

ЗЛОУПОТРЕБЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И ВОЗМОЖНОСТИ ЕГО ПРОТИВОДЕЙСТВИЯ

МОСУНОВ АНДРЕЙ, ФГБОУ ВО «ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» .КИРОВ



Современный мир стремительно меняется под воздействием новых технологий, и искусственный интеллект (ИИ) занимает в этом процессе одно из центральных мест. Однако с ростом популярности и внедрения ИИ в повседневную практику возникает ряд серьезных проблем, связанных с его злоупотреблением. Эти злоупотребления могут проявляться в различных формах, начиная от манипуляций с данными и заканчивая нарушением прав человека. В связи с этим, исследование злоупотреблений с использованием ИИ и способов их преодоления становится особенно актуальным.

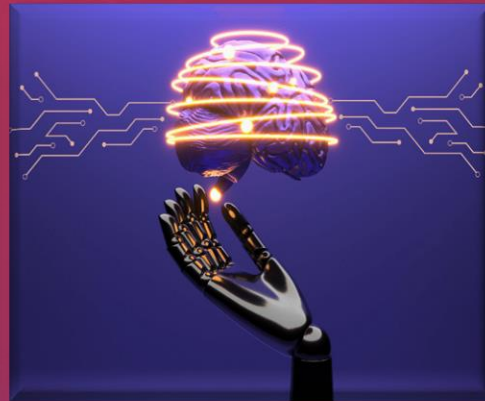


Цель исследования

- ❖ проанализировать современное состояние и особенности правового регулирования искусственного интеллекта, выявить, а также предложить возможные пути по предупреждению, совершаемых с применением ИИ злоупотреблений.

Задачи

- ❖ Анализ существующих злоупотреблений с использованием ИИ
- ❖ Разработка рекомендаций по созданию системы мониторинга и контроля за использованием ИИ.
- ❖ Проведение анализа международного опыта в области борьбы со злоупотреблением ИИ



Выводы и рекомендации

Злоупотребления с использованием искусственного интеллекта представляют серьезную угрозу для общества, затрагивая многие сферы. На современном этапе, на мой взгляд, уместны следующие шаги, позволяющие управлять рисками злонамеренного использования систем ИИ:

1. Максимальная верификация пользователей ИИ и его продуктов.
2. Любые произведения: текстовые, изображения, видеоконтент — должны иметь специальную метку о том, что при их создании использовались системы ИИ.
3. Испытания (тестирование) новых систем ИИ на предмет возможности их злонамеренного использования

Deepfake

Одним из негативных проявлений инновационной среды выступает использование методики синтеза лица и голоса, манипулируемой искусственным интеллектом, т.е. технологии Deepfake. Deepfake (дипфейк, конкатенация англ. deep learning — «глубинное обучение» и fake — «подделка») — методика синтеза изображения, основанная на искусственном интеллекте. Методика синтеза изображения используется для соединения и наложения существующих изображений и видео на исходные изображения или видеоролики.

ФИШИНГ

Фишинг — это вид интернет — мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей, таким как логины и пароли. Основными методами фишинга являются перенаправление на поддельные веб — сайты, перехват данных через вредоносные программы или злонамеренные ссылки в электронной почте, а также использование социальной инженерии для обмана пользователей и заставления их раскрывать личные данные.



ЗЛОУПОТРЕБЛЕНИЕ В СФЕРЕ БЕСПИЛОТНЫХ МОБИЛЬНЫХ СРЕДСТВ

БПМС следует рассматривать как общее понятие, объединяющее беспилотные автотранспортные средства (БПТС), летательные аппараты (БПЛА), воздушные суда (БПВС) и т.д. Использование БПЛА в противоправных целях обусловлено его несомненными преимуществами для злоумышленника по сравнению со многими другими орудиями убийства. Так, оператор может управлять дроном на довольно большом расстоянии. Другим несомненным преимуществом является анонимность оператора, а также то, что дрон может работать в автономном режиме, т.е. быть запрограммированным на определенную задачу.

