

ИИ — это вопрос власти, инфраструктуры и безопасности: TechEx North America

Источник: TechEx North America

Оригинал: <https://www.artificialintelligence-news.com/news/techex-north-america-day-one-lessons-for-all-around-ai-and-more/>

IoT

edge computing

инфраструктура

кибербезопасность

промышленный ИИ

цифровые двойники

Хотя посетители такого мероприятия, как TechEx North America, всегда хотят видеть передовые технологии в центре внимания, нюансы и детали, привнесенные на выставку спикерами и экспонентами, означают, что иногда именно небольшие аспекты должны играть важную роль — по крайней мере, в представлении лиц, принимающих решения на предприятиях.

В рамках различных направлений — **Edge Computing** (периферийные вычисления), **IoT** (интернет вещей), **Data Centre Congress** (конгресс центров обработки данных) и **Cyber Security** (кибербезопасность) — основным вопросом было: что именно необходимо выстроить вокруг **AI** (искусственного интеллекта), прежде чем он займет свое место в физическом, ориентированном на бизнес мире?

Направление **Edge Computing**, имеющее корни в традиционных отраслях промышленности, рассматривало вопросы задержки (latency), дисциплины развертывания и кибербезопасности для гибридных систем **IIoT/IT** (промышленного и информационного интернета вещей). Программа первого дня позиционировала периферийные вычисления как среду, где компании могут переоценить ценность своих информационных активов, изучить, как принимаются решения автономным оборудованием, и определить необходимую скорость обработки данных.

В рамках сессий рассматривались вопросы масштабирования периферийных развертываний (например, в компаниях с множеством площадок), агентные сетевые операции, распределенный вывод (**distributed inference**) — локальный, облачный или гибридный, — неизменяемая (**immutable**) периферийная инфраструктура, а также то, как уроки кибербезопасности с моделью нулевого доверия (**zero-trust**) могут быть применены к системам управления.

Эд Доран из **Edge AI Foundation** модерировал программу, отправной точкой которой стало утверждение, что работа на периферии — это крайне сложная задача. В состав участников направления вошли представители **Akamai**, **Spectro Cloud**, **Scylos**, **TÜV Rheinland**, **OPC Foundation** и немецкой компании **Schneider Electric**. Дискуссии охватывали вопросы производства и **IoT**, а также углублялись в промышленную автоматизацию и подключенные устройства управления и затухания.

Перенос интеллекта ближе к машине меняет профили рисков (в какую сторону — оставалось предметом споров), и более быстрые локальные решения могут снизить задержку и зависимость от центральных облачных сервисов, но где в сознании лиц, принимающих решения, находятся наблюдаемость (**observability**) и контроль?

Направление первого дня **IoT Tech Expo**, посвященное **Industrial IoT** (промышленному интернету вещей) и **Digital Twins** (цифровым двойникам), рассматривало производство; сессии охватывали тенденции «умных заводов», **AI** за пределами **Industry 4.0**, управление активами, практические дорожные карты по выходу из «пилотного чистилища» (подробнее ниже), физический **AI** в повседневных операциях и цифровые двойники.

Подобно дебатам о внедрении **AI** в интеллектуальном секторе, именно разрыв между демонстрацией и реальным развертыванием стал областью наиболее пристального внимания. Как промышленный **AI**, так и **AI** для бэк-офиса могут хорошо работать в презентации, но могут зайти в тупик при столкновении со старым оборудованием (или устаревшим программным обеспечением).

Понятие «пилотное чистилище» (**pilot purgatory**) нашло значительный отклик в нескольких сессиях на различных этапах презентаций и на выставочной площадке в первый день. Сессия **Rockwell Automation** и **Ford**, посвященная физическому **AI** и интеллектуальному управлению подключенными активами, была сосредоточена на масштабировании проектов, которые кажутся успешными в теории, но могут потерпеть

неудачу при столкновении с реальным миром. Как внедрить интеллект в ежедневные операции так, чтобы он не превратился в очередную панель мониторинга, за которую никто не несет ответственности?

Цифровые двойники получили аналогичную оценку. Лучшая версия цифрового двойника — это не визуальная копия, используемая для демонстраций (хотя и они имеют свое применение). Вместо этого несколько спикеров призвали к созданию и представили операционные модели, которые могут реально помочь заводу, городу или муниципальному объекту. Помимо предварительного тестирования решений и улучшения технического обслуживания, чего должен достигать современный цифровой двойник?

Программа **TechEx** связала идеи спикеров из **Siemens**, корейской **LG CNS**, **Boston Dynamics** и других компаний через различные направления выставки. Общим выводом стало то, что интеллектуальные системы, будь они глубоко внедрены в инженерные объекты или в бэк-офис, должны проектироваться в согласии с людьми или машинами, которым они призваны приносить пользу.

Сессии первого дня в рамках **Data Centre Congress** рассматривали основные проблемы, стоящие перед сектором сегодня: строительство, электроснабжение, закупки, охлаждение, водоснабжение и сетевой каркас, необходимый для дата-центров под **AI**. Ключевые спикеры и участники круглых столов обсуждали хаос в строительстве и проблемы с электроэнергией, а первые посетители мероприятия узнали от принимающего город **TechEx**, Санта-Клару, о его собственном пути развития центров обработки данных.

Вопрос дата-центров (DC) остается центральным в более широких дебатах об **AI**. Как технология, **AI** зависит от вычислений, причем от высокоплотных вычислений. Это, в свою очередь, зависит от электроэнергии, охлаждения, земли и разрешений. Повторяющейся темой в дискуссиях, ориентированных на инфраструктуру, было то, как экономика **AI** влияет на инфраструктурный стек: если первая меняется стремительно, то второй требуются годы для созревания.

Во многих отношениях мероприятие **TechEx** уникально тем, что оно собирает под одной крышей проблемы, затрагивающие целую отрасль; это место, где можно увидеть общую картину. На **Data Center Congress** мы узнали, что ограничения по воде и электроэнергии могут перечеркнуть всю риторику вокруг масштабов **AI**. Сессии под эгидой **AI** и **Big Data** помогли умерить энтузиазм по поводу «гонки» за продуктивностью с помощью **AI**, приводя

собственные причины, по которым незапланированное и неорганизованное внедрение технологий не подходит современному предприятию. Дата-центр теперь является одним из мест, где стратегия **AI** становится физической; соображения в залах заседаний советов директоров предприятий становятся практическими.

Направление **Cyber Security and Cloud Expo** представило свой взгляд на развертывание. Здесь программа первого дня была посвящена культуре безопасности, комплаенсу (соответствию нормативным требованиям), скорости, программам-вымогателям, «теневому» **AI (shadow AI)**, эксфильтрации данных, устаревшим системам, проблемам зависимости от открытого исходного кода и взаимоотношениям **CISO** (директора по информационной безопасности) с руководством компании (**C-suite**). Был достигнут общий консенсус относительно того, что внедрение **AI** увеличивает поверхность атаки компании, и часто повторялась мысль, что существующие уязвимости в безопасности не исчезают, когда бизнес требует более быстрых и умных инструментов.

Сессии по «теневому» **AI** и эксфильтрации данных были особенно актуальны для всего мероприятия. Сотрудники многих компаний используют сервисы **AI** в рабочих процессах, иногда без одобрения и, как правило, без возможности логирования их действий. Это делает управление данными (**data governance**) и киберуправление (**cyber governance**) фактически одной и той же темой для обсуждения.

Преимущества проведения конференции, объединяющей взаимодополняющие направления, проявились в нескольких случаях. Например, опасения направления кибербезопасности по поводу устаревших систем нашли отклик на этапах **IoT** и **Edge**, где поднимались вопросы о взаимодействии современного интеллектуального управления с более старыми заводскими системами. Безопасность в любом контексте иногда может стать второстепенной задачей, но критическая инфраструктура в виде транспорта или энергетики означает, что кибербезопасность должна играть центральную роль.

Направления первого дня **TechEx North America**, связанные с инфраструктурой, придали конференции дозу реализма, по крайней мере в некоторых аспектах. Об **AI** могут дискутировать в терминах агентной автоматизации, но развертывание зависит от сетей, мощностей дата-центров и кибербезопасности. Сессии по **Edge** и **IoT** показали, как интеллект достигает машин и насколько тщательно и продуманно его необходимо применять. Сессии, ориентированные на дата-центры, показали

материальные пределы физического строительства, в то время как сессии по кибербезопасности показали, как стремление к скорости может стать врагом.

Первый день показал тысячам участников, что ввод **AI** в эксплуатацию — это не просто нажатие кнопки включения программного обеспечения. Существует зависимость от приземленных вопросов зданий и электросетей, сетей и безопасности. Компании, понимающие эти проблемы, с большей вероятностью успешно внедряют новейшие технологии. Понимание общей картины — это то, ради чего проводится это мероприятие.

Перевод выполнен: 19.05.2026 | ai4med.ru

Машинный перевод. Рекомендуем сверять с оригиналом при клиническом использовании.