Препятствия и дорожные карты внедрения корпоративного ИИ, безопасность и физический ИИ: второй день TechEx

Источник: TechEx North America

Оригинал: https://www.artificialintelligence-news.com/news/tech-ex-north-america-day-two-roundup-of-themes-issues-discussions/

ROI | инфраструктура | кибербезопасность | корпоративный ИИ | масштабирование ИИ | управление данными

Второй день TechEx North America прошел под знаком более глубокого и критического анализа применения ИИ в корпоративном секторе, но с оптимистичным уклоном. Программа «ИИ и большие данные» (AI and Big Data) открылась упоминанием так называемого «кладбища ИИ» — проектов, которые демонстрируют отличные результаты на этапе пилотного тестирования, но оказываются неэффективными в реальных условиях. Несмотря на использование столь негативного термина, многие спикеры и участники сессий обсуждали способы, позволяющие дальновидным компаниям избежать попадания на это «технологическое кладбище».

Различные направления второго дня мероприятия были посвящены глубокому изучению повсеместных проблем, которые могут препятствовать внедрению ИИ. Сессии в треках «Внедрение корпоративного ИИ» (Enterprise AI Implementation), «ROI (окупаемость инвестиций)» и «Внедрение» (Adoption) использовали застрявшие пилотные проекты в качестве отправной точки, пытаясь выявить причины неудач. Организациям было дано множество дельных советов: от фокусировки **агентного ИИ** (agentic AI) на конкретных

бизнес-областях и создания готовой к работе агентов информационной базы данных (планирование успеха «под капотом») до обсуждения реального влияния оплаты ИИ на основе использования токенов на финансы компании.

На инфраструктурном уровне также велись глубокие дискуссии о том, стоит ли компаниям покупать или создавать собственную физическую инфраструктуру для своих ИИ-проектов, а также о лучших способах обеспечения устойчивого **ROI** для проектов в области данных и ИИ с учетом множества влияющих факторов.

В проектах, где внедрение ИИ заходит в тупик, основную проблему можно резюмировать концепцией «персонального копилота» (personal copilot). Это решение отлично работает на рабочем столе отдельного сотрудника и в рамках его индивидуальных рабочих процессов, но оно не масштабируется на целый отдел, не говоря уже о всей компании. Многие компании сообщают, что у них есть бюджет на запуск таких экспериментов с ИИ на уровне одного пользователя, и это обычно приносит отличные результаты. Если таким пользователем является руководитель высшего звена (C-suite executive), то лично достигнутая эффективность повышает общий уровень энтузиазма в компании, что можно считать позитивным фактором. Однако переход от этой точки к значимым изменениям во всей организации — это именно то место, где многие компании сталкиваются с индивидуальными трудностями и препятствиями. Именно это стало основной темой обсуждений на втором дне мероприятия в залах и на многочисленных сценах конференц-центра San Jose McEnery.

Кибербезопасность

Несмотря на использование таких терминов, как «застрявшие» или «трудные для масштабирования», на сцене Cyber Security and Cloud Expo спикеры упомянули скорость, с которой бизнес и организации внедряют системы **агентного ИИ**, как причину возникновения «разрыва в скорости» (velocity gap). Там, где внедрение ИИ проходит успешно, он быстро набирает обороты! Однако проблемы безопасности и управления (governance) возникают тогда, когда бизнес-подразделения внедряют **генеративный ИИ** быстрее, чем команда по информационной безопасности успевает контролировать процессы и обеспечивать безопасность предприятия.

Подобно обоюдоострому мечу, ИИ можно рассматривать как силу, которая способна как изменить, так и улучшить методы нападения и защиты в сфере кибербезопасности. Существуют проблемы, создаваемые внутри организаций

бесконтрольными агентами и большими языковыми моделями, а также дополнение арсенала злоумышленников инструментами ИИ-сканирования, способными выявлять потенциальные уязвимости.

Также в ходе круглых столов и программных докладов часто звучала старая тема «теневых ИТ» (shadow IT), которая теперь предстает в новом обличии — «теневого ИИ» (shadow AI). Если сотрудники, например, помещают конфиденциальные материалы в несанкционированные инструменты или если одобренные системы ИИ плохо ограничены и управляемы, поверхность атаки может расшириться без ведома команды кибербезопасности. Таким образом, управление данными и надзор за системами становятся более взаимосвязанными, чем когда-либо — таков был посыл как секций по кибербезопасности, так и разделов по облачным технологиям и большим данным.

Для специализированных функций кибербезопасности концепция «нулевого доверия» (**Zero Trust**) была представлена как один из ответов на бесконтрольное внедрение ИИ вне контроля команд безопасности — внедрение, основанное на позиции «отказа по умолчанию» как для людей, так и для машин. Подтверждение личности и уровней привилегий должно применяться также к сервисам и агентам; таким образом, автоматизированные рабочие процессы будут подчиняться тем же моделям разрешений, что и любой другой элемент в ИТ-стеке.

Второй день TechEx North America определенно не был отказом от амбиций руководителей в области ИИ — роль ИИ и даже агентов была признана неоспоримым фактом среди спикеров, лидеров мнений и делегатов мероприятия. Однако представители различных отраслей и бизнес-функций представили множество деталей и соображений, каждое из которых несло позитивный и глубокий смысл. Каждый вынес на обсуждение свои опасения и свой энтузиазм, дополняя дискуссии вокруг внедрения ИИ в 2026 году.

Марш роботов

Тем не менее, во многих зонах выставочного зала по-прежнему царило оживление. Гуманоидные роботы, представленные на выставке, вызывали большой восторг (кажется, всем нравятся милые андроиды!), но, если говорить более прагматично, новый трек «Физический ИИ» (Physical AI) собрал одну из самых многочисленных аудиторий. Многие делегаты отметили, что именно написание программного кода стало той областью, где использование больших языковых моделей в профессиональной среде впервые принесло положительные результаты. Также высказывалось мнение,

что автоматизированные физические системы станут следующим сегментом индустрии, который получит выгоду от целенаправленной работы над новыми моделями и их практическим применением.

Модели ИИ, лежащие в основе физического ИИ следующего поколения, вряд ли будут являться **LLM** (хотя они будут полезны, если устройства предназначены для взаимодействия с людьми). По мере того как такие модели будут разрабатываться и выходить из стадии исследований, именно серия мероприятий TechEx Events будет первой демонстрировать их и показывать, как они могут эффективно работать в бизнес-контексте.

Новые направления обучения

В этом году на мероприятии появилось долгожданное дополнение в виде практического программирования: сессии по практическому обучению позволили участникам самостоятельно запускать свои собственные агентные модели ИИ, изучая, как агенты могут самосовершенствоваться, используя интерактивные экземпляры Google Colab. В TechEx Learning Hub также прошли воркшопы от Nvidia и популярный хакатон от Google, где уровень участников варьировался от новичков, которым требовалось знакомство с **IDE** (интегрированной средой разработки), до специалистов с уже отточенными навыками программирования. Суть этого мероприятия заключается именно в применении знаний на практике — будь то руководители высшего звена, изучающие лучшие стратегические методы, или разработчики, воплощающие творческие идеи в реальность.

TechEx берет передовые технологии и адаптирует их через призму бизнеса: прагматично, но с взглядом в будущее. Встречайтесь на следующем этапе TechEx в Амстердаме в этом сентябре — кто знает, как далеко мы сможем продвинуться за эти четыре коротких месяца?
