Разработчики ИИ всех стран, объединяйтесь!

еженедельная газета о новостях искусственного интеллекта

ИИ-ИЗВЕСТИЯ

№ 2026.11.02
еженедельный выпуск
Цена 2 коп.

Понедельник, 2 ноября 2026 года

2 полосы

Россия и мир · 26 октября — 2 ноября 2026

Главное в этом выпуске | **Карта выпуска** | **Новости и их значение** | **Что отслеживать**

Главное в этом выпуске

За неделю ИИ сместился от чат-ассистентов к системам для корпоративных данных, симуляции миров и безопасности.

Новости подготовил Гермес — агент-обозреватель на навыках news-digest и news-monitor с проверкой источников через goap-research-ed25519; прочитал и отредактировал Дмитрий Жечков.

Карта выпуска

№	Событие	Дата
1	MWS AI Cowork.	2026-10-27
2	Genie 4.	2026-10-27
3	Gemini 4 Carbon.	2026-10-28
4	PyTorch 2.15.	2026-10-28
5	Mistral Large 4 открыла веса.	2026-10-29
6	Тестовая среда приватного федеративного обучения.	2026-10-29
7	Правила идентичности для ИИ-агентов.	2026-10-27
8	OpenAI-модели в AWS GovCloud.	2026-10-30

Что произошло

MWS AI Cowork.

MWS AI выпустила корпоративного ИИ-агента с чат-интерфейсом. Cowork ищет и анализирует сведения, работает с файлами, сайтами и подключёнными приложениями, готовит документы, таблицы, презентации и отчёты. Решение можно развернуть в закрытом российском контуре, подключить к почте, календарю, CRM и документообороту; агент действует в пределах прав конкретного пользователя. Для типовых процессов предусмотрены сохраняемые навыки.

Почему важно. Обычная автоматизация офиса распадается на разрозненные боты и ручные передачи данных между системами, а перенос документов во внешний ИИ часто неприемлем из-за доступа и размещения данных. MWS AI Cowork объединяет поиск, подготовку материалов и вызовы подключённых систем в одном рабочем интерфейсе с корпоративными правами доступа; следствием может стать постепенная автоматизация сквозных офисных процессов без отказа от внутреннего контура.

Genie 4.

DeepMind анонсировала исследовательскую систему интерактивных миров: она в реальном времени генерирует изображение, звук и диалог, позволяет текстом менять сцену и поддерживает многошаговый сценарий с помощью Gemini. Сначала доступ открыт доверенным тестировщикам.

Почему важно. Роботам, агентам и создателям интерактивных продуктов трудно и дорого проверять поведение в физическом мире или вручную делать много вариантов сцены. Genie 4 делает возможными быстро меняющиеся симуляции с управлением языком и аудиовизуальной обратной связью; это создаёт новый слой для прототипирования, обучения и предварительной проверки сценариев.

Gemini 4 Carbon.

Google представила Gemini 4 Carbon — модель для длительных инженерных задач и киберзащиты. Компания заявляет возможности поиска уязвимостей, проверки их эксплуатации и подготовки исправлений; на первом этапе Carbon получают ограниченные группы специалистов по защите.

Почему важно. Поиск, подтверждение и исправление уязвимости обычно требуют цепочки разных действий и передачи контекста между инженерами. Длинный автономный цикл модели потенциально сокращает разрыв между обнаружением дефекта и подготовкой патча, но ограниченный старт доступа показывает, что рост возможностей киберзащиты требует контролируемого развёртывания.

PyTorch 2.15.

Вышел PyTorch 2.15: переработанный NCCL-бэкенд стал вариантом по умолчанию, появились диагностика зависаний, новые возможности распределённых транспортов, улучшения FSDP2 и конвейерного распараллеливания. Есть оптимизации для NVIDIA Blackwell, Apple Silicon, AMD и Intel GPU.

Почему важно. При обучении и запуске больших моделей сбой обмена между ускорителями или лишние расходы памяти могут остановить весь кластер, а оптимизации нередко привязаны к одному поставщику. PyTorch 2.15 переносит часть надёжности и производительности в основной фреймворк для нескольких платформ; командам проще обновлять распределённые контуры и сравнивать аппаратные варианты.

Mistral Large 4 открыла веса.

Mistral выпустила открытые веса Mistral Large 4 — нативно мультимодальной модели с заявленным размером 1 трлн параметров. Доступны самостоятельное развёртывание,

Редакция сердечно благодарит за идею формата и пример реализации Станислава Гридина https://t.me/gridstan

режимы рассуждения Low, Medium и High и сценарии программирования, агентов и защитной кибербезопасности.

Почему важно. Организации, которым нужен контроль над местом запуска, данными и изменениями модели, обычно выбирают между закрытым API и менее мощными открытыми моделями. Открытие весов большой мультимодальной модели расширяет пространство для самостоятельных и суверенных внедрений; одновременно оно делает критичными оценку лицензии, стоимости инференса и собственные защитные контуры.

Тестовая среда приватного федеративного обучения.

NIST выпустил открытый PPFL Testbed и подготовленный геномный набор данных для экспериментов с федеративным обучением и дифференциальной приватностью. Среда сравнивает централизованное и распределённое обучение и показывает, как настройки приватности влияют на качество модели.

Почему важно. Полезные данные часто нельзя объединить в одном хранилище из-за коммерческой тайны, приватности или регулирования. Общая тестовая среда позволяет воспроизводимо сравнивать компромиссы между приватностью и качеством; это снижает порог для проверки распределённого обучения до переноса чувствительных данных.

Правила идентичности для ИИ-агентов.

NIST описал принципы управления идентичностями агентов: отдельная проверяемая идентичность, цепочка делегирования с сужением полномочий, минимум постоянных прав, краткосрочные разрешения, контроль человеком, разделение политики доступа и рассуждения, мониторинг и независимый журнал действий.

Почему важно. Агент с широкими постоянными правами может быть введён в заблуждение письмом, сайтом или документом и выполнить действие вне намерений владельца. Принципы NIST переносят контроль из промпта в идентичности, ограничения полномочий и проверяемые журналы; корпоративные агенты становятся ближе к управляемым сервисным учётным записям.

OpenAI-модели в AWS GovCloud.

Amazon Bedrock добавил поддержку OpenAI GPT-5.6 Terra и Luna через bedrock-runtime в AWS GovCloud (US), включая Responses, Converse и Chat Completions API. Для моделей заявлен cross-Region inference внутри двух регионов GovCloud; вызовы остаются в журналах, метриках и учёте затрат Bedrock.

Почему важно. Государственные и регулируемые организации не могут переносить рабочие нагрузки в обычные облачные контуры только ради доступа к новой модели, а отдельная интеграция усложняет аудит. Поддержка нативных API и межрегионального инференса в GovCloud позволяет использовать модели в знакомой управляемой среде, сохраняя средства наблюдаемости и контроля доступа.

Что отслеживать

- Доступность и условия развёртывания MWS AI Cowork.
- Расширение доступа к Genie 4 в Project Genie и публикации об ограничениях симуляции.
- Следующие этапы программы Google Fairwind для Gemini 4 Carbon.
- Совместимость и обратные несовместимости PyTorch 2.15.
- Лицензию и модельную карточку Mistral Large 4.
- Развитие NIST PETs Testbeds.

~/источники

- https://mts.ai/tehnologii/mws-ai-vypustila-universalnogo-ii-agenta-dlya-resheniya-ofisnyh-zadach-v-perimetre-kompanii/
- https://deepmind.google/blog/genie-4-a-new-generation-of-world-simulation/
- https://blog.google/innovation-and-ai/models-and-research/gemini-models/introducing-gemini-4-carbon/
- https://pytorch.org/blog/pytorch-2-15-release-blog/
- https://mistral.ai/news/mistral-large-4-oss/
- https://www.nist.gov/news-events/news/2026/10/privacy-preserving-federated-learning-ppfl-testbed-and-curated-dataset
- https://www.nist.gov/blogs/cybersecurity-insights/design-tenets-agent-identity-management-systems
- https://aws.amazon.com/about-aws/whats-new/2026/10/bedrock-openai-runtime-govcloud/

Редакция сердечно благодарит за идею формата и пример реализации Станислава Гридина https://t.me/gridstan