

Дипфейки как угроза правам человека¹

Аннотация. Статья посвящена такой новой угрозе правам человека в условиях цифровизации, как дипфейк-технологии. Автор показывает, что применение таких технологий является инструментом, который может иметь как положительный, так и отрицательный эффект. В частности, применение дипфейков влечет угрозу неприкосновенности частной жизни, нарушения чести и достоинства граждан. В связи с этим перед законодателем стоит задача разработать и внедрить комплекс мер, применение которых позволит минимизировать возможность нарушения прав граждан дипфейк-технологиями. Предлагается направить усилия государства: на создание автоматизированных инструментов для обнаружения дипфейков с возможностью определения даты, времени и физического происхождения их содержимого, а при наличии признаков потенциальной опасности — способных остановить размещение и распространение дипфейков; развитие сервисов и инструментов фактчекинга; нормативное закрепление требований, в соответствии с которыми в социальных сетях и мессенджерах должна проводиться обязательная маркировка дипфейк-контента; формирование нормативной базы, предусматривающей ответственность за создание и распространение дипфейк-материалов, способных нанести ущерб деловой репутации, унижить честь и достоинство человека. С позиции авторского права дипфейки предложено рассматривать через призму производного произведения, при котором использование исходного произведения без согласия его правообладателя будет незаконно. Учитывая угрозы дипфейк-технологий для прав человека, предложен комплекс мер, применение которых позволит минимизировать возможность нарушения прав граждан данными технологиями: внедрение механизма фактчекинга, развитие его сервисов и инструментов; обязательная маркировка дипфейк-контента в социальных сетях и мессенджерах; создание нормативной базы, предусматривающей ответственность за создание и распространение дипфейк-материалов, способных нанести ущерб деловой репутации, унижить честь и достоинство человека.

Ключевые слова: цифровые технологии; дипфейк-технологии; дипфейки; права человека; угроза; неприкосновенность частной жизни; честь; достоинство; репутация; авторское право; персональные данные; фактчекинг.

Для цитирования: Добробаба М. Б. Дипфейки как угроза правам человека // Lex russica. — 2022. — Т. 75. — № 11. — С. 112–119. — DOI: 10.17803/1729-5920.2022.192.11.112-119.

¹ Статья выполнена в рамках программы стратегического академического лидерства «Приоритет-2030».

© Добробаба М. Б., 2022

* Добробаба Марина Борисовна, доктор юридических наук, доцент, профессор кафедры информационного права и цифровых технологий Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
mbdobrobaba@msal.ru

Deepfakes as a Threat to Human Rights²

Marina B. Dobrobaba, Dr. Sci. (Law), Associate Professor, Professor, Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
mbdobrobaba@msal.ru

Abstract. The paper is devoted to such a new threat to human rights arising amid digitalization as deepfake technologies. The author shows that the use of such technologies is a tool that can have both positive and negative effects. In particular, the use of dipfakes entails a threat to privacy, violations of the honor and dignity of citizens. In this regard, the legislator is faced with the task of developing and implementing a set of measures, the application of which will minimize the possibility of violation of citizens' rights by deepfake technologies. It is proposed to direct the efforts of the state: to create automated tools for detecting deepfakes with the ability to determine the date, time and physical origin of their contents, and, if there are signs of potential danger, capable of stopping the placement and distribution of deepfakes; development of fact-checking services and tools; regulatory consolidation of requirements according to which mandatory marking of deepfake content should be carried out in social networks and messengers; formation of a regulatory framework providing for responsibility for the creation and distribution of deepfake materials that can damage business reputation, humiliate the honor and dignity of a person. From the standpoint of copyright, it is proposed to consider deepfakes through the prism of a derivative work, in which the use of the original work without the consent of its copyright holder will be illegal. Taking into account the threats of deepfake technologies to human rights, a set of measures has been proposed. Its use will minimize the possibility of violating citizens' rights by means of these technologies. These measures are: the introduction of a fact-checking mechanism, the development of its services and tools; mandatory labeling of deepfake content in social networks and messengers; the creation of a regulatory framework providing for responsibility for the creation and distribution of deepfake materials capable of damage the business reputation, humiliate the honor and dignity of a person.

Keywords: digital technologies; deepfake technologies; deepfakes; human rights; threat; privacy; honor; dignity; reputation; copyright; personal data; fact-checking.

Cite as: Dobrobaba MB. Dipfeyki kak ugroza pravam cheloveka [Deepfakes as a Threat to Human Rights]. *Lex russica*. 2022;75(11):112-119. DOI: 10.17803/1729-5920.2022.192.11.112-119. (In Russ., abstract in Eng.).

Стремительное развитие цифровых технологий актуализирует вопрос о защите прав человека в условиях цифровизации, поскольку даже полезные, созданные для конкретной цели цифровые технологии могут создавать угрозу правам человека. Так, в свое время популярность получил платный сервис DeepNude, разработчики которого использовали искусственный интеллект и нейросетевой анализ для того, чтобы «раздевать женщин». Сервис оказался настолько популярным, что сами авторы вынуждены были закрыть его, опасаясь многочисленных судебных исков, связанных с нарушением как ст. 12 Всеобщей декларации прав человека³, так и ст. 17 Международного пакта о гражданских и политических правах⁴, в соответствии с кото-

рыми признаются незаконными посяательства на честь и репутацию человека.

В последние годы широкое распространение получили технологии изготовления поддельных фото и видео, которые, используя методику компьютерного синтеза изображения, основанную на искусственном интеллекте, переносят черты лица с изображения человека на целевое фото (видеозапись) с высокой степенью правдоподобия. Несмотря на то что эти изображения (видео) фиктивные, они могут быть выложены в сеть «Интернет» в качестве якобы реальных. Речь идет о технологиях, получивших название дипфейк (deepfake), данный термин происходит от deep learning (англ. — глубинное обучение) и fake (англ. — фейк, подделка).

² The reported study was carried out as part of the strategic academic leadership program «Priority-2030».

³ Всеобщая декларация прав человека (принята на третьей сессии Генеральной Ассамблеи ООН резолюцией 217 А (III) от 10.12.1948) // Российская газета. 1998. 10 дек.

⁴ Международный пакт о гражданских и политических правах (Нью-Йорк, 16 декабря 1966 г.) // Ведомости Верховного Совета СССР. 1976. № 17. Ст. 291.

Несмотря на то что в 2019 г. в Российской Федерации был принят закон, устанавливающий ответственность за распространение недостоверной общественно значимой информации под видом достоверных сообщений⁵, проблема нарушения личных прав с использованием дипфейк-технологий, всё еще не до конца осознана и разработана.

Сам по себе синтез изображений, видео или аудио при применении дипфейк-технологий может не иметь социально опасных целей и не затрагивать права других граждан, более того их польза очевидна в кино, искусстве, рекламе. Так, в киноиндустрии с помощью дипфейк-технологий можно искусственно омолодить или состарить актеров, придать дублерам большее сходство с актерами, синхронизировать движения губ при дубляже перевода или даже доснять фильм с изображением внезапно умершего или переставшего участвовать в съемках актера⁶. Известно, что Музей Сальвадора Дали во Флориде «оживил» художника, который стал экспонатом в собственном музее. В настоящее время применение данной технологии позволяет с помощью наложения нескольких фрагментов изображений на одно создать качественный снимок космического объекта в детальных подробностях. В то же время при манипулировании средствами массовой информации с использованием изображений, видео или голосов реальных людей возникает целый комплекс моральных, юридических и управленческих проблем, требующих своего решения⁷.

Наряду с угрозой для прав человека, в научной литературе обращается внимание на потенциальную опасность дипфейк-технологий для государства и общества в целом, более того отмечается, что они в скором времени могут представлять угрозу национальной безопасности⁸. Подобные опасения объясняются широкими возможностями дипфейк-технологий

синтезировать не только внешность человека, но и его голос, а значит, при наличии целей, представляющих социальную опасность, их применение может стать инструментом в руках преступных организаций и виртуальных мошенников. Именно по этой причине уже сейчас в США дипфейки признаны угрозой национальной безопасности на государственном уровне, одновременно ведется активная работа над проектом федерального закона, регулирующего данную сферу⁹.

На сегодняшний день можно привести многочисленные примеры противоправного использования дипфейк-технологий в России. Так, в сентябре 2021 г. пользователей Интернета удивил нелепый дипфейк — мошенники прорекламировали фейковые «Тинькофф Инвестиции», наложив на человека в кадре лицо основателя TCS Group Олега Тинькова. По голосу он не был похож на российского предпринимателя, да и визуально легко было понять, что это фейк.

Другим примером может служить скандал, разгоревшийся вокруг главного исполнительного директора компании Dbrain Дмитрия Мацкевича¹⁰. Мошенники сделали дипфейк-копию видео с рекламой Мацкевича, в котором он рассказывает об инвестициях с доходом в 360 % годовых, при этом ссылка под роликом вела на сайт, к которому Мацкевич не имел никакого отношения. Очевидно, что в результате подобных действий могли пострадать не только лица, попавшиеся на мошенническую уловку, но и сам Дмитрий Мацкевич, чья внешность и голос были использованы преступниками.

Стоит признать наличие и более совершенных подделок. Так, в феврале 2021 г. в популярном сервисе TikTok было размещено видео Тома Круза, собравшее по состоянию на март 2021 г. более 11 млн просмотров. То, что данное видео — дипфейк, стало понятно только по-

⁵ Федеральный закон от 18.03.2019 № 27-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СЗ РФ. 2019. № 12. Ст. 1217.

⁶ URL: <https://trends.rbc.ru/trends/industry/5fc688fe9a79473e6ff9b82a> (дата обращения: 01.10.2022).

⁷ 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. 381.

⁸ См.: 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.

⁹ Иванов В. Г., Игнатовский Я. Р. Указ. соч. С. 383.

¹⁰ Мошенники придумали, как использовать deepfake-копии людей для обмана // URL: <https://news.myseldon.com/ru/news/index/244067201> (дата обращения: 01.10.2022).

сле признания самого актера. Данный пример с поддельным аккаунтом Круза продемонстрировал, что, благодаря дипфейк-технологиям, мошенники могут манипулировать общественностью. Одновременно использование дипфейк-технологий позволяет заинтересованным лицам вторгаться в частную жизнь как известных людей, например политиков, подрывая их репутацию¹¹, так и обычных граждан.

Более серьезной проблемой, способной нести угрозу правам человека, является способность дипфейк-технологий с невероятной точностью имитировать интонацию, характерные паузы между словами, акцент, корректировать эмоции при произношении слов (голосовые дипфейки).

В цифровую эпоху многие открыто делятся в Интернете видео своих близких, в том числе детей, чем пользуются антисоциальные элементы. Так, известны примеры, когда жертвы, которых мошенники отбирали через социальные сети, получали телефонные звонки с синтезированной речью от мошенников, имитирующих похищение родственников жертв, или с просьбой о срочной помощи, для чего требовалось перевести определенную денежную сумму. Нередко мошенники синтезируют речь для махинаций с банковскими счетами.

Дипфейк-технологии часто применяются при изготовлении фальсифицированных фотографий и видеороликов интимного содержания. Развитие цифровых технологий привело к тому, что появилось даже специальное приложение для смартфона FakeApp, позволяющее любому пользователю создать фейковые порнографические изображения любого человека. В результате любой из миллионов людей, выкладывающих свои фото в сети «Интернет», может против своей воли стать жертвой дипфейка.

Правовая оценка создания и распространения дипфейков в рамках российского законодательства весьма затруднительна. Преобладает мнение, что подобные действия не могут быть оценены как нарушение неприкосновенности частной жизни, поскольку не происходит сбора и распространения реальных сведений,

а данное деяние может быть квалифицировано по ст. 242 Уголовного кодекса РФ (незаконные изготовление и оборот порнографических материалов или предметов)¹². Однако при подобном подходе к квалификации деяния не учитываются психологические страдания потерпевшего, честь и достоинство которого пытались опорочить посредством выложенных на всеобщее обозрение фиктивных материалов.

Способом решения данной проблемы могло бы стать использование правоприменительной практики ряда государств, квалифицирующих использование соответствующих технологий как клевету — при условии, что будет доказано, что поддельные изображения распространялись со злым умыслом. Представляется правильным квалифицировать подобные деяния по ч. 2 ст. 128.1 «Клевета» УК РФ, предусматривающей ответственность за распространение заведомо ложных сведений, порочащих честь и достоинство потерпевшего, совершенное в Интернете. В гражданском законодательстве вопросы, связанные с защитой чести и достоинства, регулируются статьей 152 Гражданского кодекса РФ.

Еще одной областью прав граждан, требующей научного изучения и нормативного регулирования, серьезно подверженной трансформации под воздействием цифровых технологий, является авторское право¹³. Так, применение дипфейк-технологий делает актуальным решение вопроса, не является ли использование голоса или внешности другого человека нарушением авторского права. Остается открытой также проблема защиты прав умерших (например, киноактеров) в отношении использования их голоса и образа.

Поскольку российское законодательство об авторском праве не охраняет голос или образ человека, перед законодателем также встанут вопросы: относится ли голос человека и его внешность к персональным данным? Кто обладает правом на синтезированный голос: владелец оригинала или тот, кто воссоздал этот голос?

Стоит отметить, что внешность и голос человека относятся к его биометрическим данным,

¹¹ Видео станет невозможно смотреть? Дипфейки Олега Тинькова и Тома Круза атаковали Интернет, и это не предел // URL: <https://hi-tech.mail.ru/review/55975-video-stanet-nevozmozhno-smotret-dipfeyki-olega-tinkova-i-toma-kruza-atakovali-i/> (дата обращения: 01.10.2022).

¹² Капитонова Е. А. Шантаж «нюдсами» и смежные деяния: проблемы уголовно-правовой квалификации // Уголовное право. 2021. № 6. С. 19–27.

¹³ Дипфейки: как трансформируется авторское право на контент // URL: <https://trends.rbc.ru/trends/industry/5fc688fe9a79473e6ff9b82a> (дата обращения: 01.10.2022).

которыми в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных»¹⁴ являются сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность.

В разъяснениях Роскомнадзора от 02.09.2013 «О вопросах отнесения фото- и видеоизображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки» указано, что к биометрическим персональным данным относятся физиологические данные (дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др.), а также иные физиологические или биологические характеристики человека, в том числе изображение человека (фотография и видеозапись), которые позволяют установить его личность и используются оператором для определения личности субъекта.

В соответствии с приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 10.09.2021 № 930¹⁵ к биометрическим персональным данным физического лица относится не только изображение лица, но и данные его голоса, собранные текстозависимым методом.

Как отмечается в научной литературе, в случае неправомерного использования в дипфейке информации, относящейся к какой-либо личности, характеризующей физиологические и биологические особенности этой личности, можно говорить о нарушении режима использования персональных данных¹⁶.

Следует признать, что авторское право защищает произведения, которые создаются с применением дипфейк-технологий. При их создании может быть нарушено авторское право на фотографию или видео, на основании которых создается подобное произведение. Что касается голосовых дипфейков, их

создание представляет собой самую большую проблему, потому что на голос человека не распространяется право собственности. В России использование чужой речи для создания похожего голоса в явном виде не запрещено законодательством. Имитация голоса, например телефонными пранкерами, тоже не является нарушением и зависит скорее от содержания шутки, которая может подпасть под уголовную ответственность. А использование дипфейк-технологий в рекламе не должно вводить потребителей в заблуждение — например, о том, что известная личность якобы рекомендует какой-либо товар.

Представляется, что дипфейки стоит рассматривать через призму производного произведения, при котором использование исходного произведения без согласия его правообладателя будет незаконно.

Согласно российскому гражданскому законодательству (ч. 3 ст. 1228 ГК РФ) исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. Это право может быть передано автором другому лицу по договору, а также может перейти к другим лицам по иным основаниям, установленным законом. При этом для возникновения, осуществления и защиты авторских прав не требуется регистрации или соблюдения каких-либо формальностей.

Если рассматривать право авторства на дипфейк как результат интеллектуальной деятельности, созданный программой, то по российскому законодательству автором может быть только гражданин, творческим трудом которого создан этот результат (ст. 1228 ГК РФ). А правообладателем может быть лишь человек или юридическое лицо, обладающие исключительным правом на результат интеллектуальной деятельности или на средство индивидуализации (ст. 1229 ГК РФ).

¹⁴ СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

¹⁵ Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 10.09.2021 № 930 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных, порядка размещения и обновления биометрических персональных данных в единой биометрической системе и в иных информационных системах, обеспечивающих идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации».

¹⁶ Масликова Я. А. Дипфейки как угроза персональным данным // Грядущим поколениям завещаем: творить добро в защиту права : материалы Всероссийской научно-практической конференции с международным участием. Ногинск, 2021. С. 397.

Отдельные социальные сети попытались самостоятельно урегулировать распространение дипфейков. Так, новые правила китайского сервиса TikTok запрещают размещение любого синтетического или манипулирующего контента, способного ввести пользователей в заблуждение и причинить вред. Политика TikTok направлена преимущественно на недопущение очернения политических оппонентов в Интернете.

Правила американской социальной сети Twitter предусматривают пометку твитов и предупреждение пользователей об измененных новостях, а не их удаление. Удаление же недостоверных материалов осуществляется лишь в случае, если они могут причинить вред, в том числе когда они представляют угрозу конфиденциальности, или праву человека, или группы лиц свободно выражать свое мнение.

Есть и положительные примеры, позволяющие социальным сетям сделать направление дипфейк-технологий одним из ключевых в работе с инструментами для умной обработки пользовательского мультимедийного контента (видео, фото, анимация). Так, российская социальная сеть «Одноклассники» запустила дипфейк-сервис «Новый образ» для создания новогодних открыток. Социальная сеть планирует и дальше развивать собственные дипфейк-технологии: расширить возможности «Нового образа» и интегрировать его в разные механики и продукты, включая стикеры со своим лицом, фото профиля, рамки и др. Кроме того, в сервисе можно будет примерить одежду, прическу или аксессуары.

Представляется, что полностью запретить создание поддельных фото и видео людей не только крайне сложно, но и нецелесообразно, учитывая, что они широко применяются в кино, рекламе, реконструкции, юмористических шоу и т.д. Однако под запрет однозначно должны подпадать действия, связанные с обнародованием и распространением таких подделок. Отметим, что такой подход закреплен в национальном законодательстве (ст. 152.1 ГК РФ).

Закон не запрещает создание того или иного произведения с чьим-либо изображением, а формально-юридически внесение изменений в фото другого лица должно трактоваться как создание произведения¹⁷. Вместе с тем, как

отмечают Р. Амелин и С. Чаннов, установление ограничений на создание программ, систем и технологий, позволяющих вносить изменения в фото- и видеоизображения, является допустимым при условии, что такие ограничения не должны носить общий характер, в каждом конкретном случае должны учитываться цели создания программы и ее функционал¹⁸.

Несмотря на реальные угрозы дипфейк-технологий для прав человека, представляется, что данная технология является всего лишь одним из технических инструментов, имеющих как положительный, так и отрицательный эффект. В связи с этим перед законодателем стоит задача разработать и внедрить комплекс мер, применение которых позволит минимизировать возможность нарушения прав граждан дипфейк-технологиями.

Действенным способом борьбы с противоправными дипфейк-материалами, нарушающими права граждан, может стать разработка технологий искусственного интеллекта, способных выявлять следы применения дипфейк-технологий. Речь идет о механизме фактчекинга (англ. fact checking — проверка сообщений и выявления фейков), призванном сдерживать распространение дипфейков посредством инструментов оперативного тестирования информационных сообщений, аудио и видеозаписей на предмет их подделки, доступных не только медиаплатформам, но и частным лицам, просматривающим ту или иную информацию, а также пересылающим ее другим пользователям.

Представляется необходимым развитие сервисов и инструментов фактчекинга, применение которых должно быть бесплатным, простым, не требующим специального образования и серьезных IT-навыков. Наряду с фактчекингом, необходимо создание автоматизированных инструментов для обнаружения дипфейков, способных определить дату, время и физическое происхождение содержимого дипфейка, а в случае наличия признаков потенциальной опасности — остановить их размещение.

Целесообразно в социальных сетях и мессенджерах ввести обязательное упоминание создателями программного обеспечения о применении искусственного интеллекта при создании определенного рода материалов,

¹⁷ Нохрина М. Л. Субъективное гражданское право на собственное изображение в Российской Федерации // Петербургский юрист. 2017. № 1. С. 118.

¹⁸ Amelin R., Channov S. On the Legal Issues of Face Processing Technologies // Communications in Computer and Information Science. Vol. 1242. Springer Cham, 2020. P. 223–236.

введя обязательную маркировку дипфейк-контента, направленную на повышение осведомленности пользователей о таких материалах¹⁹.

Одновременно требуется создание нормативной базы, предусматривающей ответ-

ственность за создание и распространение дипфейк-материалов, которые могут нанести ущерб деловой репутации, унижить честь и достоинство человека, или материалов, распространяемых с другими преступными целями²⁰.

БИБЛИОГРАФИЯ

1. 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.
2. Капитонова Е. А. Шантаж «нюдсами» и смежные деяния: проблемы уголовно-правовой квалификации // Уголовное право. — 2021. — № 6. — С. 19–27.
3. 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.
4. Ключева А. А., Белов Д. А. Актуальное правовое исследование deepfake-технологий и новые вызовы для российской правовой системы // Вопросы российской юстиции. — 2021. — № 14. — С. 601–609.
5. Масликова Я. А. Дипфейки как угроза персональным данным // Грядущим поколениям завещаем: творить добро в защиту права : материалы Всероссийской научно-практической конференции с международным участием. — Ногинск, 2021. — С. 396–400.
6. Нохрина М. Л. Субъективное гражданское право на собственное изображение в Российской Федерации // Петербургский юрист. — 2017. — № 1. — С. 115–120.
7. Amelin R., Channov S. On the Legal Issues of Face Processing Technologies // Communications in Computer and Information Science. Volume 1242. — Springer Cham, 2020. — P. 223–236.

Материал поступил в редакцию 1 октября 2022 г.

REFERENCES

1. Ivanov VG, Ignatovskiy YaR. Deepfakes: perspektivy primeneniya v politike i ugrozy dlya lichnosti i natsionalnoy bezopasnosti [Deepfakes: Prospects of application in politics and threats to personality and national security]. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya «Gosudarstvennoe i munitsipalnoe upravlenie»* [RUDN Journal of Law. Series: State and municipal government]. 2020;4:79-386. (In Russ.).
2. Kapitonova EA. Shantazh «nyudsami» i smezhnye deyaniya: problemy ugolovno-pravovoy kvalifikatsii [Blackmail with «nudes» and related acts: Problems of criminal legal qualification]. *Ugolovnoe pravo* [Criminal Law]. 2021;6:19-27. (In Russ.).
3. Kiselev AS. O neobkhodimosti pravovogo regulirovaniya v sfere iskusstvennogo intellekta: dipfeyk kak ugroza natsionalnoy bezopasnosti [On the need for legal regulation in the field of artificial intelligence: Deepfake as a threat to national security]. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya «Yurisprudentsiya»* [Bulletin of the Moscow State Region University. Serie: Jurisprudence]. 2021;3:54-57. (In Russ.).
4. Klyueva AA, Belov DA. Aktualnoe pravovoe issledovanie deepfake-tekhnologiy i novye vyzovy dlya rossiyskoy pravovoy sistemy [Current legal research of deepfake technologies and new challenges for the Russian legal system]. *Voprosy rossiyskoy yustitsii* [Issues of Russian Justice]. 2021;14:601-609. (In Russ.).

¹⁹ Иванов В. Г., Игнатовский Я. Р. Указ. соч. С. 384.

²⁰ Ключева А. А., Белов Д. А. Актуальное правовое исследование deepfake-технологий и новые вызовы для российской правовой системы // Вопросы российской юстиции. 2021. № 14. С. 607.

5. Maslikova YaA. Dipfeyki kak ugroza personalnym dannym [Deepfakes as a threat to personal data]. In: Gryadushchim pokoleniyam zaveshchaem: tvorit dobro v zashchitu prava: materialy Vserossiyskoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiem [We bequeath to future generations: To do good in defense of the law. Proceedings of the All-Russian Scientific and Practical Conference with international participation]. Noginsk; 2021. Pp. 396–400. (In Russ.).
6. Nokhrina ML. Subektivnoe grazhdanskoe pravo na sobstvennoe izobrazhenie v Rossiyskoy Federatsii [Subjective civil right to your own Image in the Russian Federation]. *Peterburgskiy yurist [St. Petersburg Lawyer]*. 2017;1:115-120. (In Russ.).
7. Amelin R, Channov S. On the Legal Issues of Face Processing Technologies. *Communications in Computer and Information Science*. Volume 1242. Springer, Cham; 2019. Pp. 223–236.