ИИ будет знать все: утечка личных данных в новой Windows неизбежна?

Накануне ежегодной конференции для разработчиков Build компания Microsoft – это американская многопрофильная компания, занимающаяся разработкой программного обеспечения и производством компьютерной техники. Она была основана в 1975 году Биллом Гейтсом и Полом Алленом и на сегодняшний день является одной из самых крупных и известных IT-компаний в мире.

 Среди продуктов Microsoft наиболее известными являются операционные системы Windows, пакеты офисных приложений Office, браузер Internet Explorer и поисковая система Bing. Кроме того, компания занимается разработкой программного обеспечения для серверов, баз данных, игровых консолей Xbox и многих других устройств.

 Microsoft также предоставляет услуги облачных вычислений и хранения данных через свою платформу Azure, а также занимается разработкой искусственного интеллекта и других инновационных технологий. Компания имеет филиалы по всему миру и сотрудничает с многими крупными корпорациями и организациями." data-html="true" data-original-title="Microsoft" >Microsoft провела специальную презентацию, на которой объявила о начале «новой эры» персональных компьютеров с глубокой интеграцией технологий искусственного интеллекта. По мнению экспертов и журналистов, это амбициозное нововведение, с одной стороны, обещает существенно повысить производительность устройств, но с другой – ставит под угрозу безопасность личных данных пользователей.

Анонс Copilot Plus PCs

На презентации Microsoft анонсировала линейку компьютеров под названием Copilot Plus PCs. Эти устройства оснащены процессорами Qualcomm Snapdragon X Elite и Plus на архитектуре ARM, оптимизированными для работы с искусственным интеллектом. Ожидается, что позже появятся модели с процессорами от Intel и AMD. Помимо самой Microsoft, выпускать такие устройства будут Lenovo, Dell, Acer, Asus и HP.

Переход на ARM-архитектуру позволит значительно продлить время автономной работы компьютеров. Так, анонсированный Microsoft ноутбук Surface Laptop с 15-дюймовым экраном сможет проработать до 22 часов в режиме просмотра видео и до 15 часов при активном интернет-серфинге на одном заряде аккумулятора. Старт продаж этой модели запланирован на 18 июня 2024 года.

Технические требования и производительность

Для обеспечения высокой производительности, компьютеры Copilot Plus должны соответствовать определенным техническим требованиям . Они должны иметь минимум 16 гигабайт оперативной памяти, 256 гигабайт встроенной памяти и нейронный процессор (NPU), способный выполнять 40 триллионов операций в секунду. Эти процессоры будут отвечать за функции, связанные с искусственным интеллектом, Работать устройства будут на Windows 11, в которую Microsoft интегрирует более 40 ИИ-моделей, около 10 из которых будут функционировать в фоновом режиме.

Microsoft утверждает, что новинки будут работать на 58 процентов быстрее, чем MacBook Air с процессором M3, однако подробностей о методах оценки компания не представила.

Функция Recall: фотографическая память для ПК

Одной из ключевых функций ИИ, которая отличает устройства Copilot Plus PCs, является инструмент под названием Recall. Как сообщает The Verge, это новый инструмент в Windows 11, который будет отслеживать и запоминать буквально все действия пользователя – от работы внутри приложений и посещения сайтов до видеозвонков. Вся информация сохраняется в виде скриншотов, содержимое которых может распознать ИИ.

Microsoft сравнивает Recall с «фотографической памятью» компьютера. Благодаря этому пользователь сможет легко найти любой контент, с которым он работал недавно – будь то переписка в мессенджере, слайд презентации или веб-страница. Все действия будут отображаться в специальном таймлайне, по которому можно свободно перемещаться.

Опция похожа на уже существующее приложение Rewind для Mac, которое также записывает активность пользователя и позволяет быстро вернуться к нужной задаче через чат-бота. Однако Rewind – это всего лишь сторонняя программа, требующая выдачи определенных разрешений, в то время как Recall будет полностью интегрирована в сам Windows.

Проблемы конфиденциальности и безопасность данных

Введение функции Recall и всей линейки новых ПК с поддержкой ИИ вызывает вопросы по поводу безопасности данных. В Microsoft заверяют , что вся информация, которую будет собирать и использовать функция Recall, будет храниться исключительно на самом устройстве пользователя, никуда не отправляясь за его

пределы.

Кроме того, алгоритмы Recall не будут распространяться на приватные сессии веб-браузера Edge и контент, защищенный системой DRM. Пользователь сможет вручную запретить функции доступ к определенным приложениям и сайтам. В любой момент ее работу можно полностью остановить или поставить на паузу, а также удалить весь ранее собранный контент. Однако, как признают в Microsoft, строгой модерации личных данных не предусмотрено, и в таймлайн могут случайно попасть даже пароли или финансовая информация.

Несмотря на эти меры, многие специалисты называют инициативу Microsoft «кошмаром для конфиденциальности». Британские регуляторы уже обратились к представителям компании за дополнительной информацией. В соцсетях также обсуждают риск конфискации личных устройств при пересечении границы или аресте, возможность их утери или кражи.

Илон Маск сравнил возможности Recall с эпизодом сериала «Черное зеркало», подчеркнув, что эту функцию стоит отключать.

ИИ в видеоиграх: угроза сайтам с прохождениями

Еще одна потенциальная проблема связана с интеграцией ИИ-инструментов Microsoft Copilot в видеоигры. Компания планирует начать с Minecraft, где пользователи смогут задавать чат-боту вопросы о прохождении игры. Например, бот сможет проверять инвентарь и давать советы по созданию предметов или нахождению недостающих элементов.

Эта функция позволяет игрокам получать подсказки прямо во время игры, не отвлекаясь на сторонние сайты. Однако это может привести к снижению посещаемости сайтов с подсказками и прохождениями, что в перспективе негативно скажется на качестве работы самого ИИ, так как уменьшится количество источников качественной информации.