https://postnauka.org/longreads/157674

ПостНаука, Ксения Долгачева

23.05.2025

Возможно ли использовать облачные ИИ-сервисы, не раскрывая им свои приватные данные

Стартап GENXT.AI создаёт конфиденциальное ИИ-облако, где данные остаются зашифрованными даже во время обработки. Ни облачный провайдер, ни ИИ-вендор не имеют доступа к клиентским данным. Вместе с сооснователем стартапа Станиславом Никольским разбираемся, как работает Confidential AI и почему персональные данные — не только актив, но и уязвимость цифровой эпохи.

Почему доверие к данным больше не работает: что приходит на смену модели «все свои»

Каждый, кто работает с ИИ — будь то частный пользователь или крупная компания — сталкивается с выбором: использовать внешние облачные сервисы или запускать ИИ локально. Облачные ИИ-сервисы — это просто и удобно: доступ в пару кликов, масштабирование по требованию. Но есть нюанс.

В большинстве облачных ИИ-сервисов приватные данные клиента могут быть доступны широкому и часто неограниченному кругу лиц: разработчикам, администраторам облачной платформы, подрядчикам и, при необходимости, государственным органам. Эти данные могут храниться месяцами — а иногда и годами.

До недавнего времени безопасность данных строилась на доверии. Компаниям было достаточно заявить, что они «не хранят» или «не продают» информацию пользователя. Клиенты верили — или делали вид, что верят. Но эта модель разрушается. Слишком много скандалов и чёрных ящиков. Утечки не пугают обычных пользователей и не критичны для многих компаний. Однако в некоторых случаях — когда речь идёт о работе с чувствительными данными, например в здравоохранении, юриспруденции или финансовом секторе — это может стать серьёзной проблемой.

В конфиденциальных вычислениях такой тренд называют переходом к модели *Zero Trust*: никто никому не доверяет по умолчанию — ни провайдеру облака, ни инфраструктуре, ни даже самой системе, на которой запускается код. По словам Станислава Никольского, сооснователя *GENXT.AI*, «джентльмены друг другу больше не верят». Теперь компании ориентированы на полную прозрачность и математически гарантированную защиту, возвращающую уверенность.

82% утечек данных происходят в облаках. Это не значит, что локальные решения лучше, но указывает на очевидное: сама архитектура облачных платформ создаёт риски. Данные могут быть зашифрованы на входе и выходе, но когда они «в движении» — то есть в процессе обработки — они становятся уязвимыми. Именно в момент обработки и происходят основные взломы. *Confidential AI* стремится устранить эту дыру.

Что такое *Confidential AI* и как он защищает данные при вычислениях

В обычной системе данные проходят три состояния: «в покое» (на диске), «в передаче» (по сети) и «в использовании» (в оперативной памяти или на GPU). Первые два состояния давно научились защищать — с помощью шифрования. Но третье оставалось ахиллесовой пятой. Confidential Computing решает эту проблему, шифруя данные даже во время обработки.

Confidential Computing — это технология, встроенная в современные процессоры, которая создаёт внутри них защищённую область, называемую доверенной средой выполнения (Trusted Execution Environment, или TEE). Эта область полностью изолирована от всего остального: туда не могут получить доступ ни операционная система, ни администратор, ни даже облачный провайдер.

По сути, это «чёрный ящик», внутри которого данные временно расшифровываются только в момент выполнения конкретной команды. Как только задача выполнена, они снова становятся недоступными. Даже если вся система будет взломана, данные внутри TEE останутся защищёнными и скрытыми от посторонних.

GPU (графические процессоры) с поддержкой *Confidential Computing* появились только в прошлом году. На базе этих GPU стали возможны сервисы конфиденциального ИИ, в которых запросы остаются зашифрованными на всём протяжении обработки. Станислав Никольский с командой строят именно такой сервис.

Почему приватность — это конкурентное преимущество, а не проблема

Важный сдвиг в мышлении, который предлагает *Confidential AI*, — переосмысление приватности. Прежде она рассматривалась как юридическая категория или технический барьер. Сегодня она становится конкурентным преимуществом. Станислав Никольский подчёркивает: компании, которые гарантируют приватность данных на уровне вычислений, могут сотрудничать даже с теми, кто раньше был «за забором» — от медицинских центров до регуляторов.

Здесь важна не только технология, но и культура обращения с данными. Удалить данные из биотехнологической компании вроде *23andMe* — не значит, что они исчезли. Они могли быть скопированы, переданы, аннотированы. *Confidential AI* строит системы, в которых утечка невозможна технически.

Это особенно актуально в эпоху, когда персональные данные становятся новым видом капитала. Как отмечает Станислав, компании всё чаще вынуждены выбирать: либо контролировать данные и не делиться ими, либо создать защищённую среду и извлекать из них пользу в кооперации. В этом смысле приватность — не только вопрос этики, но и инфраструктура для нового типа экономики.

Такой подход ставит важный вопрос: если *Confidential AI* — это будущее, кто первым сумеет его освоить? Ответ, скорее всего, зависит не от технологии, а от готовности бизнеса переосмыслить, как устроено доверие в цифровом мире.

Как генетика стала частью массового рынка: от родословных к B2C-сервисам

Изначально коммерческие генетические тесты позиционировались как способ узнать предрасположенность к болезням. На деле самыми популярными функциями стали этнический анализ и поиск родственников. Станислав Никольский приводит показательный пример: важнейший вклад в развитие генеалогии внесла церковь мормонов, десятилетиями собиравшая родословные. Их база данных до сих пор используется в ряде сервисов.

Сегодня персональная генетика — это не только медицина, но и массовое потребление. Люди ищут отцов, подтверждают родство, воссоединяются с семьями. В *B2C*-сегменте успех приходит не через диагноз, а через эмоциональную историю. Тем не менее Станислав отмечает: из-за нестыковок в законодательстве (например, между ЕС и США) и отсутствия единого подхода к приватности эти сервисы остаются фрагментированными и закрытыми.

Ключевые цифры и тенденции

- Мировой рынок B2C-генетических тестов в *2022* году оценивался примерно в **$1,2 млрд**, к *2025* году — ожидается рост до **$3,5** млрд.
- К *2020* году было продано более **26 млн** генетических тестов *direct-to-consumer (DTC)* по всему миру.
- *CAGR* (среднегодовой темп роста) *B2C*-сегмента — **20–25%** ежегодно (отдельные отчеты прогнозируют рост всего рынка до **$25 млрд** к *2028* году с акцентом на персонализированную медицину и благополучие).
- В России текущий объем рынка *B2C*-генетических тестов оценивается в **300–400 млн** руб, ежегодный рост — порядка **20–25%**.

Почему компании не делятся чувствительными данными — и как AI может это изменить

Данные становятся главным активом, и компании не хотят ими делиться. Даже если две клиники или биобанка могли бы вместе извлечь больше пользы — например, при поиске редких мутаций, — между ними стоит барьер: юридический, репутационный, инфраструктурный. Обмен может быть невозможен даже при одинаковых интересах — просто потому, что нет безопасной среды для анализа.

В таких условиях AI-модели вроде GENXT.AI предлагают решение: не передавать данные, а передавать модель к данным. То есть код «приезжает» туда, где хранятся данные, обрабатывает их локально и возвращает обезличенные результаты. Это снимает главный страх — утечку информации.

Но, как подчёркивает Станислав Никольский, даже такой сценарий требует доверия к тому, как именно работает модель. Именно здесь вступает в силу *Confidential AI* — технология, которая обеспечивает математически подтверждённую защиту данных во время обработки, устраняя необходимость слепого доверия.

Какие ошибки тормозят развитие рынка персональных данных

Интересно, что как со стороны стартапов, так и со стороны корпораций нередко случаются стратегические ошибки.

Стартапы часто увлекаются разработкой, забывая про бизнес: «долго пилили — не успели продать». А крупные компании, наоборот, боятся экспериментировать: никто не хочет быть первым, кто нарушит правила игры, даже если результат может принести реальную пользу.

GENXT.AI сталкивался с тем, что медицинские учреждения готовы обсуждать внедрение, но требуют доказательств, сертификаций, понятных интерфейсов. Поэтому масштабирование идёт медленно, несмотря на очевидную ценность технологии.

Станислав Никольский формулирует это так: «рынок инертен не потому, что не хочет, а потому, что не знает как».

Почему локальные вычисления возвращаются: ограничения и новые возможности облаков

Несмотря на доминирование облачных платформ, интерес к локальным вычислениям растёт. Причина проста: в ряде задач — от медицинской диагностики до оборонных систем — данные не могут покидать защищённый контур.

Конфиденциальные вычисления (Confidential Computing) позволяют перенести AI ближе к источнику данных. Крупные игроки — Microsoft, Google, AWS — уже внедряют поддержку Confidential GPU в своих облачных сервисах. Это снижает барьер входа: компаниям больше не нужно строить собственные дата-центры, чтобы соблюдать нормы приватности.

Кто владеет данными: пользователь, государство или ИИ-платформы?

Сегодня данные всё чаще рассматриваются как «новая нефть», но вопрос собственности остаётся открытым. Должны ли данные принадлежать пользователю? Или платформе, которая их собирает и обрабатывает? Или, может быть, государству, которое регулирует их использование?

Станислав Никольский указывает на рост интереса к децентрализованным моделям, в которых пользователь контролирует доступ к своим данным через прозрачные протоколы.

Важно различать хранение данных и их использование. Блокчейн может решить задачу хранения — то есть, кто, где и как владеет данными. Но он не защищает данные во время вычислений. Именно здесь вступает в силу *Confidential AI*: технология, позволяющая использовать данные, не раскрывая их.

Это создаёт основу для нового поколения бизнес-моделей — от *AI as a Service* до *Confidential AI as a Service*, где безопасность встроена в саму архитектуру и не требует доверия по умолчанию.

Восточные технохабы как новая точка роста для приватных решений

В завершение подкаста Станислав Никольский делится личной историей: после учёбы в Кембридже его команда переехала в Дубай. Причина — более быстрая регуляторная среда и заинтересованность государства в поддержке AI-стартапов. В Эмиратах уже работают несколько технопарков, включая *AI Campus*, где сосредоточены проекты в области здравоохранения и финансов.

В отличие от Европы и США, рынок Ближнего Востока пока менее зарегулирован, но более открыт к экспериментам. Это делает его особенно привлекательным для компаний, работающих на стыке конфиденциальности, искусственного интеллекта и медицины.

Но, как подчёркивает Станислав, важно не просто ехать туда, где меньше барьеров, а туда, где есть поддержка компаний и реальный запрос на «долгую игру». Устойчивое развитие в новой среде требует не только технологического лидерства, но и институционального партнёрства.