ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ПРАВО: ЭПОХА НОВАЦЕНА

Абрамова Василиса Игоревна[1]
Аспирант 1 курса Института права и национальной безопасности Тамбовского государственного университета им. Г.Р. Державина
cilvectr90@mail.ru

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЭКСТРЕМИЗМ: НОВЫЕ ВЫЗОВЫ И ПРОФИЛАКТИКА

Аннотация. В статье поднимается проблема использования искусственного интеллекта и его влияние на развитие преступных схем. Описываются возможные схемы утечки данных, а также возможность использования искусственного интеллекта для дестабилизации обстановки в стране, распространения экстремистских материалов, вербовки в преступные организации и сообщества. Выделены как плюсы, так и минусы использования искусственного интеллекта, обозначены риски, а также меры по профилактике данных негативных явлений. Предложено усовершенствование нормативных правовых актов, а также совершенствование системы мер воспитательного и пропагандистского характера путем издания различного рода брошюр и памяток по использованию искусственного интеллекта. Были сделаны выводы об ответственности за использование искусственного интеллекта как в обыденной жизни, так и в правоохранительной сфере.

Ключевые слова: искусственный интеллект, виртуальные ассистенты, чатбот, синтез речи, экстремизм.

Abramova Vasilisa Igorevna
1st year graduate student at the Institute of Law and National Security FSBEI HE TSU named after G.R. Derzhavin

ARTIFICIAL INTELLIGENCE AND EXTREMISM: NEW CHALLENGES AND PREVENTION

Annotation. The article raises the problem of using artificial intelligence and its impact on the development of criminal schemes. Possible data leakage schemes

[1] Научный руководитель: Воронин Михаил Юрьевич, директор Института международного права и правосудия Московского государственного лингвистического университета.

are described, as well as the possibility of using artificial intelligence to destabilize the situation in the country, distribute extremist materials, and recruit into criminal organizations and communities. Both the pros and cons of using artificial intelligence are highlighted, the risks are outlined, as well as measures to prevent these negative phenomena. It is proposed to improve regulatory legal acts, as well as improve the system of educational and propaganda measures by publishing various kinds of brochures and leaflets on the use of artificial intelligence. Conclusions were drawn about responsibility for the use of artificial intelligence both in everyday life and in law enforcement.

Key words: artificial intelligence, virtual assistants, chat bot, speech synthesis, extremism.

В последнее время мир захватила идея робототехники и замещения деятельности человека компьютерными технологиями. Многие вещи делают привычные действия удобными и более вариативными. Например, расплатиться на кассе стало возможно просто улыбнувшись в камеру (процесс, разумеется более сложный, охватывает биометрию человека, его разрешение на использование), а доставку еды осуществляют беспилотные роботы. В то же время, все большую популярность приобретает искусственный интеллект (далее — ИИ), который постоянно учится и вырабатывает все новые методы и стратегии. Как же правильно определить, что такое искусственный интеллект? Это «комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека»[1].

Так, после описания чего-либо несколькими предложениями, ИИ может на основе них нарисовать картину, придумать стихотворение и, даже, написать научный текст, используя различные методы и способы. Не смотря на упрощение, искусственный интеллект

[1] Федеральный закон от 24.04.2020 № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» // Собрание законодательства РФ. 2020. № 17. Ст. 2701.

несет в себе некоторые угрозы, в том числе, направленные против личности и государства. Увлеченные новой «игрушкой», люди опрометчиво загружают в новомодные чаты искусственного интеллекта свои фотографии, авторские тексты, чтобы улучшить их качество, не понимая, к чему может это привести. Сервисы генерации уже умеют создавать цифровую копию человека, проанализировав всего одну фотографию. Более того, теперь они умеют делать видеоролики на основе фотографий. Таким образом, серьезно создается прецендент, когда компьютер сможет заговорить вашим голосом и показывая ваше лицо. Таким образом, мы потихоньку подходим к тому, что безобидные дипфейки (синтез правдоподобных поддельных изображений, видео и звука при помощи искусственного интеллекта[1]) могут быть использованы не только в рамках юмористических идей, но и служить способом обезличивания реальных преступников.

В социальных сетях часто происходят взломы личных страниц, к которым уже более-менее привыкли и понимают, как действовать, если в личные сообщения приходят подозрительные ссылки или просьбы об одалживании денежных средств. Однако, в силу развития обучения искусственного интеллекта, злоумышленники могут создать ролик, видео или аудиозвонок с вашим лицом и голосом, тем самым, входя в доверие к вашим знакомым. Это же может быть использовано и в качестве дестабилизации обстановки в стране, посредством публикаций, компрометирующих видео как с известными людьми, так и с обычными гражданами. Более того, искусственный интеллект может начать работать и сам, в зависимости от функционала, который пропишут разработчики.

Чат-боты — это разговор между реальным человеком и искусственным интеллектом, который постоянно учиться и подбирает слова на основе диалога. Данный способ может стать прекрасным вариантом для распространения экстремистских течений и взгля-

[1] URL: https://encyclopedia.kaspersky.ru/glossary/deepfake/. Электронный ресурс (дата обращения: 01.04.2024).

дов путем Интернет-ресурса, а также для вербовки в преступные сообщества.

Виртуальные ассистенты «Алиса», «Маруся», «Салют» и прочие голосовые помощники — это тоже искусственный интеллект, который запоминает ваши предпочтения, поездки, покупки, формирует таргетированную рекламу персонально под вас. Однако создается угроза того, что злоумышленники каким-то образом смогут обойти защиту и начать управлять безобидным приложением, расспрашивая человека о персональных данных, а также побуждая его совершить какие-то действия. Вначале это может быть что-то действительно полезное — сходить погулять, купить еды, почитать книгу, однако в скором времени, когда человек потеряет бдительность и начнет воспринимать программу как своеобразного друга или неопасное развлечение, задания и рекомендации могут стать другими.

В связи с проведением специальной военной операции, многие фото- и видео- фиксации запрещены. А тот же взломанный виртуальный ассистент может предложить дойти до завода или места падения БПЛА (беспилотный летательный аппарат). Учитывая, что у многих включена геолокация, программе даже не нужно будет просить фотографировать эти места — по координатам местоположения злоумышленники смогут вычислить нужное им расположение.

Еще одной проблемой может служить работа искусственного интеллекта в правоохранительной сфере. Отслеживание потенциальных преступлений осуществляется посредством искусственного интеллекта, который анализирует текст по ключевым словам и специальным фильтрам. В связи с осуществлением экстремисткой деятельности посредством оправдания террористических актов, использования нацисткой атрибутики, призывы, распространение и изготовление экстремистских материалов, вопрос с правильной квалификацией, прямого умысла и реальной опасности остается открытым. Переписка людей может содержать огромное количество слов, которые включены в фильтр программы, однако огромное количе-

ство действительно преступных направленностей проходят мимо, так как преступники используют обычные слова, шифры и прочее. Таким образом, мы можем увидеть, что ИИ в большей степени может, наоборот, нагрузить систему, нежели реально провести предупреждающие мероприятия. Более того, компьютерные программы не совершенны — может произойти сбой, информация может удалиться или неожиданно оказаться в руках преступников. Также, нельзя исключать хакерские атаки на сайты структур.

Будет правильным согласиться с В.В. Бычковым, который в своей статье «Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, так и борьбы с ними» предложил использовать искусственный интеллект для «не просто распознавания экстремистских материалов, но и определение местонахождения устройств, их передавших; анализа деятельности лица, распространившего в Интернете экстремистские материалы; проверки сообщений о киберэкстремизме; отграничения экстремистских материалов от неэкстремистских, выявление деятельности экстремистских групп, организаций, сообществ; прогноз экстремистской деятельности в регионе; прогноз протестных акций по экстремистским мотивам в регионе»[1].

Таким образом, мы видим, что искусственный интеллект, разумеется, может помочь в выявлении и расследовании преступлений, но создается угроза его использования против человека, общества и государства.

Технические возможности удивляют своей скоростью распространения и доступностью. Синтезы речи, система распознавания лиц, отслеживание соблюдения правил дорожного движения — для обычного человека это все кажется будущим, которое уже наступило, средством своеобразного развлечения, однако для государ-

[1] Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, так и борьбы с ними // Вестник Московского университета МВД России. 2022. № 1. С.60-65.

ства данная деятельность может вылиться в серьезную проблему. Необходимо как можно быстрее урегулировать деятельность искусственного интеллекта, его полномочия и возможности.

Что может включать профилактика распространения экстремизма в сфере регулирования искусственного интеллекта?

Во-первых, нормативно-правовое обеспечение. Необходимо дополнить статью 12 «Недопущение использования сетей связи общего пользования для осуществления экстремистской деятельности» (либо вынести в отдельную статью) Федерального Закона «О противодействии экстремисткой деятельности» информацией об искусственном интеллекте, его деятельности и ответственности за использование ИИ в экстремисткой деятельности.

Во-вторых, меры воспитательно-пропагандистского характера. Необходимо провести качественную работу по обучению людей, показать, как стоит обращаться с искусственным интеллектом, показать, какие опасности их могут подстеречь при злоупотреблении такими технологиями. Необходимо выпустить памятки, брошюры по безопасному использованию искусственного интеллекта (как, например, делается для профилактики мошеннических действий).

В-третьих, не стоит забывать о том, что любое развитие дает множество плюсов в работе правоохранительных органов (распознавание лиц, фильтр ключевых слов), но и создает определенные риски. При неправильном использовании и сознательном недооценивании приложений и чат-ботов, искусственный интеллект может стать еще одним орудием преступников, бороться с которым будет намного сложнее.

СПИСОК ЛИТЕРАТУРЫ

1. Бычков В.В. Искусственный интеллект как средство совершения преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, так и борьбы с ними // Вестник Московского университета МВД России. — 2022. — № 1. — С. 60-65.