Как искусственный интеллект угрожает конфиденциальности: новая математическая модель поможет оценить риски

Дата публикации: 24.01.2025

Современные технологии искусственного интеллекта все активнее внедряются в сферы мониторинга и идентификации, но их использование сопряжено с серьезными рисками для конфиденциальности. Новое исследование, проведенное учеными из Оксфордского университета, Имперского колледжа Лондона и Калифорнийского университета в Лувене, привело к созданию математической модели, позволяющей оценивать угрозы, связанные с идентификацией личности с использованием ИИ.

Эта модель представляет собой первое научное решение, способное оценить точность различных методов идентификации, включая такие технологии, как «браузерный отпечаток пальца», который использует данные часового пояса, настроек браузера и других факторов для идентификации пользователей. Исследование, опубликованное в журнале Nature Communications, предлагает детальный подход, позволяющий оценить точность идентификации и выявить потенциальные риски при обработке больших объемов данных.

Применение новой модели особенно важно в сферах, где точность идентификации критически важна: здравоохранение, правоохранительные органы, онлайн-банкинг, гуманитарные миссии. В условиях, где высока вероятность повторной идентификации пользователей, модель поможет предотвратить утечку конфиденциальных данных и соблюсти нормативные требования, такие как GDPR.

В основе методики лежит байесовская статистика, которая позволяет с высокой точностью оценивать идентифицируемость индивидов, экстраполируя результаты на большие популяции. Это делает метод в 10 раз эффективнее существующих подходов, обеспечивая более надежную оценку в различных условиях и сценариях.

Растущая популярность инструментов ИИ, использующих технологии распознавания лиц, голоса и поведенческих факторов, требует внедрения инструментов, способных оценить их влияние на конфиденциальность. Исследователи считают, что новый подход позволит организациям находить оптимальный баланс между технологическим прогрессом и защитой персональных данных, повышая доверие пользователей и регулирующих органов к этим решениям.

© HahgaPro, 2026

Разработанная модель также станет важным инструментом для анализа политики конфиденциальности и тестирования систем до их широкомасштабного внедрения. Это позволит компаниям заранее выявлять уязвимости и корректировать системы для минимизации рисков нарушения конфиденциальности.

Эксперты отмечают, что понимание принципов масштабируемости идентификации критически важно для компаний и государственных структур, чтобы соответствовать требованиям защиты данных, установленным международными законами. Новые научные разработки в этой области помогут разработчикам, политикам и исследователям создать безопасную цифровую среду, обеспечивающую как удобство использования, так и надёжную защиту данных.

Таким образом, данное исследование является важным шагом на пути к созданию безопасных технологий ИИ и расширяет горизонты понимания масштабных рисков, связанных с цифровыми следами человека в сети. Ожидается, что в будущем данный метод станет основой для более точной оценки рисков идентификации и поможет разработать стандарты для безопасного использования ИИ в различных отраслях.

Ссылка: «Закон масштабирования для моделирования эффективности методов идентификации» DOI: 10.1038/s41467-024-55296-6.

© HahgaPro, 2026