На основании изложенного можно резюмировать, что необходимость в исчерпывающей конкретизации в нормах уголовного закона всех возможных способов вовлечения несовершеннолетних в противоправную деятельность сегодня для правоприменителя отсутствует, а существующий открытый перечень способов имеет свои преимущества, поскольку позволит учесть всевозможные формы преступного воздействия на несовершеннолетнего. Более того, эффективная защита несовершеннолетних от вовлечения в противоправную деятельность требует комплексного подхода, включающего в себя не только совершенствование законодательной базы, но и в первую очередь усиления практической подготовки правоохранительных органов с учетом изменяющихся форм и методов преступности.

Шерстяных А.С.,

кандидат технических наук, доцент
Сибирский юридический институт МВД России (г. Красноярск)

Ложь, обман и искусственный интеллект: новые угрозы и вызовы

В настоящее время технологии искусственного интеллекта все больше и больше входят в жизнь современного человека. Сферы его использования достаточно разнообразны: от создания забавного видео до использования в профессиональной деятельности различных специалистов – маркетинговые компании используют технологии искусственного интеллекта при создании текстов и сценариев рекламных роликов, программисты – для автоматизации рутинных задач, ускоряя разработку программного обеспечения. Известны даже примеры использования технологий искусственного интеллекта при индивидуализации процесса обучения. Так, российская IT-компания CDO Global предлагает продукт DeepCheckUP, который представляет собой цифровое решение на основе искусственного интеллекта, позволяющее анализировать образовательные потребности пользователя и предоставляет персонализированный план обучения[1].

Однако технологии искусственного интеллекта также активно используют мошенники для создания более изощренных схем обмана.

Рассмотрим основные методы обмана пользователей с использованием технологий искусственного интеллекта.

1. Создание поддельных аккаунтов и ботов, которые имитируют поведение реальных людей. Это может быть точная копия страницы реального человека, чтобы попросить у его знакомых денег, для распространения спама, проведения фишинговых атак и других видов мошенничества. Кроме того, технологии искусственного интеллекта могут быть использованы для создания фальшивых отзывов и рекомендаций, чтобы ввести в заблуждение потенциальных покупателей. Фальшивыми могут оказаться аккаунты и госорганов, предназначенные для выманивая у посетителей денег за предоставление тех или иных услуг.

Мошенники создают фейковые страницы на сайтах знакомств, стараясь войти в доверие жертве с целью выманивая денег или персональной информации. На YouTube-канале в прошлом году появился ролик, в котором представлен полностью автоматизированный чат-бот, который вступает в прямой диалог с человеком. Жертва полагает, что общается со своим возлюбленным – военным врачом, находящимся за границей. Однако на самом деле она говорит с чат-ботом, контролируемым мошенником. Эти чат-боты позволяют мошенникам свободно общаться с жертвой, имитируя поведение реального человека, что значительно повышает правдоподобность аферы. Эксперты предупреждают, что к 2025 году использование полностью автономных чат-ботов с искусственным интеллектом станет обычным делом[2].

2. Создание фальшивых новостей и дезинформации. С помощью технологий искусственного интеллекта создаются фальшивые статьи, стиль повествования которых достаточно достоверно соответствует текстам

[1] Cdo-global : официальный сайт. URL: https://www.cdo-global.ru/ products/ (дата обращения: 03.01.2025).

[2] Пять трендов ИИ-мошенничества на 2025 год // Финам : официальный сайт. URL: https://www.finam.ru/publications/item/pyat-trendov-ii-moshennichestva-na-2025-god-20250106-1200/ (дата обращения: 13.01.2024).

конкретных журналистов. Современные модели позволяют имитировать структуру реальных новостных материалов, например, создавать фейковые цитаты или подделывать фактические детали, что делает их трудноотличимыми от настоящих новостей для широкой аудитории. Такие статьи могут быть распространены через социальные сети и другие платформы. Таким образом, читая определенную публикацию, пользователь уже не может быть уверен, не только в правдивости освещения события, но и в факте его существования. Это может привести к формированию ложных представлений о событиях и явлениях, а также к манипулированию общественным мнением.

Фальшивыми могут оказаться не только публикации, но и целые издания. Например, газета «ПроЗдоровье», рекламирующая опасные лекарства и различные методы лечения. Эта газета бесплатно распространяется во многих регионах России, попадает в почтовые ящики жильцов. В газете можно найти фотографии и рекомендации врачей из разных стран: России, Израиля, Германии и Швеции. Также там представлены положительные отзывы пожилых людей, которые уже испытали рекламируемые препараты на себе[1].

3. Использование технологий ИИ при создании дипфейков. Слово «deepfake» произошло от сочетания слов «deep learning» (глубокое обучение) и «fake» (фальшивка, подделка). Оно используется для обозначения технологии создания фото- и видеоматериалов с помощью искусственного интеллекта и нейронных сетей, которые имитируют внешность и голос реальных людей[2]. Все большую популярность набирают фотографии и видеоролики, сгенерированные с помощью нейросети. Современные технологии позволяют создавать достаточно реалистичную картинку, порой неотличимую от реального фото- или видеоизображения. Даже появилась новая профессия – нейрофотограф. Злоумышленники получают доступ к фото-, аудио- или видеоконтенту, разрешенного к просмотру посетителям страницы в соцсетях, и на их основе синтезируют новые с нужным контекстом. Такие фальшивые медиа-материалы придают убедительности действиям мошенников и повышают вероятность успеха атаки. Для создания дипфейков, по мнению специалистов, достаточно короткого 20-30 секундного видео- или аудиофайла.

Мошенники используют самые разные рычаги давления: например, отправляют видео от родственника, якобы попавшего в беду, выманивая деньги для решения проблемы. Или контент интимного характера, которым начинают шантажировать.

Это может быть запись обращения президента или губернатора, объявляющего о новых выплатах, для получения которых нужно пройти по ссылке или заплатить налог. Особенно распространены дипфейки с известными личностями, так как фото и видео с ними есть в свободном доступе, и их часто используют для обучения нейросети. Достаточно вспомнить прямую линию с президентом России Владимиром Путиным, когда студент СПбГУ с помощью дипфейка задал видеовопрос в образе президента. Также, в качестве примера можно привести нашумевшие фальшивые видеоролики с губернатором Курской области и Марией Захаровой, которые появились в начале вторжения Вооруженных сил Украины в Курскую область.

Ведущие производители программного обеспечения в области безопасности внедряют меры по защите и проверке подлинности данных. Но на сегодня самая надежная защита – это соблюдение правил кибербезопасности:

– использование дополнительного канала связи. Если пришло аудио- или видеосообщение от знакомого вам человека, то лучше связаться с ним другим способом (позвонить с другого номера или написать в другом мессенджере), таким образом вы сможете убедиться в подлинности отправителя;

– если поведение звонившего показалось вам по какой-то причине подозрительным, используйте контрольные вопросы, ответы на которые известны только вам (например, о конкретном событии из прошлого);

– при общении с организациями (банками, представителями органов власти или социальной сферы и пр.) используйте

[1] Нижегородцев вновь предупредили о псевдогазете с фальшивыми лекарствами // Нижегородская правда : новостное интернет-издание. URL: https://pravda-nn.ru/news/ nizhegorodtsev-vnov-predupredili-o-psevdogazete-s-falshivymi-lekarstvami/ (дата обращения: 13.01.2024).

[2] Аносов А.В. Дипфейк как инструмент экстремистской деятельности // Экстремальные ситуации, конфликты, социальное согласие : . сборник научных трудов по материалам XXVI международной научно-практической конференции «Современное обеспечение общественной безопасности: теоретические, правовые и организационные проблемы». М., 2024. С. 25-32.

контакты, указанные на их официальных сайтах или в официальных приложениях;

– старайтесь не выкладывать в свободный доступ видео, аудиозаписи и другие материалы, по которым может быть сгенерирован ваш образ или голос. Если это нужно по работе или для общения в соцсетях, настраивайте приватность и доступ только для близких или проверенных людей.

Дипфейки – это не просто временное явление, а современная технология, которая непрерывно будет развиваться и совершенствоваться. Поэтому необходимо сохранять бдительность и постоянно повышать уровень своей цифровой безопасности. Это позволит вам не попадаться на уловки мошенников.

В целом, анализ методов и технологий обмана пользователей с использованием ИИ подчеркивает необходимость постоянного совершенствования мер по борьбе с этим видом мошенничества. Это включает в себя разработку новых технологий, повышение осведомленности пользователей и сотрудничество между различными заинтересованными сторонами, такими как правоохранительные органы, компании и организации гражданского общества.

Апарина Н.А.

Университет прокуратуры Российской Федерации (Москва)

Проблемы противодействия преступности в сфере коллективных инвестиций

Столкнувшись с беспрецедентными санкциями, направленными непосредственно на российский финансовый сектор, экономика Российской Федерации показала свою устойчивость к внешним шокам и способность преодолевать кризисные явления даже еще более острые, чем те, с которыми сталкивалась в 2014-2015 гг. и в 2020 г. В то же время основной задачей развития российского финансового рынка в этих условиях становится усиление его роли в финансировании ускоренной трансформации российской экономики с опорой в первую очередь на внутренние источники финансирования инвестиций[1].

Учитывая заложенный вектор развития государственной политики, государство проявляет значительный интерес к рынку коллективных инвестиций, поскольку коллективное инвестирование позволяет привлечь в экономику средства не только крупных инвесторов, но и населения. Так, Президент России поручил Правительству Российской Федерации принять меры, направленные на привлечение граждан к участию в программе долгосрочных сбережений, формируемых негосударственными пенсионными фондами, с учетом необходимости обеспечения объема вложений граждан не менее 250 миллиардов рублей в 2024 г. и не менее 1% валового внутреннего продукта в 2026 г.[2] Указом Президента Российской Федерации от 7 мая 2024 г. № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» установлена задача по обеспечению роста капитализации фондового рынка не менее чем до 66 процентов валового внутреннего продукта к 2030 г. и до 75% валового внутреннего продукта к 2036 г.[3]

Таким образом, в настоящий период с учетом интереса государства к рынку коллективных инвестиций ощущается потребность в криминологическом прогнозировании безопасности в сфере деятельности негосударственных субъектов экономической деятельности.

В законодательстве отсутствует понятие коллективного инвестирования, нет указаний на общие принципы и подходы к его регулированию. В науке под коллективными инвестициями предлагается понимать механизм передачи денег и активов частных лиц в доверительное управление профессиональным менеджерам, управляющим средствами тысяч инвесторов как единым портфелем, в

[1] Стратегия развития финансового рынка Российской Федерации до 2030 года : утв. распоряжением Правительства Российской Федерации от 29.12.2022 № 4355.

[2] Официальный сайт Президента России // URL: http://www.kremlin.ru/acts/ assignments/orders/73267 (дата обращения: 20.01.2025).

[3] О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года : Указ Президента РФ от 07.05.2024 № 309.