УДК 343.9

Т.И. Дудко

УГРОЗЫ ИСПОЛЬЗОВАНИЯ НОВЫХ ТЕХНОЛОГИЙ С ЭЛЕМЕНТАМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

В центре любого значительного изменения общественной жизни находится та или иная технология. Развитие информационно-коммуникационных и цифровых технологий обусловило трансформацию направлений человеческой деятельности. Резкий технологический скачок определил формирование специфичной информационной среды, в которой отмечается экспоненциальной рост генерируемых человечеством данных. Именно в этой информационной среде современный человек создает и развивает новые идеи и направления, которые впоследствии задают тенденции эволюции общества.

Общество вступило в постиндустриальную стадию развития, в которой важнейшим ресурсом и движущей силой прогресса становится информация и знания. Человечество с каждым днем становится все более восприимчивым к быстро меняющимся технологиям. Технологическое мировосприятие задает образцы рациональной и целенаправленной деятельности, в соответствии с которыми организуются едва ли не все сферы жизнедеятельности. Возложенные надежды на дальнейшее совершенствование человеческой деятельности исследователи связывают с развитием нанотехнологий, генно-инженерных, аддитивных технологий, технологий искусственного интеллекта.

Наиболее перспективными и при этом предельно неоднозначными являются технологии, базирующиеся на принципах и методах искусственного интеллекта. В настоящее время идея создания разумных и мыслящих компьютеров, способных превзойти человека по своим интеллектуальным способностям для решения технологических, промышленных и иных задач, обрела новый виток развития. За последние несколько лет технологии, основанные на искусственном интеллекте, из числа сугубо технологических вопросов перешли в разряд наиболее обсуждаемых вопросов развития мирового сообщества. Это обстоятельство обусловлено целым рядом факторов, среди которых выделяются: широкое распространение вычислительной техники, рост вычислительных мощностей программно-аппаратных комплексов, общедоступность больших объемов информации, а также изменение взглядов к рассматриваемой технологии по причине стремительного роста ее капитализации.

Технологии с элементами искусственного интеллекта развиваются стремительно и интенсивно и уже активно применяются в экономике, промышленности, медицине, образовании. Использование искусственного интеллекта оказывает положительное влияние на многие сферы деятельности, упрощая отдельные производственные процессы, однако одновременно возникают новые вызовы и угрозы его применения. В связи с этим актуальными становятся вопросы осмысления таких рисков и угроз.

Наиболее уязвимой в последние годы становится сфера получения достоверной информации в цифровом пространстве. Как известно, само по себе наличие информации и возможность доступа к ней – благо для современного человека. Вместе с тем не всегда получаемая информация может использоваться во благо. Возможность свободного доступа к информации порождает различного рода негативные воздействия на нее, которые реализуются новыми технологическими способами.

Так, в настоящее время в цифровом пространстве используется новая технология, размывающая границы между фактом и вымыслом. Она основана на применении алгоритмов искусственного интеллекта, в частности искусственных нейронных сетей. На основании этой технологии создаются дипфейки (от англ. deep learning – глубокое обучение и fake – фальшивый) – обработанные цифровые фото- и видеоизображения, которые человеком воспринимаются как оригинальные.Технология дипфейков обладает огромными потенциальными возможностями в модификации цифрового материала.

Процесс создания дипфейка предполагает работу по редактированию изображения, в котором части или элементы заменяются искусственным интеллектом на желаемые образы посредством алгоритмов генеративно-состязательной нейронной сети [1]. Генеративно-состязательные нейронные сети используют две нейронные сети: одну для создания поддельного цифрового образа, другую – для его оценки. Первая нейронная сеть обучается на реальных изображениях объекта, генерирует все более точные копии изображения этого объекта с изменениями и пытается обмануть вторую нейронную сеть, заставляя ее поверить, что копия изображения объекта с изменениями и есть оригинал. В результате такого состязания две нейронные сети совершенствуют свои навыки, и такая постоянно самообучающаяся и самосовершенствующаяся система непосредственно творит дипфейки.

Принимая во внимание то, что отдельные инструменты искусственного интеллекта имеют открытый код и доступны в цифровом пространстве широкому кругу лиц, а также учитывая широкое качественно-количественное разнообразие исходного цифрового материла (фотовидеоизображений), хранящегося в сети Интернет, можно сделать вывод о том, что в настоящее время убедительный поддельный цифровой материал создать стало проще, чем когда-либо прежде, и, по

всей вероятности, станет более доступно в ближайшем будущем. Соответственно, дипфейки могут нести серьезную потенциальную угрозу для различных сфер жизнедеятельности.

Уже сегодня технология дипфейков активно используется в преступных целях. Так, по информации компании Deeptrace, занимающейся кибербезопасностью, в 2019 г. в сети Интернет насчитывалось свыше 14 600 единиц видеодипфейков, которые в подавляющем большинстве представляют собой порноролики с изображением известных актеров [2]. Кроме того, серьезные опасения вызывает использование технологии дипфейков в политических целях, поскольку создание политических дипфейков может быть направленно на подрыв авторитета, имиджа и доверия к определенному политику, политической партии или даже государству.

Таким образом, можно констатировать, что потенциал использования искусственного интеллекта в интересах человечества колоссален. Вместе с тем, если не предпринять соответствующие меры контроля в ближайшем будущем, преступники, прибегнув к технологическим разработкам, могут причинить значительный вред не только отдельному человеку, но и обществу в целом. Поэтому в целях минимизации криминогенных факторов необходим тщательный анализ потенциальных рисков человеческой деятельности в условиях соответствующего технологического уклада развития, а также разработка надлежащих мер защиты человека, общества и государства от возникающих угроз.

1. Deepfake // Википедия. URL: https://ru.wikipedia.org/wiki/Deepfake (дата обращения: 29.09.2020).

2. Как швейцарские ученые хотят помешать нейросетям копировать реальность // Swiswissinfo.ch. URL: https://www.swissinfo.ch/rus/45605836 (дата обращения: 29.09.2020).

УДК 343.980

В.И. Елётнов

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ТРАДИЦИОННЫХ И РАЗВИВАЮЩИХСЯ ОТРАСЛЕЙ КРИМИНАЛИСТИЧЕСКОЙ ТЕХНИКИ

В настоящее время идет непрерывный поступательный процесс внедрения в сложившиеся отрасли криминалистической техники современных достижений естественных и технических наук, совершенствования собственных технико-криминалистических средств, создания новых

методик исследования криминалистических объектов. Дополнение этого раздела криминалистики новыми научными знаниями не может не сопровождаться возникновением теоретических пробелов, наличием спорных положений. Остановимся на них более детально в рамках отдельных отраслей криминалистической техники.

Криминалистическая фотография и видеозапись. В настоящее время в проблемном поле этой отрасли находятся такие вопросы, как доказательственное значение цифровых снимков и видеозаписи; конкретизация норм законодательства, регламентирующих использование цифровых камер в уголовном процессе; работа с графическими редакторами и др. Особенно остро стоят вопросы противодействия фальсификации фото- и видеофайлов и правомерности применения графических редакторов для обработки изображений и их последующего использования в деятельности правоохранительных органов. Учеными предлагаются различные решения обозначенных проблем, а именно: применение устройств, работающих по принципу «после съемки – сразу на печать» [1, с. 133], незамедлительный перенос файлов на неперезаписываемый CD-диск (иные аналогичные носители информации), использование правовых средств защиты и др. [2; 3, с. 292–293]. Однако единое мнение по этому вопросу до сих пор не выработано.

С положениями криминалистической фотографии и видеозаписи тесно связаны вопросы криминалистической фоноскопии. Современный уровень развития фоноскопии, научные основы которой находятся в процессе формирования, характеризуется наличием ряда проблем, прежде всего теоретического характера. Во-первых, все еще отсутствует четкое разграничение предмета ее исследования, содержание которого составляют такие разные направления, как идентификация личности по голосу, идентификация звукозаписывающих устройств, исследование признаков монтажа, копирования записи и др. Во-вторых, в криминалистической науке наблюдается некоторая терминологическая разобщенность относительно фоноскопии и фоноскопической экспертизы. Для их обозначения употребляются термины «криминалистическая акустика», «вокалографическая экспертиза», «криминалистическое исследование фонограмм», «криминалистическая видео- и звукозапись» и т. п. [4]. В криминалистической литературе также отсутствует единое мнение относительно места криминалистической фоноскопии в системе криминалистической техники: одни авторы рассматривают ее обособленно [5], другие – совместно с криминалистической фотографией и видеозаписью [6].

Трасология. Она на современном этапе развития криминалистической техники является ее базовой отраслью со сложившейся системой,