

Е.А.Виноградова

Злонамеренное использование политических дипфейков и попытки их нейтрализации в странах Латинкой Америки

Технология дипфейк (*Deepfake*) произвела революцию в области искусственного интеллекта и коммуникационных процессов, создав настоящую угрозу распространения дезинформации среди целевых аудиторий на цифровых платформах. Злонамеренное использование политических дипфейков активно распространилось в период 2017—2023 гг. Атакам с элементами доксинга подверглись политические лидеры Аргентины, Бразилии, Колумбии и Мексики. Поддельные видео, в которых демонстрировались лица политиков, подрывали их репутацию, снижая доверие электората. Эти видео стали передовым инструментом манипулирования общественным мнением. Целая серия политических дипфейков поставила перед странами латиноамериканского региона вопрос о необходимости разработки своевременного правового регулирования. Цель данного исследования — выявить угрозы, связанные с неконтролируемым применением политического дипфейка в государствах Латинской Америки. В соответствии с поставленной целью автор анализирует политические дипфейки; выделяет основные угрозы, возникающие в ходе применения технологии дипфейк; рассматривает законодательные особенности их использования в странах Латинской Америки. В статье дается характеристика основных детекторов и программ по обнаружению злонамеренного использования дипфейков; в научный оборот вводится определение политический дипфейк.

Ключевые слова: политический дипфейк, доксинг, дезинформация, законодательно-правовая база, информационно-психологическое влияние, внутривнутриполитическая безопасность, технологии искусственного интеллекта, политический лидер, социальные сети, СМИ, выборы.

DOI: 10.31857/S0044748X0025404-3

Статья поступила в редакцию 05.02.2023.

Екатерина Алексеевна Виноградова — кандидат политических наук, независимый исследователь (<https://orcid.org/0000-0001-8055-6612>, vinogradovacatherine7@gmail.com).

В последние годы важным направлением в области международной и внутривнутриполитической безопасности является внедрение технологий искусственного интеллекта (ИИ) в политический, дипломатический и экономический инструментарий. Вместе с тем применение новейших информационных технологий приводит к возникновению новых угроз безопасности и конфиденциальности информации, затрагивает правовые и этические вопросы.

Появление технологии дипфейк в 2017 г. привело к ее молниеносному распространению с целью распространения ложной информации и манипулирования общественным мнением. Примерами этого могут послужить политические манипуляции в период 2018—2023 гг. в США, Индии, странах Евросоюза и Латинской Америки. Российские ученые Д.Ю.Базаркина и Е.Н.Пашенцев в своей статье «Злонамеренное использование искусственного интеллекта: вызовы информационно-психологической безопасности в Латинской Америке» справедливо отмечают, что высокий уровень присутствия латиноамериканцев в Интернете, острый экономический кризис, другие тяжелые последствия пандемии коронавируса, социальная нестабильность, активная политическая борьба, высокий уровень коррупции и преступности, а также столкновение геополитических интересов в регионе делают угрозу злонамеренного использования искусственного интеллекта здесь все более актуальной [1, сс. 259-260].

Латиноамериканские государства, занимающие ведущие позиции в мире по числу интернет-пользователей, являются наиболее уязвимым регионом в отношении намеренного использования дипфейков. В странах региона активно применяют игровые приложения дипфейк. К примеру, Бразилия является второй страной после США по количеству пользователей данной платформы (20% от общего числа пользователей во всем мире) [2, р. 7]. Несмотря на это, согласно исследованию, проведенному компанией «Лаборатория Касперского», 70% латиноамериканских пользователей не знают о существовании этой технологии. Из проведенного опроса следует, что доля пользователей, которым неизвестна эта технология, выше всего в Перу (75%), затем следуют Мексика и Чили (72%), Аргентина (67%), Бразилия (66%) и Колумбия (63%) [3].

Условно все дипфейки можно поделить на несколько групп:

— дипфейки развлекательного характера. Создаются при помощи специальных программ (*Doublicat, FaceApp, DeepFaceLab* и др.), где возможно сделать юмористические видеоролики;

— дипфейки-компроматы, направленные на подрыв репутации того или иного лица с целью манипулирования или пиара. Часто жертвами дипфейков-компромата становятся звезды шоу-бизнеса и публичные лица. В 2020 г. более 100 тыс. женщин по всему миру стали жертвами порнографических дипфейков [4];

— политические дипфейки, целью которых является искажение информации о том или ином политике для манипулирования общественным мнением и подрыва репутации.

В связи с этим автор вводит в научный оборот следующее определение: политический дипфейк — специальная кампания с применением технологии искусственного интеллекта для подрыва репутации политических лидеров с целью изменения хода избирательной борьбы или для дискредитации действующего политика.

Методология данного исследования основана на системном подходе, направленном на изучение технологии дипфейк, используемой в качестве политического инструмента и направленной на дискредитацию политических лидеров в странах Латинской Америки. В статье использованы следующие группы источников: статистические данные латиноамериканских и российских исследовательских лабораторий, нормативные документы латиноамериканских стран (проекты законов, законы, статьи уголовного кодекса, пакты), интервью, СМИ, научные работы зарубежных и отечественных исследователей.

В работе использовались такие методы, как дискурсивный анализ для интерпретации отдельных фейковых видеороликов и новостей политической направленности, метод *case study* для детального изучения законодательной базы в отношении ложных новостей в странах Латинской Америки, метод классификации для систематизации научной литературы и полученных результатов исследования.

ТЕХНОЛОГИЯ ДИПФЕЙК В ТРУДАХ ОТЕЧЕСТВЕННЫХ И ЗАРУБЕЖНЫХ СПЕЦИАЛИСТОВ

На сегодняшний день существует немало научных трудов, посвященных изучению дипфейков, которые можно разделить на несколько групп. К первой группе источников можно отнести общетеоретические работы. Так, обзор существующей научной литературы, посвященной дипфейкам, приводится в статье португальского специалиста Сони Гомеш-Гонсалвес [5]. В монографии американского исследователя Тима Хвана [6] детально рассмотрена техническая литература по ИИ и дана основная классификация дипфейк-угроз. Социально-медийный сценарий этого феномена изучается в работе мексиканского ученого Якоба Банюэлоса Капистрана «Дипфейк: изображения во времена постправды» [7]. Использование дипфейков как части стратегии информационно-психологической войны рассмотрено в статье Хитоси Насу [8]. Влияние дипфейков на политическую сферу и методы технической защиты от данной угрозы анализируются в монографии, выпущенной амстердамским центром *Deeprance* [9]. Бразильский исследователь Кристиане Пантоха де Мораес проводит анализ последствий манипуляций дипфейками в социальных сетях [10]. В статье Ж.Ботхи и К.Пиетерсе [11] подробно рассмотрены инструменты и технологии, применяемые для создания и обнаружения фальшивых новостей и роликов. Также методы и технологии обнаружения дипфейков в различных видеороликах изучаются в работе испанских ученых Виктора Сердана Мартинеса, Марии Луизы Гарсии Гуардиа, Грасиэлы Падиллы Кастильо [12].

Ко второй группе источников относится литература, посвященная изучению влияния дипфейков на политические институты разных стран. В статье австралийского исследователя Эндрю Райя [13] анализируется действующее австралийское законодательство и готовящиеся поправки к федеральным избирательным законам в отношении политических дипфейков для уменьшения угрозы, которую они представляют для выборов. Натали Люссье в своей работе [4] рассматривает основные угрозы намеренного использования дипфейков и правовые решения в отношении этой технологии. Американские ученые из Института Брукингса Дэниел Л.Байман, Чунъян Гао, Крис Мезероле, В.С.Субрахманян на примере конфликтов на Ближнем Востоке анализируют угрозы, исходящие от применения технологии дипфейк в вооруженных конфликтах [14]. В статье американского исследователя Тодда Хельмуса [15] рассмотрены технологии ИИ, в том числе дипфейк, которые оказали влияние на выборы в США и были использованы во внешнеполитическом дискурсе Китая. Не менее интересной представляется работа отечественного исследователя Я.В.Лексютинной [16], в которой автор раскрывает общую картину масштабов и направленности использования дипфейков в мире, а также оценивает риски применения этой технологии для Японии и восприятие рисков японской стороной. Российские специалисты Я.Р.Игнатовский и В.Г.Иванов [17] рассматривают потенциальные угрозы от применения технологии дипфейк и законодательные инструменты как метод противодействия распространению дезинформации и ложных новостей. Дефиниция дипфейка и оценка его характеристик в зависимости от способов и целей распространения этого инструмента для воздействия на политический дискурс в современной России представлена в работе М.А.Фалеева., Н.А.Ситдиковой, Е.Е.Нечай [18].

Третья группа источников состоит из научной литературы, посвященной применению технологии дипфейк в странах Латинской Америки. В статье бразильского исследователя Пауло Карлоса Лопес-Лопеса [19] приводится множество примеров влияния фальшивых новостей на дискредитацию политической власти в странах латиноамериканского региона. Влияние дипфейк-роликов на политические выборы в странах Латинской Америки подробно описываются в диссертации Сары Марсенес Пинейру де Резенде [2]. В работе описано множество конкретных примеров политических дипфейков, направленных на подрыв репутации латиноамериканских лидеров. Коллектив авторов из Массачусетского технологического университета [20] на примере президентов Бразилии раскрывают особенности политической сатиры, которая создается при помощи технологии дипфейк. Колумбийский ученый Хуан Фелипе Родриго Лопес [21] обращает внимание на растущую угрозу применения данной технологии и использование ее в популярных социальных сетях для оказания давления на выборы в Колумбии. Российские исследователи Н.А.Цветкова, Т.А.Гришанина [22] на примере китайской цифровой платформы *TikTok* приводят примеры деструктивного использования интернет-ресурсов, раскрывая особенности

влияния технологии дипфейк на политические события в странах Латинской Америки.

ИСПОЛЬЗОВАНИЕ ПОЛИТИЧЕСКИХ ДИПФЕЙКОВ В СТРАНАХ ЛАТИНСКОЙ АМЕРИКИ

Политический дипфейк стал одним из важных инструментов, применяемых для подрыва авторитета государственных лидеров Латинской Америки. Согласно исследованию, проведенному компанией «Лаборатория Касперского» и консалтинговой фирмой *CORPA*, около трети латиноамериканцев ежедневно используют социальные сети: в Мексике (35%), Бразилии (33%), Чили (32%), Перу (31%), Аргентина (28%), в Колумбия (26%), и только 17% читают новости, транслируемые традиционными медиасайтами [23].

Исследование, проведенное сотрудниками Массачусетского технологического института (*Massachusetts Institute of Technology, MIT*) за 2018 г., показало, что фейковые новости на 70% чаще попадают в новостную ленту и распространяются с большей скоростью, чем достоверная информация традиционных СМИ [24]. Так, в 2018 г. дипфейковое видео было направлено против кандидата в президенты Мексики Андреса Мануэля Лопеса Обрадора (2018 — н/в), где будущий лидер был запечатлен в нетрезвом состоянии [25]. Вирусный ролик с элементами доксинга* моментально распространился в популярных социальных сетях и мессенджерах, вызвав шквал критики в адрес Обрадора.

В 2019 г. технология дипфейк была использована против президента Аргентины Альберто Фернандеса (2019 — н/в) с целью его дискредитации внутри страны. В социальных сетях и мессенджере *WhatsApp* было распространено видео главы государства, где его речь специально была замедлена. После этого на него посыпались обвинения в пьянстве и употреблении наркотиков. Источником для видео стало оригинальное выступление президента в рамках Экономического и социального совета (*Consejo Económico y Social, ESC*). На встрече были представлены основные принципы Аргентинского производственного плана до 2030 г., который направлен на создание 2 млн официальных рабочих мест в частном секторе, сокращение числа безработных на 9 млн и формирование 100 тыс. компаний к 2030 г. [26].

В *Facebook* скандальный ролик был опубликован более пяти раз и сопровождался текстом из популярного мультфильма «Симпсоны» с изображением пьяного персонажа Гомера Симпсона, распивающего пиво. В *Instagram* он набрал более 21,6 тыс. «лайков», в *TikTok* воспроизводился бо-

* Доксинг (*Doxing*) — поиск и публикация персональной или конфиденциальной информации о человеке без его согласия. Этот процесс не всегда включает в себя незаконные действия, но доксинг относится к нарушению сетевого этикета и часто запрещен внутренними правилами интернет-сообществ.

лее 100 тыс. раз. В *Twitter* появилась другая версия этого видеоролика уже без кадров из мультфильма, которая была опубликована под заголовком «Президент Альберто Фернандес пьян или одурманен? Боже мой, этот парень болен, он больше не может продолжать что-либо возглавлять» [27].

В этом же году жертвой подобной манипуляции стала министр безопасности Аргентины Патрисия Буллич, которую также обвиняли в злоупотреблении алкогольными напитками.

Позже специалисты известного в стране центра по борьбе с дезинформацией во время избирательных кампаний *Reverso*, объединивший более 100 СМИ и технологических компаний, сумели развенчать политический дипфейк, сравнив два ролика и наглядно показав, как он создается.

В мае 2019 г. жертвой вирусного видео стал президент Колумбии Иван Дуке Маркес (2018—2022 гг.). В фальшивом видеоролике президент объявляет об отставке со своего нынешнего поста. В *Facebook* фальшивое видео набрало более 430 тыс. просмотров. Ролик был смонтирован из видео за 2018 г., где политик действительно сделал заявление об отставке с поста члена сената в связи с предстоящими президентскими выборами [28].

Бразилия является страной-чемпионом по дипфейк-атакам на политических лидеров страны. За 2018 г. сразу несколько видных политических чиновников стали жертвами фальшивых видео. Так, кандидат в президенты Жаир Болсонару (2019—2022 гг.) использовал фальшивые новости для нападок на своего соперника Фернанду Аддада и продвижения к победе, распространяя дезинформацию для нанесения вреда репутации последнего [29, с. 41]. В этом же году губернатор бразильского штата Сан-Паулу Жуан Дориа за несколько дней до выборов стал жертвой порнографического фейкового видео. В 2022 г. политический дипфейк был направлен на президента Луиса Инасиу Лула да Силва (2003—2011, 2023 — н/в). 5 августа в социальных сетях появилось фальшивое видео, где популярная в стране телеведущая Рената Васконселлос якобы дает ложную информацию об итогах голосования на президентских выборах [27]. В период 2020—2021 гг. дипфейки использовались в ходе политических кампаний в Боливии, Эквадоре и Чили.

НОРМАТИВНО-ПРАВОВАЯ БАЗА В ОТНОШЕНИИ ДИПФЕЙКОВ В СТРАНАХ ЛАТИНСКОЙ АМЕРИКИ

На сегодняшний день законы в отношении дипфейков приняты в США и Китае. Начиная с 2021 г. штаты Вирджиния, Техас и Калифорния применяют юридические нормы в отношении дипфейков. Закон в Вирджинии предусматривает уголовные наказания за распространение клеветнических дипфейков порнографического характера. В Техасе законом запрещено создание и распространение дипфейковых видео, сделанных с целью нанесения вреда кандидатам, избираемым на государственные должности, или влияния на выборы.

10 января 2023 г. закон о дипфейках вступил в силу в Китае. Согласно документу, дипфейк-контент несет в себе риски заражения вирусом (сетей и компьютеров) и кражи личных данных. Среди ключевых новых правил — необходимость предоставлять согласие на использование изображений пользователем и запрет использования технологий такого типа для распространения новостей. Еще одним нововведением является следующее: перед публикацией контента с использованием технологии дипфейк обязательным становится размещение уведомления, указывающего пользователям, что это — отредактированное или измененное изображение. В случае, если создатель не выполнит это требование, он будет вынужден удалить контент и привлечен к уголовной ответственности за угрозу национальной безопасности [30].

Евросоюз принял решение о наложении штрафов на крупные технологические компании (*Google, Facebook и Twitter*), которые будут продолжать публикации дипфейк-контента.

В странах Латинской Америки еще нет специальных законов в отношении дипфейк-роликов; намеренное применение этой технологии рассматривается в рамках действующих законов о фейковой дезинформации.

Среди стран Латинской Америки Венесуэла является первым государством, затронувшим тему фейковой дезинформации в своем законодательстве. В 2005 г. в Уголовный кодекс была добавлена статья 297-А, предусматривающая до пяти лет лишения свободы для лиц, которые «распространяют ложную информацию, вызывающую панику в общественной среде» [31]. По инициативе Уругвайской ассоциации прессы (*Asociación de la Prensa Uruguaya, APU*) в 2019 г. политические партии Уругвая подписали пакт против фейковых новостей [32].

Парламент Никарагуа в сентябре 2020 г. одобрил закон, направленный против киберпреступлений. В документе предусмотрено наказание до десяти лет лишения свободы за распространение ложной информации среди населения, вызывающей страх и наносящей ущерб чести и достоинству человека, ставящей под угрозу общественный порядок и суверенную безопасность [33].

В Перу в октябре 2020 г. группа депутатов внесла законопроект о запрете распространения фейковых новостей во время предвыборной агитации. Нарушение данного закона влечет за собой уголовную ответственность в виде минимального тюремного заключения сроком до двух лет для тех, кто «преднамеренно, искусственно через СМИ и социальные сети распространяет ложную информацию» [34].

За 2017—2021 гг. законопроекты в отношении ложной информации во время политических выборов были рассмотрены в Бразилии (проект о создании бразильского Закона о свободе, ответственности и прозрачности в Интернете [35]), в Аргентине, Колумбии (Конституционный суд признал распространение фейков нарушением прав человека, а также был принят закон о кибербезопасности, включающий меры по борьбе с киберпреступлениями и распространением дезинформации в 2019 г.), Парагвае (законо-

проект, принятый в марте 2020 г., был направлен на сдерживание распространения ложной информации во время пандемии *COVID-19* [36]), в Чили (три законопроекта об ответственности за распространение ложной информации в Интернете обрабатываются палатой депутатов), в Сальвадоре и Панаме.

В августе 2018 г. Национальная избирательная палата Аргентины (*Cámara Nacional Electoral, CNE*) создала специальный портал-реестр аккаунтов в социальных сетях и на официальных сайтах для кандидатов, политических групп и высших партийных органов власти [37]. Согласно требованиям *CNE*, в обязанности партий входит публикация на портале всех агитационных аудиовизуальных материалов, которые будут использоваться в социальных сетях. Кроме того, для контроля цифровых кампаний, разработанных рекламными агентствами и консультантами, проводился аудит по поведению автоматизированных аккаунтов (ботов), атак (троллей) и распространения ложной информации (фейковых новостей) в течении избирательной кампании [38].

В октябре 2020 г. правительство Аргентины запустило Обсерваторию дезинформации и символического насилия в СМИ и на цифровых платформах (*Observatorio de la desinformación y la violencia simbólica en medios de prensa y plataformas digitales, NODIO*) [39] с целью «защиты граждан от ложных новостей», распространяемых в Интернете [40].

Громкое дело о заказных дипфейках во время президентских выборов Жаира Болсонару в 2018 г. было передано в Верховный суд для расследования. Команда Болсонару была официально обвинена в использовании фейковых новостей, направленных на подрыв репутации Фернанду Аддада [38]. С 2020 г. в Бразилии действует кампания Высшего избирательного суда (*Tribunal Superior Eleitoral, TSE*) «Я голосую без фальсификаций» (*EuVotoSemFake*), направленная против дезинформации на выборах [41]. Передовым техническим инструментом кампании стал виртуальный помощник в *WhatsApp*, который был запущен для разъяснения различных вопросов, касающихся избирательного процесса. Как отмечал цифровой координатор *TSE* Тьяго Рондон, «основной целью кампании является передача точной информации об избирательном процессе. Имея доступ к достоверной информации, население будет более подготовлено к борьбе с фейковыми новостями» [41]. Избирательный суд также создал специальный сайт «Дезинформация» (*Desinformação*), где содержится информация по фейкам, используемым во время выборов в Бразилии. Граждане также имеют свободный доступ к галерее разъяснительных видеороликов, подготовленных телецентром консультативного отдела по коммуникациям суда.

Тема дипфейков в настоящий момент носит дискуссионный характер, а законопроекты в отношении них зачастую оспариваются журналистским сообществом стран Латинской Америки. Так, в Колумбии в 2017 г. под давлением СМИ был отменен целый абзац решения по реформе избирательной системы, которое запрещало раскрытие «ложных или оскорби-

тельных новостей посредством пропаганды или рекламы, регулируемой действующим кодексом, как «запрет говорить плохо о политиках» [42].

В Уругвае проект-предложение о криминализации электоральной дезинформации от 2018 г. за использование фейковых новостей (включая письменные слова, песни, символы, изображения, записи и видео), который предусматривал до четырех лет лишения свободы, был отклонен в результате его критики многими известными журналистами страны [43]. При активном давлении со стороны журналистского сообщества в Парагвае в 2020 г. была сорвана попытка утвердить законопроект, направленный на сдерживание распространения ложной информации во время пандемии *COVID-19*.

Создание упомянутой выше обсерватории *NODIO* вызвало журналистскую критику за связь с управлением национального омбудсмана (*Defensoría del Pueblo de la Nación*), которое, в свою очередь, является органом, созданным в соответствии с законом, регулирующим деятельность СМИ в Аргентине. *NODIO* была вынуждена провести качественное и количественное исследование уже транслируемых новостей о символическом насилии и злонамеренных действиях [42].

В 2019 г. мексиканская организация «Гражданское предложение» (*Propuesta Cívica*), оказывающая поддержку журналистам, находящимся в группе риска, использовала технологию дипфейк для того, чтобы обратить внимание правительства на преступления, совершенные в отношении журналистов, и насилие в отношении прессы. Акция началась с трансляции дипфейк-ролика убитого журналиста и писателя Хавьера Вальдеса, который обращается к президенту со следующими словами: «Господин президент Андрес Мануэль Лопес Обрадор, я Хавьер Вальдес, журналист и писатель. 15 мая 2017 г. меня убили по приказу кого-то, кому не понравилось то, что я разместил. Но вот я, вы меня видите, и я разговариваю с вами. Я не боюсь, господин президент, потому что они не могут убить меня дважды» [44]. Источником для данного видео послужило старое интервью погибшего журналиста. Создать точный образ своего мужа помогла вдова Вальдеса Гризельда Триана, предоставив его личные вещи [45]. Акция способствовала ускоренному проведению расследования в отношении убийства журналиста. Прокуратура Мексики запросила 50-летний тюремный срок для одного из обвиняемых в убийстве.

В этом же году кампания «Мы продолжаем говорить» (*Seguimos Hablando*) восстановила *Twitter*-аккаунты четырех убитых в Мексике журналистов, «вернувшихся на неделю, чтобы написать о тех проблемах, которые стали причиной их убийства». Кампания была популярной новостной темой в Мексике, завоевала многочисленные награды и не раз упоминалась в мировых СМИ.

Стремительное развитие технологий искусственного интеллекта в последние годы способствовало эскалации их преднамеренного использования в политической и международной среде. Исключением не стали и

страны Латинской Америки, где активно применяются такие технологии ИИ, как дипфейки и чат-боты, для давления на политических акторов и нарушения информационно-психологической безопасности.

С момента своего появления технология дипфейк стала применяться в странах Латинской Америки для манипулирования общественным мнением и дискредитации политических лидеров на региональном и внутриполитическом уровне. Жертвами политических дипфейков за последние шесть лет стали президенты Мексики, Аргентины, Колумбии и Бразилии, а также известные политики, прокуроры и министры.

За период с 2005 по 2022 г. в ряде латиноамериканских государств были разработаны законы, направленные на борьбу с ложной информацией. Наиболее жесткие меры, такие, как введение уголовной ответственности, приняты в Венесуэле, Никарагуа и Перу. Среди конкретных мер можно выделить реформу уголовного кодекса в Венесуэле, закон против киберпреступлений в Никарагуа, законопроект о запрете распространения фейковых новостей в Перу. Законопроекты в отношении дипфейков находятся в активной разработке в Бразилии, Мексике, Аргентине, Уругвае, Чили, Парагвае, Сальвадоре и Панаме.

Кроме того, в странах Латинской Америки активно работают специальные организации, изучающие и вырабатывающие методы нейтрализации преднамеренного использования фейковых новостей в политических и иных целях: мексиканский центр по борьбе с дезинформацией во время избирательных кампаний *Reverso*, аргентинская обсерватория по дезинформации на цифровых платформах *NODIO*, бразильская коалиция *Comprova*, отслеживающая фальшивые новости в социальных сетях.

Растущие угрозы использования технологии дипфейк ставят перед латиноамериканским регионом задачу своевременного реагирования путем выработки жестких законопроектов, которые будут регулировать деятельность СМИ и политических институтов, использовавших технологию дипфейк в политических и лоббистских целях, по примеру США и Китая.

В качестве передовых технологий, выявляющих дипфейк, могут использоваться следующие платформы:

— платформа, запущенная компанией *Sensity* в 2021 г. Уникальность данной технологии заключается в том, что она позволяет пользователю проверять подлинность видео в режиме реального времени с помощью любого типа устройства, имеющего доступ к Интернету. Достоверность обнаружения подделки составляет 95-99,9%;

— камеры для мобильных устройств, разработанные компанией *Truepic*;

— детектор фальшивых новостей *Google Chrome*;

— сайты для обнаружения дипфейков. Предлагают начальные шаги для выявления и потенциального устранения фальшивых новостей (*Blogs.ifla.org*, *Snopes* www.snopes.com, *politiFact* www.politifact.com, *Fact-Check* www.factcheck.org, *Channel-4-Fact-Check* www.channel4.com/news/factcheck, *Africa-Check* <https://africacheck.org>).

ИСТОЧНИКИ И ЛИТЕРАТУРА / REFERENCES

1. Базаркина Д.Ю., Пашенцев Е.Н. Злонамеренное использование искусственного интеллекта: вызовы информационно-психологической безопасности в Латинской Америке. *Социально-гуманитарные знания*, М, 2020, № 4, сс. 248-260. [Bazarkina D.U., Pashentsev E.N. Zlonamerennoye ispol'zovaniye iskusstvennogo intellekta: vyzovy informatsionno-psikhologicheskoy bezopasnosti v Latinskoj Amerike. [The Malicious Use of Artificial Intelligence: Challenges to Information and Psychological Security in Latin America]. *Sotsial'no-gumanitarnyye znaniya*, Moscow, 2020, N 4, pp. 248-260. (In Russ.) (DOI 10.34823/SGZ.2020.4.51416).
2. Pinheiro de Resende S.M. The effects of deepfakes on politics and on data justice issues – a perspective from Brazil and the United States. A thesis submitted for the degree of Master of Law & Technology, Tilburg, 2021, 52 p.
3. El 70% de los latinoamericanos ignora la existencia de los DeepFake. Available at: <https://www.innovaciondigital360.com/i-a/el-70-de-los-latinoamericanos-ignora-la-existencia-de-los-deepfake/> (accessed 10.10.2022).
4. Lussier N. Nonconsensual deepfakes: detecting and regulating this rising threat to privacy. University of Idaho College of Law, L. Rev, 2022. Available at: <https://digitalcommons.law.uidaho.edu/idaho-law-review/vol58/iss2/6> (accessed 21.03.2023).
5. Gomes-Gonçalves S. Los deepfakes como una nueva forma de desinformación corporativa – una revisión de la literature. *International review (Irocamm)*, Sevilla, 2022, Vol. 5, N 2, pp. 22-38. (DOI: [dx.doi.org/10.12795/IROCMM.2022.v05.i02.02](https://doi.org/10.12795/IROCMM.2022.v05.i02.02)).
6. Hwang T. Deepfakes. A Grounded Threat Assessment. Center for Security and Emerging Technology (CSET), Washington, 2020, 50 p.
7. Bañuelos Capistrán J. Deepfake: la imagen en tiempos de la posverdad. *Revista Panamericana De Comunicación*, México, 2020, Vol. 2(1), pp. 51–61. (DOI: <https://doi.org/10.21555/rpc.v0i1.2315>).
8. Nasu H. Deepfake Technology in the Age of Information Warfare. New York, 2022. Available at: <https://lieber.westpoint.edu/deepfake-technology-age-information-warfare/> (accessed 26.12.2022).
9. Ajder H., Patrini G., Cavalli F., Cullen L. The State of Deepfakes: Landscape, Threats, and Impact. 2019, 27 p. Available at: https://regmedia.co.uk/2019/10/08/deepfake_report.pdf (accessed 28.03.2022).
10. Pantoja De Moraes C. «Deepfake» como ferramenta de manipulação e disseminação de «fakenews» em formato de vídeo nas redes sociais. *Biblios*, Rio de Janeiro, 2020, N 79, pp. 63-72. (DOI: 10.5195/biblios.2020.864).
11. Botha J., Pieterse H. Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security. Conference: 15th International Conference on Cyber Warfare and Security At: Old Dominion University, Norfolk, 2020. Available at: https://www.researchgate.net/publication/341454354_Fake_News_and_Deepfakes_A_Dangerous_Threat_for_21st_Century_Information_Security (accessed 14.01.2022).
12. Martínez V. C., García Guardia M. L., Padilla Castillo G. Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales. *CIC. Cuadernos de Información y Comunicación*, Madrid, 2020, N 25, pp. 165-181. (DOI: <https://doi.org/10.5209/ciyc.68762>).
13. Ray A. Disinformation, Deepfakes and Democracies: The Need for Legislative Reform. *The University of New South Wales law journal*, Sydney, 2021, Vol. 44(3):983, pp. 983-1013. (DOI:10.53637/DELS2700).
14. Byman D. L., Gao C., Meserole C., Subrahmanian V.S. Deepfakes and international conflict. 2023, 22p. Available at: <https://www.brookings.edu/research/deepfakes-and-international-conflict/> (accessed 21.01.2023).
15. Helmus T. C. Artificial Intelligence, Deepfakes, and Disinformation. 2022, 24 p. Available at: <https://www.rand.org/pubs/perspectives/PEA1043-1.html> (accessed 3.01.2023).

16. Лексютина Я.В. Злонамеренное использование дипфейков: риски информационно-психологической безопасности Японии. *Японские исследования*, М, 2021, № 3, сс. 90-101. [Leksyutina Y.V. Zlonamerennoye ispol'zovaniye dipfeykov: riski informatsionno-psikhologicheskoy bezopasnosti Yaponii. [Malicious use of dipfakes: information-psychological security risks for Japan]. *Yaponskiye issledovaniya*, Moscow, 2021, N 3, pp. 90-101. (In Russ.). (DOI: 10.24412/2500-2872-2021-3-90-101).
17. Игнатовский Я. Р., Иванов В.Г. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности. *Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление*, М, 2020, Т.7, № 4, сс. 379-386. [Ignatovskiy Y. R., Ivanov V.G. Dipfeyki: primeneniye v sfere politiki i vozdeystviya na lichnuyu zhizn' i natsional'nyu bezopasnost'. [Deepfakes: Prospects for Political Use and Threats to the Individual and National Security]. *Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Gosudarstvennoye i munitsipal'noye upravleniye*, Moscow, 2020, Vol. 7, N 4, pp. 379-386. (In Russ.). (DOI: 10.22363/2312-8313-2020-7-4-379-386).
18. Фалеев М.А., Ситдикова М.А., Нечай Е.Е. Дипфейк как феномен политической коммуникации. *Вестник ЗабГУ*, Чита, 2021, Т. 27, № 6, сс. 101-106. [Faleyev M.A., Sitdikova M.A., Nechay Ye.Ye. Dipfeyk kak fenomen politicheskoy kommunikatsii. [Deepfake as a phenomenon of political communication]. *Vestnik ZabGU*, Chita, 2021, Vol. 27, N 6, pp. 101-106. (In Russ.) DOI: 10.21209/2227-9245-2021-27-6-101-106).
19. López-López P.C., Dagatti M., Mendoza M. El impacto de las noticias falsas y la desinformación en las democracias de América Latina y el Caribe. *Cuadernos del Centro de estudios de diseño y comunicación*. Palermo, 2022, Vol. 161, pp. 11-18. (DOI: <https://doi.org/10.18682/cdc.vi161.6975>).
20. Just Joking. Deepfakes, satire, and the politics of synthetic media. Cambridge, 2022. 48p. Available at: <https://cocreationstudio.mit.edu/wp-content/uploads/2021/12/JustJoking.pdf> (accessed 25.12.2022).
21. López J. Tragic Realism: How to regulate Deepfakes in Colombia? *Latin American Law Review*, Bogotá, 2022, N. 8, pp. 125-145 (DOI:<https://doi.org/10.29263/lar08.2022.08>).
22. Цветкова Н. А., Гришанина Т. А. Цифровая сила в странах Латинской Америки: хэштеги и дипфейки как политические инструменты. *Латинская Америка*, М, 2023, №3, сс. 21-33. [Tsvetkova N. A., Grishanina T. A. Tsifrovaya sila v stranakh Latinskoy Ameriki: kheshtegi i dipfeyki kak politicheskiye instrumenty [Digital Power in Latin America: Hashtags and deep-fakes as political tools]. *Latinskaya Amerika*, Moscow, 2023, N 3, pp. 21-33. (In Russ.). (Doi 10.31857/S0044748X0024414-4).
23. Gandulfo D. Tenemos que hablar del impacto de las fakes news en las democracias latinoamericanas. Available at: <https://www.iade.org.ar/noticias/tenemos-que-hablar-del-impacto-de-las-fakes-news-en-las-democracias-latinoamericanas> (accessed 16.02.2023).
24. The spread of true and false news online. Available at: <https://www.science.org/doi/10.1126/science.aap9559> (accessed 19.02.2023).
25. Martínez L. Es falso el video de Alberto Fernández en el que habla como «borracho»: las imágenes fueron manipuladas. Available at: <https://chequeado.com/el-explicador/es-falso-el-video-de-alberto-fernandez-en-el-que-habla-como-borracho-las-imagenes-fueron-manipuladas/> (accessed 19.10.2022).
26. El Gobierno presentó los ejes de un programa de Desarrollo. Plan 2030 para crear dos millones de empleos. Available at: <https://www.pagina12.com.ar/411724-plan-2030-para-crear-dos-millones-de-empleos> (accessed 17.10.2022).
27. Pacheco V. El primer deepfake electoral muestra números falsos en la encuesta para president. Available at: <https://www.showmetech.com.br/deepfake-das-eleicoes-mostra-pesquisa-falsa/> (accessed 17.12.2022).
28. Fact Check-Video de la renuncia de Duque a su cargo es de 2018, cuando era senador. Available at: <https://www.reuters.com/article/factcheck-ivanduke-renuncia-idUSL1N2MY1IB> (accessed 8.12.2022).

29. Виноградова Е.А. Технологии искусственного интеллекта и нарастающие киберугрозы в Латинской Америке. *Латинская Америка*, М, 2023, № 3, сс. 34-48. [Vinogradova E.A. Tekhnologii iskusstvennogo intellekta i narastayushchiye kiberugrozy v Latinskoy Amerike. [Artificial intelligence technologies and the rise of cyber threats in Latin America]. *Latinskaya Amerika*, Moscow, 2023, N 3, pp. 34-48. (In Russ.). (DOI: 10.31857/S0044748X0024415-5).
30. Los deepfakes y cómo los medios están combatiendo la desinformación creada con Inteligencia Artificial. Available at: <https://www.elnacional.com/ciencia-tecnologia/los-deepfakes-y-como-los-medios-estan-combatiendo-la-desinformacion-creada-con-inteligencia-artificial/> (accessed 20.12.2022).
31. Gaceta Oficial N° 5.763 Extraordinario de la República Bolivariana de Venezuela. 16 de marzo de 2005. Available at: <http://www.annaobserva.org/observatorio/wp-content/uploads/2018/03/C%C3%93DIGO-PENAL-DE-VENEZUELA.pdf> (accessed 23.03.2022).
32. Partidos políticos uruguayos firmaron compromiso contra generación y difusión de noticias falsas. Available at: <https://www.gub.uy/presidencia/comunicacion/noticias/partidos-politicos-uruguayos-firmaron-compromiso-contra-generacion-difusion> (accessed 23.11.2022).
33. Ley Especial de Ciberdelitos - Asamblea Nacional de Nicaragua. Available at: [http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/7B68B3A67F9B9C65062585F10059EFF6/\\$File/LEY%20ESPECIAL%20DE%20CIBERDELITOS%2030092020.pdf?Open](http://legislacion.asamblea.gob.ni/SILEG/Iniciativas.nsf/7B68B3A67F9B9C65062585F10059EFF6/$File/LEY%20ESPECIAL%20DE%20CIBERDELITOS%2030092020.pdf?Open) (accessed 27.12.2022).
34. La Ley Orgánica de Elecciones señala en su artículo 181 que la propaganda electoral debe hacerse dentro de los límites que señalan las leyes. Available at: https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL06567-20201029.pdf (accessed 25.03.2022).
35. Projeto de Lei 2630/20 institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Available at: <https://legis.senado.leg.br/sdleg-getter/documento?dm=8110634&disposition=inline> (accessed 29.12.2022).
36. Proyecto de Ley «Que sancional el incumplimiento de las medidas dispuestas ante alertas epidemiológicas e en estado de emergencia sanitaria declarada», presentado por el senador Pedro Arturo Santa Cruz Insaurralde, de fecha 16 de marzo de 2020. Available at: <http://silpy.congreso.gov.py/expediente/120258> (accessed 29.03.2022).
37. La Cámara Electoral creó un registro de sitios web y redes sociales oficiales de candidatos y agrupaciones políticas. Available at: <https://www.cij.gov.ar/nota-31460-La-C-mara-Electoral-cre--un-registro-de-sitios-web-y-redes-sociales-oficiales-de-candidatos-y-agrupaciones-pol-ticas.html> (accessed 27.12.2022).
38. Gandulfo D. Tenemos que hablar del impacto de las fakes news en las democracias latinoamericanas. Available at: <https://www.iade.org.ar/noticias/tenemos-que-hablar-del-impacto-de-las-fakes-news-en-las-democracias-latinoamericanas> (accessed 23.12.2022).
39. NODIO, el Observatorio de la desinformación y violencia simbólica. Available at: <https://defensadelpublico.gob.ar/llego-nodio-el-observatorio-de-la-desinformacion-y-la-violencia-simbolica/> (accessed 28.12.2022).
40. Lubianco J. Once leyes y proyectos de ley contra la desinformación en América Latina implican multas, cárcel y censura. Available at: <https://latamjournalismreview.org/es/articles/leyes-contra-desinformacion-america-latina/> (accessed 29.12.2022).
41. TSE lança campanha “#EuVotoSemFake”, contra a desinformação nas eleições. Available at: <https://www.tre-mt.jus.br/comunicacao/noticias/2020/Setembro/tse-lanca-campanha-201c-euvotosemfake201d-contra-a-desinformacao-nas-eleicoes> (accessed 21.03.2022).
42. Higuera S. Por iniciativa de asociación de periodistas, partidos políticos de Uruguay firmarán pacto contra la desinformación. Knight Center for Journalism in the Americas. Austin, 2019. Available at: <https://latamjournalismreview.org/es/articles/por-iniciativa-de-asociacion-de-periodistas-partidos-politicos-de-uruguay-firmaran-pacto-contra-la-desinformacion/> (accessed 19.03.2022).

Екатерина Виноградова

43. Iciar_gutierrez pic.twitter.com. Available at: https://t.co/ePGO7vtbn0Por@iciar_gutierrezpic.twitter.com/oN1QUjBZLR (accessed 17.03.2023).

44. Gutiérrez I. Un vídeo recrea con inteligencia artificial la imagen y la voz de un periodista asesinado en México: «Aclaren este crimen». Available at: https://www.eldiario.es/internacional/video-recrea-inteligencia-artificial-imagen-voz-periodista-asesinado-mexico-aclaren-crimen_1_6372262.html (accessed 10.02.2022).

Ekaterina A. Vinogradova (vinogradovacatherine7@gmail.com)
Cand. Sci. (Political Science), Independent researcher

The malicious use of political deepfakes and attempts to neutralize them in Latin America

Abstract. Deepfake technology has revolutionized the field of artificial intelligence and communication processes, creating a real threat of misinformation of target audiences on digital platforms. The malicious use of political deepfakes has become widespread between 2017 and 2023. The political leaders of Argentina, Brazil, Colombia and Mexico were attacked with elements of doxing. Fake videos that used the politicians' faces undermined their reputations, diminishing the trust of the electorate, and became an advanced tool for manipulating public opinion. A series of political deepfakes has raised an issue for the countries of the Latin American region to develop timely legal regulation of this threat. The purpose of this study is to identify the threats from the uncontrolled use of political deepfake in Latin America. According to this purpose, the author solves the following tasks: analyzes political deepfakes; identifies the main threats from the use of deepfake technology; examines the legislative features of their use in Latin America. The article describes the main detectors and programs for detecting malicious deepfakes, as well as introduces a scientific definition of political deepfake.

Key words: political deepfakes, doxing, disinformation, legal framework, information-psychological influence, internal political security, artificial intelligence technologies, political leader, social networks, media, elections.

DOI: 10.31857/S0044748X0025404-3

Received 05.02.2023.