Умелые цифровые фейки стали главным кибероружием 21 века.

OpenAI — это компания, которая занимается исследованиями и разработкой в области искусственного интеллекта. Она была основана в 2015 году и создана с целью сделать искусственный интеллект более доступным и безопасным для людей. Компания разрабатывает и использует нейронные сети и другие методы искусственного интеллекта для решения различных задач, включая анализ данных, генерацию текста, голоса, изображений и т.д." data-html="true" data-original-title="OpenAI" >OpenAI, Meta* – это американская технологическая компания, которая владеет и управляет такими продуктами и сервисами, как Facebook, Instagram, WhatsApp и другими.

 Компания была основана в 2004 году Марком Цукербергом и его друзьями под названием TheFacebook, Inc., в 2005 году переименована в Facebook, Inc., а в 2021 году в Meta Platforms, Inc., чтобы «отразить свой фокус на создании метавселенной» — интегрированной среды, которая связывает все продукты и сервисы компании.

 * Компания Meta и её продукты признаны экстремистскими, их деятельность запрещена на территории РФ." data-html="true" data-original-title="Meta" >Meta * и TikTok — это китайская социальная медиа-платформа, разработанная компанией ByteDance. Приложение позволяет пользователям создавать короткие видеоролики с музыкой, фильтрами и другими спецэффектами, а также просматривать, комментировать и делиться контентом с другими пользователями. За последние годы TikTok стал невероятно популярным среди молодежи и обрел миллионы пользователей по всему миру.   Однако с ростом популярности приложения возникли опасения о возможных проблемах кибербезопасности, связанных с TikTok: <ol> Данные пользователей: Как китайская компания, TikTok может передавать личные данные пользователей китайским властям, что вызывает опасения о конфиденциальности и нарушении прав частной жизни.   Цензура и пропаганда: TikTok обвиняли в цензурировании контента, критического по отношению к китайскому правительству, а также в использовании алгоритма для распространения пропагандистских материалов или содействия разжиганию раздоров в других странах.   Возможные шпионские возможности: Обсуждаются опасения о том, что TikTok может использоваться для слежки и сбора информации о пользователях, что может быть использовано китайскими спецслужбами.   Вредоносное ПО и кибератаки: Так как TikTok является популярным приложением, злоумышленники могут использовать его для распространения вредоносного ПО или проведения кибератак на устройствах пользователей.   Ответственность разработчиков: Существует опасение, что компания ByteDance может не предпринимать достаточных усилий для обеспечения безопасности пользовательских данных и предотвращения киберугроз.

 В связи с этими проблемами кибербезопасности, правительства многих стран, включая США и Великобританию, рассматривают возможность ограничения или полного запрета TikTok на своей территории. " data-html="true" data-original-title="TikTok" >TikTok активно борются с кампаниями скрытого влияния, многие из которых используют искусственный интеллект для манипуляции общественным мнением и политическими результатами. Действия компаний помогли выявить и пресечь несколько таких операций, что мы и рассмотрим подробнее ниже.

OpenAI раскрыла сразу пять операций по влиянию, связанных с различными странами, включая Китай, Иран, Израиль и Россию. Эти операции использовали ИИ-модели для создания комментариев и статей, создания фальшивых профилей в соцсетях, проведения исследований, отладки кода и перевода текстов.

Сеть под кодовым названием Bad Grammar использовала Telegram для рассылки некачественного контента, нацеленного на аудиторию в разных странах. Вторая сеть, Doppelganger, генерировала комментарии и переводила статьи для публикации на фейковых новостных сайтах в социальных сетях.

Другие выявленные сети включают сеть Spamouflage, IUVM и Zero Zeno, все из которых использовали ИИ для создания и распространения пропагандистского контента.

Meta также активно противостоит координированным кампаниям скрытого влияния. В своём квартальном отчёте о противодействии угрозам, компания сообщила об удалении почти 500 фейковых и скомпрометированных аккаунтов на Facebook* и Instagram*, связанных с операцией STOIC.

Meta также удалила сотни аккаунтов из различных стран за координированное неаутентичное поведение, направленное на влияние на общественное мнение и продвижение политических нарративов.

Помимо этого, Meta обнаружила, что многие кампании скрытого влияния используют современные цифровые инструменты, включая ИИ, для создания реалистичного текста, изображений и даже видео. Несмотря на это, компания подчеркнула, что пока не зафиксировала значительного увеличения аудитории этих кампаний.

Видеоплатформа TikTok также выявила и пресекла несколько сетей скрытого влияния. Эти сети, берущие начало в разных странах, пытались манипулировать общественным мнением и политическими результатами, используя ИИ и другие современные технологии.

В целом, платформа TikTok, находящаяся под пристальным вниманием американских властей, в последнее время стала весьма популярным местом для распространения дезинформации. Так, недавно на площадке была обнаружена сложная кампания влияния, известная как Emerald Divide, использующая ИИ для создания и распространения контента, направленного на дестабилизацию израильского общества.

Совместные усилия OpenAI, Meta и TikTok показывают важность глобального сотрудничества в борьбе с кампаниями скрытого влияния. Использование ИИ для создания и распространения дезинформации становится всё более распространённым, и технологические компании играют ключевую роль в противодействии этим угрозам.

Исследователи продолжают внимательно следить за ситуацией и делиться информацией, чтобы предотвратить дальнейшее распространение дезинформации и манипуляций в сети.

* Компания Meta и её продукты признаны экстремистскими, их деятельность запрещена на территории РФ.