Технологии повышения конфиденциальности: барьеры, вызовы и будущее

Ассоциация ФинТех,
2025

Ассоциация ФинТех

МИССИЯ

Ассоциация является площадкой для диалога и координации взаимодействия заинтересованных сторон с целью развития цифровых финансовых сервисов и технологий на основе российских решений.

13 ЧЛЕНЫ АФТ

Банк России · ВТБ · СБЕР · Альфа Банк · ГАЗПРОМБАНК · НСПК · ПСБ · ВСК Страховой дом · РСХБ | ЦИФРА · MOEX GROUP · Т БАНК · Райффайзен БАНК · ДОМ РФ

33 АССОЦИИРОВАННЫЕ ЧЛЕНЫ

СОВКОМБАНК · base alt · РНКО Платежный центр · ART искусство прибыли · МКБ · Яндекс · МТС · НСИС Национальная Страховая Информационная Система · Почта Банк · Ростелеком · Avito · РЕСО Гарантия · Ак Барс Банк · DIASOFT всё по-настоящему · Банк Центр-Инвест · РЕДСОФТ · Капитал Life Страхование жизни · отпбанк · Альфа Страхование · K2TEX · Доход управляющая компания · сравни · Кредит ЕвропаБанк · синара банк · TI · билайн бизнес · БПС Инновационные решения · ВБРР · АСТРА · точка банк для предпринимателей и предприятий · SWORDFISH SECURITY · FLEX Software Systems

Содержание

Предпосылки обмена данными

КЛИЕНТ

Субъект данных: частные лица, коммерческие организации, государственные институты

- Персонализация продуктов
- Расширенный выбор
- Повышение удобства и сервиса
- Своевременность, эффективность и точность данных и услуг

БИЗНЕС

Финансовые организации, Экосистемы, БигТех

- Монетизация «данных» (данные- нематериальных актив)
- Эффективность процессов
- Улучшенная бизнес аналитика
- Улучшенная идентификация
- Привлечение клиентов
- Разработка новых продуктов
- «Расширенные» модели оценки (андеррайтинга)
- Общая безопасность

ГОСУДАРСТВО

ФОИВы, Банк России

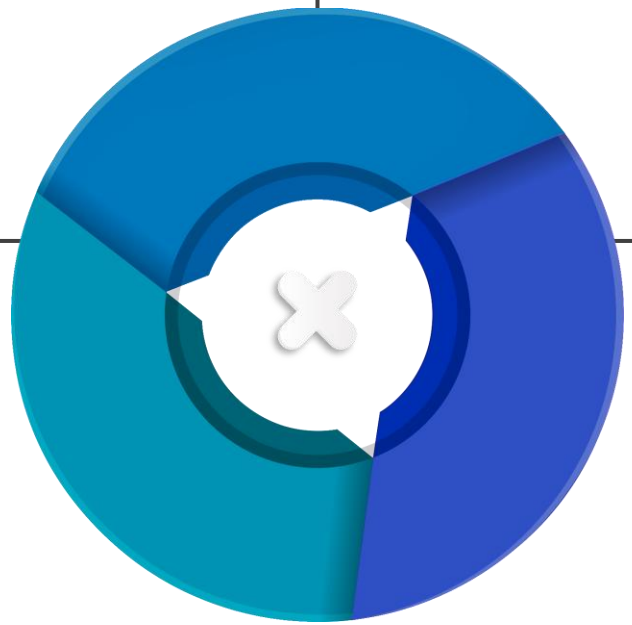
- Обнаружение нарушений
- Эффективность политики (моделирование мер поддержки, стресс-тестирование и т.д.)
- Дополнительные данные для анализа
- Развитие конкурентного доступа к данным
- Поддержка инноваций и создание нового рынка
- Укрепление цифрового суверенитета

Барьеры обмена данными

1

Организационные

Конфликт мотиваций владельцев и потребителей данных из разных отраслей



2

Технологические

Неструктурированность данных, необходимость участия человека, высокие требования к вычислительной инфраструктуре

3

Юридические

Строгие нормы регулирования, устаревшие стандарты, отсутствие четких границ, критериев и таксономии

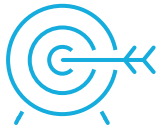
Что такое конфиденциальные вычисления?

Конфиденциальные вычисления — это способ обработки данных таким образом, чтобы они **оставались защищёнными и недоступными** для посторонних лиц даже во время выполнения вычислений.

Конфиденциальные вычисления решают эту проблему, позволяя **выполнять операции над данными в зашифрованном виде** или внутри специальных защищённых сред.

Что такое PET — Privacy-Enhancing Technologies?

PET (Технологии Повышения Конфиденциальности) — это совокупность методов и технологий, обеспечивающих обработку и анализ данных без раскрытия их исходного содержания неавторизованным сторонам. PETs позволяют сохранять приватность информации на всех этапах её жизненного цикла (передача, хранение, обработка), минимизируя риски утечек и несанкционированного доступа.



ЦЕЛЬ PET

Минимизировать утечки и несанкционированный доступ к данным.

Почему PETs сегодня особенно важны

Бизнесу нужно использовать данные, но без риска утечек. Компании хотят извлекать ценность из персональных данных, но обязаны защищать конфиденциальность.

Нужно сотрудничество между организациями: банки, клиники и т. д. Но никто не хочет раскрывать свои данные.

Технологии повышения конфиденциальности

01

Гомоморфное шифрование (Homomorphic Encryption)

Позволяет выполнять вычисления над зашифрованными данными без их расшифрования. Результат операций остается в зашифрованной форме и может быть расшифрован только владельцем ключа.

Применение: облачные вычисления, конфиденциальный ИИ, финтех.

02

Безопасные многопользовательские вычисления (SMPC — Secure Multi-Party Computation)

Несколько участников совместно выполняют вычисления, не раскрывая свои входные данные друг другу. Каждый участник получает только результат, не зная данных других.

Применение: совместная аналитика, голосования, приватная статистика.

03

Дифференциальная приватность (Differential Privacy)

Добавляет контролируемый шум в данные или ответы на запросы, чтобы скрыть наличие или отсутствие конкретной записи. Гарантирует, что вывод не меняется существенно при добавлении/удалении одного пользователя.

Применение: сбор статистики, машинное обучение, большие данные.

04

Федеративное обучение (Federated Learning)

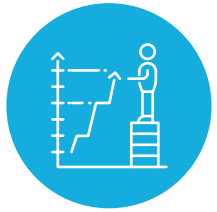
Позволяет обучать модели машинного обучения на распределённых устройствах без передачи исходных данных на центральный сервер. Данные остаются локально, а передаются только обновления модели, которые затем агрегируются.

Применение: персонализированные рекомендации, медицина, мобильные устройства, приложения с усиленной конфиденциальностью.

Барьеры

Неопределённый экономический эффект (ROI)

Сложность интеграции



Высокая вычислительная нагрузка

Дефицит специалистов

Практические примеры использования

Общие сценарии применения:

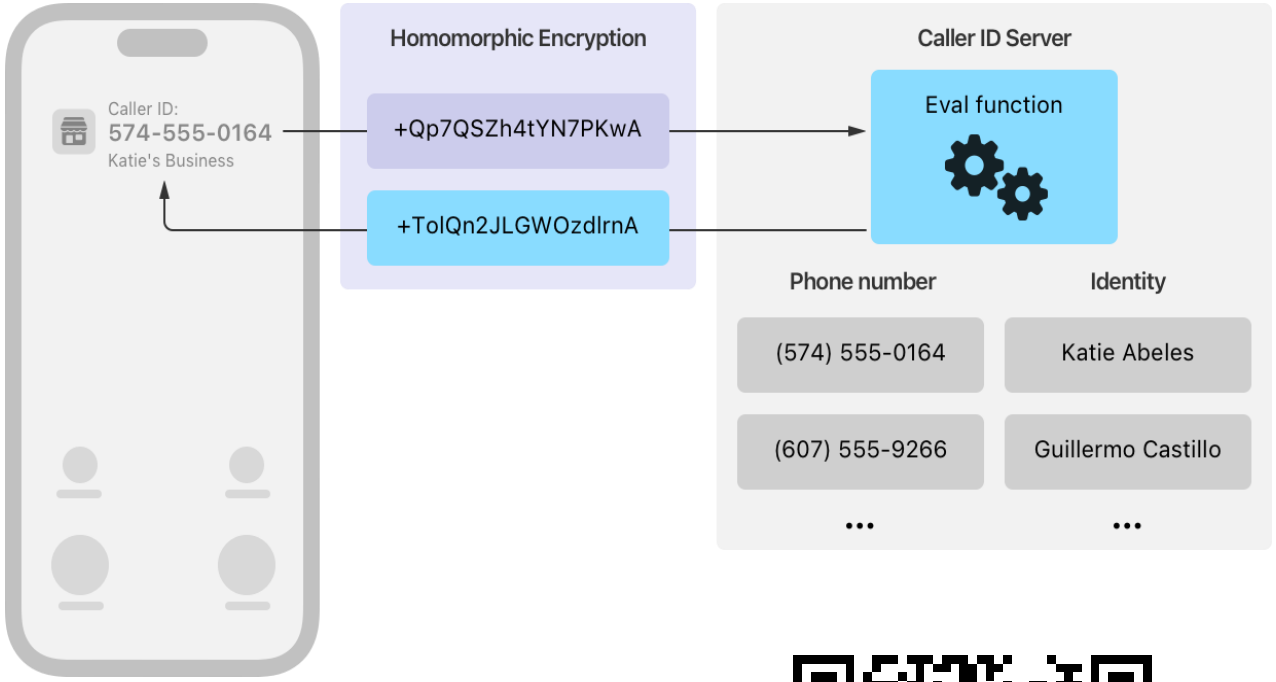
- Облачные вычисления: клиент может зашифровать данные и отправить в облако для анализа.
- Приватный машинный интеллект (AI/ML): модель обучается или делает предсказания на зашифрованных данных.
- Финансовые и медицинские данные: чувствительные данные никогда не раскрываются, даже при обработке.

Зарубежная практика:

1. Microsoft SEAL & Azure Confidential Computing
Microsoft разработала библиотеку **SEAL** для гомоморфного шифрования (C++), которая используется в **Azure Confidential ML** для обучение и инференс моделей машинного обучения на зашифрованных данных.

2. IBM & Медицинские исследования
IBM активно применяет FHE в проектах с медицинскими учреждениями, например, **совместная обработка геномных данных** разных лабораторий с полным сохранением приватности.

Практические примеры использования



Компания Apple объявила о создании открытой библиотеки с реализацией методов гомоморфного шифрования на языке Swift. Библиотека позволяет создавать приложения, обрабатывающие данные, доступные только в зашифрованном виде, без промежуточной расшифровки ни на одном из этапов вычислений. На выходе выдаётся зашифрованный результат, который аналогичен шифрованию результата выполнения тех же вычислений над исходными незашифрованными данными.

Код проекта распространяется под лицензией Apache 2.0. Реализация основана на схеме BFV (Brakerski-Fan-Vercauteren), которая, в свою очередь, основана на задаче обучения с ошибками в кольце (RLWE), защищённой от криптоанализа квантовыми компьютерами. Низкоуровневые примитивы для шифрования используются из библиотеки Swift Crypto.

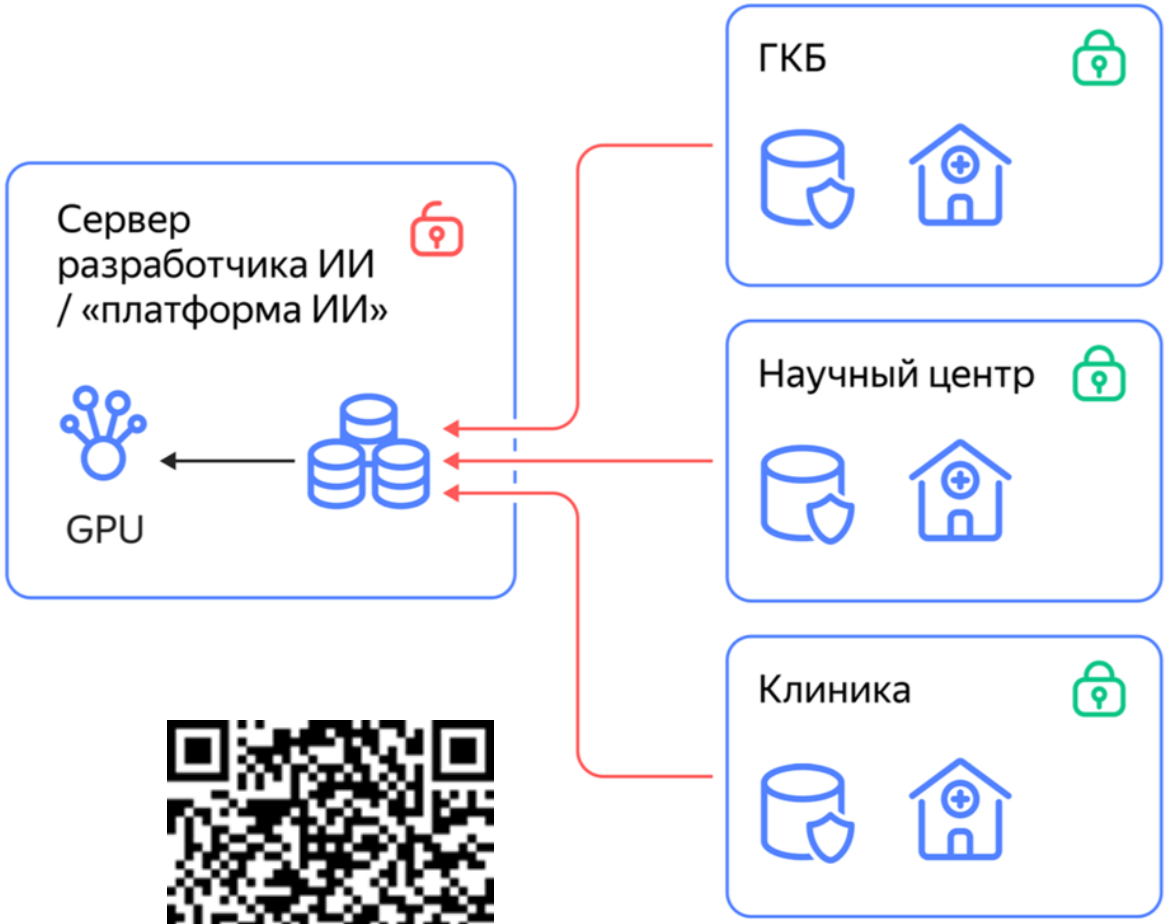
Кейс: ВТБ, МФТИ и Т1
Комплекс инструментов для передачи больших массивов данных

Крипто-анклав — инновационный программно-аппаратный комплекс, использующий технологии слепого машинного обучения, AutoML и защищённых вычислений в анклавах. Это первое в России решение, позволяющее организациям безопасно обмениваться данными в зашифрованном пространстве без раскрытия конфиденциальной информации.

Благодаря использованию принципа «**чёрного ящика»,** информация в крипто-анклаве хранится и обрабатывается в закодированном виде, без возможности доступа для человека или несанкционированного вмешательства. Это позволяет банкам, телеком-операторам и другим организациям надёжно строить совместные прогнозные модели и работать с данными в условиях полной конфиденциальности.

Кейс: Яндекс, ИСП РАН и Сеченовский университет
Федеративное обучение в здравоохранении

Яндекс, ИСП РАН и Сеченовский университет разработали нейросетевую модель для выявления фибрилляции предсердий — одной из наиболее распространённых сердечных патологий — на основе данных ЭКГ.
Проект реализует технологию **федеративного обучения (FL)**, при которой данные остаются у владельцев и не передаются между организациями. Каждая сторона обучает модель локально, передавая только параметры, а не сами данные.
Это решение доказывает, что **совместные исследования в медицине и ИИ** возможны без нарушения приватности и безопасности данных. Подход особенно эффективен в чувствительных сферах, где невозможна централизация хранения информации



Тренды и будущее PETs

1

PET в облаках по умолчанию

Конфиденциальность станет встроенной частью облачных сервисов (Cloud PET).

2

PET + ИИ и машинное обучение

Обучение ИИ без доступа к личным данным (federated learning, приватный AI).

3

Поддержка со стороны государства

Разработка стандартов, регулирование, внедрение в здраво-охранении, финансах, образовании.

4

Специализиро-ванное «железо» для PET

Аппаратные ускорители (новые процессоры, чипы) сделают PET быстрее и доступнее.

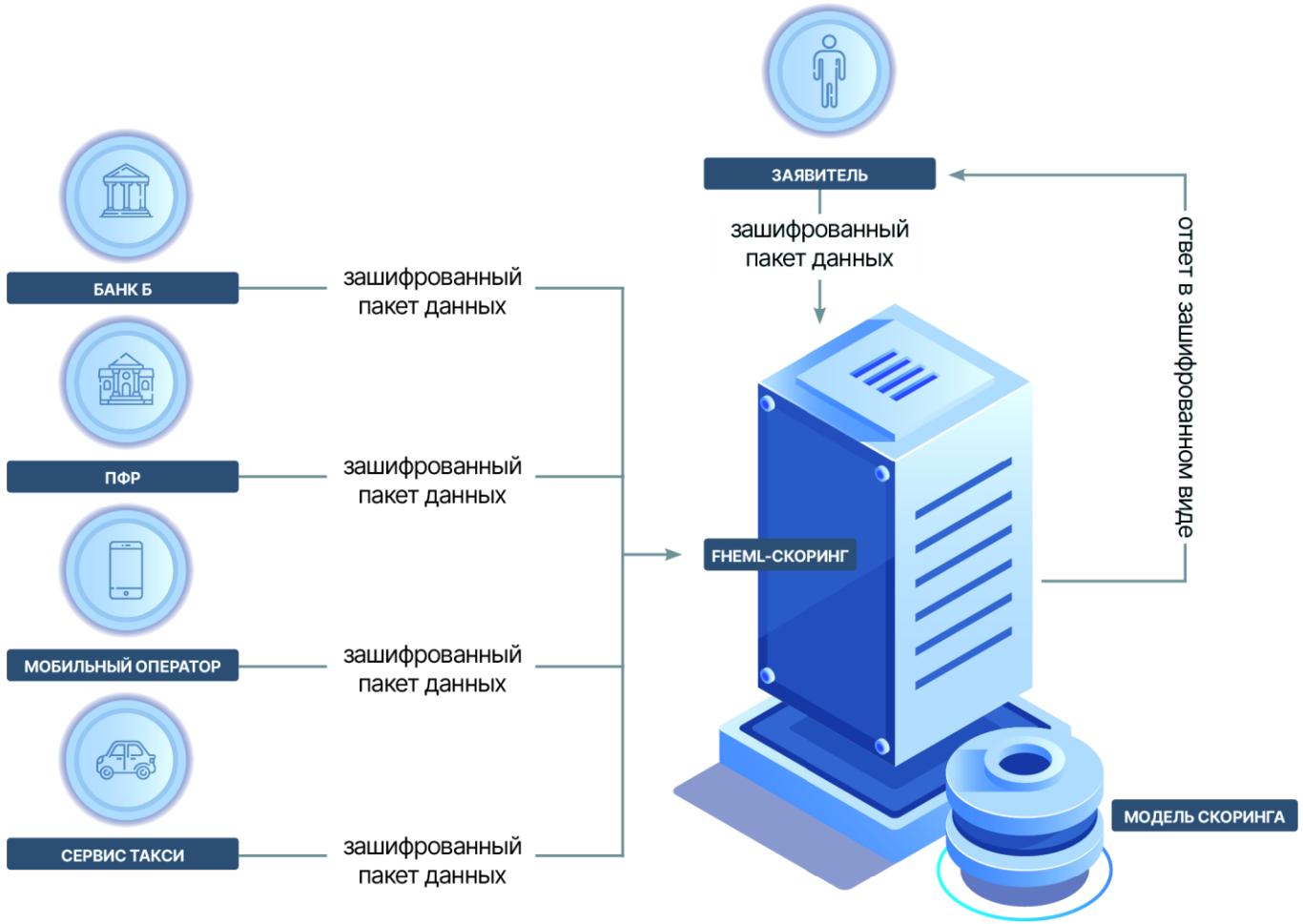
PET — это не про «спрятать всё навсегда», а про «делиться безопасно и контролируемо».
Технологии уже работают, но успех — в правильном **комбо «железо + крипто + процессы + право»**.

Кредитный скоринг с применением FHE

Пилот в лаборатории конфиденциальных вычислений технологической песочницы АФТ демонстрирует возможность проведения оценки кредитоспособности на зашифрованных данных с использованием FHE.

Традиционно, для оценки кредитного риска финансовые учреждения требуют доступа к личной информации клиентов, что может вызывать опасения по поводу конфиденциальности.

С применением FHE, финансовые организации могут анализировать зашифрованные данные клиентов без их расшифрования, обеспечивая при этом высокий уровень приватности.



Конфиденциальные вычисления

ИССЛЕДОВАНИЕ ДОСТУПНО ПО ССЫЛКЕ

СПАСИБО ЗА ВНИМАНИЕ!

Сергей Лапин

Эксперт по информационной безопасности

s.lapin@fintechru.org

Telegram - канал

Исследование