УДК 34.096
DOI: 10.18384/2310-6794-2021-3-54-64

О НЕОБХОДИМОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ДИПФЕЙК КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Киселёв А. С.
Московский государственный областной университет,
141014, Московская обл., г. Мытищи, ул. Веры Волошиной, д. 24, Российская Федерация
Финансовый университет при Правительстве Российской Федерации
125057, г. Москва, Ленинградский пр-т, д. 55, Российская Федерация

Аннотация
Цель. Исследовать сущность и правовую природу «дипфейков» – новейшей технологии, основанной на применении генеративно-состязательных нейросетей, способной в скором будущем стать угрозой национальной безопасности, а также изучить уровень правового регулирования искусственного интеллекта в России и за рубежом.
Процедура и методы. В статье рассмотрены конкретные примеры применения дипфейков на выборах в США. При проведении исследования применены методы анализа и синтеза, дедукции и индукции, обобщения, абстрагирования, формально-юридический и сравнительно-правовой.
Результаты. В ходе работы выявлены сущность и основные виды дипфейков, применяемых в противоправных целях, сделан вывод о необходимости принятия международной конвенции о регулировании дипфейков.
Теоретическая и/или практическая значимость. Результаты исследования вносят вклад в теорию государства и права и теорию информационного права.

Ключевые слова: дипфейк, искусственный интеллект, информационные технологии, генеративно-состязательная нейросеть, национальная безопасность

ON THE EXPANSION OF LEGAL REGULATION IN THE FIELD OF ARTIFICIAL INTELLIGENCE: DEEPFAKE AS A THREAT TO NATIONAL SECURITY

A. Kiselev
Moscow Region State University
24 Very Voloshinoi ul., Mytishchi 141014, Moscow region, Russian Federation
Financial University under the Government of the Russian Federation,
55 Leningradsky prosp., Moscow 125057, Russian Federation

Abstract
Aim. To explore the essence and legal nature of "deepfakes", the latest technology based on the use of generative-adversarial neural networks, which in the near future can become a threat to national security, as well as to study the level of legal regulation of artificial intelligence in Russia and abroad.
Methodology. The article discusses specific examples of the use of deepfakes in the US elections. Methods of analysis and synthesis, deduction and induction, generalization, abstraction, formal legal, comparative legal methods were used in the research.
Results. In the course of the work, the essence and main types of digs used for illegal purposes were identified, the conclusion was made that an international convention on the regulation of digs should be adopted.

© CC BY Киселёв А. С., 2021.

Research implications. The results of the research contribute to the theory of state and law in the theory of information law.

Keywords: deepfake, artificial intelligence, information technology, generative-adversarial neural network, national security

Введение

Ещё в начале XXI в. было сложно представить, что через 20 лет у каждого пятого жителя Земли будет по мобильному телефону, а в развитых странах, например в США, мобильные устройства будут у 75% населения, в России – около 65%. Подобная статистика говорит о том, что уровень цифровизации за два десятилетия текущего столетия значительно вырос. Отечественные и зарубежные авторы убеждены, что в ближайшие годы всё большее количество сфер нашей жизни будут преобразовываться благодаря цифровизации [12, с. 35–39; 13, с. 27–37; 14, с. 12–23], соответственно, будут появляться новые цифровые угрозы национальной безопасности. Для того, чтобы научиться им противостоять, требуются всецелое теоретическое осмысление их сущности, свойств, функциональных особенностей, а также определение правового положения технологических новшеств, законодательное закрепление пределов их использования и ответственности за неправомерные действия.

Цель настоящего исследования состоит в теоретико-правовом и сущностном изучении дипфейков – новых технологий, с помощью которых уже сегодня совершаются преступления и правовое регулирование которых в настоящее время, к сожалению, отсутствует. Задачи: раскрыть определение дипфейка, изучить его разновидности, сферы применения; определить, кто и каким образом может использовать дипфейки; попытаться оценить уровень опасности и угрозы для национальной безопасности; предложить пути решения проблемы в будущем.

Основные методы исследования: формально-логический метод будет применён при обобщении признаков и изучении внешней и внутренней формы дипфейка, сравнительно-правовой метод будет использован при изучении зарубежного опыта законодательного регулирования дипфейков, с помощью анализа и синтеза будет раскрыто содержание дипфейка как единой категории, так и элементов, составляющих дипфейк, с помощью индукции будет произведены сбор информации и осуществлены выводы, дедуктивный метод послужит при выявлении опасных и вредоносных признаков дипфейка, с помощью моделирования будут представлены ситуации, которые могут произойти без осуществления правового регулирования искусственного интеллекта.

О постановке проблемы правового регулирования «дипфейка»

А. И. Овчинников приводит следующее мнение: «Современный человек, фиксируя свои данные в разнообразных «личных кабинетах», растворяется в цифровой сфере, полностью переходит под контроль разнообразных цифровых платформ, теряет свою индивидуальность, даже имя, которое заменяют разнообразные логины и пароли. Создаётся впечатление, что не цифровая среда для человека, а человек для цифровой среды» [11, с. 132]. В обозначенной позиции учёного кроется серьёзное опасение, касающееся утраты возможности для человека и гражданина влиять на общественные процессы, не прибегая к интернету. Соответственно, для современного человека необходимо уметь пользоваться смартфоном, компьютером, подписывать бесчисленные пользовательские соглашения на обработку персональных данных, чтобы довольствоваться благами современного цифрового мира. Вполне очевидно, что граждане боятся кражи личных сведений и обращают внимание на несовершенство защиты мо-

бильных устройств и иных гаджетов, располагающих персональной информацией и доступом к банковским приложениям. Уже несколько лет активно применяются системы биометрической защиты, тем не менее пользователи как Android, так и iOS-устройств регулярно жалуются как на ложные отказы в доступе, так и на ошибочную авторизацию чужаков.

Наибольший скепсис у большинства пользователей вызывают намерения некоторых организаций в будущем проводить аутентификацию исключительно с помощью биометрических параметров. Подобная тенденция складывается несамобытно: в 2019 г. была подготовлена правовая основа и введена в действие государственная программа по созданию единой системы биометрических данных (ЕБС) в России, к которой присоединилось большинство банков страны, в т. ч. и Сбербанк. Именно Сбербанк стал лидером по сбору биометрии и обещает уже к концу 2021 г. предоставлять многие услуги с помощью биометрии[1]. С помощью СберID – системы распознавания людей по физическим характеристикам (лицу и голосу) – клиенту проще, например, оплатить услуги ЖКХ или провести иной платёж, получить кредит и др.

Возникает закономерный вопрос: возможна ли подделка биометрии? Разработчики системы безопасности Сбербанка утверждают, что «за всё время не установлено ни одного совпадающего голосового отпечатка. Не было также ни одной успешной попытки воспрепятствовать установлению тождественности путём искусственного изменения голоса без использования электронных средств»[2]. С правовой точки зрения банки имеют возможность самостоятельно корректировать степень защиты пользователей, не нарушая при этом личных прав граждан.

Оппонируя обозначенной позиции, Р. Б. Гасанова высказывает мнение, что «несмотря на высокую точность технических и опытных достижений в области исследования звучащей речи, нельзя утверждать, что совпадение может быть стопроцентным» [1, с. 45]. Аналогичной позиции придерживаются и В. Н. Сорокин, В. В. Вьюгин, А. А. Тананькин [13, с. 27]. Нельзя утверждать, что голосовая идентификация безупречна и позволяет полностью обеспечить безопасность денежных средств. Например, работники банков не говорят о возможных фактах записи голоса клиента с целью воспроизведения и последующего получения доступа к личному кабинету и услугам банка.

Именно поэтому в России в рамках действия единой биометрической системы (ЕБС) предусмотрена повышенная степень защиты данных. Драйвером для создания ЕБС стала национальная программа «Цифровая экономика Российской Федерации»[3]. Одним из главных принципов системы является многоуровневая аутентификация: помимо голоса для идентификации ещё используется фото лица, при этом специальная программа считывает расстояние от носа до глаз и от носа до губ, которые у каждого человека индивидуально. Для удалённой идентификации необходима комбинация голоса, лица и некоторых других параметров, при этом используется защита, исключающая подмену фотографий.

Можно предположить, что панацея найдена, и с введением подобной системы не стоит опасаться за безопасность своего банковского счёта. К сожалению, это было бы очень громким и оптимистичным заявлением, поскольку сегодня существует угроза совершенно иного порядка – дипфейк.

Дипфейками называют реалистичную замену лиц и голоса посредством использования генеративно-состязательных

[1] Осипенко Д. Технологии близкого будущего: как работает биометрия в Сбербанке и что это даёт клиентам? // Банки сегодня : [сайт]. URL: https://bankstoday.net/last-articles/tehnologii-blizkogo-budushhego-kak-rabotaet-biometriya-v-sberbanke-i-chto-eto-daet-klientam (дата обращения: 11.07.2021).

[2] Биометрия в СберБанке // Сбербанк : [сайт]. URL: https://www.sberbank.ru/ru/person/dist_services/bio (дата обращения: 11.07.2021).

[3] О единой биометрической системе [Электронный ресурс]. URL: https://bio.rt.ru/about (дата обращения: 11.07.2021 г.).

нейросетей. В основе дипфейка (название происходит от слов «deep learning», т. е. «глубокое изучение» и «fake», т. е. «подделка») – нейросеть, которая детально изучает лицо человека, а затем подставляет к исходному файлу лицо «реципиента», т. е. с максимальной реалистичностью «оживляет» изображение человека и заставляет его говорить и делать то, чего он не делал и не говорил [9, с. 186]. Технологию разработал студент Стэнфордского университета Ян Гудфеллоу в 2014 г. О массовом использовании программы тогда речи не шло.

Рассмотрим значение термина «нейросеть» – инструмента, который может создавать дипфейки. Искусственные нейронные сети (ИНС) – математические модели, а также их программные или аппаратные реализации, построенные по принципу организации и функционирования биологических нейронных сетей – сетей нервных клеток живого организма[1].

Виды дипфейков и сферы применения нейросетей

На сегодняшний день существует несколько разновидностей дипфейков: звуковые, фото- и видео дипфейки (сочетающие комбинацию динамического изображения и голоса человека). Одна из самых популярных программ – *DeepFaceLab*, открытое ПО от российского разработчика, называющего себя *iperov*. Позволяет не только вставлять лицо в видео, но и менять движения губ говорящего, т. е. подделывать содержание речи. Компания *Vera voice* на текущий момент достаточно далеко продвинулась в создании голосовых дипфейков, которые невозможно отличить от оригинала без помощи компьютерных программ. Сейчас инженеры воссоздают голоса умерших певцов и поэтов по фрагментам оставшихся фонограмм (например, Владимира Высоцкого).

Послушав несколько часов записи голоса человека, нейросеть сможет точно его скопировать и воспроизвести любой текст. Речь звучит реалистично, голоса, создаваемые нейросетью, уже говорят практически без ошибок и «машинного» акцента. Разработчики считают, что технология пригодится в озвучивании книг, игр, фильмов, создании голосовых ассистентов. Создатели понимают, что *Vera Voice* можно использовать как для невинных розыгрышей, так и в мошеннических целях. Фальсификация голосов политиков и других влиятельных людей может привести к серьёзным последствиям, поэтому авторы проекта сейчас находятся в поиске легальных и безопасных способов использования *Vera Voice*[2]. Нейросети посредством обучения на основе произведений известных композиторов также способны самостоятельно генерировать классическую музыку. Пока нейросеть не может создать осмысленное произведение, но она может скопировать стиль игры намного лучше человека.

Нейросети умеют копировать лица и голос на видеозаписях. Но как и любому алгоритму, им нужен материал для обучения – чем его больше, тем лучше результат. Генеративно-состязательная система составляет карту лица по нескольким десяткам точек и линий между ними. Своеобразный цифровой слепок создаётся за считанные секунды.

Помимо этого нейросети учатся распознавать без ошибок рукописные символы и переводить их [10, с. 9–20], помогают заполнять резюме в электронной форме[3], осуществляют прогнозирование [7, с. 95–102], производят судебно-портретную экспертизу [5, с. 66–69], даже оценивают государственные закупки [12, с. 46–48], соответственно, оказывают помощь человеку во многих отраслях жизнедеятельности, в т. ч. в юридической сфере.

[1] Искусственная нейронная сеть // Академик : [сайт]. URL: https://dic.academic.ru/dic.nsf/ruwiki/13889 (дата обращения: 11.07.2021).

[2] Нейросеть Vera Voice точно имитирует голоса людей // DNS Клуб : [сайт]. URL: https://club.dns-shop.ru/digest/22282-neiroset-vera-voice-tochno-imitiruet-golosa-ludei (дата обращения: 11.07.2021).

[3] Онлайн помощник для заполнения вакансий и резюме с нейросетью для бинарных вопросов. Свидетельство о регистрации программы для ЭВМ 2021612493, 18.02.2021. Заявка № 2021611475 от 09.02.2021.

Л. М. Кирова и М. Л. Макаревич приводят пример, когда нейросети позволяют оказывать поддержку в юридической сфере: «Российская юридическая компания "Право.ру" использует технологии ИИ, чтобы рассчитать временную продолжительность дела и судебного процесса и предсказать его исход. При этом в систему заложены все судебные решения по похожим и аналогичным делам, анализируя которые, программы выдают свой результат. Также ещё в 2016 г. у этой же компании появился бот, которому можно задать юридический вопрос через мессенджер Telegram, причём он примет и поймет как текстовое сообщение, так и голосовое. В США планируют допустить ИИ и до зала судебного заседания. Разработанная учёными университета Мэриленд система *Dare* умеет разоблачать лживые показания. Распознавание построено на анализе мимики, голоса и жестов подсудимого и свидетелей. Достоверность *Dare* сейчас достигает 92%» [6].

Нейросети используются для чтения слов по губам человека. Так, в Оксфорде учёными была создана программа *LipNet*, точность распознавания слов которой составляет 88%[1] (точность чтения по губам у человека 52%). В Токийском университете разработали нейросеть, способную преобразовывать черно-белые снимки в цветные. Нейросеть научилась определять в изображениях общие мотивы и раскрашивать объекты в наиболее подходящие цвета (стоит отметить американский аналог *Algorithmia*, российский проект Артемия Лебедева «Колор», *DeOldify* и др.).

Уже через несколько лет будет сложно представить нашу повседневную жизнь без применения систем искусственного интеллекта, которые в значительной мере облегчают функции человека и выводят качество нашей работы и жизни на новые высоты. Несмотря на позитивный вектор развития, в 2018 г. много шума наделало видео с Бараком Обамой, который нелестно отзывался о 45-м президенте США Дональде Трампе. Этот дипфейк сделал режиссер Джордан Пил вместе с изданием *BuzzFeed*, чтобы продемонстрировать, насколько далеко шагнули технологии и почему нужно тщательно проверять источники информации и не верить своим глазам[2]. В последние два года индустрия переживает бурный рост: софта для дипфейков становится всё больше, а правовое регулирование отсутствует.

Совершенно справедливы опасения М. А. Желудкова: «Подобные технологии в условиях удалённого доступа могут быть использованы для оформления подложных товарно-денежных операций, изменения доказательств по реальным уголовным делам. Если сегодня такие программы пока ещё недостаточно совершенны, то пройдет небольшой промежуток времени, и технология дипфейков с открытым кодом создаст серьёзные трудности в идентификации аудио- и видеоинформации в интернет-пространстве. В этом случае увеличится количество мошеннических действий, где от имени руководства или собственников предприятий будут поступать указания на перевод денежных средств или продажу активов, проведение по телефону банковских операций и др.» [4, с. 66-67]. Но в то же время нейросети можно использовать в целях предотвращения преступлений и противодействия злоумышленникам [2, с. 30–32].

В правовом поле на данный момент не закреплены такие термины, как «дипфейк», «нейростеть», однако они уже стали неотъемлемой частью современной жизни. Их применение может как служить благим целям, так и использоваться при совершении преступлений. Запретить использование нейросетей не представляется возможным, также невозможен учёт лиц, применяющих нейросети – любой человек может уста-

[1] Assael Y. M., Shillingford B., Whiteson S., Nando de Freitas. LipNet: End-to-End Sentence-level Lipreading // Cornell University : [сайт]. URL: https://arxiv.org/abs/1611.01599 (дата обращения: 11.07.2021).

[2] Эксперты рассказали, кто может стать жертвой дипфейков // РИА Новости: [сайт]. URL: https://ria.ru/20210814/dipfeyk-1745306675.html (дата обращения: 11.07.2021).

новить программу на компьютер или написать собственную. Полагаем, что стоит сконцентрировать основное внимание на установлении административной или уголовной ответственности за совершение неправомерных действий посредством применения нейросетей.

Потребуется издание нового закона, поскольку единственный на данный момент в России Федеральный закон № 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"»[1], регулирующий сферу применения искусственного интеллекта, не распространяет своё действие на сферу пользования нейросетями частными лицами.

В соответствии с Указом Президента № 490[2] была разработана и принята Национальная стратегия развития искусственного интеллекта на период до 2030 г. (Стратегия 2030), в которой определяются цели и основные задачи развития искусственного интеллекта в Российской Федерации и закрепляется общий подход: «Использование технологий искусственного интеллекта в отраслях экономики носит общий («сквозной») характер и способствует созданию условий для улучшения эффективности и формирования принципиально новых направлений деятельности хозяйствующих субъектов».

В январе 2021 г. планировалось запустить экспериментальные правовые режимы – «цифровые песочницы», – которые позволят гибко подходить к регулированию деятельности в данных сферах, в т. ч. временно отменять действующие предписания, запреты или вводить новые, если это понадобится для нормального функционирования экспериментального режима. В Москве подобный экспериментальный режим запущен с 1 июля 2021 г.[3]. Верится, что такие меры позволят быстро адаптироваться к новым угрозам, не прибегая к негибкому и долгому официальному процессу внесения изменений в законодательство.

Использование цифрового образа личности в коммерческих целях

Если сегодня допустимо использовать образ человека без его ведома, то вполне очевидно, что в будущем может появиться институт использования образа актера (певца или другой знаменитости) после смерти. Уже не новость, что по всему миру проходят концерты умерших певцов – на сцене «оживали» Тупак Шакур, Майкл Джексон, Элвис Пресли и др. Хоть в указанных случаях использовалась голограмма, основной подход неизменен: некая группа людей или конкретный человек получает за организацию и проведение концерта определенную сумму денег, дефакто наживаясь на образе умершего исполнителя. Никакой гражданско-правовой или уголовной ответственности за подобные действия в настоящий момент не предусмотрено, что порождает достаточно большой спектр возможностей для неограниченного круга лиц по использованию образа знаменитости в коммерческих целях.

Возможно, что в ближайшие несколько лет будет расширен институт завещания, где будет предусмотрена передача права

[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» // Российская газета. 2020. Федеральный выпуск № 92 (8146).

[2] Указ Президента РФ от 10.10.2019. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Президент России : [сайт]. URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 11.07.2021).

[3] Утверждена концепция правового регулирования искусственного интеллекта // Российская газета: [сайт]. URL: https://rg.ru/2020/08/24/utverzhdena-koncepciia-pravovogo-regulirovaniia-iskusstvennogo-intellekta.html (дата обращения: 11.07.2021).

на использование личности (образа) гражданина. Если наследники смогут распоряжаться данным правом, то на использование образа придется получать специальное разрешение (например, лицензию).

Соответствующие изменения, на наш взгляд, должны быть внесены в раздел 5 ГК РФ в ст. 1112 «Наследство», а гл. 65 ГК РФ «Наследование отдельных видов имущества» дополнить новой статьёй «Наследование цифрового образа личности и прав на его использование». Стоит отдельно осмыслить и разрешить вопрос, кто и каким образом будет наследовать цифровой образ личности при наследовании по закону, а также кто из нескольких наследников одной очереди будет обладать таким правом: каждый из них или только один конкретный наследник.

По своей правовой природе цифровой образ личности наиболее близок институту интеллектуальной собственности, поскольку является нематериальным правом, тем не менее есть одно коренное отличие – образ личности не обладает творческим началом, не является результатом труда человека, поэтому регулироваться должен отдельными нормами права.

Решение проблем с незаконным размещением дипфейков на сегодняшний день в сети можно осуществить, применяя по аналогии ч. 1 ст. 152.1. «Охрана изображения гражданина»: Обнародование и дальнейшее использование изображения гражданина (в т. ч. его фотографии, а также видеозаписи или произведения изобразительного искусства, на которых он изображён) допускаются только с согласия этого гражданина. После смерти гражданина его изображение может использоваться только с согласия детей и пережившего супруга, а при их отсутствии – с согласия родителей. В то же время фото и видео с изображением человека также имеет существенное различие с дипфейковыми аналогами – фейк может сделать, сказать или показать то, чего никогда бы не мог позволить себе настоящий человек (к примеру, можно разрушить репутацию известной личности после смерти, создав видеоряд, где производится умышленное оскорбление людей, выдав дипфейк за реальное видео, записанное при жизни). Считаем, что подобные действия выходят за рамки регулирования ст. 152.1. «Охрана изображения гражданина», т. к. в принципе реальным изображением не считается. Помимо этого, противоправные деяния, связанные и использованием дипфейков, не могут регулироваться ст. 5.61 «Оскорбление» Кодекса об административных правонарушениях РФ и ст. 128.1 «Клевета» УК РФ. Сам процесс совершения правонарушения имеет ряд особенностей, которые не учитывают указанные статьи.

Если мыслить глобально, можно навредить самой истории человечества, изменить её ход, соответственно, последствия применения дипфейка гипотетически могут иметь совершенно иной масштаб. Итак, напрашивается вывод, что в Гражданский кодекс РФ, КОАП РФ, Уголовный кодекс РФ должны быть внесены изменения, касающиеся особой ответственности за использование дипфейка в противоправных целях.

О законодательном регулировании распространения дипфейков

К правовому регулированию использования нейросетей, в частности, дипфейков необходимо отнестись с особой щепетильностью, поскольку проблема, на наш взгляд, гораздо серьёзнее: нейросети позволяют использовать образы политиков, лидеров мировых держав. Дипфейк-технология позволяет синтезировать не только внешность, но и голос, именно по этой причине в США дипфейки признали на государственном уровне угрозой национальной безопасности. Deepfakes может стать «золотой жилой» для преступных организаций и виртуальных мошенников. В настоящий момент в США завершается подготовка проекта федерального закона, регулирующего данную сферу [3].

В штате Калифорния некоторые виды дипфейков запретили на уровне штата и

предусмотрели ответственность за их противоправное использование. Губернатор штата Калифорния Гэвин Ньюсон подписал законопроект, регулирующий распространение дипфейков. Данный законопроект – первый известный закон, ограничивающий распространение именно дипфейков в интернете. Действие законопроекта ограничивает распространение дипфейков с участием политических кандидатов в форме аудио, видео и фото в течение 60 дней до выборов. Закон будет действовать как в отношении материалов, в которых подменены лица и голоса политиков, так и на материалы, в которых на изображения политиков накладываются чужие лица и речь. При этом в законопроекте уточняется, что кадры или ролики с политиками, в которых используются материалы с участием других людей, должны сопровождаться предупреждением. Закон будет действовать до 1 января 2023 г.[1].

Поводом послужило скандальное дипфейк-видео со спикером палаты представителей Конгресса США Нэнси Пелоси, на котором была изменена её речь. Создавалось впечатление, что политик была пьяна и едва выговаривала свои слова. Видео было опубликовано на Facebook, и компания не согласилась удалить его сразу, заявив, что вместо этого разместит статью-опровержение, в которой будет подчёркиваться факт редактирования речи. Представитель Ассамблеи Калифорнии Марк Берман, который является автором законопроекта, утверждает, что видеоролики, созданные с помощью технологии *Deepfake*, в которых к тому же фигурируют политики, могут обмануть общественность и повлиять на результаты выборов[2].

Власти Китая пошли ещё дальше: они объявили любую публикацию заведомо ложной информации, в т. ч. с применением дипфейков, уголовным преступлением. Согласно новым нормам, все дипфейки нужно будет отмечать специальной пометкой, которая будет предупреждать пользователей о том, что это ненастоящая новость. Закон приняла Администрация киберпространства Китая. Чиновники отметили, что использование дипфейк-технологий может «поставить под угрозу национальную безопасность, подорвать социальную стабильность, а также нарушить общественный порядок и ущемить законные права и интересы граждан»[3]. Дипфейковые технологии вполне могут в будущем стать обычным инструментом в предвыборной гонке в России, если сегодня не принять аналогичный законопроект, то завтра мы будем бороться с последствиями проблем, с которыми уже столкнулись наши зарубежные коллеги.

Дипфейк как угроза национальной безопасности

Опасность дипфейка весома и по следующим основаниям: например, злоумышленники начнут распространять в интернете видеообращение (Президента США, к примеру) с угрозой к началу новой мировой войны. Многие граждане и руководство других стран могут поверить данной информации, поэтому подобные технологии становятся «ящиком Пандоры», который может привести к катастрофическим последствиям, в связи с этим ограничение на использование дипфейков вполне оправдано.

Вне всякого сомнения, «копии изображения политического деятеля или видео оказывают психологическое воздействие на зрителя. Это воздействие будет тем больше, чем меньше зритель сомневается в подлинности изображения или видео. Развитие информационных технологий и Интернета, программных средств обработки и использования «больших данных»,

[1] Dent S. California cracks down on political and pornographic deepfakes // Engadget : [сайт]. URL: https://www.engadget.com/2019-10-07-california-deepfake-pornography-politics.html (дата обращения: 11.07.2021).

[2] Калифорния ввела два закона против дипфейков // Хабр : [сайт]. URL: https://habr.com/ru/news/t/470652 (дата обращения: 11.07.2021).

[3] В Китае публикацию дипфейков отнесли к уголовным преступлениям // Хабр: [сайт]. URL: https://habr.com/ru/news/t/478362 (дата обращения: 11.07.2021).

увеличение быстродействия и мощности суперкомпьютеров, опережающие разработки «искусственного интеллекта» ставят на повестку дня проблему политического воздействия дипфейков на массовую аудиторию, посредством которых обходится языковой барьер, и при этом используются различные психологические инструменты» [8, с. 94].

Американский исследователь Дуглас Харрис убеждён, что «пока мы ждём, что национальные правовые механизмы по регулированию дипфейков потенциально могут вступить в действие, технологии будут развиваться. Сейчас требуется несколько часов, чтобы сделать фальшивку. Скоро потребуется несколько секунд, и продукт будет неотличим от реального видео. Поэтому обсуждать опасность и регулирование дипфейков нужно уже сейчас»[1].

На наш взгляд, стоит установить запрет на использование изображений политических лидеров государств и предусмотреть уголовную ответственность за распространение дипфейков, как это уже сделано в Китае.

Заключение

Основная проблема дипфейков на сегодняшний день заключается в том, что сфера искусственного интеллекта слабо охраняется и регулируется законом. Ответственность за использование и распространение технологий на основе ИИ предусмотрена пока что в одном штате США и в Китае, хотя угроза, которую несут дипфейки, можно смело назвать мировой. В будущем одним из способов решения обозначенной проблемы видится создание нормативно-правовой базы, закрепляющей как категориальный аппарат, так и ответственность за халатное и преступное поведение с искусственным интеллектом. Интернет сегодня охватывает практически весь земной шар, поэтому распространение угроз, которые несёт дипфек, может происходить повсеместно. Поэтому, на наш взгляд, следует принять международную конвенцию и отразить основополагающие положения в национальных законодательствах государств всего мира.

Статья поступила в редакцию 20.07.2021.

ЛИТЕРАТУРА

1. Гасанова Р. Б. Идентификационное значение голосовых сообщений при расследовании преступлений // Закон и власть. 2021. № 2. С. 43–46.
2. Гарифуллин И. М. Использование нейросетей для выявления мошеннеческих транзакций // Инновационная наука. 2021. № 3. С. 30–32.
3. Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2020. № 4. С. 379–386.
4. Желудков М. А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica. 2021. № 4 (173). С. 63–70.
5. Зинин А. М. Нейросети и судебно-портретная экспертиза // Вестник криминалистики. 2020. № 2 (74). С. 66–69.
6. Кирова Л. М., Макаревич М. Л. Правовые аспекты использования нейронных сетей // Инновационная экономика: перспективы развития и совершенствования. 2018. № 1 (27). С. 58–63.
7. Коробейников А. В., Мкртчян А. Ф., Ситников В. В., Наговицын А. В. Прогнозирование периода стойкости металлорежущего инструмента на основе нейросети // Интеллектуальные системы в производстве. 2020. Т. 18. № 3. С. 95–102.
8. Красовская Н. Р., Гуляев А. А. Технологии манипуляции сознанием при использовании дипфейков как инструмента информационной войны в политической сфере // Власть. 2020. Т. 28. № 4. С. 93–98.

[1] Harris D. Deepfakes: false pornography is here and the law cannot protect you [Электронный ресурс]. URL: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1333&context=dltr (дата обращения: 11.07.2021).

9. Масленкова Н. А. Дипфейк: пользовательский контроль визуального контента в интернете // Пользовательский контент в современной коммуникации: сборник / сост. И. В. Топчий. Челябинск, 2021. С. 186–189.
10. Моржов И. И., Сай С. В. Особенности построения нейросетей в задачах распознавания рукописных символов // Вестник Тихоокеанского государственного университета. 2020. № 4 (59). С. 9–20.
11. Овчинников А. И. Право и правосознание в условиях цифровизации общества // Вестник юридического факультета Южного федерального университета. 2020. Т. 7. № 2. С. 131–134.
12. Симанович Л. Н. Искусственный интеллект: оценивать государственные закупки будут машины // Вестник Академии Следственного комитета Российской Федерации. 2017. № 2 (12). С. 46–48.
13. Сорокин В. Н., Вьюгин В. В., Тананыкин А. А. Распознавание личности по голосу: аналитический обзор // Информационные процессы. 2012. № 1. С. 1–30.
14. Bondarenko V. M., Aleshkovski I. Social and Economic Development Models in the Digital Transformation Era // Journal of Economic Science Research. 2019. Vol. 2. № 1. P. 35–39.
15. Goloventchik G. G., Zhyrkevich A. B. Assessment of the digital transformation of european countries with small open economies // Журнал Белорусского государственного университета. Экономика. 2020. № 2. С. 27–37.
16. Gutbrod M. Digital transformation in economy and law // Digital Law Journal. 2020. Vol. 1. № 1. P. 12–23.

REFERENCES

1. Gasanova R. B. [The identification value of voice messages in the investigation of crimes]. In: *Zakon i vlast* [Law and power], 2021, no. 2, pp. 43–46.
2. Garifullin I. M. [Using neural networks to detect fraudulent transactions]. In: *Innovatsionnaya nauka* [Innovation Science], 2021, no. 3, pp. 30–32.
3. Ivanov V. G., Ignatovsky Ya. R. [Deepfakes: Political Perspectives and Threats to Personality and National Security]. In: *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Gosudarstvennoe i munitsipalnoe upravlenie* [Bulletin of the Peoples' Friendship University of Russia. Series: State and Municipal Administration], 2020, no. 4, pp. 379–386.
4. Zheludkov M. A. [Justification of the need to adapt the activities of law enforcement agencies to the digital transformation of the criminal environment]. In: *Lex russica*, 2021, no. 4 (173), pp. 63–70.
5. Zinin A. M. [Neural networks and forensic examination]. In: *Vestnik kriminalistiki* [Forensic Science Bulletin], 2020, no. 2 (74), pp. 66–69.
6. Kirova L. M., Makarevich M. L. [Legal aspects of using neural networks]. In: *Innovatsionnaya ekonomika: perspektivy razvitiya i sovershenstvovaniya* [Innovative economy: prospects for development and improvement], 2018, no. 1 (27), pp. 58–63.
7. Korobeinikov A. V., Mkrtchyan A. F., Sitnikov V. V., Nagovitsyn A. V. [Forecasting the service life of a metal-cutting tool based on a neural network]. In: *Intellektualnye sistemy v proizvodstve* [Intelligent Systems in Production], 2020, vol. 18, no. 3, pp. 95–102.
8. Krasovskaya N. R., Gulyaev A. A. [Consciousness manipulation technologies using deepfakes as a tool of information warfare in the political sphere]. In: *Vlast* [Power], 2020, vol. 28, no. 4, pp. 93–98.
9. Maslenkov N. A. [Deepfake: User Control of Visual Content on the Internet]. In: Topchiy I. V., ed. *Polzovatelskii kontent v sovremennoi kommunikatsii* [User content in modern communication]. Chelyabinsk, 2021, pp. 186–189.
10. Morzhov I. I., Sai S. V. [Features of building neural networks in problems of handwritten character recognition]. In: *Vestnik Tikhookeanskogo gosudarstvennogo universiteta* [Bulletin of Pacific State University], 2020, no. 4 (59), pp. 9–20.
11. Ovchinnikov A. I. [Law and legal awareness in the context of digitalization of society]. In: *Vestnik yuridicheskogo fakulteta Yuzhnogo federalnogo universiteta* [Journal of Law Faculty, Southern Federal University], 2020, vol. 7, no. 2, pp. 131–134.
12. Simanovich L. N. [Artificial intelligence: machines will evaluate government procurement]. In: *Vestnik Akademii Sledstvennogo komiteta Rossiiskoi Federatsii* [Bulletin of the Academy of the Investigative Committee of the Russian Federation], 2017, no. 2 (12), pp. 46–48.
13. Sorokin V. N., Vyugin V. V., Tananykin A. A. [Personality recognition by voice: an analytical overview]. In: *Informatsionnye protsessy* [Information processes], 2012, no. 1, pp. 1–30.
14. Bondarenko V. M., Aleshkovski I. Social and Economic Development Models in the Digital Transformation Era. In: *Journal of Economic Science Research,* 2019, vol. 2, no. 1, pp. 35–39.

15. Goloventchik G. G., Zhyrkevich A. B. Assessment of the digital transformation of european countries with small open economies. In: *Zhurnal Belorusskogo gosudarstvennogo universiteta. Ekonomika* [Journal of the Belarusian State University. Economy], 2020, no. 2, pp. 27–37.
16. Gutbrod M. Digital transformation in economy and law. In: *Digital Law Journal*, 2020, vol. 1, no. 1, pp. 12–23.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Киселёв Александр Сергеевич – кандидат юридических наук, доцент кафедры гражданского права Московского государственного областного университета, старший преподаватель департамента международного и публичного права юридического факультета Финансового университета при Правительстве Российской Федерации;
e-mail: pain068@yandex.ru

INFORMATION ABOUT THE AUTHOR

Alexander S. Kiselev – Cand. Sci. (Law), Assoc. Prof., Department of Civil Law, Moscow Region State University, senior lecturer, Department of International and Public Law, Faculty of Law Financial University under the Government of the Russian Federation;
e-mail: pain068@yandex.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Киселёв А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия: Юриспруденция. 2021. № 3. С. 54–64.
DOI: 10.18384/2310-6794-2021-3-54-64

FOR CITATION

Kiselev A. S. On the Expansion of Legal Regulation in the Field of Artificial Intelligence: Deepfake as a Threat to National Security. In: *Bulletin of Moscow Region State University. Series: Jurisprudence*, 2021, no. 3, pp. 54–64.
DOI: 10.18384/2310-6794-2021-3-54-64