Крипто-анклав ВТБ-МФТИ

Денис Суржко
Начальник управления перспективных алгоритмов машинного обучения, ВТБ

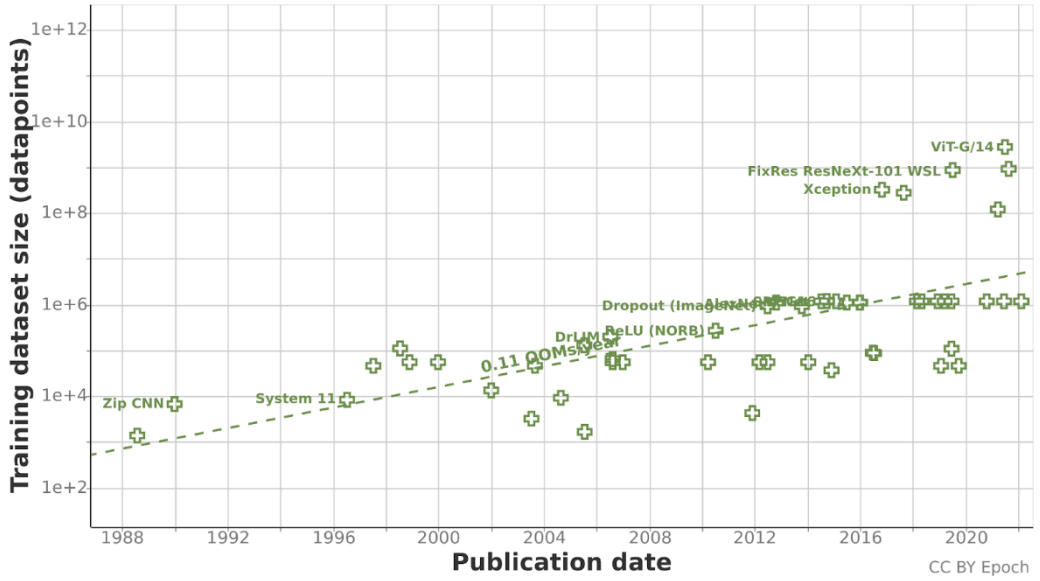
Data Driven AI

Существует гипотеза о том, что ключевую роль в развитии технологий ИИ играет объем доступных для исследователей выборок данных

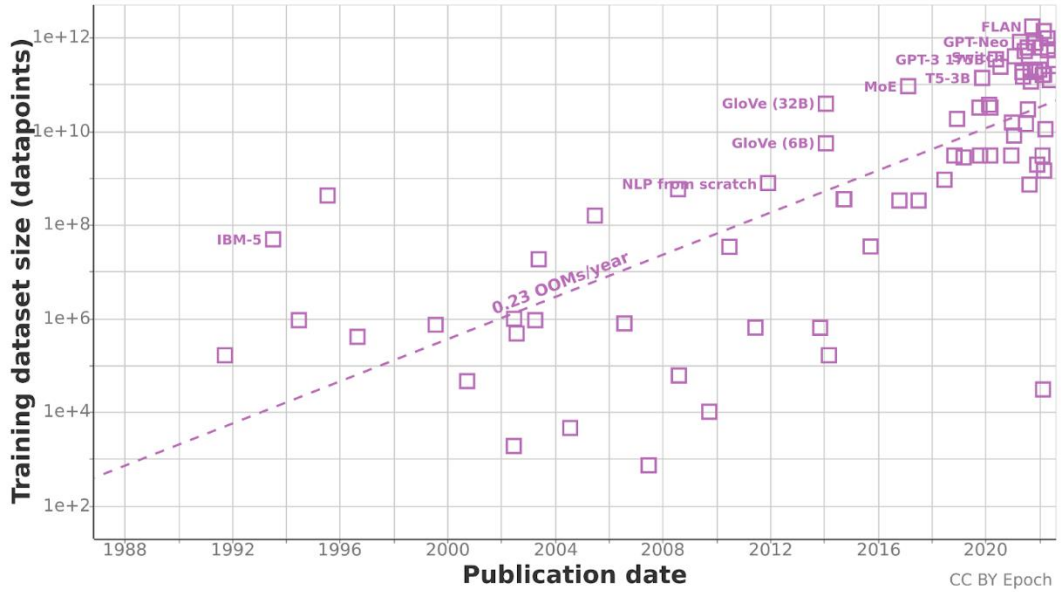
Появление новых дата-сетов в ряде отраслей проблематично в связи с этическими и законодательными ограничениями:

- Финтех
- Медицина
- Синергия данных бизнеса и государства

CV Data Sets (log scale)



NLP Data Sets (log scale)



Системный подход к Data Fusion

Большинство крупных розничных компаний уже затратили «20%» усилий для получения «80%» результата от анализа собственных данных

Наиболее «маржинальное» направление анализа данных – ПАРТНЕРСТВА В ОБЛАСТИ ДАННЫХ

Для достижения синергетического Data Fusion эффекта сейчас для каждого партнера / источника данных требуется:

- Обучение специализированных Deep Learning моделей (эмбединги) либо проработка нетривиальных подходов к обезличиванию данных (гео-сетка, обезличенный граф и т.п.)
- Организация наукоемкого и трудоемкого процесса, в том числе, на стороне партнеров

? Можно ли системно подойти к решению Data Fusion задачи, двигаясь в сторону универсального решения?

! ДА, ИСПОЛЬЗУЯ ТЕХНОЛОГИЮ КРИПТО-АНКЛАВОВ

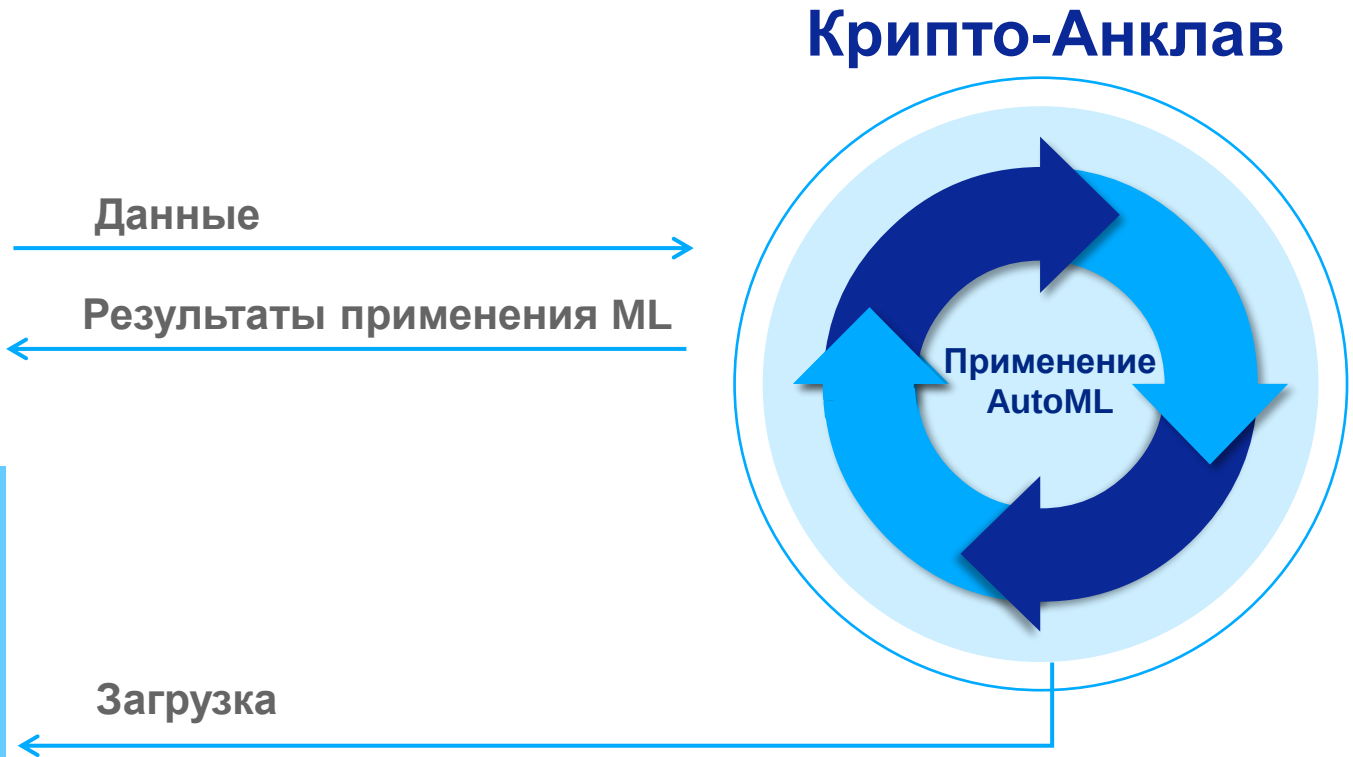
Что такое крипто-анклав?

Партнеры передают данные в крипто-защищенную область, получая гарантии

- Отсутствие доступа у других участников анклава к их данных
- Применение строго регламентированных алгоритмов для анализа их данных
- Возможности получения «на выходе» из анклава исключительно результатов применения моделей на данных участников анклава без доступа к исходной информации.

Пользователи платформы

AutoML модуль «слепого» машинного обучения



Процессы технологии

Слой основных технологических процессов

Подготовка и контроль качества данных →

- Профилирование данных
- Управление сервисными соглашениями об их составе и качестве

Формирование пространства признаков →

- Определение профиля генерации признаков относительно знаний о задаче моделирования и данных
- Уточнение знаний о данных

Отслеживание показателей качества моделирования

- Обучение модели
- Валидация результатов
- Установка модели на применение и отслеживание процесса с периодической валидацией

Слой конвейеризированной обработки данных в Анклаве

Сопоставление данных с единой моделью →

Конвейеризированные процессы автоматической обработки данных инициируются сотрудником участника анклава, но выполняются автоматически

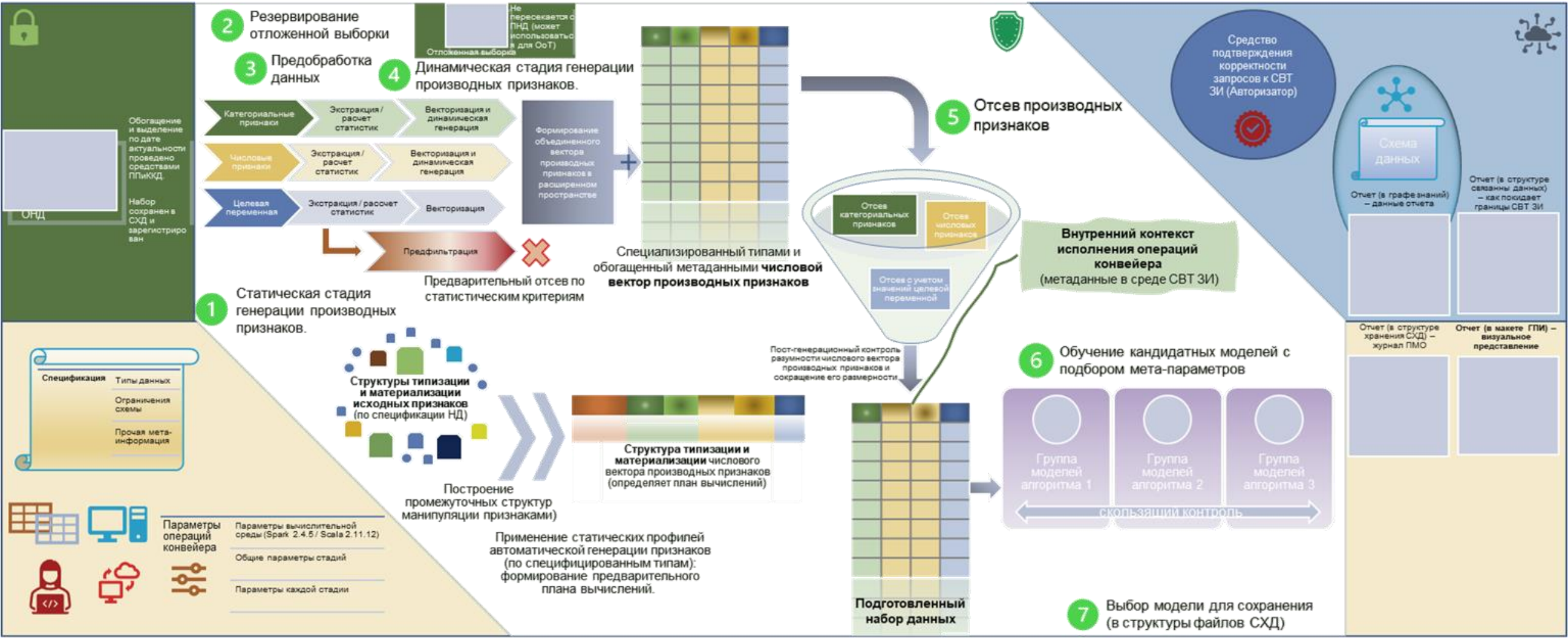
Обогащение данных →

Стадии обработки могут возвращать мета-информацию

Автоматическое машинное обучение

Сами данные в Анклаве защищены от постороннего доступа

Автоматическое машинное обучение: технический взгляд



Какие есть решения на рынке?

Фактически монопольное положение на рынке занимает технология

Intel SGX

Алгоритм крипто-анклава «зашит» в процессор, который гарантирует отсутствие доступа у кого-либо к защищенной части памяти

Недостатки Intel SGX:

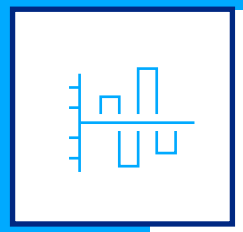
- Защита на уровне процессора ограничивает адресацию доступной памяти, для снятия ограничений необходима закупка специализированного железа Intel SGX Card
- Реализация анклава в РФ на Intel SGX несет потенциальные риски, так как лицензировать импортную технологию защиты информации для широкого круга задач будет затруднительно

ПРЕДЛАГАЕМОЕ РЕШЕНИЕ

Разработка совместно с МФТИ специализированного Программно-Аппаратного Комплекса (ПАК)

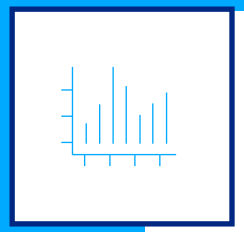
- ПАК будет защищен на программном и физическом уровне на базе наработок кафедры защиты информации МФТИ
- ПАК может быть официально сертифицирован при поддержке кафедры защиты информации МФТИ

Преимущества решения и роли участников



Используя ПАК становится возможным легкое масштабирование вычислительных мощностей

В перспективе станет возможным «зашивать» в него AutoML для любых типов данных (графы, тексты, картинги, звук) с использованием GPU, а также использовать как универсальный защищенный вычислительный комплекс



Первый продукт по обучению в анклаве на полностью импортозамещенных технологиях

Может быть применим как в Банке ВТБ, так и в широком периметре задач гос. органов, гос. и коммерческих компаний

Сферы применения данной технологии:

- Разработка CRM моделей в любых B2C компаниях (Банки, Телекомы, FMCG и т.п.)
- Разработка моделей оценки рисков (Банки)
- Разработка моделей диагностики и оценки влияния препаратов (Медицина)
- Государственные данные (синергия гос данных и бизнес данных).