УДК 343

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И УГОЛОВНОЕ ПРАВО

И. Н. Архипцев
Белгородский юридический институт
МВД России имени И. Д. Путилина,
доцент кафедры уголовно-правовых дисциплин,
кандидат юридических наук
e-mail: ArhiptsevIN@yandex.ru

А. В. Сарычев
Белгородский юридический институт
МВД России имени И. Д. Путилина,
преподаватель кафедры тактико-специальной подготовки
e-mail: w0773@yandex.ru

Аннотация. *Авторами установлено, что в зависимости от преследуемых его разработчиком (создателем) целей, искусственный интеллект может использоваться не только в общественно полезных целях, но и как средство в достижении преступного результата.*
Ключевые слова: *искусственный интеллект, уголовное право, технологии искусственного интеллекта, предупреждение.*

Annotation. *The authors found that, depending on the goals pursued by its developer (creator), artificial intelligence can be used not only for socially useful purposes, but also as a means to achieve a criminal result.*

Keywords: *artificial intelligence, criminal law, artificial intelligence technologies, prevention.*

Искусственный интеллект и технологии, связанные с его применением, в настоящее время все больше проникают в нашу повседневную жизнь. И этот процесс порой происходит незаметно. Уже сейчас «умные» машины выполняют различные функции, начиная от роботов, анализирующих прогноз погоды, изменение физических данных человека, составляющих индивидуальное расписание дня, и заканчивая автономным управлением транспортными средствами, нанороботами, используемыми в медицине, роботами, выполняющими функции педагога, полицейского и т. д.

При этом, как и любая другая новая технология или изобретение, как показывает историческая практика, искусственный интеллект и элементы, с ним связанные, к сожалению, могут использоваться злоумышленниками в своих преступных целях. Так, по данным международных организаций, в последнее время в мире увеличивается доля мошенничеств, совершенных с применением искусственного интеллекта. Европолом совместно с аналитиками компании Trend Micro, специализирующейся на кибербезопасности, и Межрегиональным

научно-исследовательским институтом Организации Объединенных Наций по вопросам преступности и правосудия в 2020 году был подготовлен доклад «Злонамеренное использование и злоупотребление искусственным интеллектом». В нем, в частности, указывается, что одним из популярных видов мошенничества на сегодняшний день является дипфейк — поддельные фото- и видеоизображения реального человека. Кроме того, в докладе указываются возможные риски дальнейшего использования искусственного интеллекта в преступных целях: искусственный интеллект может использоваться в создании «умных» программ-вымогателей, генерации чит-кодов в компьютерных играх, позволяющих зарабатывать деньги, в имитации голоса или стиля письма конкретного человека для совершения мошеннических действий [1].

В связи с тем, что человечество в лице ведущих государств мира, в том числе и Российской Федерации как его неотъемлемой части, находится в настоящее время на пути создания нового индустриального общества (Industrie 5.0), в котором определяющее, если не главное значение будут в будущем иметь связанные с информацией и созданные на ее основе сети, технологии, продукты и другие важные компоненты такого общества. Остро встает вопрос об обеспечении надлежащей защиты критически важной информационной составляющей деятельности предприятий, учреждений и организаций.

Далее кратко рассмотрим наиболее распространенные сейчас преступления, которые совершаются с применением искусственного интеллекта:

1. Актуальным направлением преступных посягательств, например, на объекты энергетики, а также топливно-энергетического комплекса является использование в преступных целях автономных боевых дронов. Как указывает Г. Г. Камалова, искусственные интеллектуальные системы могут быть использованы для совершения разнообразных преступлений, включая причинение смерти или вреда здоровью человека; нарушение права на неприкосновенность частной жизни; незаконное получение или неправомерное разглашение охраняемой законом тайны; нарушение правил охраны труда; мошенничество; нарушение безопасности дорожного движения и эксплуатации транспорта; террористический акт; нарушение правил обращения с оружием и предметами, представляющими повышенную опасность для окружающих; нарушение правил оборота наркотических и психотропных веществ; преступления в сфере компьютерной информации; иные [2, с. 383]. Несомненно, к приведенному списку с полным правом следует отнести и посягательства на объекты энергетики, которые однозначно представляют повышенную общественную опасность, и возможность их применения для совершения актов незаконного вмешательства (террористических актов, диверсий, нанесения непоправимого ущерба и устранения конкурирующих организаций), а также другие сферы преступного при-

менения приборов, функционирующих на основе искусственного интеллекта. Так, большой мировой резонанс в 2019 году вызвала атака на нефтяные месторождения Саудовской Аравии, которая была совершена с использованием беспилотных летательных аппаратов [3]. Несмотря на то, что в приведенном примере беспилотные летательные аппараты, скорее всего, управлялись людьми, уже сейчас подобное способен совершить автономный робот. Возможно уже в недалеком будущем такой признак, как использование в процессе совершения преступления (в том числе и при совершении посягательств на объекты топливно-энергетического комплекса) технологий, машин, приборов, созданных на основе и принципах искусственного интеллекта, будет законодательно прописан в качестве отягчающего наказание обстоятельства в Уголовном кодексе.

2. Преступления, связанные с секс-роботами. Не затрагивая всех правовых, а также морально-этических проблем их использования, которые возникают автоматически с их созданием и эксплуатацией, в силу ограниченности объема нашего исследования отметим, что данная сфера сейчас очень активно развивается в мире, и, по нашим прогнозам, она и дальше будет развиваться опережающими темпами. Так, И. С. Алихаджиева справедливо полагает, что в связи с прогнозом дальнейшего развития этого вида легального предпринимательства возникает ряд вопросов, касающихся налогообложения, норм морали, защиты прав потребителей и роботов (искусственный интеллект), уголовной ответственности за оказание услуг, не отвечающих требованиям безопасности (к примеру, за заражение инфекцией, передающейся половым путем, при непроведении дезинфекции куклы, особенно в период пандемий) и др. [4, с. 163–164].

Дэвид Леви мотивирует возможность использования секс-роботов инвалидами, социопатами, психически нездоровыми и другими категориями людей, что окажет на них позитивное воздействие [5]. Однако, как показывает практика, во-первых, услугами секс-роботов пользуются, как правило, обеспеченные слои населения, и, во-вторых, вряд ли секс-роботы снимут основные проблемы этих людей, а скорее всего, вызовут у них еще большую зависимость, теперь уже от самих секс-роботов.

Как подтверждение сказанного нами выше, открывшейся проблемой в этой сфере стал выпуск в странах Юго-Восточной Азии секс-кукол, которые изображают несовершеннолетних. Сейчас ряд стран уже в уголовном порядке преследуют лиц, эксплуатирующих такие куклы, например, Великобритания, Норвегия, Австралия. Так, в Австралии житель Брисбена был приговорен к двум годам тюрьмы за владение секс-куклой или другим предметом, похожим на ребенка в возрасте до 18 лет, попытку завладеть секс-куклой в виде несовершеннолетнего и хранение материалов для эксплуатации детей [6]. Не ис-

ключено, что в будущем выпуск «умных» секс-роботов несовершеннолетних будет продолжаться (только на нелегальной основе) и подогреваться нездоровыми желаниями таких людей. Поэтому мы присоединяемся к позиции В. С. Соловьева, который предлагает установить законодательный запрет на реализацию и использование такой продукции [7, с. 54].

3. В настоящее время мир столкнулся с новой проблемой в информационной сфере, которая получила название дипфейк. Ее краткое объяснение состоит в том, чтобы использовать нейросеть для создания принципиально новых изображений (фото- или видеоизображений). Технология дипфейков используется в архитектуре, дизайне, создании игр, киноиндустрии, шоу-бизнесе и других сферах, где задействованы большие объемы данных. Например, с ее помощью в России была создана полностью цифровая копия известной актрисы советского кино Людмилы Гурченко, которая могла обдуманно отвечать на вопросы аудитории голосом актрисы [8]. С помощью технологии дипфейков на основе ряда алгоритмов машинного обучения можно «наложить» профиль с изображением любого человека на любое другое тело или изображение, причем реальное изображение и поддельное изображение человека будут практически неотличимы для обычного пользователя. Как часто происходит со всем хорошим и революционным, данная технология стала использоваться некоторыми людьми при создании видеороликов и изображений порнографического содержания, что не могло не вызвать обоснованную тревогу и опасения среди правоохранительных органов. В частности, первым государством, точнее штатом США, где впервые была введена уголовная ответственность за создание и распространение дипфейков стала Калифорния [9, с. 119–122]. В основном сфера действия данного закона вначале ограничивалась политическими дипфейками, в дальнейшем была установлена ответственность за создание и опубликование сексуально откровенных материалов без согласия участников. По пути запрета политических дипфейков пошел Китай.

Мы полностью поддерживаем мнение М. А. Желудкова, что, с одной стороны, подобная технология позволяет развивать системы искусственного интеллекта, в частности при реализации программы «Безопасный город» при распознавании личности. С другой стороны, использование биометрических данных в этой методике, а именно голоса и лица человека, позволяет преступникам понизить уровень защищенности населения перед угрозой подмены их фото- и видеоизображений при незаконном получении кредитов, переоформлении недвижимости, дискредитации любого юридического и физического лица [10, с. 266].

4. Кибермошенничества. Дипфейки. Уязвимость банковских приложений. Та же самая технология дипфейков может применяться мошенниками

при создании ложного аудио- или видеоконтента с изображением людей. С ростом информационных технологий, особенно в период пандемии COVID-19, такие угрозы, увы, становятся реальностью. Так, например, в Великобритании руководителю компании позвонил якобы деловой партнер, который попросил перевести крупную сумму денег. Как в дальнейшем было выяснено Скотленд-Ярдом, голос бизнесмена был сгенерирован искусственным интеллектом, а за совершением преступления стоял мошенник [11]. Другим опасным явлением в сети Интернет стали «умные ботнеты». Как следует из доклада Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России (ФинЦЕРТ), итогом исследования злоумышленниками мобильного приложения поднадзорной организации и системы ДБО стало хищение денежных средств клиентов путем совершения операций без согласия с использованием в качестве транспорта платежной системы. Переводы были осуществлены двумя авторизованными клиентами поднадзорной организации через подмену номера счета отправителя на номер счета другого клиента банка (жертвы). Подмена произведена в сообщении, направленном из мобильного приложения в поднадзорную организацию после подтверждения платежа авторизованным клиентом. Указанные авторизованные клиенты организации в предыдущие дни провели успешную атаку по использованию недокументированной возможности API-интерфейса ДБО, в процессе которой смогли перебором получить номера счетов жертв. Злоумышленники, используя режим отладки мобильного приложения, подменяют в исходящем на сервер ДБО сообщении о подтверждении платежа значение поля «Номер счета отправителя» на номер счета жертвы. При отправке сообщений на стороне сервера ДБО не осуществлялась проверка принадлежности счета списания (поле CustT_Contract_RID) авторизованному пользователю, что позволило злоумышленникам осуществить подмену.

В ходе формирования распоряжения на перевод денежных средств СМС-сообщение с кодом подтверждения операции направлялось авторизованному пользователю. То есть все подтверждения злоумышленники осуществляли от лица своей легитимной учетной записи — клиента банка. Пострадавшие получали СМС-уведомления только по факту проведения операции после списания денежных средств со счета [12].

1. Exploiting AI. How Cybercriminals Misuse and Abuse AI and ML [Electronic resource]. URL: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml (date of access: 12.03.2022). Перейти к источнику Вернуться к статье

2. Камалова Г. Г. Некоторые вопросы уголовно-правовой ответственности в сфере применения систем искусственного интеллекта и робототехники // Вестн. Удмурт. ун-та. Сер. Экономика и право. 2020. Т. 30. Вып. 3. С. 382–388. Вернуться к статье

3. В Саудовской Аравии беспилотники атаковали нефтепровод [Электронный ресурс]. URL: https://ria.ru/20190514/1553476581.html (дата обращения: 12.03.2022). Перейти к источнику Вернуться к статье

4. Алихаджиева И. С. О новых тенденциях современной секс-индустрии и ее криминологических рисках // Актуальные проблемы российского права. 2021. Т. 16. № 4. С. 163–164. Вернуться к статье

5. Levy D. Love and Sex with Robots. The Evolution of Human-Robot Relationships [Electronic resource]. Imprint : Harper Perennial. 2007. 352 p. URL: https://www.harpercollins.com/9780061359804/love-and-sexwith-robots (date of access: 12.03.2022). Перейти к источнику Вернуться к статье

6. Педофила из Австралии «застукали» дома с похожими на детей куклами [Электронный ресурс]. URL: https://nation-news.ru/619751-pedofila-iz-avstralii-zastukali-doma-s-pohozhimi-na-detei-kuklami (дата обращения: 12.03.2022). Перейти к источнику Вернуться к статье

7. Соловьев В. С. Криминологические риски цифросексуализма // Вестн. Рос. правовой акад. 2020. № 3. С. 54. Вернуться к статье

8. Ведущей «Битвы престолов» Валерия Комиссарова станет Людмила Гурченко [Электронный ресурс]. URL: https://rg.ru/2020/02/11/vedushchej-bitvy-prestolov-valeriia-komissarova-stanet-liudmila-gurchenko.html (дата обращения: 12.03.2022). Перейти к источнику Вернуться к статье

9. Дельфино Р. А. Порнографические дипфейки: следующий трагический акт феномена «порно из мести» и необходимость принятия уголовного закона на федеральном уровне // Актуальные проблемы экономики и права. 2020. Т. 14. № 1. С. 119–122. Вернуться к статье

10. Желудков М .А. Изучение влияния новых цифровых технологий на детерминацию мошеннических действий (технология deepfake) // Развитие наук антикриминального цикла в свете глобальных вызовов обществу : сб. тр. по материалам всерос. заочной науч.-практ. конф. с междунар. участием. Саратов, 2021. С. 266. Вернуться к статье

11. Технология с вашим лицом. Как бороться с дипфейками [Электронный ресурс]. URL: https://www.dp.ru/a/2020/02/17/Tehnologija_s_vashim_licom (дата обращения: 12.03.2022). Перейти к источнику Вернуться к статье

12. Отчет «Основные типы компьютерных атак в кредитно-финансовой сфере в 2019–2020 годах» [Электронный ресурс]. С. 32. URL: http://www.cbr.ru/Collection/Collection/File/32122/Attack_2019-2020.pdf (дата обращения: 12.03.2022). Перейти к источнику Вернуться к статье