Как компания защищает наши данные и обеспечивает конфиденциальность?

Компания Apple Inc. – американская корпорация, которая занимается производством персональных и планшетных компьютеров, телефонов, аудиоплееров и программного обеспечения. Наиболее известные продукты компании это линейка персональных компьютеров Macintosh, мобильные телефоны iPhone, планшетные компьютеры iPad, операционная система Mac OS X, медиаплеер для проигрывания и систематизации аудио и видеофайлов iTunes, набор мультимедийного программного обеспечения iLife, набор приложений iWork, web-браузер Safari и мобильная операционная система Apple iOS.

 Международное исследовательское агентство Millward Brown признало торговую марку Apple самым дорогим брендом в мае 2011 года. В начале августа 2011 года Apple стала самой дорогой компанией по рыночной капитализации, которая составляла $338,8 млрд 10 августа." data-html="true" data-original-title="Apple" >Apple представила Apple Intelligence — набор функций, привносящих возможности генеративного ИИ, такие как переписывание черновиков электронных писем, составление резюме уведомлений и создание пользовательских эмодзи, в iPhone, iPad и Mandatory Access Control, или MAC (обязательное управление доступом) — это стратегия безопасности, которая определяет, кто или что (обычно определенный пользователь или программное обеспечение) может получить доступ к информации или системе. Всеми доступами управляет только система, не пользователи. Даже если пользователь допускает ошибку или пытается предоставить доступ к информации, которую не должен разглашать, система этого не допустит.

 В основе системы MAC лежит концепция уровней безопасности и меток. Доступ к данным определяется не по пользователю, а по меткам, прикрепленным к информации и уровням безопасности, прикрепленным к пользователям.

 К примеру, есть военная база данных, в которой хранится информация различных уровней секретности: "секретно", "совершенно секретно" и "особой важности". Каждому сотруднику этой базы присваивается уровень доступа в соответствии с их ролью и доверенностью. Так, простому аналитику может быть присвоен уровень "секретно", начальнику отдела – "совершенно секретно", а руководителю всей базы – "особой важности". Если аналитик попытается получить доступ к данным "особой важности", система MAC не позволит этого сделать.

 Модель широко используется в государственных организациях и корпоративных структурах, где важно строгое соблюдение политики безопасности и сохранность конфиденциальной информации.

" data-html="true" data-original-title="MAC" >Mac. Во время презентации на конференции WWDC представители компании подробно рассказали о пользе самих инструментов. Также много внимания было уделено

обещаниям полной конфиденциальности при использовании новых ИИ-инструментов.

По словам разработчиков, высокий уровень приватности обеспечивается двусторонним подходом Apple. С одной стороны, Apple Intelligence работает локально на устройстве, что позволяет быстро решать базовые ИИ-задачи. Но для более сложных запросов, требующих передачи личных данных, задействуются облачные серверы.

Ключевая особенность — использование Apple собственных ИИ-моделей . В отличие от конкурентов, компания не обучает их на частных данных или информации о взаимодействии пользователей. Вместо этого используются лицензионные материалы и публичные сведения, собранные краулером Applebot. Авторы могут запретить индексацию своего контента, как у Google и OpenAI. Из обучающих данных также исключаются кредитные карты, соцномера и нецензурная лексика.

Одним из главных преимуществ Apple Intelligence является ее глубокая интеграция в операционные системы и приложения Apple, а также оптимизация моделей по энергоэффективности и размеру для работы на iPhone. Локальная обработка запросов снимает многие опасения касательно приватности, но при этом приходится использовать более компактные и ограниченные по возможностям ИИ-инструменты.

Чтобы повысить эффективность локальных моделей, Apple применяет метод финальной подстройки (fine-tuning), специально обучая их для конкретных задач вроде проверки правописания или резюмирования текста. Эти специализированные навыки реализуются в виде «адаптеров», которые можно гибко подключать к базовой модели под конкретную задачу, наделяя ее новыми возможностями.

Чтобы ускорить работу ИИ, компания применяет специальные техники вроде «спекулятивного декодирования», «выборочной обработки контекста» и «группирования похожих запросов». Для этого задействуются нейронные ядра процессоров Apple Silicon. Чипмейкеры недавно начали встраивать специализированные нейропроцессоры в новые системы на кристалле, что позволяет разгрузить ЦП и ГП от обработки алгоритмов машинного обучения и ИИ. Именно поэтому Apple Intelligence работает только на устройствах с чипами серии M, включая iPhone 15 Pro и Pro Max.

Согласно внутренним исследованиям Apple, из 750 проанализированных ответов по резюмированию текста, локальная ИИ-модель компании (с соответствующим адаптером) показала результаты, более привлекательные для людей, чем модель Microsoft Phi-3-mini. Это звучит как большое достижение, но современные чат-боты

обычно используют гораздо более мощные облачные модели для получения лучших результатов. Здесь Apple пытается найти баланс между качеством и сохранением приватности, предлагая беспрепятственную отправку сложных запросов на облачные серверы с конфиденциальной обработкой данных.

Если запрос требует более производительной ИИ-модели, Apple отправляет его на свои серверы Private Cloud Compute (PCC). PCC работает на собственной операционной системе (на базе iOS) и имеет собственный программный стек для Apple Intelligence. По словам компании, PCC обладает собственным модулем Secure Enclave для хранения ключей шифрования, совместимых только с запрашивающим устройством. Также специальный монитор гарантирует, что на PCC работает только проверенный код.

Перед отправкой запроса устройство пользователя создает соединение с кластером PCC, защищенное сквозным шифрованием. Apple утверждает, что не может получить доступ к данным на PCC, так как у серверов отсутствуют инструменты удаленного управления и командная оболочка. На PCC также нет постоянного хранилища, поэтому запросы и любые личные данные из семантического индекса Apple Intelligence удаляются после обработки в облаке.

Каждая сборка PCC будет иметь публичную виртуальную версию для исследовательского аудита. В производственную среду будут внедряться только подписанные и зарегистрированные сборки, прошедшие проверку.

Еще одним способом, которым Apple справляется с опасениями касательно конфиденциальности, является перекладывание этой проблемы на сторонние компании. Обновленный голосовой помощник Siri может перенаправлять некоторые сложные запросы в облако ChatGPT от OpenAI, но только с разрешения пользователя после того, как он задаст действительно непростой вопрос. По словам генерального директора Apple Тима Кука в интервью Маркесу Браунли, система ChatGPT будет подключаться для ответов на вопросы общего характера, выходящие за рамки личного контекста.

Apple — не первая компания, решившая сочетать локальную и облачную обработку данных для своих ИИ-инструментов. Google использует локальную модель Gemini Nano на устройствах Android наряду с облачными моделями Pro и Flash. Microsoft также задействует локальную обработку на компьютерах с Copilot Plus, опираясь при этом на ресурсы OpenAI и разрабатывая собственную модель MAI-1. Однако ни один из конкурентов Apple пока не делал такого серьезного упора на обязательства по сохранению конфиденциальности пользовательских данных.

Конечно, все это выглядит впечатляюще на подготовленных демонстрациях и в официальных документах. Но сейчас для исследователей самое важное — убедиться в эффективности Apple Intelligence на практике, когда она станет доступна позднее в этом году.