: параметры модели · итог: по данным организаторов

Объект данных: комплекс белок–лиганд



5
фармкомпаний в первом проекте

20 000+
закрытых структур

< 10
недель на проект

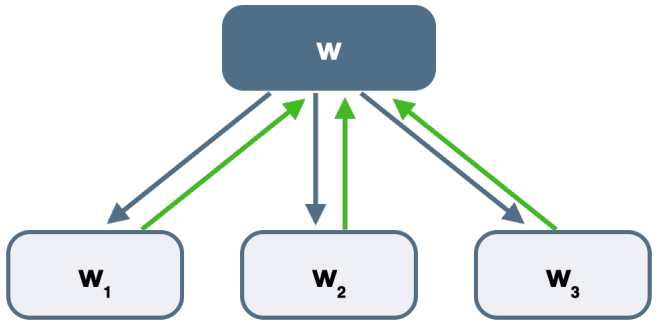
Консорциум AISB: как устроено

- AbbVie, Astex, BMS, Johnson & Johnson, Takeda дообучают OpenFold3 каждая в своём контуре
- Агрегируются только параметры модели, структуры не объединяются
- Научный партнёр — лаборатория AlQuraishi, Колумбийский университет
- Следующий проект — AISB Bind: от структуры к связыванию

Оговорка. Результаты — по сообщению организаторов: лучше метрики на интерфейсах и шире область применимости, чем у публичной OpenFold3. Цифры сверяйте с первоисточником.

Apheris, AI Structural Biology Network, 2025

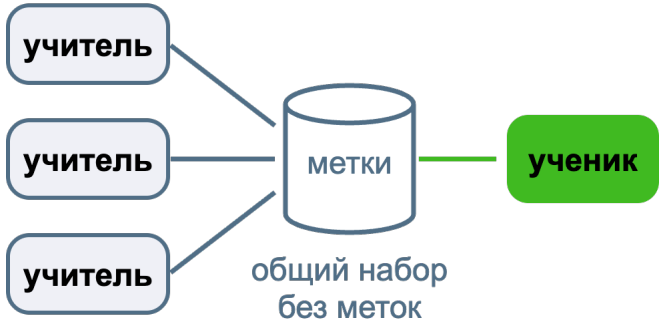
Не только усреднение весов: три схемы федерации



Усреднение весов

Участники равноправны, архитектура у всех одна. Обмениваются весами.

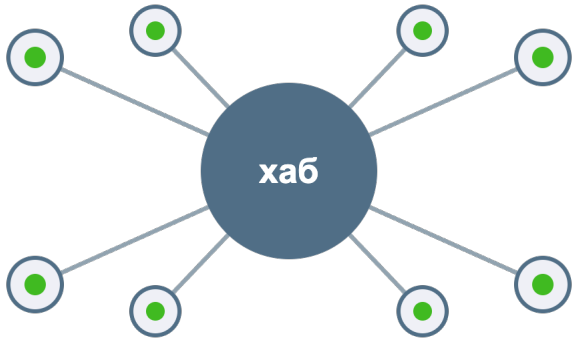
Примеры. Кейсы 1, 2, 5 и 6.



Федеративная дистилляция

Локальные учителя размечают общий набор, ученик учится на этих метках. Архитектуры могут различаться.

Пример. FLuID: восемь фармкомпаний, Nature Machine Intelligence, 2025.



Модель-хаб

Владелец большой модели раздаёт её партнёрам, обратно получает только обновления.

Пример. Lilly TuneLab: 18 моделей, обученных на данных стоимостью более 1 млрд $, с сентября 2025.

Общее у всех трёх

Сырые данные остаются у владельца. Различается то, что пересекает периметр: веса, метки на общем наборе или обновления чужой модели.

Hanser et al., Nat. Mach. Intell., 2025 · Eli Lilly, TuneLab, 2025

03

Безопасность



Модель угроз, конфиденциальность, целостность модели

КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

Модель угроз: данные на месте, поверхность атаки остаётся



1 Отравление

Участник портит свои данные или обновления, внедряет бэкдор

Робастная агрегация, проверка вклада

2 Канал

Перехват и подмена обновлений в пути

Взаимная аутентификация, шифрование, подпись

3 Любопытный сервер

Восстанавливает обучающие примеры из градиентов

Secure aggregation, TEE, шифрование

4 Любопытный участник

По общей модели делает выводы о чужих данных

Дифференциальная приватность

5 Внешний пользователь

Membership inference, извлечение модели через API

DP, лимиты и аудит запросов

Конфиденциальность: обновления весов раскрывают данные

Атака: восстановление входа по градиенту



Сервер подбирает вход, градиент которого совпадает с присланным. Иллюстрация принципа.

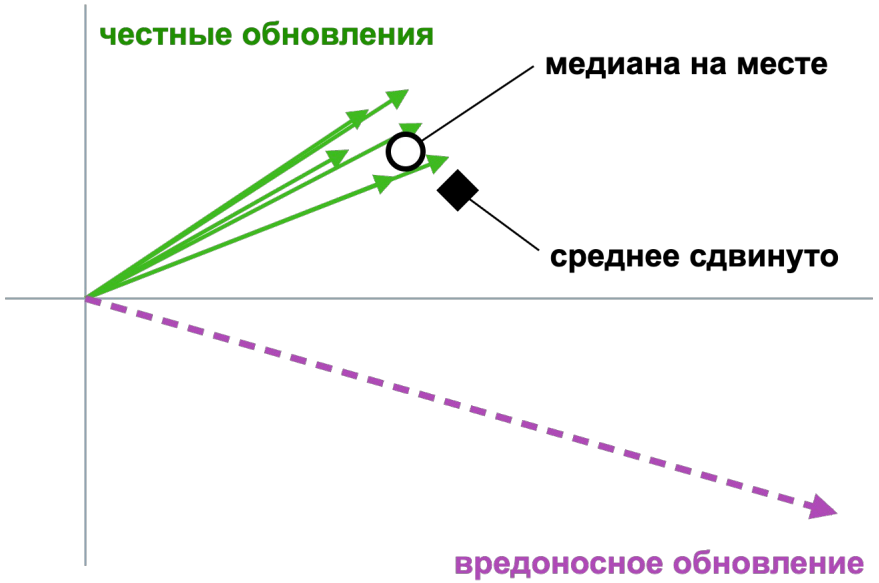
Защита: что закрывает и какой ценой

Мера	Что закрывает	Цена
Secure aggregation	Сервер видит только сумму обновлений	Криптопротокол; труднее искать отравленные вклады
Дифференциальная приватность	Вывод о записи или участнике по модели	Шум и клиппинг снижают точность
Гомоморфное шифрование	Агрегация прямо над шифртекстом	Вычисления и трафик растут на порядки
Доверенные среды, TEE	Оператор сервера и облака	Доверие к железу, побочные каналы
Сжатие и прореживание обновлений	Меньше утечка и меньше трафик	Формальной гарантии не даёт

FL сам по себе — минимизация данных, а не гарантия конфиденциальности. Гарантии дают меры из таблицы — по модели угроз.

Целостность: отравление и бэкдоры

Одно вредоносное обновление сдвигает среднее

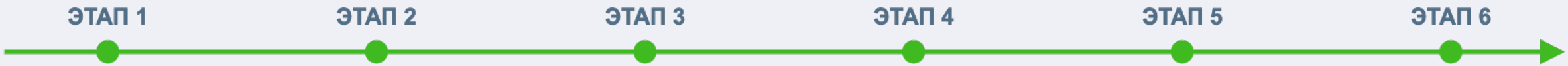


Атаки на модель и чем их закрывают

Атака	Что делает	Чем закрывают
Отравление данных	Подмена меток и измерений у себя	Проверка вклада на отложенной выборке
Отравление модели	Подобранное или усиленное обновление	Клиппинг нормы; Krum, медиана, усечённое среднее
Бэкдор	Модель штатна везде, кроме входов с триггером	Клиппинг и шум, поиск аномальных обновлений
Free-rider, Sybil	Модель без вклада; фиктивные участники	Аттестация участников, учёт вклада
Сговор	Несколько нарушителей действуют согласованно	Агрегатор, устойчивый к доле f из n участников

Меры конфликтуют — Secure aggregation скрывает отдельные обновления — и мешает искать отравленные. Приватность и целостность проектируют вместе, а не по очереди.

Как запускать: шесть этапов от идеи до пилота



Задача и участники

Одна измеримая задача, для которой каждому не хватает своих данных

Соглашение о целях и правах на модель

Гармонизация

Общая схема, единицы, метки и сплиты

Общий код подготовки данных

Локальные бейзлайны

Каждый учит модель только на своих данных

Планка, которую федерация обязана превзойти

Симуляция

Федерация на открытых или синтетических данных с искусственным non-IID

Выбран алгоритм и бюджет связи

Модель угроз

Кому не доверяем, что защищаем, какие меры включаем

Согласование со службой ИБ

Пилот

Три–пять участников, затем расширение и мониторинг дрейфа

Прирост у каждого участника

Критерий успеха

Прирост у каждого участника относительно его собственной локальной модели. Средняя метрика по федерации этого не показывает: участник без выигрыша выйдет из проекта.

Что унести с собой

Модель едет к данным. Дальше — инженерия, безопасность и договорённости.



1 **Зачем.** Общая модель там, где данные нельзя объединить: тайна, КИИ, объём, конкуренция.

2 **Безопасность.** Обновления — тоже информация. Нужны secure aggregation, DP и робастная агрегация по модели угроз.

3 **Трудности.** Гармонизация данных и non-IID съедают больше времени, чем сам алгоритм.

4 **Масштаб.** Работает: 10 фармкомпаний и 2,6 млрд точек, 30+ институтов, парки турбин.

5 **Старт.** Одна задача, локальные бейзлайны, симуляция, модель угроз — и только потом пилот.

КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

Спасибо за внимание

Руслан Лукин

Руководитель лаборатории ИИ в новых материалах,
Университет Иннополис

r.lukin@innopolis.ru

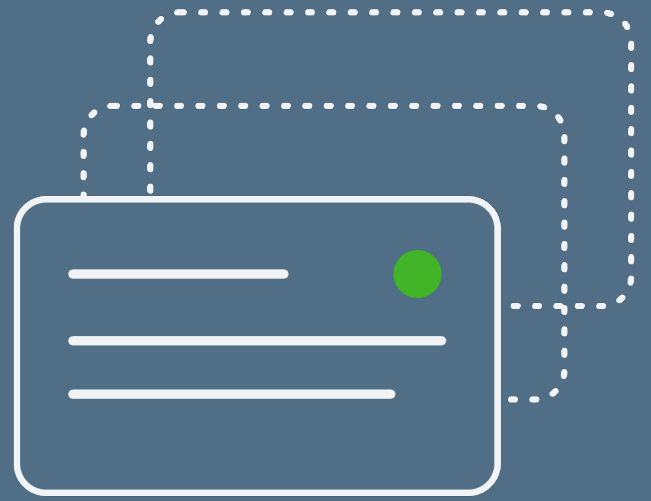
Telegram: @kvikk_ruskinkot

Вопросы?



Дополнительные слайды

Для вопросов: источники, неоднородные данные, модели, инструменты



КОД ИБ КАЗАНЬ · 12 НОЯБРЯ 2026

Источники

Алгоритмы и безопасность

- McMahan et al. FedAvg. AISTATS, 2017
- Kairouz et al. Advances and Open Problems in FL. 2021
- Li et al. FedProx. MLSys, 2020
- Karimireddy et al. SCAFFOLD. ICML, 2020
- Li et al. FedBN. ICLR, 2021
- Zhu, Liu, Han. Deep Leakage from Gradients. NeurIPS, 2019
- Bonawitz et al. Secure Aggregation. CCS, 2017
- McMahan et al. DP-FedAvg. ICLR, 2018
- Blanchard et al. Krum. NeurIPS, 2017
- Yin et al. Byzantine-Robust Learning. ICML, 2018
- Bagdasaryan et al. How To Backdoor FL. AISTATS, 2020
- Cheng et al. SecureBoost. IEEE Intell. Syst., 2021

Кейсы

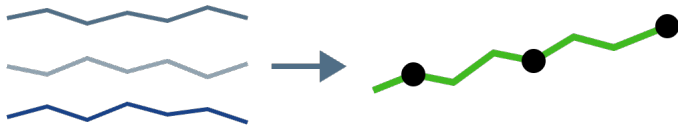
- Hiessl et al. Industrial Federated Learning. PAAMS, 2020
- Jenkel, Jonas, Meyer. Ветротурбины. Energies, 2023
- Grataloup, Jonas, Meyer. Ветропарки. IEEE Access, 2025
- Liu et al. Аномалии в IIoT. IEEE IoT J., 2021
- Dai, Low, Jaillet. Federated BO. NeurIPS, 2020
- Tao et al. Батареи. Nat. Commun., 2023
- Wang et al. MatSwarm. Nat. Commun., 2024
- Heyndrickx et al. MELLODDY. JCIM, 2024
- Zhu, Luo, White. FedChem. Patterns, 2022
- Hanser et al. FLuID. Nat. Mach. Intell., 2025
- Pati et al. FeTS. Nat. Commun., 2022
- Apheris AISB; Eli Lilly TuneLab — материалы компаний, 2025

Тот же приём — ещё шесть промышленных задач



Предиктивное обслуживание

Вибрация, токи, температуры → остаточный ресурс узла



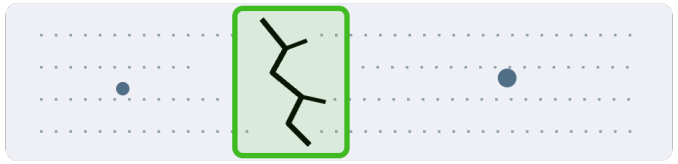
Виртуальные анализаторы

Режимные параметры → качество продукта между лабораторными пробами



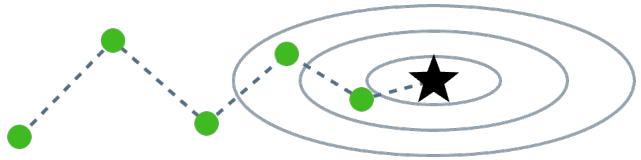
Поиск аномалий

Телеметрия АСУ ТП → автоэнкодеры, CNN-LSTM



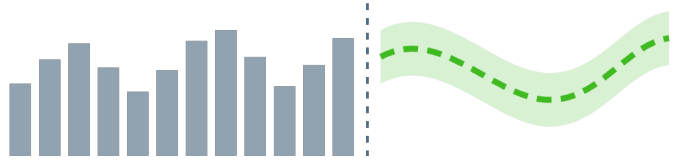
Контроль дефектов

Снимки и дефектоскопия → сегментация дефектов



Режимы и рецептуры

История плавок и опытов → суррогат и байесовская оптимизация

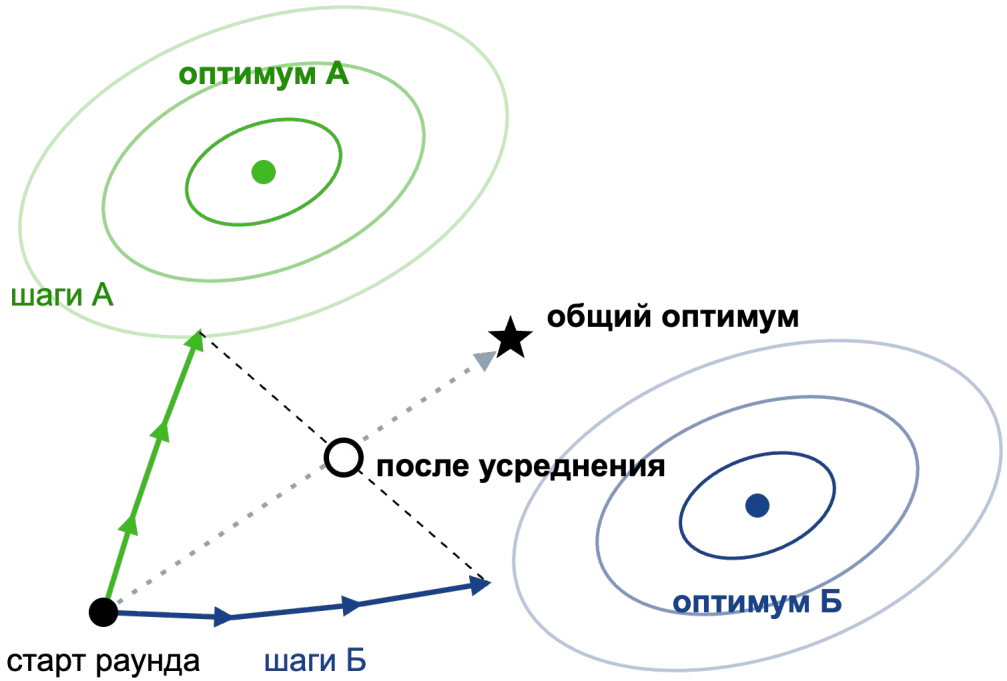


Прогноз нагрузки

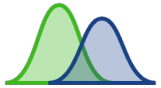
Счётчики и графики потребления → прогноз на сутки вперёд

Неоднородные данные: у каждого участника свой режим

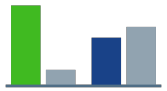
Дрейф клиентов: каждый тянет модель к своему оптимуму



Откуда берётся неоднородность



Сдвиг признаков: разные режимы и оборудование



Сдвиг меток: разная доля брака и отказов



Разный объём: тысяча записей против миллиона



Разные датчики: своя частота и набор тегов

Чем лечат

- **FedProx, SCAFFOLD** — поправка к локальному шагу
- **FedBN** — нормализация остаётся локальной
- **Персонализация** — общий энкодер, свои «головы»
- **Кластерная FL** — когорты похожих участников

Li et al., MLSys 2020 · Karimireddy et al., ICML 2020 · Li et al., ICLR 2021 · Hiessl et al., 2020

До обучения: привести данные к общему языку

Одна и та же температура печи на трёх заводах

Участник	Тег в АСУ ТП	Единицы	Шаг	Сырое значение	После гармонизации
Завод А	TI-4021.PV	°C	1 с	1247,3	T_furnace = 1520,45 K, шаг 1 мин
Завод Б	Печь2_Темп_зона3	K	10 с	1519,8	T_furnace = 1519,80 K, шаг 1 мин
Завод В	FURN.T3	°F	1 мин	2277,0	T_furnace = 1520,37 K, шаг 1 мин

Иллюстративные данные: имена тегов и значения условные, пересчёт единиц точный.

Препроцессинг тоже федеративный

Один и тот же код подготовки данных запускается у каждого участника локально. В MELLODDY для этого сделали общий пайплайн MELLODDY-TUNER.

1

Единая схема

Общий словарь тегов и признаков

2

Единицы и сетка времени

Пересчёт единиц, ресемплинг на общий шаг

3

Согласованные метки

Что считать браком, отказом, активным соединением

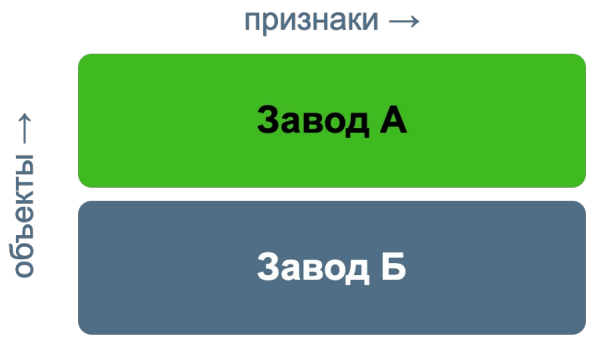
4

Общая валидация

Сплиты по времени и партиям, одни метрики у всех

Три сценария: как данные разрезаны между участниками

Горизонтальное



Признаки одинаковые, объекты разные.

Пример. Пять заводов с однотипными линиями учат общую модель износа оборудования.

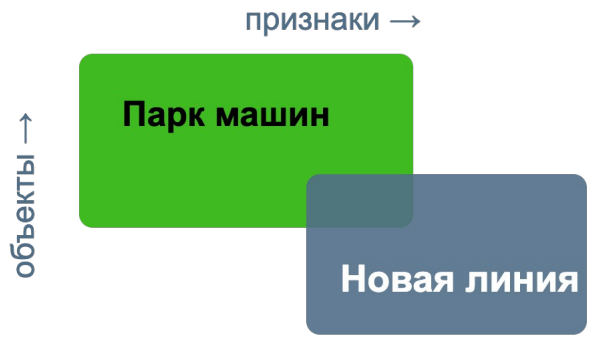
Вертикальное



Объекты общие, признаки у каждого свои.

Пример. Поставщик знает состав партии сырья, завод — режим обработки и качество изделия (y).

Федеративный перенос



Мало общих и объектов, и признаков.

Пример. Модель, обученная на парке машин вендора, дообучается на новой линии заказчика.

В R&D почти всегда cross-silo — От двух до примерно ста организаций, надёжные узлы, большие датасеты у каждого. Cross-device — миллионы телефонов — требует другой инженерии.

Kairouz et al., Advances and Open Problems in Federated Learning, 2021

Какие модели обучают федеративно

Класс модели	Задачи R&D	Как федерируют	Пример
Линейные модели, GLM	Базовые зависимости «состав → свойство»	Усреднение весов или сумм статистик	Первый шаг пилота
Градиентный бустинг	Табличные данные процессов и рецептур	Обмен гистограммами градиентов; SecureBoost	SecureBoost в FATE
Мультизадачные MLP	QSAR, ADMET, свойства материалов	Общий ствол, частные головы	MELLODDY
CNN, U-Net	Дефекты, микроструктуры, медицинские снимки	FedAvg, локальная нормализация FedBN	FeTS: 71 центр, 6 314 пациентов
RNN, TCN, трансформеры рядов	Аномалии, остаточный ресурс, виртуальные анализаторы	FedAvg со сжатием обновлений, персонализация	Ветропарки; IIoT: −50 % трафика
Графовые сети	Молекулы и кристаллы	FedAvg, перевзвешивание FLIT	Бенчмарк FedChem
Фундаментальные модели	Структуры белков, тексты и документация	Дообучение весов или адаптеров LoRA	OpenFold3 в консорциуме AISB
Гауссовы процессы	Оптимизация режимов и рецептур	Федеративный Thompson sampling	Dai et al., NeurIPS 2020

Cheng et al., SecureBoost, 2021 · Pati et al., Nat. Commun., 2022 · Liu et al., IEEE IoT J., 2021

Инструменты, российский контур и когда FL не нужен

Фреймворки с открытым кодом

Фреймворк	Кто развивает	Чем известен
Flower	Flower Labs	Универсальный, работает с любым ML-фреймворком
NVIDIA FLARE	NVIDIA	Медицина и крупные модели; предшественник — в проекте EXAM, 20 клиник
OpenFL	Intel, Linux Foundation	FeTS: 71 клинический центр
Substra	Owkin, Linux Foundation	MELLODDY: 10 фармкомпаний
FATE	WeBank	Вертикальная FL, гомоморфное шифрование, SecureBoost
APPFL	Аргоннская лаборатория	Научные задачи и суперкомпьютеры

С чего начать. Симуляция федерации на одной машине — до закупок и согласований.

Российский контур: что учесть

- **187-ФЗ, КИИ:** узел FL — внутри периметра, наружу один согласованный канал
- **152-ФЗ:** при персональных данных FL не снимает обязанностей оператора
- **98-ФЗ:** веса и обновления могут нести коммерческую тайну — классифицируйте их
- **Криптография:** каналы и подписи — по требованиям регулятора

Не юридическая консультация: согласуйте с ИБ и юристами.

Когда FL не нужен

- Данные можно законно объединить: централизованно проще и точнее
- У участников нет общей задачи и общих признаков
- Каждому хватает собственных данных