



АССОЦИАЦИЯ  
ФИНТЕХ

# Конфиденциальные вычисления

методы и технологии безопасной  
обработки данных

**ФИНТЕХ**  
— РАДАР

№8 МАЙ 2025

**Конфиденциальные вычисления –**  
это набор инструментов  
обеспечения безопасности  
и повышения конфиденциальности,  
ориентированный на защиту  
используемых данных.



АССОЦИАЦИЯ  
ФИНТЕХ

**Ассоциация ФинТех** основана в конце 2016 г. по инициативе Банка России и ключевых участников отечественного финансового рынка. Это уникальная аналитическая площадка для конструктивного диалога регулятора с представителями бизнеса. Здесь формируется экспертная оценка инновационных технологий с учетом международного опыта, а также разрабатываются концепции финансовых технологий и подходы к их внедрению.

# СОДЕРЖАНИЕ

---

|                                                                               |     |
|-------------------------------------------------------------------------------|-----|
| Что такое Финтех-Радар?                                                       | 04. |
| Почему конфиденциальные вычисления важны? Мнение экспертов                    | 06. |
| Ключевые выводы                                                               | 08. |
| Организация обмена данными                                                    | 10. |
| Таксономия данных                                                             | 12. |
| Ключевые барьеры для обмена данными в России                                  | 14. |
| Иерархия ценности данных                                                      | 15. |
| Подходы к обеспечению конфиденциального обмена данными                        | 16. |
| Прорывные технологии в области конфиденциальных вычислений                    | 17. |
| Обзор перспективных методов криптографии для конфиденциального обмена данными | 22. |
| Регулирование технологий конфиденциальных вычислений в России                 | 25. |
| Международный опыт организации конфиденциального обмена данными               | 27. |
| Разработка инструментов конфиденциального обмена данными в России             | 30. |
| Платформы обмена данными                                                      | 34. |
| Инициативы Ассоциации ФинТех в области технологий конфиденциальных вычислений | 37. |

# ОБ ИССЛЕДОВАНИИ

---

Вот уже третий год Ассоциация ФинТех отслеживает ключевые технологические тенденции, которые трансформируют финансовый рынок. Технологии конфиденциальных вычислений были выбраны ключевой темой не случайно. Из-за роста киберугроз защита данных становится критически важной. В 2025 году на площадке АФТ создана Лаборатория конфиденциальных вычислений, которая дает возможность участникам Ассоциации «почувствовать» все возможности этой технологии «здесь и сейчас».

Большинство международных аналитических агентств, таких как Gartner, Forrester, MIT сосредотачивают внимание именно на технологиях информационной безопасности и борьбе с новым поколением рисков и угроз. Мы со своей стороны также следим за тем, что происходит в мире и в России, и как организован обмен данными и их защита у крупнейших технологических компаний.

Этот выпуск подготовлен совместно с ведущим экспертами в области кибербезопасности. Совместно мы определили таксономию данных, выделили прорывные технологии конфиденциальных вычислений и криптографии и попытались доступным языком рассказать о ключевых методах безопасной обработки данных, которые используют участники российского финтеха. Надеемся, что наша совместная работа будет полезна для понимания, куда движется рынок кибербезопасности.

## **МАРИАННА ДАНИЛИНА**

*Руководитель управления стратегии, исследований и аналитики **Ассоциации ФинТех***

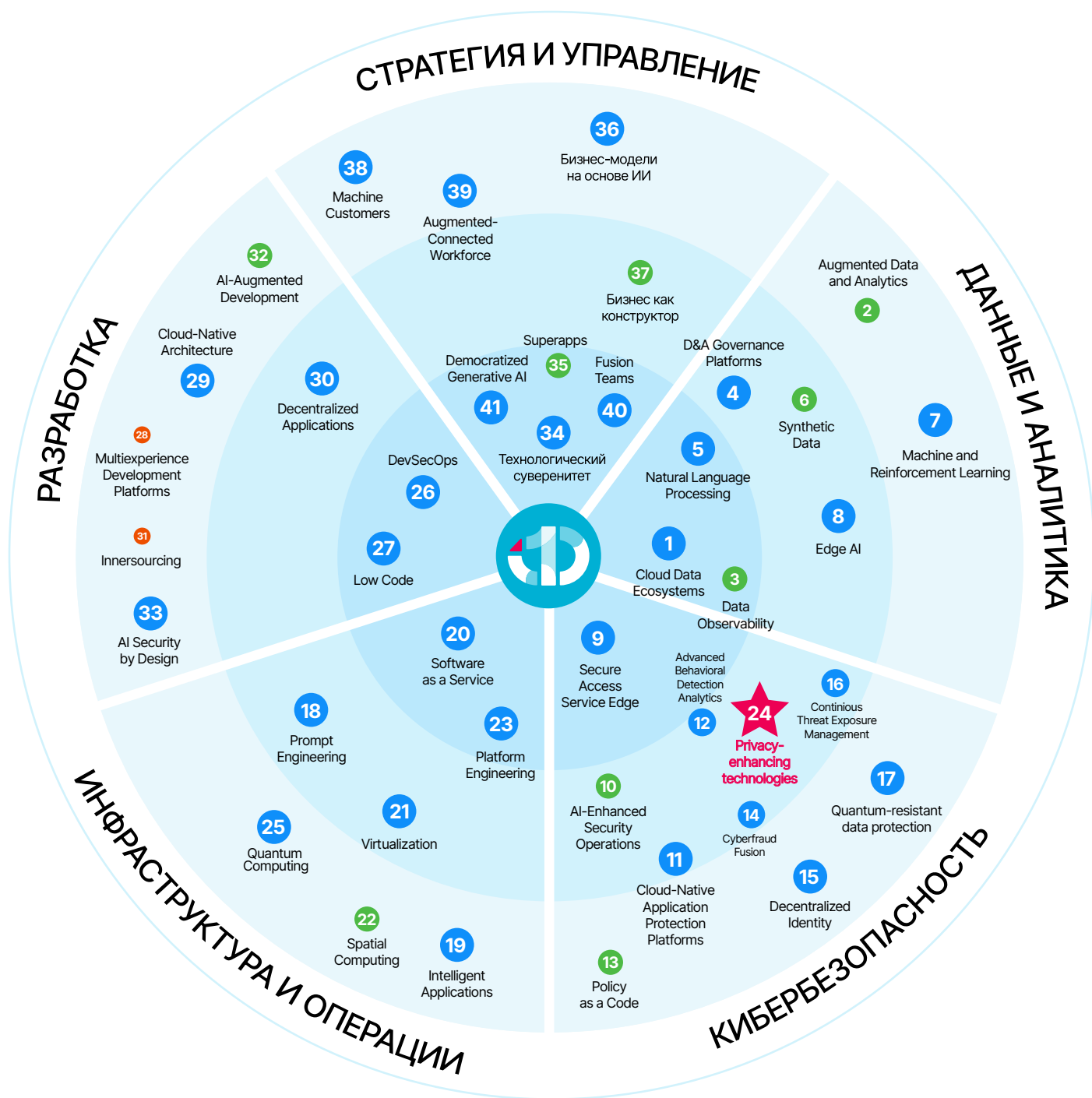
По вопросам Финтех-Радара и с обратной связью, пожалуйста, обращайтесь к команде исследований и аналитики Ассоциации ФинТех

---

[research.analytics@fintechru.org](mailto:research.analytics@fintechru.org)



# ТЕХНОЛОГИЧЕСКИЙ ФИНТЕХ-РАДАР 2024-2025 ГОДА



**Горизонт адаптации\*:**

3-6 лет    1-3 года    Сейчас (до 1 года)

**Степень влияния:**

Высокая    Средняя    Низкая

**Технология выпуска:**

★ Privacy-enhancing technologies (PET)

\* Для российского рынка горизонт адаптации трендов может увеличиваться на 1-3 года



АССОЦИАЦИЯ  
ФИНТЕХ

# ПОЧЕМУ КОНФИДЕНЦИАЛЬНЫЕ ВЫЧИСЛЕНИЯ ВАЖНЫ? МНЕНИЕ ЭКСПЕРТОВ

---



**АЛЕКСЕЙ НЕЙМАН**

*Исполнительный директор,  
Ассоциация больших данных*

Развитие технологий и продуктов в сфере больших данных требует надежных решений для защиты информации. Для бизнеса это означает возможность использовать ценную аналитику, не подвергая риску конфиденциальность клиентских и корпоративных данных. Технологии частных вычислений, включая гомоморфное шифрование, многосторонние вычисления (MPC) и дифференциальную приватность, позволяют анализировать данные без их раскрытия. Это способствует развитию совместных проектов, безопасному обмену информацией и созданию инновационных продуктов и услуг.

Ассоциация больших данных готовится к запуску Библиотеки методов конфиденциальной работы с данными — ресурса, который станет площадкой для сотрудничества специалистов и обмена знаниями. В Библиотеке будут собраны материалы о передовых технологиях защиты и безопасной обработки данных. Цель ресурса — сформировать единую терминологию, делиться актуальными практиками и поддерживать развитие технологических решений в сфере работы с данными.



**ПЕТР ЕМЕЛЬЯНОВ**

*CEO, Bloomtech*

Существуют сотни задач, успешное решение которых зависит от информационной коллаборации. У кредитных организаций это — оценка доходов, разные скоринги, антифрод. В медицине, например, зависимость фенотипа от генотипа. В промышленности — отраслевая и межотраслевая статистика. В науке — объединение данных исследований, в том числе международных. В инновациях — конфиденциальный искусственный интеллект. Примеров очень много. Как правило, такие задачи решают централизацией: давайте сложим все данные в одно место и посмотрим, что будет.

Минусы такого подхода очевидны. Коллективное бессознательное формулирует их так: не складывайте все яйца в одну корзину. Совместные конфиденциальные вычисления — новый, альтернативный подход: представьте, вы анализируете данные других компаний, а они анализируют ваши, но никто никому ничего не передает и не консолидирует у третьей стороны. Вы полностью контролируете использование ваших данных, сохраняете их перманентную ценность и выполняете обязательства перед своими клиентами. Прозрачное сотрудничество. И все это — благодаря математическому алгоритму, безопасность которого можно обосновать. Конфиденциальность больше не ограничение, конфиденциальность — это инструмент прогресса.



**АНТОН ГУГЛЯ**

Генеральный директор, QApp

Технологии конфиденциальных вычислений способны решать задачи не только финансового сектора, но и медицинской, нефтегазовой и других отраслей экономики. Последние несколько лет в России наблюдается стремительное развитие как программных, так и аппаратных подходов реализации, увеличилось число пилотных проектов, модернизируется регуляторика и профильные образовательные программы.

Сформированы первые отраслевые рабочие группы (например, рабочая группа Ассоциации ФинТех, Газпромбанка и QApp по применению конфиденциальных вычислений в финансовой отрасли уже включает более 15 организаций-участников). Проводятся образовательные мероприятия на базе профильных университетов (например, открытый митап в МГТУ им. Н. Э. Баумана собрал более 150 человек).

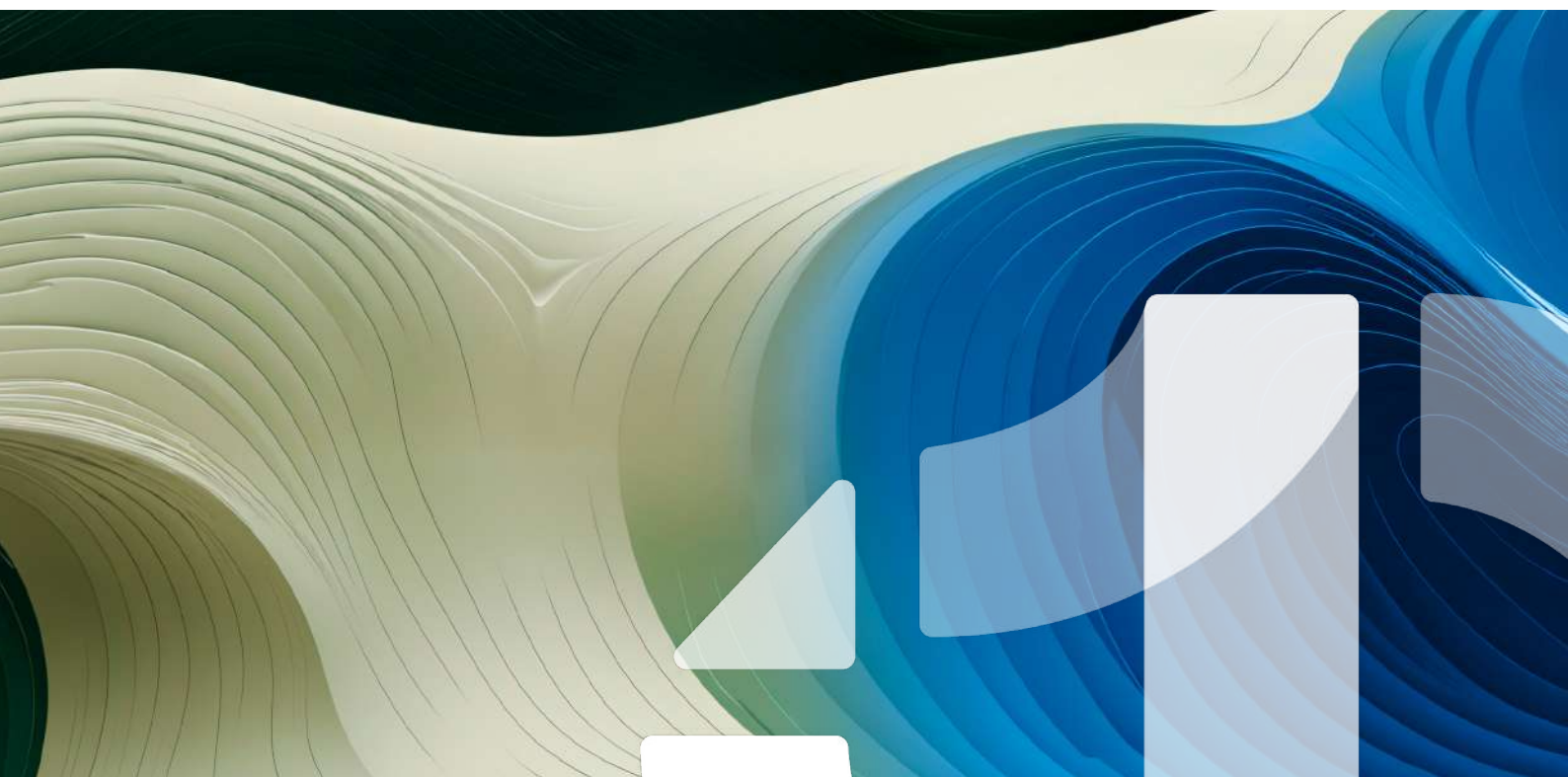
В своих прикладных исследованиях и пилотных проектах мы в QApp фокусируемся на программном SMPC-подходе, который позволяет выполнять процедуры вычислений на оборудовании и операционных системах общего назначения.



**ИЛЬЯ ЛИВАШВИЛИ**

Начальник Департамента аналитики  
и внедрения технологий, Газпромбанк

Конфиденциальные вычисления — технология новой эры цифровой безопасности в финтехе. Хотя технология пока не получила массового внедрения, ее потенциал сложно переоценить. В Газпромбанке мы целенаправленно тестируем решения на базе конфиденциальных вычислений, так как видим в них ключ к обновлению работы с клиентскими данными. Мы ожидаем, что в ближайшие годы конфиденциальные вычисления станут стандартом для отрасли. Внедрение таких решений — важный шаг к созданию по-настоящему эффективной и защищенной цифровой экосистемы.



# КЛЮЧЕВЫЕ ВЫВОДЫ

---

**01.** Данные становятся «топливом» для экономики и важнейшим нематериальным активом.

**02.** Эффективный и безопасный обмен данными решает проблему нехватки «топлива» для технологий и может стать катализатором для экономического роста.

**03.** Вопрос обмена и совместного доступа к данным очень сложен и многогранен.

Для его эффективной проработки необходимо комплексное решение юридических, технических и организационных барьеров, снижение возникающих рисков и соблюдение баланса между достижением роста и обеспечением принципов этики.

**04.** Ценность для рынка имеют не сами данные, а «информация» и «знание». Именно на их основе можно принимать решения, учитывая риски и стратегические цели в долгосрочной перспективе.

**05.** Оптимальное сочетание подходов и технологий для обеспечения защищенного обмена и совместного доступа к данным складывается из следующих слагаемых:

Криптозащита каналов  
и среды обработки данных



Продвинутые методы  
обработки данных



Снижение  
«чувствительности»  
данных

**06.** В рамках текущего регулирования, технологии повышения конфиденциальности позволяют организовывать совместное получение доступа к данным, обмен ими и совместную обработку.



# Организация обмена данными

Активная цифровизация, развитие информационных технологий и интернета вещей приводят к **увеличению объемов данных**, доступных для обмена и последующей обработки.

## ЧТО ТАКОЕ ДАННЫЕ?

**Данные** – электронное представление информации в пригодном для передачи, обработки и интерпретации виде.

Благодаря возможностям аналитики, в том числе продвинутых методов на основе ИИ, данные могут быть **эффективно обработаны**, что способствует созданию дополнительной ценности и повышению производительности всей экономики.

**Данные** становятся **«топливом» современной экономики**, особенно в контексте развития искусственного интеллекта. Они представляют собой **важный нематериальный ресурс**, способный существенно влиять на эффективность, доходы и издержки компаний. Однако компаниям часто **не хватает высококачественных данных**, и при обмене данными, который мог бы решить эту проблему, они сталкиваются с рядом юридических, организационных и технологических проблем.

## ЧТО ТАКОЕ ОБМЕН ДАННЫМИ?

**Обмен данными:**

- 1) **передача** структурированных/неструктурированных исходных данных,
- 2) **обмен результатами обработки данных** в виде информации и знаний (без передачи исходных данных), а также совместный доступ к данным, в том числе **Data Fusion**, для улучшения/обучения инструментов аналитики (в том числе AI/ML), помогающих принимать решения на основе «мудрости».

**Data Fusion** — процесс объединения и интеграции данных из различных источников для создания ценной информации, цель которого — достичь максимального синергетического эффекта данных при их совместной обработке.

## ОБМЕН ДАННЫМИ ПОЗВОЛЯЕТ УЛУЧШИТЬ:

Данные могут быть разными и включать в себя, например, информацию реального мира – о физических и юридических лицах или окружающей среде. Как правило, выделяют **три составляющих общества** и, соответственно, **троих участников обмена данными**: клиент, бизнес-организации и государство.



**Более 60%** российских финансовых компаний считают недостаток данных для обучения моделей ИИ одним из наиболее значимых барьеров для развития ИИ.

Однако, сегодня многие компании сталкиваются с **проблемой недостатка данных**. Качество и широта доступных данных быстро исчерпывают себя, что ограничивает возможности для развития указанных современных технологий. Особенно остро эта проблема стоит для обучения передовых моделей искусственного интеллекта.

## ПРОБЛЕМА НЕДОСТАТКА ДАННЫХ



### Потребности рынка

- Обеспечить поток ценной информации, **обогащать** данные о клиентах и рынке и **улучшить их качество**
- Внедрить **инструменты продвинутой аналитики и ИИ** для повышения эффективности принятия решений
- Улучшить **взаимодействие с клиентом** путем персонализации на основе данных
- Получить способ **монетизации данных**



### Риски сохранения текущей ситуации

- Сохранение **«серого» статуса** обмена чувствительной информацией
- Сохранение **барьеров для развития** инструментов анализа данных и ИИ
- Отсутствие эффекта масштаба и сетевого эффекта от совместного использования данных
- Усугубление монополизации рынка – **рост «стратификации»** организаций
- Сохранение исключительности БигТехов в области владения и монетизации данных

Итоговый эффект от обмена данными будет зависеть от их качества, разнообразия, уровня развития и доступности технологий их сбора, обработки и аналитики. Расширение возможностей использования данных может создать синергетический эффект в повышении эффективности участников рынка и экономики в целом.

# Таксономия данных

Существуют различные подходы к классификации данных, которые стоит учитывать при их обмене и обработке. Таксономия данных зависит не только от содержания, но и от способа их получения и источника информации – необходимо взаимное однозначное соответствие типов данных между собой (единый стандарт семантики данных).

## ПО ЭТАПАМ ОБРАБОТКИ

1. Необработанные (исходные) данные
2. Псевдонимизированные
3. Анонимизированные
4. Зашифрованные
5. Производные/Агрегированные
6. Синтетические
7. Мета-данные

## ПО НЕОБХОДИМОСТИ УЧАСТИЯ ЧЕЛОВЕКА

1. Пригодные для обработки с помощью человека
2. Пригодные для обработки с помощью «машинного зрения»/ ИИ
3. Машиночитаемые / пригодные для обработки традиционными программными средствами

## ПО ТИПУ СБОРА ДАННЫХ

1. Авторские данные
2. Добровольно предоставленные данные
3. «Захваченные» данные
4. Производные данные
5. Идентификационные данные
6. Транзакционные данные
7. Справочные данные
8. Мета-данные
9. Неструктурированные данные
10. Результаты измерений

## ПО ИСТОЧНИКУ

1. Персональные данные
2. Коммерческие данные
3. Данные государственного сектора
4. Данные окружающего мира

## ПО КАЧЕСТВУ

- |                            |                |               |
|----------------------------|----------------|---------------|
| 1. Верифицированные данные | 4. Неполные    | 7. Устаревшие |
| 2. Частично качественные   | 5. Зашумленные |               |
| 3. Некачественные          | 6. Дублирующие |               |

## ПО СТЕПЕНИ КОНФИДЕНЦИАЛЬНОСТИ (ПО РОССИЙСКОМУ ЗАКОНОДАТЕЛЬСТВУ)\*

Данные

1. **Общедоступные**
2. **Ограниченного доступа**
  - 2.1 **Государственная тайна**
  - 2.2 **Конфиденциальная информация**
    - 2.2.1 Персональные данные
    - 2.2.2 Служебная тайна
    - 2.2.3 Профессиональная тайна
    - 2.2.4 Коммерческая тайна
    - 2.2.5 Иные данные

*\* Для цели этого исследования рассматривается классификация по степени конфиденциальности данных*

Таксономия данных в России формируется с учётом различных подходов к их классификации (например, по чувствительности, источнику и способу обработки), однако из-за отсутствия единого стандарта между регулируемыми организациями возникают противоречия, что особенно заметно в финансовом секторе, где данные ограниченного доступа не имеют чётко определённых целей обработки.



## ПРИМЕР КЛАССИФИКАЦИИ ДАННЫХ



<sup>1</sup>Определения «тайны» соответствует контексту закона:

**Тайна** – режим конфиденциальности (коммерческая)

**Тайна** – информация ограниченного доступа (государственная, налоговая)

Обязательное для выполнения лицом, получившим доступ к определенной информации, **требование** не передавать такую информацию третьим лицам **без согласия** ее Владельца (NDA)

Классификация данных зависит от их чувствительности, источника и способа обработки, при этом разные категории информации (общедоступная, государственная, конфиденциальная) регулируются отдельно.

# Ключевые барьеры для обмена данными в России

Концепция Открытых данных и вопрос обмена данными уже несколько лет активно обсуждаются участниками рынка не только в контексте развития решений ИИ, но и в рамках повышения общей эффективности бизнеса, улучшения клиентоориентированности и государственного регулирования за счет аналитики.

Тем не менее, на этом пути существуют ряд всем известных барьеров, связанных с обеспечением конфиденциальности «чувствительных» данных и информационной безопасностью, правовой неопределенностью и вопросами средств взаимодействия (несовместимости систем).

Помимо этого, существует важный организационный вопрос – **конфликт мотиваций**: участникам интересно получать и «обогащать» свои данные, но не делиться ими. Этот вопрос особенно актуален в случае организации обмена между ФинТехом и БигТехом в связи с возможностью регуляторного арбитража.

## БАРЬЕРЫ ДЛЯ ОБМЕНА ДАННЫМИ В РОССИИ:



Развитие механизмов эффективного обмена данными возможно **только в условиях комплексного решения** юридических, технических и организационных барьеров.

Несмотря на долгое обсуждение, «прямой» обмен конфиденциальной информацией до сих пор находится в «серой» зоне регулирования. Ослабление требований к защите данных и информационной безопасности может повлечь серьезные последствия как с точки зрения развития киберпреступности и неконкурентных практик, так и с точки зрения снижения доверия граждан к информационным системам.

Развитие рынка данных требует настройки регулирования, в том числе классификации участников и определения общей таксономии данных. Такие изменения требуют большой вовлеченности и координации от регуляторов и участников рынка. Таким образом, вопрос обмена «чувствительной» информацией с использованием традиционных способов обеспечения конфиденциальности далек от решения, поиск таких компромиссов требует много времени и ресурсов.

# Иерархия ценности данных

Современный рынок зачастую гонится за большими объемами данных, стремясь получить как можно больше информации. Однако сырые, необработанные данные, лишенные структуры и контекста, не представляют ценности для компании. Они остаются лишь набором разрозненных фактов, из которых невозможно извлечь полезные выводы.

Гораздо важнее **не просто собирать данные, а преобразовывать их в знания** – качественную, структурированную информацию с четкими механизмами использования. Только такие данные позволяют принимать обоснованные решения и создавать реальные конкурентные преимущества.

Именно поэтому простой обмен сырыми данными не имеет смысла. Ключевая **задача рынка – разработать механизм передачи** уже обработанной и структурированной информации, который обеспечит ее практическую пользу, но при этом сохранит конфиденциальность и предотвратит нежелательное разглашение.

Технологии конфиденциальных вычислений могут помочь в решении поставленной задачи и обеспечить безопасную обработку данных.

## ЦЕННОСТЬ ДАННЫХ ДЛЯ РЫНКА:



**Сырые данные** – это как **неочищенная нефть**: они содержат скрытую ценность, но в исходном виде практически непригодны для непосредственного использования. Их сбор и хранение – лишь первый шаг, как добыча нефти. Далее продукт переходит в стадию **«информация»** – это **первичная переработка**, например, синтез бензина. С целью снижения рисков, роста эффективности маркетинга и логистики, бензин становится **«знанием»** – например, производятся растворители, химические компоненты. В части **формирования решения на основе качественных данных** – изготавливаются высокомаржинальные продукты, а именно пластмассы, синтетический каучук.

Как нефть становится дороже после переработки в специализированные материалы, так и **данные превращаются в ключевой актив бизнеса лишь после преобразования в знания и решения**. Максимальную прибыль приносят не «сырые», а готовые продукты – алгоритмы, сервисы и стратегии, меняющие рынок.

**«Данные → Информация → Знание → Мудрость»** – это **эволюция ценности**, где на каждом этапе повышается качество и полезность для принятия решений.

# Подходы к обеспечению конфиденциального обмена данными

Изучение вопроса организации обмена данными показало, что существующие отечественные практики состоят в основном из комбинации простых методов обезличивания и криптографических инструментов защиты данных, а также каналов их передачи, сред хранения. При этом сохраняется большая часть «чувствительной» информации передаваемых данных, что сразу связывает их с соответствующими режимами конфиденциальности и ограничениями на передачу.

**Оптимальное сочетание подходов и технологий** для обеспечения защищенного обмена и совместного доступа к данным складывается из следующих слагаемых:

Криптозащита каналов  
и среды обработки данных



Снижение  
«чувствительности»  
данных



Продвинутые методы  
обработки данных

Методы, демонстрирующие высокие значения одной из составляющих (например, конфиденциальности), могут обеспечивать надежную защиту данных, но при этом снижать доступность информации.

## ФОРМУЛА ДЛЯ РЕШЕНИЯ ДИЛЕММЫ «ДОСТУПНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ»

В контексте той или иной технологии, формула для решения дилеммы состоит из 3-х направлений:

### ПОДХОДЫ К ОБЕСПЕЧЕНИЮ КОНФИДЕНЦИАЛЬНОСТИ

#### Криптозащита каналов и среды

##### Методы криптозащиты каналов

Шифрование  
Хэширование  
Токенизация

##### Методы защиты среды обработки данных

Вычисления в анклаве

#### Снижение «чувствительности» данных

Введение идентификаторов  
Перемешивание  
Агрегация  
Декомпозиция  
Изменение состава  
Маскирование  
Синтетические данные

#### Продвинутые методы обработки информации

##### Методы, основанные на криптографии

Гомоморфное шифрование  
Доказательство с нулевым разглашением  
Дифференциальная конфиденциальность  
Конфиденциальные многосторонние  
вычисления («SPMC»)

##### Статистические методы

Трансферное обучение  
Федеративное обучение  
Методы дополнения моделей ИИ  
Имитация поведения  
AutoML

**Конфиденциальные вычисления (Privacy-Enhancing Technologies, PETs)** – 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.

**Обмен данными в конфиденциальных вычислениях — это ключевой элемент для безопасного сотрудничества между организациями.** Он позволяет сохранять конфиденциальность, соблюдать законы и при этом использовать преимущества распределённых вычислений и ИИ. Без защищённого обмена данные остаются изолированными, что ограничивает их аналитическую и бизнес-ценность.

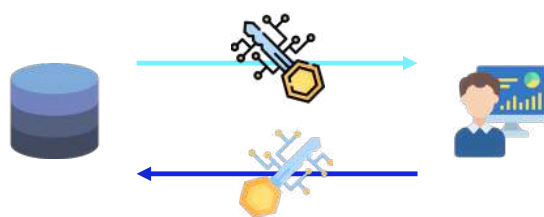
# Прорывные технологии в области конфиденциальных вычислений

Технологии конфиденциальных вычислений (Privacy Enhanced Technologies, PETs) позволяют компаниям выполнять вычисления с зашифрованными данными, предотвращая несанкционированный доступ к конфиденциальной информации и в то же время извлекая ценную информацию. Таким образом, современные технологии позволят преодолеть указанные выше барьеры без значительных на то ресурсов и изменений в текущем регулировании.

## ПРОРЫВНЫЕ МЕТОДЫ КОНФИДЕНЦИАЛЬНОЙ ОБРАБОТКИ ДАННЫХ:

1

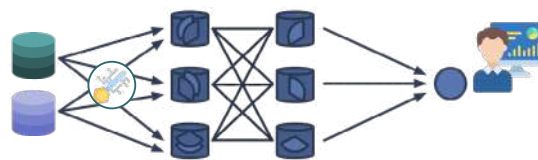
**Гомоморфное шифрование** – метод шифрования, который позволяет выполнять вычислительные операции с зашифрованными данными. Он генерирует зашифрованный результат, который при расшифровке соответствует результату операций, как если бы они были выполнены с незашифрованными исходными данными.



Гомоморфное шифрование **сложно использовать широко из-за ограничений методов и отсутствия общепринятых стандартов**. Гомоморфные схемы шифрования обычно поддерживают только один тип операций, а анализ полностью зашифрованных данных значительно медленнее, чем анализ открытых данных. Использование этого метода ограничивается сценариями с узким функционалом или сценариями, где скорость вычислений не критична.

2

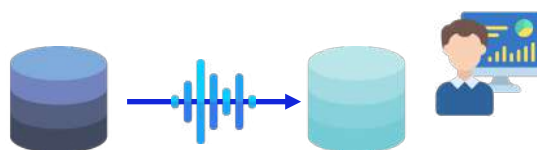
**Безопасные многосторонние вычисления («SMPC»)** – «подраздел» гомоморфного шифрования с одним отличием: пользователи могут вычислять значения из нескольких зашифрованных источников данных. Таким образом, модели машинного обучения могут быть применены к зашифрованным данным, поскольку SMPC используется для большего объема данных.



**SMPC** – новая технология, **применение которой в финансах ограничено**. Причина в том, что она требует индивидуальной настройки для каждого случая использования и имеет высокие затраты на настройку. Разрабатываются «компиляторы» для общих вычислений и приложений анализа данных. Современные системы SMPC дорогие из-за высокой стоимости обеспечения специальных каналов связи.

3

**Дифференциальная конфиденциальность** – криптографический алгоритм добавляет слой «статистического шума» к набору данных, который позволяет описывать структуры групп внутри набора данных, сохраняя конфиденциальность отдельных лиц.



Технология дифференциальной конфиденциальности **хорошо подходит для использования в финансовых учреждениях**. Добавление «шума» позволяет создать баланс между точностью и конфиденциальностью, что делает этот метод подходящим для анализа общих тенденций, но не для выявления аномалий (таких как мошенничество) или точного сравнения.

4

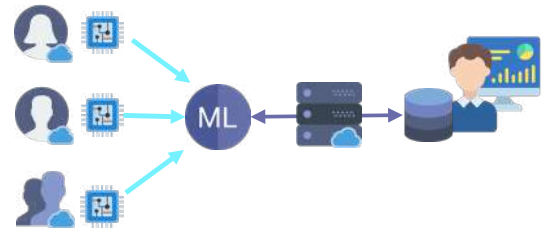
**Доказательства с нулевым разглашением** – совокупность методов, которые используют набор криптографических алгоритмов, позволяющих проверять/подтверждать информацию, не раскрывая исходные данные.



Доказательства с нулевым разглашением **недавно стали применяться на практике и будут играть ключевую роль** в развитии технологий распределенных реестров, таких как блокчейн. Методология продолжает развиваться и уже используется в различных областях, включая платежи, инфраструктуру интернета и цифровую идентификацию.

5

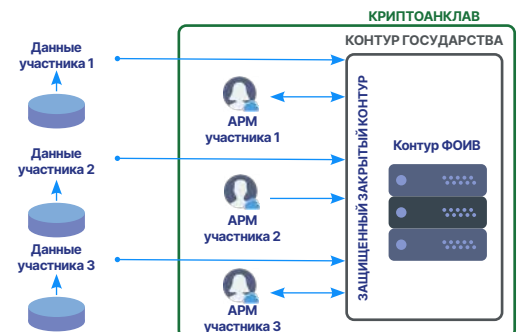
**Федеративное обучение** – это метод машинного обучения, который тренирует алгоритм на нескольких удаленных устройствах или серверах без обмена данными между ними. Этот метод позволяет минимизировать объем данных, хранящихся на централизованных серверах или в облаке, повышая тем самым конфиденциальность пользователей.



Федеративное обучение является технически развитой методикой, но в финансовой индустрии **её применение пока что ограничено**. Наибольшая ценность объединенного анализа проявляется при большом количестве отдельных источников данных, например, на смартфонах, устройствах интернета вещей, ноутбуках. В сфере финансовых услуг обычно не хранят в таком количестве конфиденциальную информацию из сотен и тысяч источников.

6

**Вычисления в криптоанклаве** – это метод обработки данных, при котором операции выполняются внутри защищенной аппаратно-программной среды (анклава), изолированной от основной системы. Данные остаются зашифрованными вне анклава и расшифровываются только внутри него, что исключает возможность их перехвата или несанкционированного доступа.



Наибольшую ценность вычисления в криптоанклаве представляют для задач, требующих высокой степени защиты, например: проверка кредитоспособности без раскрытия истории клиента, анализ мошеннических операций без доступа к исходным транзакциям, совместные вычисления между конкурирующими организациями (например, банками) без обмена сырыми данными.

7

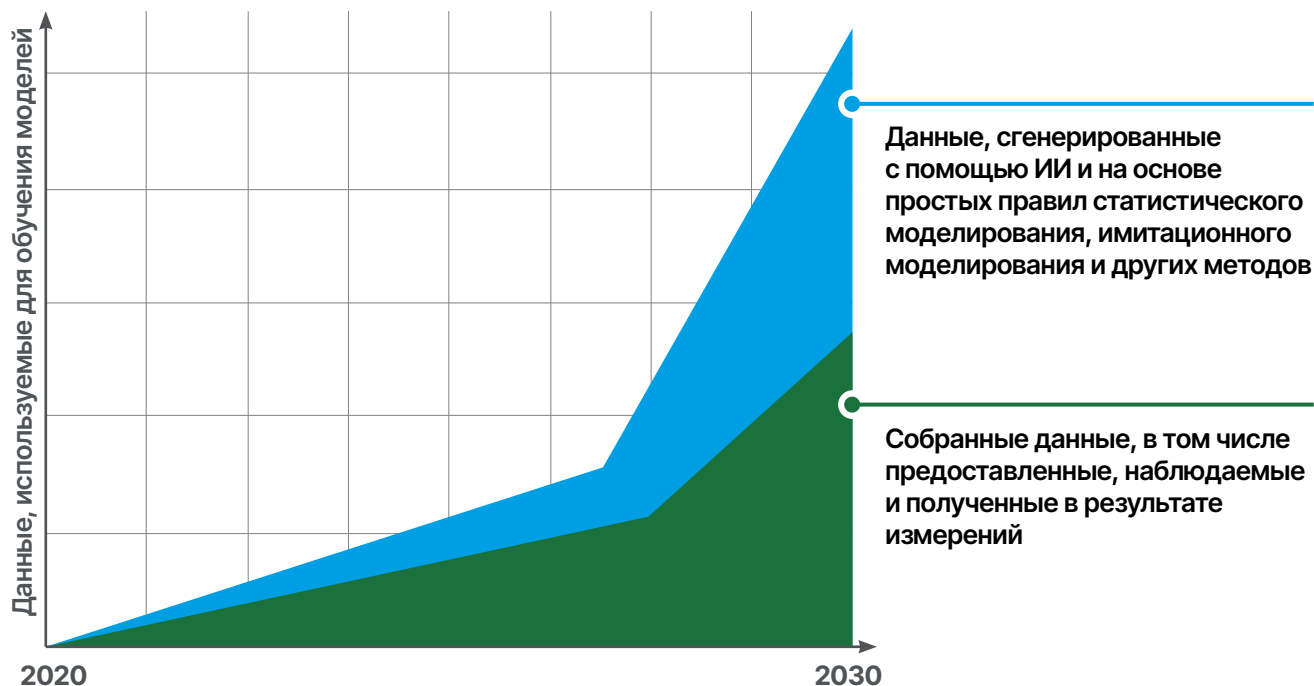
**Синтетические данные** – это искусственно сгенерированные наборы данных, которые статистически схожи с реальными, но не содержат персональной или конфиденциальной информации. Они создаются с помощью алгоритмов машинного обучения или генеративных моделей (например, GAN), сохраняя полезные закономерности исходных данных, но исключая риск утечки.



Подход позволяет безопасно тестировать алгоритмы, делиться данными с третьими сторонами и проводить исследования без юридических ограничений. В финансовой индустрии синтетические данные применяются для обучения скоринговых моделей без использования реальных персональных данных или разработки и отладки финтех-решений.

**Синтетические данные** - это искусственные данные, сгенерированные для замены реальных данных в различных целях, таких как тестирование, исследования и обучение моделей. Они сохраняют структуру и характеристики исходных данных, не содержат личной информации и могут использоваться для защиты конфиденциальности. Синтетические данные относятся к информации, созданной на основе знаний.

## ПЕРСПЕКТИВЫ РАЗВИТИЯ ДАННЫХ, ИСПОЛЪЗУЕМЫХ ДЛЯ ОБУЧЕНИЯ МОДЕЛЕЙ (2020 - 2030 гг.)



**Gartner:** в 2024 году >60% данных, используемых для разработки ИИ, были сгенерированы **синтетическим** путем<sup>1</sup>

Применимость и эффективность синтетических данных напрямую зависит от применяемых алгоритмов, качества и «широты» использованных для генерации исходных данных.

Использование современных решений, таких как PETs, может способствовать **преодолению барьеров** при решении дилеммы доступа и конфиденциальности в рамках совместной **обработки «чувствительной информации»** между организациями.

## ЧТО ПОЧИТАТЬ ПО ТЕМЕ?

### МИНЦИФРЫ

Ведомство подготовило правила работы по обезличиванию персональных данных, которые должны начать действовать с сентября 2025 г. Операторам данных предложены пять методов, они будут проводиться только через софт Минцифры.

Источник:



kommersant.ru

<sup>1</sup>По данным Gartner: [gartner.com](https://www.gartner.com)



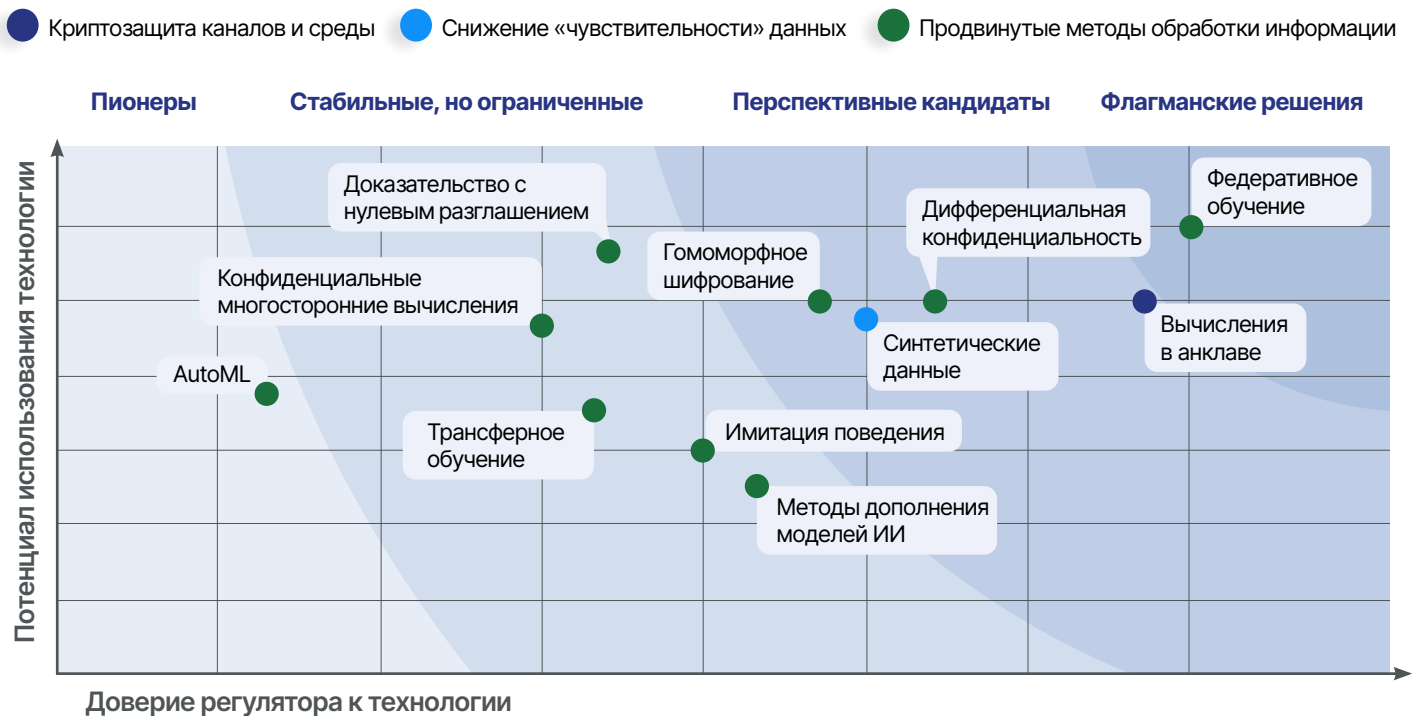
## МНЕНИЕ ЭКСПЕРТОВ О ТЕХНОЛОГИЯХ

Состав экспертов, включающий участников рынка, членов Ассоциации ФинТех и приглашенных консультантов, оценил доверие регулятора к перечисленным технологиям, а также потенциал их использования.

В результате анализа мнений, технологии были распределены по двум схемам:

- «Доверие регулятора к технологии» и «Потенциал использования технологии».
- «Текущее использование технологии (в организациях)» и «Потенциал использования технологии».

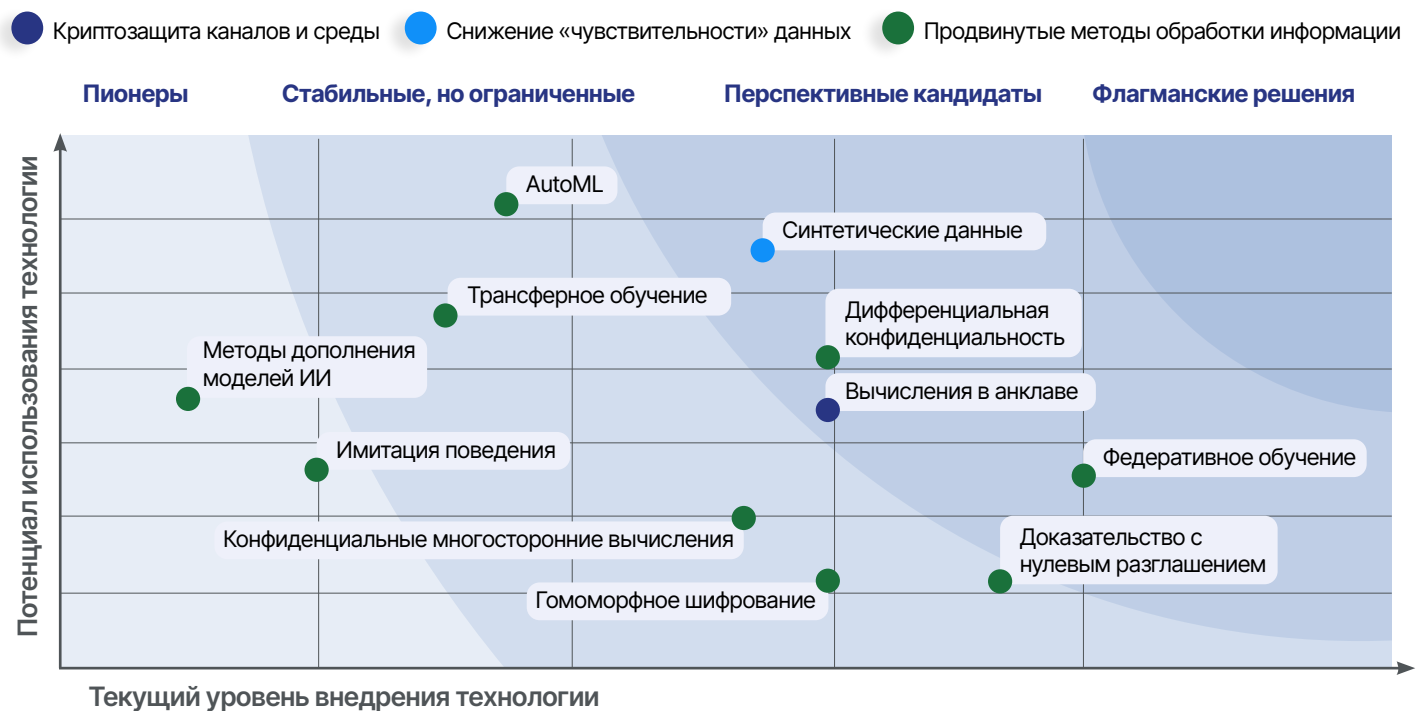
### ВЗАИМОСВЯЗЬ ДОВЕРИЯ РЕГУЛЯТОРА К ТЕХНОЛОГИИ И ПОТЕНЦИАЛА ЕЕ ИСПОЛЬЗОВАНИЯ



Подготовлено АФТ при участии экспертов

**Более 45% технологий** при сравнении взаимосвязи доверия и потенциала использования относятся к разделу **«стабильные, но ограниченные»** – они достаточно быстро масштабируются, но нуждаются в дополнительном регулировании.

## ВЗАИМОСВЯЗЬ ТЕКУЩЕГО УРОВНЯ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ И ПОТЕНЦИАЛА ЕЕ ИСПОЛЬЗОВАНИЯ



Подготовлено АФТ при участии экспертов

Анализ соотношения текущего уровня внедрения технологий и их перспектив развития показал, что свыше 54% решений обладают значительным потенциалом для масштабирования и дальнейшего роста.

Эффективный формат взаимодействия для обмена данными должен быть **гибким и адаптивным** (принцип «конструктора»), и учитывать разнообразие подходов, технологий и инструментов, а также участников этого процесса.

# Обзор перспективных методов криптографии для конфиденциального обмена данными

Одними из самых перспективных методов криптографии для защиты данных можно назвать **доказательство с нулевым разглашением** и **гомоморфное шифрование**.

## ДОКАЗАТЕЛЬСТВО С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

**Доказательство с нулевым разглашением** (Zero-Knowledge Proof, ZKP) или протокол с нулевым разглашением – метод криптографии, с помощью которого одна сторона (доказывающая сторона) может доказать другой стороне (проверяющей стороне), что данное утверждение истинно, не раскрывая при этом ни самой информации, ни какой-либо дополнительной информации.

### Свойства доказательства с нулевым разглашением

| Свойства                                       | Описания                                                                                                                                                                                  |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Полнота</b><br>(Completeness)               | Если утверждение истинно, а доказывающий и проверяющий действуют честно, доказательство может быть принято.                                                                               |
| <b>Корректность</b><br>(Soundness)             | Если утверждение ложно, лживый доказывающий не может обмануть честного проверяющего, заставив его поверить в то, что неверное утверждение истинно (за исключением ничтожной вероятности). |
| <b>Нулевое разглашение</b><br>(Zero-knowledge) | Если утверждение истинно, ни один проверяющий не узнает ничего, кроме того факта, что утверждение истинно.                                                                                |

Существуют **два типа доказательств** с нулевым разглашением: интерактивные, когда происходит прямой обмен информацией между сторонами, и неинтерактивные, когда обмен информацией не требуется между доказывающим и проверяющим.

<sup>1</sup> По данным Bessemer Venture Partners: [bvp.com](https://bvp.com)

<sup>2</sup> По данным РБК: [rbc.ru](https://rbc.ru)

## Основные категории доказательств с нулевым разглашением:

- Краткие неинтерактивные аргументы знаний (Succinct Non-Interactive ARguments of Knowledge, SNARK);
- Масштабируемые прозрачные аргументы знаний (Scalable Transparent ARgument of Knowledge, STARK);
- Верифицируемое полиномиальное делегирование (Verifiable Polynomial Delegation, VPD);
- Краткие неинтерактивные аргументы (Succinct Non-interactive ARGuments, SNARG).

## Примеры систем, поддерживающих доказательства с нулевым разглашением:

| Система                    | Virgo <sup>1</sup>   | zk-STARK <sup>2</sup> | Zilch <sup>3</sup>       |
|----------------------------|----------------------|-----------------------|--------------------------|
| Год публикации             | 2020                 | 2019                  | 2021                     |
| Протокол                   | zk-SNARK             | zk-SNARK              | zk-SNARK                 |
| Прозрачный протокол        | Да                   | Да                    | Да                       |
| Универсальный протокол     | Да                   | Да                    | Да                       |
| Постквантовый протокол     | Да                   | Да                    | Да                       |
| Подходы к программированию | Арифметические схемы | Ассемблер             | Объектно-ориентированный |

**Прозрачный протокол** – не требует какой-либо надежной настройки и использует публичную случайность;

**Универсальный протокол** – не требует отдельной доверенной настройки для каждого канала;

**Постквантовый протокол** – не подвержен известным атакам с использованием квантовых алгоритмов.

<sup>1</sup> По данным IEEE Symposium on Security and Privacy (SP)

<sup>2</sup> По данным Crypto

<sup>3</sup> По данным IEEE Transactions on Information Forensics and Security: [homomorphicencryption.org](https://homomorphicencryption.org)

## ГОМОМОРФНОЕ ШИФРОВАНИЕ

**Гомоморфное шифрование** (Homomorphic Encryption, HE) – метод криптографии, который позволяет выполнять вычисления над зашифрованными данными без необходимости их расшифровки. Отличие от типичных методов шифрования состоит в том, что метод позволяет выполнять вычисления непосредственно с зашифрованными данными, не требуя доступа к секретному ключу. Результат такого вычисления остается в зашифрованном виде и может быть позже раскрыт владельцем секретного ключа<sup>1</sup>.

### Распространенные типы гомоморфного шифрования

| Типы                                                                                              | Описания                                                                                                                                        |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Частично гомоморфное шифрование</b><br>(Partially Homomorphic Encryption, PHE)                 | Позволяет проводить только одну из операций – либо сложение, либо умножение на зашифрованных данных.                                            |
| <b>Отчасти гомоморфное шифрование</b><br>(Somewhat Homomorphic Encryption, SHE)                   | Позволяет выполнять операции сложения и умножения на ограниченном наборе зашифрованных данных.                                                  |
| <b>Уровневое полностью гомоморфное шифрование</b><br>(Leveled Fully Homomorphic Encryption, LFHE) | Поддерживает выполнение произвольных операций над зашифрованными данными – сложение и умножение, с ограниченной, заранее определенной глубиной. |
| <b>Полностью гомоморфное шифрование</b><br>(Fully Homomorphic Encryption, FHE)                    | Поддерживает выполнение произвольных операций над зашифрованными данными. Является самым сильным типом гомоморфного шифрования.                 |

### Примеры библиотек с открытым кодом для полностью гомоморфного шифрования:

| Название                    | Разработчик                                                                                                              | Описание                                                             |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| Helib <sup>2</sup>          | IBM                                                                                                                      | Поддерживаемые схемы: BGV, CKKS                                      |
| Microsoft SEAL <sup>3</sup> | Microsoft                                                                                                                | Поддерживаемые схемы: BGV, CKKS, BFV                                 |
| OpenFHE <sup>4</sup>        | Duality Technologies, Samsung Advanced Institute of Technology, Intel, MIT, University of California, San Diego и другие | Поддерживаемые схемы: BGV, CKKS, BFV, FHEW, CKKS Bootstrapping, TFHE |
| Lattigo <sup>5</sup>        | EPFL-LDS, Tune Insight                                                                                                   | Поддерживаемые схемы: BGV, CKKS, BFV, CKKS Bootstrapping             |

<sup>1</sup> По данным Homomorphic Encryption Standardization: [homomorphicencryption.org](https://homomorphicencryption.org)

<sup>2</sup> По данным GitHub: [github.com](https://github.com)

<sup>3</sup> По данным Microsoft SEAL: [microsoft.com](https://microsoft.com)

<sup>4</sup> По данным OpenFHE: [openfhe.org](https://openfhe.org)

<sup>5</sup> По данным GitHub: [github.com](https://github.com)

# Регулирование технологий конфиденциальных вычислений в России

Современные технологии защиты данных требуют **комплексного подхода к регулированию**, который бы одновременно стимулировал инновации и обеспечивал надежную защиту информации. Для этого необходимо создать сбалансированную систему мер, охватывающую как экономические стимулы, так и четкие процедурные рамки.



АССОЦИАЦИЯ  
БОЛЬШИХ ДАННЫХ

Разработка технических стандартов уже ведется в рамках «Технического комитета по стандартизации (ТК-22)» экспертами Ассоциации Больших Данных.

## СТИМУЛЫ ДЛЯ РАЗВИТИЯ ТЕХНОЛОГИЙ

Формирование благоприятной регуляторной среды является ключевым условием для внедрения перспективных технологий защиты данных. В качестве основных стимулов предлагается:



Учет применения технологий при оценке мер по обеспечению безопасности



Снятие ограничений на обработку и введение дополнительных оснований обработки



Совершенствование процедур сертификации за счет стандартизации требований

Подготовлено при участии экспертов АБД

Для обеспечения системного подхода к защите информации необходимо определить последовательность этапов внедрения защитных технологий.

## ПРЕДЛОЖЕНИЯ ПО РЕГУЛИРОВАНИЮ ОБРАБОТКИ ДАННЫХ

Процесс регулирования должен включать:



Разработка сервиса (продукта) с применением технологии повышения конфиденциальности



Сертификация сервиса (продукта) на соответствие нормативным требованиям и требованиям ПНСТ



Предоставление сервиса (продукта) операторам персональных данных с целью обработки данных



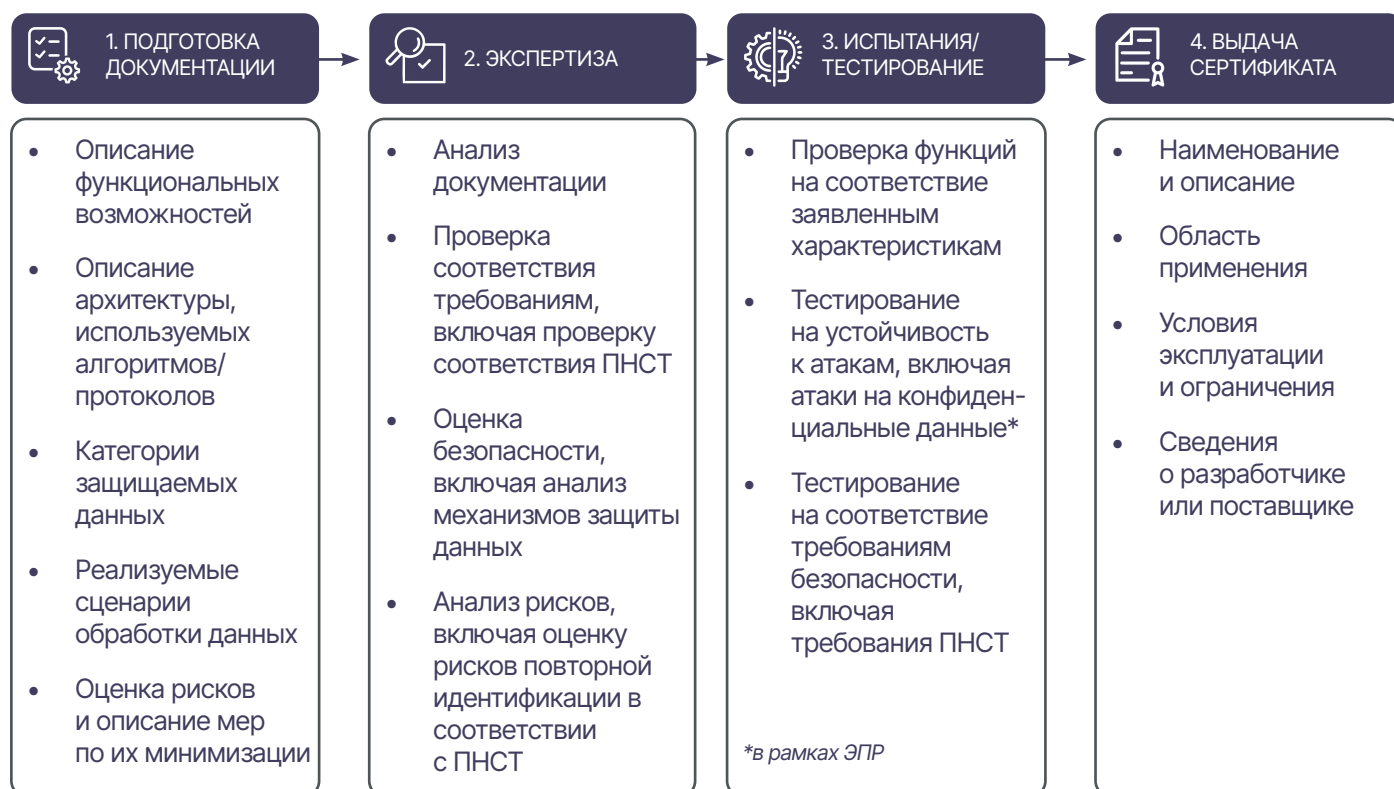
Обработка данных на законном основании в соответствии с сертификатом (область применения и условия эксплуатации)

Подготовлено при участии экспертов АБД

Для обеспечения доверия к таким решениям критически важен **прозрачный и стандартизированный процесс сертификации**, который подтверждает их надежность.

Создание унифицированной системы сертификации является важнейшим элементом регуляторной инфраструктуры.

## ПОРЯДОК СЕРТИФИКАЦИИ ТЕХНОЛОГИЙ КОНФИДЕНЦИАЛЬНЫХ ВЫЧИСЛЕНИЙ



Подготовлено при участии экспертов АБД

Разработка единых технических стандартов представляет собой **фундамент для эффективного регулирования** в данной области. В рамках стандартизации необходимо:

- **Описание технологий**, включая конкретные методы (например, гомоморфное шифрование, федеративное обучение) и протоколы их применения.
- **Типовые сценарии использования** с указанием подходящих моделей угроз (включая возможных нарушителей).
- **Закрепление модели оценки рисков** повторной идентификации данных в зависимости от типа применяемой технологии.

Стандартизация не только упростит внедрение новых технологических решений, но и поможет регуляторам, разработчикам и бизнесу говорить на одном языке, **минимизируя риски и повышая доверие** к ним.

## ЧТО ПОЧИТАТЬ ПО ТЕМЕ?

### РОСКОМНАДЗОР

**«Об утверждении требований к обезличиванию персональных данных и методов обезличивания персональных данных»**

Федеральная служба подготовила проект нового приказа, регламентирующего порядок обезличивания персональных данных. Основное требование к операторам – сохранить безопасность обезличенных данных, чтобы их невозможно было полностью восстановить без дополнительной информации.

Источник:



regulation.gov.ru

# Международный опыт организации конфиденциального обмена данными данными

## ЕВРОПЕЙСКИЙ СОЮЗ<sup>1</sup>



**Common European Data Spaces** – инициатива Европейского Союза, направленная на создание единого рынка данных. Она охватывает стратегические области, такие как здравоохранение, сельское хозяйство, производство, энергетика, мобильность, финансы и другие. Общие пространства данных обеспечивают безопасное и надежное взаимодействие между участниками, предоставляя возможность обмена данными для инноваций и улучшения продуктов и услуг.

**Data Act** – закон о данных, который регулирует справедливый доступ и использование данных в рамках цифровой экономики ЕС. Он предоставляет пользователям контроль над данными, генерируемыми их устройствами, защищает коммерческие тайны и способствует развитию конкурентного рынка данных. Закон также позволяет публичным органам использовать данные частного сектора для решения общественных задач.

**Green Deal Data Space (GDDS)** – пространство данных «Зеленого курса», которое охватывает климатические изменения, круговую экономику (экономика замкнутого цикла), загрязнение окружающей среды и биоразнообразие. Оно основано на принципах FAIR (возможность поиска, доступность, интероперабельность и повторное использование) для обеспечения качественного обмена данными между участниками.

**Interoperable Europe Act** – закон об интероперабельности Европы. Он способствует обмену данными между государственными органами ЕС через открытые стандарты и повторное использование решений. Это помогает сократить изолированность данных и ускорить цифровую трансформацию публичного сектора.

Европейские регуляторы непосредственно участвуют и финансируют создание **межотраслевых инициатив** в области обмена и совместной обработки данных, в том числе в рамках проектов развития ИИ.

## ГЕРМАНИЯ<sup>1</sup>



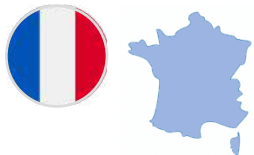
**Financial Big Data Cluster (FBDC)** – проект общерыночной облачной платформы данных финансового сектора в рамках **Gaia-X**, которая объединяет ранее не связанные данные компаний, регуляторов и научного сообщества в общий пул данных, и в перспективе будет оптимизирована для разработки приложений и систем ИИ.

**Национальная инфраструктура исследовательских данных (NFDI)** – проект, поддерживаемый Немецким научным фондом (DFG), организует обмен научными данными в социальных, поведенческих, образовательных и экономических науках. Он использует модель FDO для стандартизации обмена данными и создания экосистемы услуг для управления исследовательскими данными.

<sup>1</sup>По данным Digital Strategy: [digital-strategy.ec.europa.eu](https://digital-strategy.ec.europa.eu)

Европейское регулирование – один из **наиболее детализированных режимов**, определяющих подходы и платформы обмена данными и описывающих стандарты при взаимодействии с ними.

## ФРАНЦИЯ<sup>2</sup>



**Dawex** – международная компания, разрабатывающая решения для организации экосистем обмена данными для различных секторов. Dawex активно участвует в дискуссиях Европейской комиссии, Всемирного экономического форума и саммита G7. Платформа обмена данными Dawex обеспечивает безопасность данных с помощью современных методов анонимизации и шифрования, а также способствует соблюдению правовых аспектов обмена

**Французская платформа открытых данных** предоставляет доступ к более чем 47 000 наборов данных, включая проект «Сигналы», который помогает прогнозировать финансовые трудности компаний. Она способствует прозрачности и инновациям в публичных услугах через сотрудничество с государственными органами и объединение данных.

## БЕЛЬГИЯ<sup>3</sup>



**Data Broker Global** – маркетплейс-платформа данных, разработанная и управляемая провайдером SettleMint. Data Broker Global использует технологию блокчейн для обеспечения безопасной передачи данных между продавцом и покупателем. Дополнительные услуги, предлагаемые на платформе, включают бесплатный сервис **DataMatch**, который помогает клиентам найти подходящие данные у потенциальных партнеров.

**Национальный портал открытых данных Бельгии** объединяет более 10 000 наборов данных от федеральных, региональных и местных властей. Среди приложений — мониторинг качества воздуха через инструменты Plume Air Report и BreezoMeter, которые демонстрируют потенциал открытых данных для решения экологических проблем.

Активно развивающееся регулирование в рамках ЕС стимулирует **создание частных и государственных инициатив** в области данных на национальном уровне.

## СИНГАПУР<sup>1</sup>



**Trusted Data Sharing Framework** – инициатива, целью которой является обеспечение безопасного обмена данными между организациями, включая стандартизацию методологий, юридические шаблоны и рекомендации по оценке данных. Это способствует развитию цифровой экономики и поддерживает инновации, такие как искусственный интеллект.

<sup>1</sup> По данным Semantic Scholar: [semantic scholar.org](https://www.semantic scholar.org)

<sup>2</sup> По данным DataEuropa: [data.europa.eu](https://data.europa.eu)

<sup>3</sup> По данным DataEuropa: [data.europa.eu](https://data.europa.eu)

## КИТАЙ<sup>2</sup>



**Глобальная инициатива по сотрудничеству в области трансграничных потоков данных** – инициатива объединяет международные потоки обмена данными для создания более открытой и недискриминационной среды. В рамках решения Китай позиционирует себя как сторонник сотрудничества в области данных, что может способствовать улучшению международных отношений и экономического взаимодействия.

**Пространство доверенных данных** – часть стратегии по развитию цифровой экономики в стране. Проект направлен на формирование безопасной и регулируемой среды для обмена и использования данных к 2028 году и будет объединять владельцев, поставщиков и пользователей данных на основе единых стандартов и правил.

Проактивное участие регулятора может стать определяющим фактором развития сферы обмена данными и доступа к ним, а также важной составляющей для возможности их монетизации.

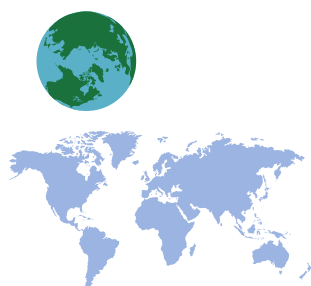
## ЯПОНИЯ<sup>3</sup>



**Japan Data Exchange (JDEX)** – биржа данных, созданная в сотрудничестве с Dawex, позволяющая организациям из различных отраслей безопасно приобретать, распространять, торговать и коммерциализировать данные в соответствии с японскими и международными нормами.

Большинство платформ обмена данными в мире находятся на стадии активной разработки и внедрения инициатив во все основные направления деятельности.

## МИР<sup>4</sup>



**Открытая библиотека методов гомоморфного шифрования** – решение, созданное компанией Apple на языке Swift. Технология позволяет создавать приложения, обрабатывающие данные, доступные только в зашифрованном виде, без промежуточного раскрытия ни на одном из этапов вычислений. На выходе выдаётся безопасный ответ, который аналогичен шифрованию результата выполнения тех же вычислений над исходными данными.

<sup>1</sup> По данным PwC: [pwc.com](https://www.pwc.com)

<sup>2</sup> По данным Crowell, SCMP: [crowell.com](https://www.crowell.com), [scmp.com](https://www.scmp.com)

<sup>3</sup> По данным Jast: [jast.jp](https://www.jast.jp)

<sup>4</sup> По данным OpenNET: [opennet.ru](https://www.opennet.ru)

# Разработка инструментов конфиденциального обмена данными в России

Эффективный обмен информацией и данными является критически важной задачей, позволяющей раскрыть потенциал технологий ИИ. В мире идет активная работа в данном ключе, однако большинство платформ обмена данными все еще находятся на стадии формирования и тестирования.

## ИНИЦИАТИВЫ ПО РАЗРАБОТКЕ ИНСТРУМЕНТОВ ОБМЕНА И СОВМЕСТНОГО ДОСТУПА С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ В РОССИИ

### КЕЙС. ВТБ, МФТИ И Т1<sup>1</sup>



#### Комплекс инструментов для передачи больших массивов данных

**Крипто-анклав** – инновационный комплекс инструментов, использующий технологии слепого машинного обучения, AutoML и безопасных вычислений в анклавов. Это первое в России решение, позволяющее организациям обмениваться данными в криптозащищенном пространстве для совместного построения прогнозных моделей без раскрытия конфиденциальной информации.

Криптоанклав представляет собой высокозащищенный программно-аппаратный комплекс, обеспечивающий полную конфиденциальность данных. Банки, телеком-операторы и другие компании могут безопасно загружать свои данные в зашифрованное пространство, где информация хранится и обрабатывается по принципу «черного ящика» – в закодированном виде, без возможности человеческого вмешательства или несанкционированного доступа.

Источник:



zanauku.mipt.ru

### КЕЙС. АССОЦИАЦИЯ БОЛЬШИХ ДАННЫХ<sup>2</sup>



#### Supervised & Unsupervised ML на основе данных от различных поставщиков

**Сервис «Собственное дело»** – аналитика для старта бизнеса на основе анализа обезличенных данных от разных участников рынка, в том числе кредитных организаций, поисковых систем и телекоммуникационных компаний. Клиент сервиса сможет получить конкретные рекомендации по наиболее выгодной локации, более востребованному направлению бизнеса, среднему чеку и другим показателям.

По оценке экспертов АБД, запуск сервиса «Собственное дело» позволит создать 85 тысяч новых малых предприятий, а также 192 тысячи новых рабочих мест.

Источник:



rubda.ru

<sup>1</sup>По данным ЗаНауку: [zanauku.mipt.ru](http://zanauku.mipt.ru)

<sup>2</sup>По данным АБД: [rubda.ru](http://rubda.ru)

КЕЙС. ЯНДЕКС, ИСП РАН И СЕЧЕНОВСКИЙ УНИВЕРСИТЕТ<sup>3</sup>Yandex  
Cloud

ИСП РАН

СЕЧЕНОВСКИЙ  
УНИВЕРСИТЕТ  
НАУКА О ЖИЗНИ

## Федеративное обучение в здравоохранении

Яндекс, Институт системного программирования РАН и Сеченовский Университет разработали нейросетевую модель, способную выявлять фибрилляцию предсердий – одну из самых распространённых сердечных патологий — на основе данных электрокардиограмм (ЭКГ).

Главный фокус проекта – практическая проверка технологии федеративного обучения (FL) в условиях, когда исходные данные остаются у владельцев и не покидают периметр организаций. Каждая сторона локально обучала модель на своём датасете, обмениваясь только параметрами, а не самими данными. Этот проект стал примером того, как можно запускать совместные исследования в области ИИ и медицины, соблюдая требования к приватности и безопасности медицинской информации.

Подход подтверждает применимость FL в чувствительных сферах, где невозможно централизованное хранение данных.

Источник:



yandex.ru

КЕЙС. HFLABS<sup>4</sup>

H F Labs

## Обезличивание персональных данных с сохранением контекста

Продукт «Маскировщик» компании HFLabs предназначен для защиты персональных данных при тестировании ИТ-систем. Решение успешно применяется в банковском секторе, страховых компаниях и промышленности и подтвердило свою эффективность в ходе тестирования на риск-модели, разработанной Ассоциацией больших данных. Продукт представлен в виде коробочного решения.

Используя логику умной замены, «Маскировщик» при обезличивании сохраняет качество и контекст данных и делает их максимально похожими на настоящие. Продукт снижает риски утечки, упрощает внутреннюю передачу данных и позволяет использовать обезличенную информацию для обучения ML-моделей.

Источник:



cnews.ru

КЕЙС. BLOOMTECH<sup>5</sup>

B L ∞ M T E C H

## Расчет агрегированных клиентских метрик для скоринга

Флагманский продукт компании Bloomtech — **скоринговая инфраструктура** на транзакционных данных. Банки получают доступ к финансовой аналитике по клиентам, при этом:

- Не передают свои транзакционные данные другим участникам.
- Не хранят информацию у третьих сторон.
- Полностью контролируют собственные данные.

Решение позволяет осуществлять не просто обмен данными, а их совместное использование.

Источник:



bloomtech.ru

<sup>3</sup> По данным Яндекса: [yandex.ru](https://yandex.ru)

<sup>4</sup> По данным CNews: [cnews.ru](https://cnews.ru)

<sup>5</sup> По данным Bloomtech: [bloomtech.ru](https://bloomtech.ru)

КЕЙС. ГАЗПРОМБАНК И QAPP<sup>1</sup>

Источник:



futurebanking.ru

**Конфиденциальные вычисления в кредитном скоринге**

Завершен проект по анализу применения конфиденциального обучения модели оценки вероятности дефолта юридических лиц. В проекте использовался протокол конфиденциального вычисления SMPC (Secure multi-party computation) — семейство криптографических протоколов, которые распределяют вычисления между несколькими участниками, при этом ни одна из сторон не может узнать конфиденциальные данные других участников.

## КЕЙС. SWORDFISH SECURITY

**Использование чувствительных данных без угрозы раскрытия и с сохранением контекста**

**AppSec.Copilot** – интеллектуальный нейроинженер по управлению уязвимостями на основе ИИ. При обучении имена файлов не используются, а имена переменных и методов, которые могли бы выдать принадлежность к владельцу данных, экранируются и преобразуются в токены. Таким образом, нельзя восстановить оригинальные данные из обучающего датасета.

Сама технология обучения с подкреплением (Reinforcement Learning, RL) не имеет зависимостей за контуром обучения, то есть обучается в закрытой инфраструктуре заказчика. Это, в свою очередь, исключает утечку данных, что для этой разработки является одним из приоритетов и знаком качества.

## КЕЙС. GUARDORA

**Платформа конфиденциальных вычислений**

Guardora разрабатывает платформу для конфиденциальных вычислений, позволяющую компаниям использовать сторонние данные для обучения своих ML-моделей, без раскрытия данных.

Флагманский продукт — Guardora VFL на основе вертикального федеративного обучения ориентирован на улучшение качества моделей скоринга физических лиц. Работает с табличными данными, поддерживает градиентный бустинг и линейные модели.

Безопасность обеспечивается:

- Федеративным обучением: данные не покидают защищенный контур владельца данных.
- Гомоморфным шифрованием передаваемых между участниками обучения промежуточных результатов вычислений локальных моделей.
- Алгоритмами PSI (Private Set Intersection) для синхронизации сущностей.

Доступные версии: облачная (приватное облако) и серверная (Docker-контейнер).

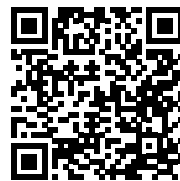
<sup>1</sup>По данным Futurebanking: [futurebanking.ru](https://futurebanking.ru)

## ЧТО ПОЧИТАТЬ ПО ТЕМЕ?

### АССОЦИАЦИЯ БОЛЬШИХ ДАННЫХ

Ассоциация больших данных в рамках проекта «Библиотека практик» размещает примеры успешных отечественных кейсов в области защищенной обработки, конфиденциальных вычислений и доверенных сред исполнения данных.

Источник:



[rubda.ru](https://rubda.ru)

# Платформы обмена данными

Несмотря на длительные обсуждения, вопрос прямого обмена конфиденциальной информацией по-прежнему остаётся в «серой» зоне регулирования. Для устойчивого развития рынка данных необходимо совершенствование нормативного регулирования, в частности – чёткая классификация участников и унификация таксономии данных. Однако реализация этих изменений требует согласованных усилий регуляторов и представителей рынка.

В настоящее время обмен конфиденциальными данными с использованием традиционных механизмов защиты остаётся сложной и не до конца решённой задачей, требующей значительных временных и ресурсных затрат. В рамках данного исследования предлагается новая структура платформ обмена данными, которая может стать шагом к решению этой проблемы.

## Структура платформ обмена данными:

### ГОСУДАРСТВЕННЫЕ ПЛАТФОРМЫ

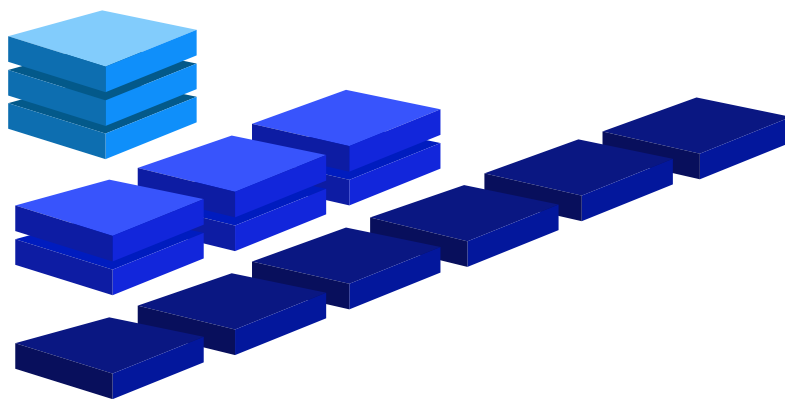
Федеральные

Отраслевые

Муниципальные

### КОММЕРЧЕСКИЕ ПЛАТФОРМЫ

### ОДНОРАНГОВЫЙ ОБМЕН



#### ГОСУДАРСТВЕННЫЕ ПЛАТФОРМЫ

**Особенности:** небольшое количество инструментов обработки и анализа, стандартизация, единые высокие требования к ИБ, фиксированная структура организации обмена, тарификация.

**Данные:** государственные (в т.ч. ограниченного доступа), востребованные отраслевые, верифицированные, частные (санитанизированные), научно-исследовательские.

#### ОДНОРАНГОВЫЙ ОБМЕН

**Особенности:** партнерские отношения, согласованные требования ИБ, ограниченная «широта» данных, слабая возможность монетизации.

**Данные:** двух организаций, информация для выполнения условий соглашений, иные NDA.

В рамках однорангового обмена функционирует технология Open API.

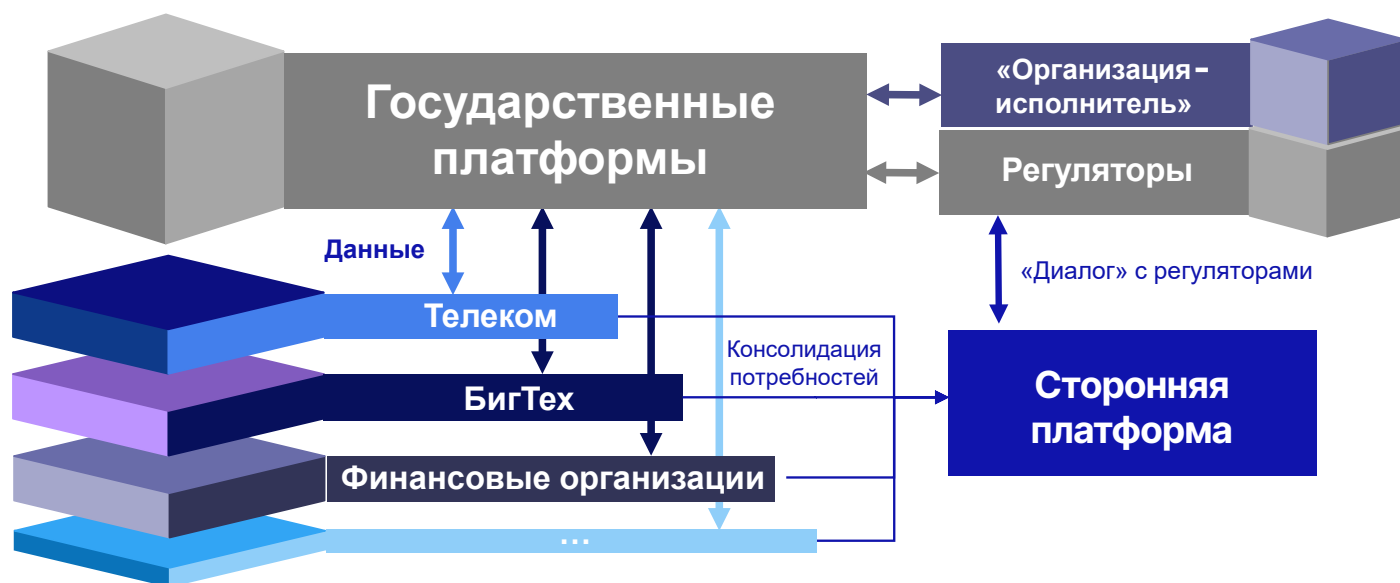
#### КОММЕРЧЕСКИЕ ПЛАТФОРМЫ

**Особенности:** широкий инструментарий, пилоты, стандартизация, гибкая структура организации, вариативный подход к методам, монетизация.

**Данные:** уникальные отраслевые (иные NDA), синтетические, полученная информация и знания, необработанные в различных форматах.

Будущая экосистема обмена данных может **состоять из трех «слоев»:** государственных платформ, коммерческих платформ и однорангового взаимодействия между участниками обмена.

## ПРЕДЛОЖЕНИЯ ДЛЯ УЧАСТНИКОВ РЫНКА: ГОСУДАРСТВЕННЫЕ ПЛАТФОРМЫ



### Возможная организационная форма

- Посредственное взаимодействие (оператор - Государство).
- Гибридное взаимодействие.

### Обрабатываемые данные

- Общедоступные статистические данные.
- Агрегированные рыночные данные.
- Важные отраслевые данные.
- Санитизированные частные данные (ПДн, ...).
- Государственные (конфиденциальная информация).
- Служебная тайна (банковская, ...).
- Другие виды информации ограниченного доступа.

### Принципы и условия функционирования

- Общий доступ для организаций (клиентов).
- Монетизация: тарификация.
- Общее регулирование.
- Использование одобренных отечественных технологий (КИИ).
- Интеграция платформ между собой.

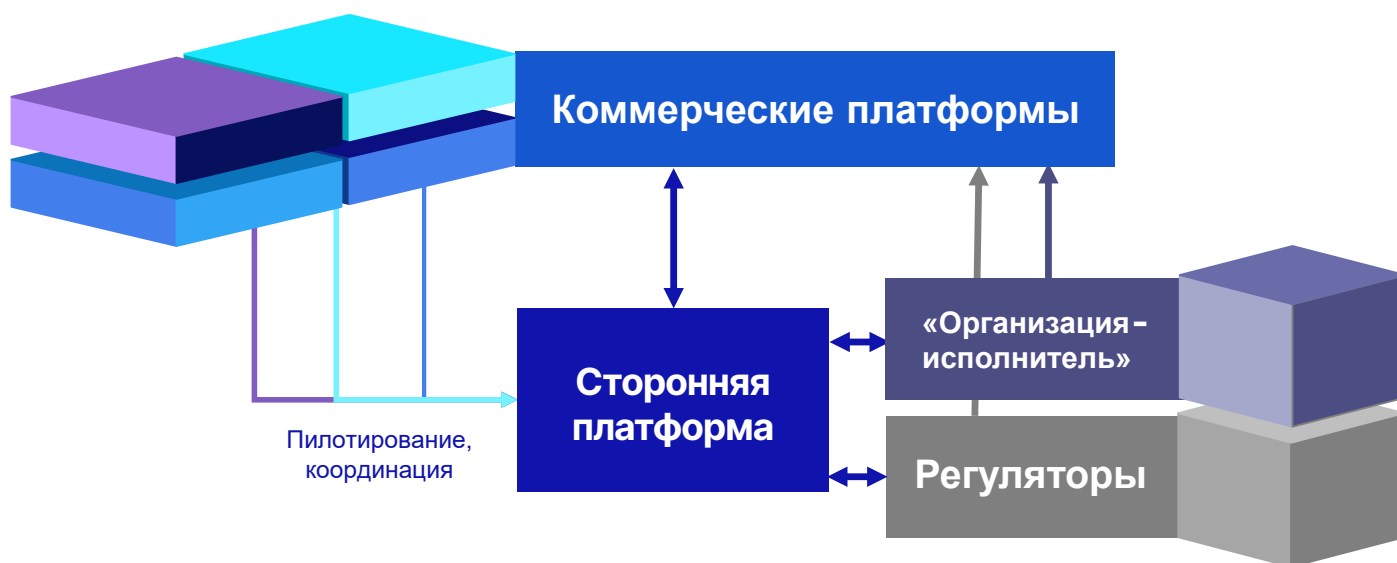
### Предполагается:

- «Санитизированные» данные на гос. платформах будут обрабатываться по общим стандартам, лишая их части семантической информации.
- Масштаб и уровень возможного ущерба при утечке не позволит гибко подходить к организации обмена и тестировать современные подходы обеспечения конфиденциальности.

### Возможная роль сторонней платформы при создании государственной платформы обмена данными:

- Консолидация потребностей рынка в типах данных и функционале общих платформ.
- Поиск и адаптация лучших практик в области обмена и обработки данных рынка на базе пилотов для государственных платформ.

## ПРЕДЛОЖЕНИЯ ДЛЯ УЧАСТНИКОВ РЫНКА: КОММЕРЧЕСКИЕ ПЛАТФОРМЫ



### Возможная организационная форма

- Организация-посредник.
- Консорциум.
- Децентрализованная платформа (блокчейн).

### Обрабатываемые данные

- Общедоступные данные (МСФО, отчетность).
- Иная информация (NDA).
- Профессиональная тайна\* (коммерческая тайна, ...).
- Служебная тайна\* (банковская, ...).
- Обезличенные ПДн\*.
- Синтетические «чувствительные»\*.

*\*при условии положительной оценки надзора*

### Принципы и условия функционирования

- «Метчинг» - Обмен.
- Монетизация: покупка/продажа/комиссия.
- Специализированное регулирование (ИБ, риск-ориентированный подход) – экспериментальный режим.
- Использование одобренных технологий.

### Предполагается:

- Платформы будут обладать возможностью гибко подходить к обработке выбранных типов данных и выбирать методы в зависимости от целей и запросов пользователей платформы.
- Создание нескольких платформ для решения как отдельных проблем (например, Антифрод), так и функционирующих по принципу «конструктора».

### Возможная роль сторонней платформы при создании коммерческих платформ обмена данными:

- Пилотирование платформ и объединение усилий по улучшению общих решений на коммерческих платформах.
- Координация при внедрении современных и эффективных методов обеспечения конфиденциальности, тестировании технологий и проверки гипотез.
- Проведение рыночных исследований рынка данных и донесение консолидированного мнения до регуляторов.



# **Инициативы Ассоциации ФинТех в области технологий конфиденциальных вычислений**

# Лаборатория конфиденциальных вычислений

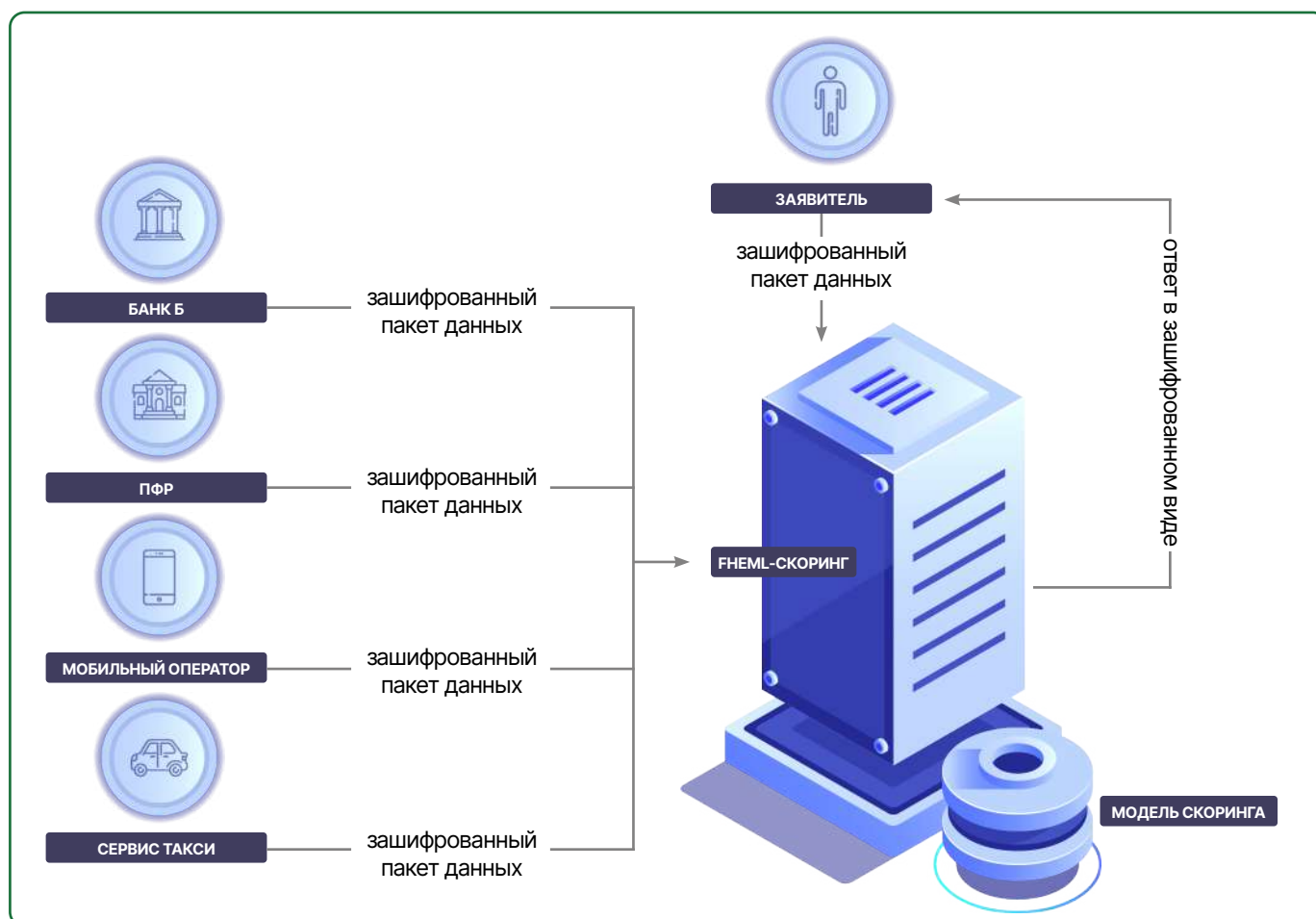
## Как Технологическая песочница АФТ ускоряет внедрение инноваций:

Технологическая песочница, созданная и успешно функционирующая несколько лет в Ассоциации ФинТех для пилотирования цифровых решений и сервисов, позволяет участникам быстрее выполнять совместные проекты и сокращать расход времени и ресурсов на их реализацию. Песочница предоставляет **механизмы по апробации инновационных финансовых и информационных технологий**, продуктов и услуг, а также российских и независимых технологических решений и является **безопасным окружением для проверки гипотез** о положительных эффектах для финансового рынка и потребителей.

В одном из доменов Технологической песочницы, отвечающем за апробацию новых технологий и инструментов информационной безопасности, создана **Лаборатория конфиденциальных вычислений**. Лаборатория, в отличие от пилотных окружений, является более **доступным местом для возможности тестирования продуктов и решений** и представляет собой простой и оперативный доступ к оборудованным экспериментальным стендам.

Эксперты видят высокий будущий потенциал конфиденциальных вычислений в разных областях, а Лаборатория дает возможность «прочувствовать» все возможности конфиденциальных вычислений «здесь и сейчас».

## МАКЕТ ПРИМЕНЕНИЯ ПОЛНОСТЬЮ ГОМОМОРФНОГО ШИФРОВАНИЯ



**Макет применения** одного из подходов конфиденциальных вычислений – полностью гомоморфного шифрования (Fully Homomorphic Encryption, FHE), в отличие от традиционной парадигмы вычислений, **обеспечивает возможность создания новых бизнес-моделей с вычислениями** на зашифрованных данных без их расшифровки.

В основе решения лежит **машинное обучение**, сохраняющее конфиденциальность (Privacy-Preserving ML), которое открывает окно в мир обработки и использования данных.

*Конфиденциальные вычисления скоро станут стандартной практикой на финансовом рынке, в здравоохранении, в корпоративной среде. Лаборатория конфиденциальных вычислений Технологической песочницы АФТ предоставляет уникальную возможность прикоснуться к решениям будущего уже сегодня.*

*Особый интерес вызывают решения с применением полностью гомоморфного шифрования, обеспечивающие приватность данных, обеспеченную криптографией, помноженной на силу технологий ИИ. Лаборатория предоставляет широкий спектр вариантов использования стендов с такими решениями, от «просто попробовать» до возможностей доработки и дообучения и создания собственных экспериментальных приложений для апробаций новых моделей принятия решений и кейсов их применения.*

#### **КИРИЛЛ КУЗЬМИН**

Заместитель генерального директора,  
Руководитель управления пилотирования и прототипирования, **АФТ**



### **Макет позволяет специалистам по данным без каких-либо предварительных знаний криптографии выполнять:**

- Автоматическое преобразование моделей машинного обучения в их FHE-эквивалент.
- Обучение для сохранения конфиденциальности непосредственно на зашифрованных данных.
- Предварительная обработка зашифрованных данных с использованием структурой DataFrame.

Пользователи Лаборатории легко могут настроить макет под апробацию своих собственных задач для прогнозирования, моделирования и оптимизации ключевых бизнес-процессов и функций. Гибкость решения, в основе которого лежит модель ИИ, предоставляет практически неограниченные возможности для экспериментов.

*PET-технологии становятся ключевым инструментом достижения баланса между цифровизацией и защитой данных граждан и бизнеса. Поэтому развитие экспертизы в области PET-технологий критически важно — только так мы сможем создавать эффективные решения, которые позволяют оперативно (превентивно) реагировать на растущие угрозы нарушения конфиденциальности информации в цифровую эпоху, и позволяют развиваться технологиям и бизнесу.*

#### **АЛЕКСАНДР ТОВСТОЛИП**

Руководитель Управления информационной безопасности, **АФТ**





# Рабочая группа по технологиям конфиденциальных вычислений на базе АФТ

Рабочая группа по технологиям конфиденциальных вычислений — это профессиональное объединение представителей финансовой отрасли, технологических компаний и регуляторов, целью которого является исследование и апробация технологий конфиденциальных вычислений в контексте задач российской экономики.

## Организаторы



АССОЦИАЦИЯ  
ФИНТЕХ



ГАЗПРОМБАНК



QApp

## Участники

# 14

крупнейших компаний  
финансового рынка

## Основные цели рабочей группы:

- **Гармонизация знаний участников** о текущем статусе развития технологий конфиденциальных вычислений и их применимости в финансовом секторе РФ.
- **Выявление технологических и регуляторных барьеров** на пути внедрения решений в промышленную эксплуатацию на горизонте 2025–2027 гг., а также определение возможных путей их преодоления.
- **Координация** усилий индустрии и регуляторов в сфере апробации технологий, направленных на безопасную и приватную работу с данными.
- **Поиск точек синергии** с национальными программами, включая проект «Экономика данных» и другие государственные инициативы.

В ходе встреч рабочей группы **участники обсуждают прикладные кейсы и делятся опытом** внедрения технологий. В частности, были представлены:

- Результаты тестирования программно-аппаратного комплекса «Крипто-анклав» для задач антифрода в банках.
- Кейс использования федеративного обучения для защиты конфиденциальности медицинских данных при обучении ИИ-сервисов.

Подробная информация о работе группы представлена на сайте QApp [qapp.tech](http://qapp.tech).

# НАД ИССЛЕДОВАНИЕМ РАБОТАЛИ:

## ИССЛЕДОВАНИЯ & АНАЛИТИКА АФТ



**МАРИАННА  
ДАНИЛИНА**

Руководитель Управления стратегии,  
исследований и аналитики **АФТ**



**МАРИЯ  
ЧЕРНЫШЕВА**

Младший бизнес-аналитик  
**АФТ**



**АННА  
АНДРЕЙЧЕВА**

Руководитель исследовательских  
проектов **АФТ**



**АЛЕКСАНДРА  
ЩЕДРИНА**

Арт-директор **АФТ**

## ЭКСПЕРТЫ АФТ



**АЛЕКСАНДР ТОВСТОЛИП**

Руководитель Управления  
информационной  
безопасности **АФТ**



**КИРИЛЛ КУЗЬМИН**

Руководитель управления  
Пилотирования  
и прототипирования **АФТ**



**СЕРГЕЙ ЛАПИН**

Эксперт Управления  
информационной  
безопасности **АФТ**

Заместитель генерального  
директора **АФТ**

## ПРИВЛЕЧЕННЫЕ ЭКСПЕРТЫ



**АЛЕКСЕЙ НЕЙМАН**

Исполнительный директор  
Ассоциация Больших  
Данных



**АНТОН ГУГЛЯ**

Генеральный директор  
«QApp» (ООО «КуАпп»)



**МАРАТ ТАХАВИЕВ**

Руководитель GR-проектов  
Ассоциация Больших  
Данных



**ПЕТР ЕМЕЛЬЯНОВ**

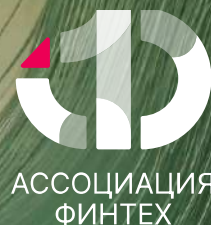
CEO Bloomtech



**АРТЕМИЙ СЫЧЕВ**

Директор направления  
Центр ИИ Сколтех

# АССОЦИАЦИЯ ФИНТЕХ ИССЛЕДОВАНИЯ & АНАЛИТИКА



✉ [research.analytics@fintechru.org](mailto:research.analytics@fintechru.org)

ТЕЛЕГРАМ-КАНАЛ АФТ



[WWW.FINTECHRU.ORG](http://WWW.FINTECHRU.ORG)

**Ассоциация ФинТех** основана в конце 2016 г. по инициативе Банка России и ключевых участников отечественного финансового рынка. Это уникальная площадка для конструктивного диалога регулятора с представителями бизнеса.

Здесь формируется экспертная оценка инновационных технологий с учетом международного опыта, а также разрабатываются концепции финансовых технологий и подходы к их внедрению.

Информация, содержащаяся в настоящем документе (далее – Исследовании), предназначена только для информационных целей и не является профессиональной консультацией или рекомендацией. Ассоциация ФинТех не дает обещаний или гарантий относительно точности, полноты, своевременности или актуальности информации, содержащейся в Исследовании. Материалы Исследования полностью или частично нельзя распространять, копировать или передавать какому-либо лицу без предварительного письменного согласия Ассоциации ФинТех.