УДК 341.9; 343.9.018.3
DOI 10.17150/2500-4255.2021.15(3).372-379

БОРЬБА С РАСПРОСТРАНЕНИЕМ РЕАЛИСТИЧНЫХ АУДИОВИЗУАЛЬНЫХ ПОДДЕЛЬНЫХ МАТЕРИАЛОВ ЗА РУБЕЖОМ (DEEPFAKE): УГОЛОВНО-ПРАВОВЫЕ И КРИМИНОЛОГИЧЕСКИЕ АСПЕКТЫ

Р.И. Дремлюга, А.И. Коробеев
Дальневосточный федеральный университет, г. Владивосток, Российская Федерация

Информация о статье

Дата поступления
12 марта 2021 г.

Дата принятия в печать
21 июня 2021 г.

Дата онлайн-размещения
2 июля 2021 г.

Ключевые слова
Реалистичные поддельные аудиовизуальные материалы; киберпреступление; компьютерное преступление; криминализация; преступление в Интернете; цифровая экономика

Финансирование
Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16129

Аннотация. В публикации рассматривается достаточно новый феномен распространения реалистичных аудиовизуальных поддельных материалов (deepfake). Данное общественно опасное деяние не отражено в российском уголовном законодательстве в качестве самостоятельного состава преступления. Вместе с тем некоторые страны приступили к формированию уголовной политики в данной сфере. Методика исследования предполагает сравнительно-правовой анализ действующего законодательства США, Китая и Европейского союза в части ответственности за распространение реалистичных аудиовизуальных подделок. Анализ уголовного законодательства направлен на систематизацию и выявление основных подходов к криминализации распространения реалистичных аудиовизуальных поддельных материалов в странах, лидирующих в цифровизации общества и экономики. В работе выявлено, что подходы к регламентации уголовной ответственности за рассматриваемое деяние кардинальным образом различаются. В публикации проанализирована уголовная политика Соединенных Штатов Америки на федеральном и региональном уровне в сфере уголовно-правовой охраны от посягательств посредством использования deepfake. Выявлено, что прежде всего преступным признается использование реалистичных аудиовизуальных поддельных материалов для вмешательства в выборы. В законодательстве некоторых штатов строго регламентируется порядок размещения таких материалов перед выборами, наиболее серьезные нарушения которого предполагают уголовную ответственность. Кроме того, в Соединенных Штатах Америки уголовно наказуемо использование deepfake для создания материалов интимного характера и преступления в виде кражи идентичности. В свою очередь Китайская Народная Республика устанавливает ответственность, в том числе уголовную, за размещение любых поддельных реалистичных аудиовизуальных материалов без упоминания об их нереалистичности. В праве Европейского союза пока отсутствуют специальные нормы уголовно-правового характера, регламентирующие ответственность за распространение deepfake. Такое деяние может рассматриваться как посягательство на правомерный оборот персональных данных. В работе также дается оценка некоторым криминологическим характеристикам рассматриваемого общественно опасного деяния в России и мире. Несмотря на относительную новизну технологии deepfake, реалистичные поддельные видео достаточно распространены. Общество поддерживает тезис о необходимости криминализации данного общественного опасного деяния.

A FIGHT AGAINST THE DISSEMINATION OF DEEPFAKES IN OTHER COUNTRIES: CRIMINAL AND CRIMINOLOGICAL ASPECTS

Roman I. Dremliuga, Alexander I. Korobeev
Far Eastern Federal University, Vladivostok, the Russian Federation

Article info

Received
2021 March 12

Accepted
2021 June 21

Available online
2021 July 2

Abstract. The authors analyze a relatively new phenomenon of spreading realistic audiovisual fake materials (deepfakes). This socially dangerous phenomenon is not reflected in the Russian criminal legislation as a separate offence. At the same time, some countries have started developing a criminal policy in this sphere. The methodology of the study presupposes a comparative law analysis of current legislations of the USA, China and the European union regarding the liability for the dissemination of realistic audiovisual fakes. The analysis of criminal legislation is aimed at the identification and systematization of key approaches to criminalizing the dissemination

ISSN 2500-4255

Keywords
Deepfake; cybercrime; computer crime; criminalization; crime in the Internet; digital economy

Financing
The reported study was funded by the RFBR within the research project № 18-29-16129

of realistic audiovisual fakes in the countries that are the leaders in digitizing their social and economic life. It showed that there are radically different approaches to regulating criminal liability for the actions under consideration. The authors analyzed criminal policy of the United States at the federal and state levels on the criminal law protection against infringements through deepfakes. They found that the first action to be recognized as criminal is the use of realistic audiovisual fakes for electoral intervention. The legislations of some states strictly regulate the procedure of posting such content before elections, the most serious violations leading to criminal liability. Besides, the United States recognizes as criminally punishable the use of deepfakes for creating materials of intimate nature and for identity theft. The People's Republic of China establishes liability, including criminal liability, for posting any fake realistic-looking audiovisual materials without mentioning that they are fake. Currently there are no special criminal law norms regulating liability for the dissemination of deepfakes in the law of the European Union. This action should be viewed as infringement of the lawful use of personal data. The authors give their assessment of some criminological characteristics of the analyzed publicly dangerous phenomenon in Russia and in the world. In spite of the relative novelty of the deepfake technology, realistic fake videos are quite common. The society supports the necessity of criminalizing this publicly dangerous action.

Технология deepfake стала настоящей сенсацией цифровых платформ в последние годы. Программное обеспечение, используя технологию искусственного интеллекта, позволяет достаточно реалистично подделать любые аудиовизуальные материалы. Например, существует канал в социальной сети Tik Tok, где размещены сгенерированные видео с Президентом Российской Федерации[1]. В опубликованных видеороликах первое лицо государства танцует молодежные танцы, парится в русской бане, прыгает в сугробы, режет салаты на Новый год и многое другое. При этом реалистично сымитировано не только видеоизображение, но и голос гаранта российской Конституции.

Видео или аудио, имитирующие отображение или речь реальных или вымышленных людей, вызвали огромный общественный резонанс [1]. Такие аудиовизуальные материалы называют deepfake (дословный перевод с английского — «глубокая подделка»). Несмотря на то что подобный прием давно используется в киноиндустрии, технологии такого высокого уровня реалистичности не были доступны ранее для широкого круга лиц. Такие цифровые подделки применялись исключительно кинематографическими студиями, для этого требовалось дорогостоящее оборудование и специалисты в сфере компьютерной графики.

В связи с увеличением доступности упомянутой технологии ситуация в корне изменилась. Стало широко распространенным бесплатное программное обеспечение, которое позволяет добиться высокого уровня реалистичности для сфабрикованных видео даже на домашнем компьютере. Для создания поддельного аудиовизуального материала больше не требуются глубокие познания в сфере компьютерной графики. Любой человек со скромными познаниями в сфере ИТ, потратив от одного часа времени, может сделать реалистичное видео или аудио. Например, в глобальной сети Интернет можно найти программный продукт DeepFaceLab, распространяемый абсолютно бесплатно, с подробной инструкцией для создания высоко реалистичных видеоподделок[2].

В основе технологии создания реалистичных аудиовизуальных материалов deepfake лежит один из подвидов искусственного интеллекта — генеративно-состязательные нейронные сети (GAN). Посредством машинного обучения искусственные нейронные сети на реальном наборе аудио-, видео- и фотоматериала учатся генерировать реалистичный поддельный контент. После процедуры обучения искусственного интеллекта можно продуцировать поддельные записи с выбранной персоной. Исследования показывают, что у пользователя при просмотре полученного с помощью технологии deepfake видео складывается впечатление, что он смотрит реально снятое видео [2]. Создание таких видео не единственный общественно опасный способ применения искусственного интеллекта [3–5].

В рамках исследования угроз, которые исходят от распространения поддельных реалистичных аудиовизуальных материалов, было установлено, что deepfake подрывает общее ощущение социальной и политической реаль-

[1] Первое лицо // TikTok. URL: https://www.tiktok.com/@1facerussia.

[2] URL: https://github.com/iperov/DeepFaceLab.

ности, может провоцировать насилие, а также смывает грань между реальностью и вымыслом. Цифровые подделки могут использоваться для дезинформации, манипулирования обществом. Кроме того, существует риск информационного раскола общества и провоцирования конфронтации отдельных социальных групп [6, с. 41].

Результаты некоторых исследований демонстрируют, что реалистичные поддельные материалы могут быстро распространяться в соцсетях без каких-либо усилий со стороны авторов такого контента. Такое быстрое и стремительное распространение через социальные сети называют вирусным. Иногда видеоролики набирают десятки миллионов просмотров за сутки [7, с. 68].

Потенциальный вред, причиняемый поддельными вирусными видео, сложно оценить, но некоторые примеры демонстрируют, что быстро распространяющиеся видео способны спровоцировать массовые случаи насилия и широкомасштабные беспорядки. Так, вирусное распространение сфальсифицированных видеоматериалов через мессенджер WhatsApp привело к массовым актам насилия и погромам против религиозных и этнических меньшинств в Индии [8].

Некоторые ученые прогнозируют «информационный апокалипсис», вызванный фальшивыми сообщениями. В информационном поле, наполненном поддельной информацией (неотличимой от настоящей), будет сложно ориентироваться при принятии решений экономического и политического характера [9, с. 283]. Увеличение доли поддельной информации, которая воспринимается как реальная, угрожает не отдельным жертвам или брендам, а существованию общества, основанного на информации в целом. Это угрожает успешному развитию цифровой экономики и информационного общества, так как посягает на их основу — отношения по поводу компьютерной информации. Под влиянием поддельных аудиовизуальных материалов в обществе могут приниматься политические и экономические решения, может совершаться морально-этический выбор.

По мнению некоторых исследователей, существующий подход в правовом регулировании отношений по поводу создания и использования поддельных аудиовизуальных материалов вызывает обеспокоенность общества. В законодательстве государств отсутствуют уголовно-правовые нормы, охраняющие от злонамеренных действий, нарушения неприкосновенности частной жизни или причинения морального вреда, вызванного реалистичными подделками, а также в случаях нарушения авторских прав, выдачи себя за другое лицо и мошенничества, связанного с deepfake [10, с. 145]. На сегодняшний день существует мало правовых инструментов для борьбы с высокотехнологичными подделками. Нельзя не согласиться с авторами, которые отмечают недостаток специальных норм правового регулирования отношений, связанных с распространением и созданием реалистичных подделок в зарубежном законодательстве.

Вместе с тем некоторые страны уже распознали угрозу, исходящую от бесконтрольного распространения реалистичных поддельных аудиовизуальных материалов. Соединенные Штаты Америки как один из лидеров глобальной цифровой трансформации считают deepfake долгосрочным вызовом безопасности государства. В отчете Счетной Палаты США говорится о том, что реалистичные цифровые подделки могут быть использованы как для дестабилизации общества, так и для шантажа официальных лиц[3]. Согласно закону, принятому в 2019 г. (Deepfake Report Act of 2019), Министерство национальной безопасности должно ежегодно оценивать угрозу использования технологий подделки цифрового контента (англ. Digital content forgery) и представлять рекомендации по разработке мер противодействия данной угрозе[4].

Первым в мире нормативным актом, регламентирующим уголовную ответственность за создание и распространение deepfake, стал закон штата Техас, который вступил в силу 1 сентября 2019 г., — «закон, касающийся уголовного преступления путем фальсификации видео с намерением повлиять на результат выборов», определяет контекст, в котором подделка видеоматериалов считается наказуемой. В законе для обозначения поддельных видеоматериалов применяется термин deepfake, который часто используется в технической литературе или в повседневном обороте. Рассматриваемый нормативный акт устанавливает уголовную ответственность за создание и распространение поддельных видео за 30 дней до выборов. В законе дается определение поддельного видео как «ви-

[3] National Security: Long-Range Emerging Threats Facing the United States as Identified by Federal Agencies // U.S. Government Accountable Office. 2018. Dec. URL: https://www.gao.gov/assets/700/695981.pdf.

[4] Deepfake Report Act of 2019 // 116th Congress (2019–2020), S. 2065. URL: https://www.congress.gov/bill/116th-congress/senate-bill/2065/text.

део, созданного с помощью искусственного интеллекта с целью ввести в заблуждение, что человек на видео совершал действия, которые он в действительности не совершал»[5]. Закон штата Техас признает уголовным деянием не любое использование поддельных видео, а только направленное против проведения выборов.

Существуют и другие штаты, в законодательстве которых регламентирована ответственность за распространение deepfake, созданных против лиц, участвующих в выборах. Согласно закону штата Калифорния наказуемы производство, распространение, публикация или передача в эфир поддельных аудиовизуальных материалов, сфабрикованных с умыслом, без прямого упоминания, что это подделка. Действие акта также распространяется только на время предвыборной кампании[6]. В законе установлено, что материалы должны быть действительно реалистичными, и их реалистичность может ввести в заблуждение разумное лицо (англ. reasonable person). Таким образом, в соответствии с принятым законом подделки, которые потребитель информации не признает в качестве реальных, не несут в себе общественной опасности. Также одним из необходимых признаков является формирование ложного образа кандидата на выборах посредством подделки. То есть если «цифровая фальшивка» воспроизводит реальные события, она также не является опасной. Законодательство штата Калифорния не считает наказуемыми деяния в виде создания и распространения видео, которые создают ложное впечатление о политическом деятеле, который не участвует в выборах.

Самый большой срок запрета на распространение предвыборных поддельных аудиовизуальных материалов предусмотрен в законодательстве штата Мериленд. Закон на уровне штата предусматривает наказание за умышленную публикацию и распространение реалистичных поддельных видео, направленных против кандидатов, за 90 дней до дня выборов. Это не относится к аудио и видео, в которых содержится упоминание о поддельности, соответствующее по форме и содержанию требованиям, указанным в законе.

Практика установления ответственности за распространение реалистичных поддельных аудиовизуальных материалов с кандидатами на выборы нашла свое отражение и на федеральном уровне. Так, в январе 2021 г. в Сенат США поступил на рассмотрение проект закона, который вводит запрет на умышленное распространение deepfake за 60 дней до выборов федерального значения. Для привлечения к ответственности аудио или видео должны публиковаться со злым умыслом с целью нанесения ущерба репутации кандидата, а также манипуляции выбором избирателя. Исключение, как и в законах штатов, составляют материалы, в которых явно указано, что это подделка[7].

Законодательство США регламентирует уголовную ответственность не только в сфере вмешательства в избирательный процесс посредством deepfake. В уголовном законодательстве некоторых штатов предусмотрена ответственность за реалистичную поддельную порнографию, в которой использовались лица реальных персон. Это достаточно частая практика, так как одними из первых поддельных реалистичных видео, привлекших внимание общественности, были порнографические видео, где использовались лица голливудских актрис [11]. По мнению некоторых авторов, с этической и нормативной точек зрения реалистичные поддельные порнографические видео, прежде всего, рассматриваются как новая форма посягательства на частную жизнь. Сексуальная приватность выполняет неоценимую функцию в обществе: она способствует развитию личности, интимности и равенства. Кроме того, сексуальная приватность является одним из краеугольных камней человеческой самостоятельности и автономии [12]. Кроме того, такие видео могут использоваться для преследования лиц и их сексуального порабощения [13].

Примером закона, регламентирующего уголовную ответственность за распространение порнографических реалистичных подделок, является нормативный акт штата Вирджиния § 18.2-386.2. Нормы закона устанавливают уголовную ответственность для любого лица, которое с намерением принудить, притеснить или запугать злонамеренно распространяет или продает любое видео или неподвижное изображение, созданное любым способом. Это относится к ложно созданным видео, которые изображают другое лицо, полностью обнаженное, когда демонстри-

[5] An act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election : Texas Senate Bill No. 751. Takes effect 1 Sept. URL: https://capitol.texas.gov/ tlodocs/86R/billtext/pdf/SB00751I.pdf.

[6] California Assembly Bill № 730. URL: http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730.

[7] For the People Act of 2021 H.R.1, 4 Jan. 2021. URL: https://www.congress.gov/117/bills/hr1/BILLS-117hr1ih.pdf.

руются половые органы, лобковая область, ягодицы или женская грудь. Преступник в данном случае виновен в совершении преступления небольшой тяжести (англ. misdemeanor 1)[8].

В некоторых штатах создание и распространение реалистичных поддельных видео, использующих чье-либо лицо, рассматривается как преступление подделки личности (англ. crime of identity fraud). Например, законодательство штата Массачусетс регламентирует уголовную ответственность за использование реалистичных поддельных видео для совершения правонарушений. Deepfake (именно такой термин используется в законе) определяется как аудиовизуальная запись, созданная или измененная таким образом, что эта запись будет воспринята вменяемым наблюдателем как подлинная запись реальной речи или поведения человека. Такое преступление, согласно тексту закона, относится к категории подделки личности[9].

В штате Нью-Йорк законодатели неоднократно выносили на рассмотрение законопроект о защите права на «цифровое подобие человека»[10]. Законопроект был представлен на рассмотрение в законодательный орган штата в 2019 г., но его срок истек. В 2020 г. переработанный проект закона вновь был вынесен на рассмотрение. Он подразумевает правовую охрану цифрового сходства человека в течение 40 лет после его смерти.

Таким образом, в США регламентирована уголовная ответственность за создание и распространение трех категорий реалистичных поддельных аудиовизуальных материалов. Во-первых, deepfake, изображающие кандидатов, участвующих в выборах, во время предвыборной кампании (от 30 до 90 дней до выборов). Во-вторых, порнографические реалистичные поддельные видео, имитирующие конкретных лиц. В-третьих, поддельные материалы, посягающие на идентичность лица.

Другой лидер цифровой сферы — Китай — также установил уголовную ответственность за публикацию поддельных реалистичных видео или аудиоматериалов [14]. Кроме того, компании и лица, которые работают с компьютерной информацией, должны маркировать поддельные аудио- и видеоматериалы в качестве таковых. Статья 11 Правил администрирования сервисов аудио- и видеоинформации (англ. Regulations on the Administration of Network Audio and Video Information Services, далее — Правила) регламентирует, что поставщики услуг и пользователи, применяющие новые технологии и прикладные программы, основанные на машинном обучении (речь о deepfake) и виртуальной реальности, для производства, публикации и распространения искусственно созданной аудио- и видеоинформации, должны маркировать подобную компьютерную информацию так, чтобы это было заметно[11].

В Китае не запрещено распространение реалистичных поддельных аудиовизуальных материалов, но существует обязанность маркировать такую компьютерную информацию для лиц, ее распространяющих. В рассматриваемом законе перечислены основные негативные последствия от распространения реалистичных поддельных материалов (ст. 13–14), среди нежелательных эффектов значатся распространение и возникновение слухов. В основном законодательный акт предусматривает для нарушителей меры административно-правового характера, но ст. 18 Правил обозначает, что за незаконное распространение реалистичных аудиовизуальных подделок нарушитель может быть привлечен к уголовной ответственности.

В Европе пока не приняты специальные нормы, регламентирующие ответственность за распространение реалистичных поддельных аудиовизуальных материалов. Вместе с тем публикация deepfake охватывается действием Общего регламента по защите данных (англ. General Data Protection Regulation). Текст ст. 4 (1) гласит, что «персональные данные — любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу (субъект данных); идентифицируемое физическое лицо — это лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, фамилия, идентификационный номер, данные о местоположении, онлайн-идентификатор или один или несколько характерных для

[8] Bill to amend and reenact § 18.2-386.2 of the Code of Virginia, relating to unlawful dissemination or sale of images of another; falsely created videographic or still image; penalty. House Bill no. 2678, 2019. URL: https://lis.virginia.gov/cgi-bin/legp604.exe?191+ful+HB2678S1&191+ful+HB2678S1.

[9] An Act to protect against deep fakes used to facilitate criminal or torturous conduct. House Bill no. 3366. URL: https://malegislature.gov/Bills/191/H3366.Html.

[10] Draft Bill of the State of New York, 5605-B, 2019-2020 Regular Sessions, Febr. 14, 2019. URL: https://legislation.nysenate.gov/pdf/bills/2019/A5605B.

[11] Regulations on the Administration of Network Audio and Video Information Services, Issued by Cyberspace Administration of China, 1 Jan. 2020. URL: http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm.

указанного лица физических, физиологических, генетических, духовных, экономических, культурных факторов или ссылка на факторы социальной идентичности»[12]. Таким образом, если для создания реалистичной подделки используется реальное лицо, такой аудиовизуальный материал будет рассматриваться как персональные данные.

Общий регламент по защите данных не предусматривает уголовную ответственность за распространение реалистичных поддельных аудио- и видеоматериалов. Общеевропейский нормативный акт предоставляет охрану и защиту прав для жертв deepfake посредством запрета на распространение такой информации и обязанности компаний, предоставляющих услуги и сервисы, удалить подобные материалы [15]. Вместе с тем, как отмечалось выше, реалистичная подделка может расцениваться как персональная информация, если данную информацию можно связать с конкретным физическим лицом. В случае если в deepfake используется лицо, которое можно идентифицировать, применяются традиционные уголовно-правовые нормы, регламентирующие уголовную ответственность за посягательства на персональную информацию или за клевету [16].

В России вопрос о криминализации распространения поддельных видео также назрел. Согласно проведенному нами опросу 158 специалистов в ИТ и кибербезопасности, около 79 % респондентов считают, что реалистичное поддельное видео с использованием чужого лица, размещаемое в сети Интернет, необходимо выделять специальным текстом о том, что видео является сгенерированным. Лишь около 13 % интервьюируемых заявили об отсутствии необходимости сообщать о поддельном характере видео. Таким образом, анкетирование показало, что большинство поддерживает вменение обязанности по надлежащему информированию пользователей о том, что материал был сгенерирован посредством специальных технологий. Зарубежные исследования также подтверждают осознание социумом общественной опасности использования технологии deepfake [17].

Официальной статистики по распространенности реалистичных поддельных видео в русскоязычном Интернете не ведется. Тем не менее сопутствующие данные свидетельствуют, что в России такое явление достаточно распространено. Например, профиль с поддельными видео Президента РФ в социальной сети Tik Tok в мае 2021 г. набрал более 6,5 млн подписчиков и 250 млн просмотров (одно из видео более 90 млн просмотров). Реалистично сфабрикованные видео гаранта Конституции опубликованы и в других популярных социальных сетях[13]. Эти данные свидетельствуют о том, что в России реалистичные поддельные аудиовизуальные материалы достаточно популярны.

Криминолого-социологические исследования показывают, что широкое распространение поддельных реалистичных видео угрожает существованию современного общества, основанного на информации. Так как любое лицо может стать потерпевшим от подобных видео. Технические решения, разработанные в данный момент, в основном направлены на защиту известных политиков и представителей шоу-бизнеса и не рассчитаны на противодействие deepfake в повседневной жизни общества. Вместе с тем именно использование правдоподобных поддельных видео против обычных лиц несет в себе большую угрозу, так как создает в обществе массовое недоверие любой распространяемой информации. В условиях цифровой трансформации это означает дестабилизацию социума [18].

Исследование, проведенное компанией Deeptrace (работает в сфере кибербезопасности) в сентябре 2019 г., показало, что за девять месяцев, предшествующих опубликованию результатов, количество так называемых фальшивых видео удвоилось. Большая часть deepfake были порнографическими видео, используемыми для причинения вреда женщинам. В отчете об исследовании также подчеркивался потенциал использования этой технологии в политических кампаниях. В опубликованном исследовании отмечалась угроза, исходящая от поддельных аудиовизуальных материалов, не только для политической стабильности. В частности были получены доказательства о растущем использовании deepfake для совершения мошенничества или кибербуллинга [19].

По мнению некоторых авторов, существующая динамика роста количества опубликования

[12] О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС (Общие правила защиты данных) : регламент (ЕС) 2016/679 Европ. парламента и совета. URL: https://ogdpr.eu/ru/gdpr-2016-679.

[13] Путин в Казино Рояль // YouTube. URL: https://www.youtube.com/watch?v=WWnTs2MMYs0.

реалистичных поддельных аудиовизуальных материалов угрожает институту выборов в целом. Дезинформация, распространяемая посредством deepfake, может представлять собой проблему во время выборов, поскольку сложно отличить современную подделку от настоящего видео. Любой политический игрок может попытаться дискредитировать оппонента или спровоцировать политический скандал с целью продвижения собственной повестки. После просмотра deepfake граждане могут, например, изменить свое отношение к политику, изображенному в нем, или к партии этого политика. Это может привести к принятию решения на основе ложной информации в соответствии с целями политического актора, стоящего за распространением поддельного материала [20].

Проведенный в работе анализ показывает, что некоторые страны признали распространение поддельных реалистичных аудиовизуальных материалов общественно опасным деянием. В основном публикация deepfake угрожает общественно-политической сфере, поэтому в США на федеральном уровне и на уровне штатов признается уголовно наказуемым именно вмешательство в выборы посредством реалистичных подделок. Вместе с тем существуют примеры криминализации других видов использования поддельных реалистичных аудиовизуальных материалов. В Европе использование чужого лица в сфабрикованном ролике есть прежде всего посягательство на персональные данные.

Следует отметить, что в российском Интернете достаточно распространены подобные ролики. Их использование угрожает политической и социальной стабильности государства. Российскому законодателю также стоит принять меры по совершенствованию уголовно-правовой охраны общества от посягательств посредством поддельных реалистичных аудиовизуальных материалов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Chesney R. Disinformation on Steroids: The Threat of Deep Fakes / R. Chesney, K.C. Danielle // Council on Foreign Relations. — 2018. — 16 Oct. — URL: https://www.cfr.org/report/deep-fakedisinformation-steroids.

2. Кондратьев Р.Я., Миронова Н.Г. Фейк-новости как инструмент социального управления и объект применения методов информационной безопасности // Современные технологии управления. — 2020. — № 1 (91). — URL: https://sovman.ru/article/9106.

3. Roman D. Artificial Intelligence Legal Policy: Limits of use of some Kinds of AI / D. Roman, P. Natalia // ACM International Conference Proceeding Series. — 2019. — Pt. F147956. — P. 343–346.

4. AI-enabled Future Crime / M. Caldwell, J. Andrews, T. Tanay, L.D. Griffin // Crime Science. — 2020. — Vol. 9. — P. 1–14.

5. Dremliuga R. Combating the Threats of Cybercrimes in Russia Evolution of the Cybercrime Laws and Social Concern / R. Dremliuga, O. Dremliuga, P. Kuznetsov // Communist and Post-Communist Studies. — 2020. — Vol. 53, iss. 3. — P. 123–136.

6. Yadlin-Segal A. Whose Dystopia is it Anyway? Deepfakes and social Media Regulation / A. Yadlin-Segal, Y. Oppenheim // Convergence. — 2021. — Vol. 27. — P. 36–51.

7. Wuebben D. Getting Likes, Going Viral, and the Intersections Between Popularity Metrics and Digital Composition / D. Wuebben // Computers and Composition. — 2016. — Vol. 42. — P. 42–69.

8. Mukherjee R. Mobile Witnessing on WhatsApp: Vigilante Virality and the Anatomy of Mob Lynching / R. Mukherjee // South Asian Popular Culture. — 2020. — Vol. 18, iss. 1. — P. 79–101.

9. Stover D. Garlin Gilchrist: Fighting Fake News and the Information Apocalypse / D. Stover // Bulletin of the Atomic Scientists. — 2018. — Vol. 74, iss. 4. — P. 283–288.

10. Deepfakes: Trick or Treat? / J. Kietzmann, L.W. Lee, I.P. McCarthy, T.C. Kietzmann // Business Horizons. — 2020. — Vol. 63, iss. 2. — P. 135–146.

11. Maddocks S. 'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities Between Pornographic and 'Political' Deep Fakes / S. Maddocks. — DOI: 10.1080/23268743.2020.1757499 // Porn Studies. — 2020. — Vol. 7, iss. 5. — P. 415–423.

12. Regulating deep Fakes: Legal and Ethical Considerations / E. Meskys, A. Liaudanskas, J. Kalpokiene, P. Jurcys // Journal of Intellectual Property Law and Practice. — 2020. — Vol. 15, № 1. — P. 24–31.

13. Chesney B. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security / B. Chesney, D. Citron // California Law Review. — 2019. — Vol. 107, iss. 6. — P. 1753–1820.

14. Statt N. China Makes it a Criminal offense to Publish Deepfakes or Fake News without Disclosure / N. Statt // The Verge. — 2019. — 29 Nov. — URL: https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality.

15. Wulff C.M. The Right to be Forgotten in Post-google Spain Case Law: An Example of Legal Interpretivism in Action? / C.M. Wulff // Comparative Law Review. — 2020. — № 26. — P. 225–253.

16. Kozlowski D. «For the Protection of the Reputation or Rights of Others»: The European Court of Human Rights' Interpretation of the Defamation Exception in Article 10 (2) / D. Kozlowski. — DOI: 10.1207/s15326926clp1101_4 // Communication Law and Policy. — 2006. — Vol. 11, iss. 1. — P. 133–178.

17. Cochran J.D. Deepfakes: Awareness, Concerns, and Platform Accountability / J.D. Cochran, S.A. Napshin // Cyberpsychology, Behavior, and Social Networking. — 2021. — Vol. 24, iss. 3. — P. 164–172.

18. Ascott T. Microfake: How Small-scale Deepfakes can Undermine Society / T. Ascott // Journal of Digital Media and Policy. — 2020. — Vol. 11, iss. 2. — P. 215–222.

19. Dasilva J.P. Deepfakes on Twitter: Which Actors Control their Spread? / J.P. Dasilva, K.M. Ayerdi, T.M. Galdospin // Media and Communication. — 2021. — Vol. 9, № 1. — P. 301–312.

20. Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes? / T. Dobber, N. Metoui, D. Trilling [et al.] // International Journal of Press/Politics. — 2021. — Vol. 26, iss. 1. — P. 69–91.

REFERENCES

1. Chesney R., Danielle K.C. Disinformation on Steroids: The Threat of Deep Fakes. *Council on Foreign Relations*, 2018, Oct. 16. URL: https://www.cfr.org/report/deep-fakedisinformation-steroids.

2. Kondrat'yev R.Ya., Mironova N.G. Fake News as a Tool of Social Management and an Object of Application of Information Security Methods. *Sovremennye tekhnologii upravleniya = Modern Management Technology*, 2020, no. 1. URL: https://sovman.ru/article/9106. (In Russian).

3. Roman D., Natalia P. Artificial Intelligence Legal Policy: Limits of use of some Kinds of AI. *ACM International Conference Proceeding Series*, 2019, pt. F147956, pp. 343–346.

4. Caldwell M., Andrews J., Tanay T., Griffin L.D. AI-enabled Future Crime. *Crime Science*, 2020, vol. 9, pp. 1–14.

5. Dremliuga R., Dremliuga O., Kuznetsov P. Combating the Threats of Cybercrimes in Russia Evolution of the Cybercrime Laws and Social Concern. *Communist and Post-Communist Studies*, 2020, vol. 53, iss. 3, pp. 123–136.

6. Yadlin-Segal A., Oppenheim Y. Whose Dystopia is it Anyway? Deepfakes and social Media Regulation. *Convergence*, 2021, vol. 27, iss, pp. 36–51.

7. Wuebben D. Getting Likes, Going Viral, and the Intersections Between Popularity Metrics and Digital Composition. *Computers and Composition*, 2016, vol. 42, pp. 42–69.

8. Mukherjee R. Mobile Witnessing on WhatsApp: Vigilante Virality and the Anatomy of Mob Lynching. *South Asian Popular Culture*, 2020, vol. 18, iss. 1, pp. 79–101.

9. Stover D. Garlin Gilchrist: Fighting Fake News and the Information Apocalypse. *Bulletin of the Atomic Scientists*, 2018, vol. 74, iss. 4, pp. 283–288.

10. Kietzmann J., Lee L.W., McCarthy I.P., Kietzmann T.C. Deepfakes: Trick or Treat? *Business Horizons*, 2020, vol. 63, iss. 2, pp. 135–146.

11. Maddocks S. 'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities Between Pornographic and 'Political' Deep Fakes. *Porn Studies*, 2020, vol. 7, iss. 5, pp. 415–423. DOI: 10.1080/23268743.2020.1757499.

12. Meskys E., Liaudanskas A., Kalpokiene J., Jurcys P. Regulating deep Fakes: Legal and Ethical Considerations. *Journal of Intellectual Property Law and Practice*, 2020, vol. 15, no. 1, pp. 24–31.

13. Chesney B., Citron D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 2019, vol. 107, iss. 6, pp. 1753–1820.

14. Statt N. China Makes it a Criminal offense to Publish Deepfakes or Fake News without Disclosure. *The Verge*, 2019, Nov. 29. URL: https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality.

15. Wulff C.M. The Right to be Forgotten in Post-google Spain Case Law: An Example of Legal Interpretivism in Action? *Comparative Law Review*, 2020, no. 26, pp. 225–253.

16. Kozlowski D. «For the Protection of the Reputation or Rights of Others»: The European Court of Human Rights' Interpretation of the Defamation Exception in Article 10 (2). *Communication Law and Policy*, 2006, vol. 11, iss. 1, pp. 133–178. DOI: 10.1207/s15326926clp1101_4.

17. Cochran J.D., Napshin S.A. Deepfakes: Awareness, Concerns, and Platform Accountability. *Cyberpsychology, Behavior, and Social Networking*, 2021, vol. 24, iss. 3, pp. 164–172.

18. Ascott T. Microfake: How Small-scale Deepfakes can Undermine Society. *Journal of Digital Media and Policy*, 2020, vol. 11, iss. 2, pp. 215–222.

19. Dasilva J.P., Ayerdi K.M., Galdospin T.M. Deepfakes on Twitter: Which Actors Control their Spread? *Media and Communication*, 2021, vol. 9, no. 1, pp. 301–312.

20. Dobber T., Metoui N., Trilling D., Helberger N., de Vreese C. Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes? *International Journal of Press/Politics*, 2021, vol. 26, iss. 1, pp. 69–91.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Дремлюга Роман Игоревич — доцент Юридической школы Дальневосточного федерального университета, кандидат юридических наук, г. Владивосток, Российская Федерация; e-mail: dremliuga.ri@dvfu.ru.

Коробеев Александр Иванович — заведующий кафедрой уголовного права и криминологии Дальневосточного федерального университета, доктор юридических наук, профессор, заслуженный деятель науки РФ, г. Владивосток, Российская Федерация; e-mail: akorobeev@rambler.ru.

INFORMATION ABOUT THE AUTHORS

Dremliuga, Roman I. — Ass. Professor, Law School, Far Eastern Federal University, Ph.D. in Law, Vladivostok, the Russian Federation; e-mail: dremliuga.ri@dvfu.ru.

Korobeev, Alexander I. — Head, Department of Criminal Law and Criminology, Far Eastern Federal University, Doctor of Law, Professor, Honored Scientist of the Russian Federation, Vladivostok, the Russian Federation; e-mail: akorobeev@rambler.ru.

ДЛЯ ЦИТИРОВАНИЯ

Дремлюга Р.И. Борьба с распространением реалистичных аудиовизуальных поддельных материалов за рубежом (deepfake): уголовно-правовые и криминологические аспекты / Р.И. Дремлюга, А.И. Коробеев. — DOI 10.17150/2500-4255.2021.15(3).372-379 // Всероссийский криминологический журнал. — 2021. — Т. 15, № 3. — С. 372–379.

FOR CITATION

Dremliuga R.I., Korobeev A.I. A fight against the dissemination of deepfakes in other countries: criminal and criminological aspects. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2021, vol. 15, no. 3, pp. 372–379. DOI: 10.17150/2500-4255.2021.15(3).372-379. (In Russian).