

УДК 165.0

## **РОСТ ЗАБЛУЖДЕНИЙ В СВЯЗИ С ГЛОБАЛИЗАЦИЕЙ ИНТЕРНЕТА**

Садовников В.Е., студент гр. ИТм-201, I курс

Научный руководитель: Баумгартэн М.И., к.ф.-м.н., доцент

Кузбасский государственный технический университет

имени Т.Ф. Горбачева, г. Кемерово

Заблуждения преследуют человечество с древнейших времен. Они проходят сквозь века. С каждым годом, месяцем, даже днем их становится только больше. Этот рост подстегивает распространение способов передачи информации. Сначала устный, затем через письменные источники и т.д. Но настоящий рассвет заблуждений начался относительно недавно с появлением и распространением глобальной сети Интернет.

В современном быстроразвивающемся мире глобальная сеть Интернет занимает все большую часть нашей жизни. Благодаря ней у нас есть доступ к огромнейшему количеству информации. Проблемой этого блага является то, что не вся информация правдива. Проверка информации в любую эпоху была сложной и дорогой. Однако сейчас проверять информацию становится все сложнее. И с каждым днем эта сложность увеличивается из-за роста количества генерируемых человечеством данных, больше времени уходит на проверку информации чем на ее поиск. В глобальной сети всегда был процент ложной информации.

Интернет является самым совершенным средством доставки фейковой информации. Сфабриковать ложную новость, в современной глобальной сети очень просто, достаточно отправить сообщение в социальной сети. Раньше, когда Интернет не приносил больших прибылей, было мало смысла публиковать фейковую информацию. Сейчас же на получении сверхприбылей заточены почти большинство сайтов СМИ. Главная цель с своевременного донесения информации сменилась на завлечение читателя захватывающим заголовком. При этом в самой новости может содержаться абсолютно противоположная информация. Главная цель выполнена пользователь перешел на страницу и просмотрел несколько рекламных баннеров [1].

Как сказано выше, на проверку информации всегда уходило много времени. В современном капиталистическом мире, где во главе стоит получение прибыли, проверка информации приносит лишь убытки. Еще одним минусом является то, что проверка требует времени. Это значит, что другие интернет-ресурсы распространяют информацию раньше. Что в свою очередь уж точно не приведет новых читателей.

Но опасность ввода в заблуждение может исходить не только от интернета. В современном Интернете все больше занимают места социальные сети. Поскольку они представляют собой и новостную площадку, и личный блог, так и место сбора по интересам и множество других полезных вещей.

Благодаря устойчивому росту популярности социальные сети превратились в удобный источник новостей и любой другой информации.

До эпохи социальных сетей чтобы распространить информацию в глобальной сети, нужно было хотя-бы обладать минимальными навыками в «сайтостроении». Но сейчас не составляет большого труда распространить какое-либо ложное суждение, заблуждение, ложь. Достаточно одного предложения на странице в социальной сети, и люди сами растиражируют его на всю глобальную сеть. Новость облетит весь Земной шар за несколько секунд. И при этом необязательно чтобы новость опубликовал известный человек, лидер мнений и т.д. Достаточно так называемого «репоста». Репост – это вторичная публикация сообщения, размещенного другим пользователем в социальной сети, с ссылкой на источник.

Также социальные сети дали толчок к развитию лженаук и давно развенанных заблуждений. Одно из таких заблуждений — это то, что планета Земля плоская. До эпохи Интернета людям, имеющим такие заблуждения было сложно влиять на общество, это могли быть только мелкие тиражи литературы или другие незначительные способы. Но Интернет, а в особенности сообщества в социальных сетях, дали им возможность объединиться, чем значительно увеличили распространение этих псевдонаучных материалов.

Вдобавок, сейчас люди очень мало времени уделяют поиску достоверной и полной информации. Благодаря этому развились так называемые «научпоп» группы. В основном такие сообщества строятся на ежедневной, а иногда и ежечасной публикации нескольких фактов из нашей жизни с примесью рекламы. Такой метод познания не способствует составлению полной картины в какой-либо области человеческого познания. Большинство сообществ такого плана не заинтересовано в проверке этих фактов. Ведь их основная цель — это получение прибыли с рекламных интеграций. Так что, кроме расплывчатых знаний, люди могут получить ложную информацию.

Еще одной важной частью глобальной сети является использование на сайтах особых алгоритмов, показывающих пользователю сайта только то, что ему интересно. Цель этих алгоритмов задержать посетителя сайта на максимально длительное время, что в свою очередь принесет дополнительные прибыли владельцу сайта.

Конечно, такие алгоритмы несут свои плюсы и минусы. Плюсом является то, что пользователь тратит меньше времени на поиск интересующей его информации. Информация при обновлении веб-страницы буквально сама выводится человеку на экран. По сути, прекраснейшее изобретение. Но есть один очень существенный недостаток, человек «лишается» доступа к другой информации, а также другим точкам зрения. Огромное количество пользователей не заинтересованно в поиске информации. Зачем искать информацию если есть рекомендации от веб-сайта. Так человек попадает в пузырь фильтров [2].

Пузырь фильтров существует не только на сайтах, но и в поисковых системах. То есть, даже при поиске другой точки зрения, поисковые системы выдают персонализированные результаты. Получается, что каждому человеку выдаются результаты поиска отличные от других. Что лишь дальше отдаляет от широкого понимания ситуаций, событий и т.д. Борьба с пузырем фильтров в поисковых системах можно с помощью отключения персонализированного поиска. Это очень простое действие, но поскольку большинство даже не догадывается о проблеме, то не делают и этого. С веб-сайтами сложнее. Большинство людей отвыкло искать информацию по интересующей их теме, увлечению. И полагается полностью на рекомендации сайта. Пузырь фильтров - это одна из главных проблем современного Интернета. Чем дольше человек в нем находится, тем более он уверен в своей точке зрения. Ведь пользователь может даже не предполагать о других точках зрения. С каждым днем все сложнее и сложнее переубедить таких людей. Даже множество фактов, документов и других доказательств перестают восприниматься. Из-за этих алгоритмов множество людей находятся в заблуждении.

Но не только пузырь фильтров ограничивает кругозор людей. Сами люди ограничивают себя. Большинство выбрало для себя несколько источников, основанных на их жизненных взглядах. Другие источники либо воспринимаются искаженно, либо вообще не просматриваются. При таком подходе к получению информации человек погружается в удобный для себя мир, который не отражает действительности. В сочетании с пузырем фильтров такому пользователю очень сложно выйти из своей «зоны комфорта».

Одним из самых современных способов ввода в заблуждение является использование нейросетей. Нейросети - математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей. Благодаря данной технологии люди получили мощнейший инструмент редактирования информации. Нейросеть может превратить черно-белую фотографию в цветную, может определить, что находится на фотографии и множество других полезных вещей.

Но нейросети принесли и еще один способ ввода в заблуждение. Он получил название Deepfake (дипфейк). Дипфейк (от англ. Deep learning «глубинное обучение» и англ. Fake «подделка»). Этот метод позволяет подменять отдельные части кадров в видео или изображении, а также манипулирование голосом и другими аудио материалами, часто не вызывая сомнений [3].

Сейчас тема дипфейков очень популярна. Есть множество сайтов, программ и мобильных приложений, которые позволяют абсолютно любому человеку, обладающему смартфоном, заменить лицо с фотографии или видеоролика.

Пока алгоритмы недостаточно совершенны и большинство может сразу распознать подделку. Но уже сейчас в некоторых случаях выходят фотографии и видеоролики практически неотличимые от оригинала. С видеороликами прогресс улучшения идет медленнее, чем с изображениями, в виду сложности входящего материала, состоящего из множества изображений в секунду.



Рисунок 1 - Пример «безобидного» дипфейка на основе кадра из фильма

Поскольку дипфейки часто создаются с заинтересованными и провокационными темами, то они очень быстро разлетаются по социальным сетям, выходя на сайты интернет СМИ и на другие интернет-ресурсы. Заинтересованные люди готовы вкладывать большие деньги, поскольку пока нет быстрых и гарантированных способов распознать фальсификацию. А когда получится распознать, то будет уже поздно: ведь оно уже разошлось по глобальной сети. Дипфейки в купе с современной вездесущей глобальной сетью Интернет, представляет собой мощнейший комплекс по дискредитированию медийных личностей, политиков, да и вообще любого человека. Все это позволяет манипулировать мировоззрением как конкретных фанатов актеров, так и населением целых государств.

Одним из самых известных примеров дипфейков является переработка видео с речью руководителя социальной сети «Facebook» Марка Цукерберга. Оригинальное видео содержит речь в связи со скандалом о, якобы, «русском следом» в выборах президента США. Сам дипфейк является вырезкой фрагмента длиной в 21 секунду, с переработкой движений губ, мимики, голоса. Получился ролик с очень провокационным содержанием, в котором Марк Цукерберг, якобы, рассказывает о том, что «Facebook» «управляет будущим» с помощью украденных данных пользователей. Благо подделку

получилось довольно легко распознать из-за не самой лучшей имитации голоса.

Пока что технологии создания дипфейков еще недостаточно совершенны, и признаки подделки зачастую видны невооруженным глазом. Нужно обращать внимание на следующие характерные признаки:

1. Неровное движение.
2. Перемены освещения в соседних кадрах.
3. Различия в оттенках кожи.
4. Человек на видеоролике как-то странно моргает или вообще не моргает.
5. Плохая синхронизация движений губ с речью.
6. Плохо поставленная речь.
7. Отличия в голосе.
8. Цифровые артефакты в изображении.

По приблизительным оценкам, сейчас по Сети гуляет более 15 000 дипфейк-видео. Некоторые из них шуточные, но есть и такие, которые создавались для манипуляций общественным сознанием. Сейчас изготовление нового дипфейка занимает от силы пару дней, так что вскоре их может стать намного больше [4]. Распознавание дипфейков стало одной из приоритетных задач человечества. Данной проблемой занимаются крупные мировые организации как DARPA, так и ученые из множества университетов по всему миру. Уже сейчас есть значительные успехи в данной области. Но проблема глубже чем кажется. С каждым годом совершенствуются алгоритмы, не только распознающие дипфейки, но и которые их создают. Эта борьба затянется на долгие годы, если не на века. Все это похоже на соревнование снаряда и брони, которое не закончится пока идет научно-технический прогресс человеческой цивилизации.

Все описанное выше показывает, что распространение глобальной сети Интернет — это не только большое благо для всего человечества, но и большая сложность. Действительная информация о событиях скрыта за большим потоком ложной информации, которая вводит неподготовленного человека в заблуждение, и может остаться скрытой большой промежуток времени, благодаря пузырю фильтров. А вскоре информацию придется проверять еще тщательнее из-за роста популярности дипфейков.

#### Список литературы:

1. Характеристика современных Интернет-СМИ как разновидности аудиовизуальных СМИ. – Текст : электронный // Studbooks.net : [сайт]. – 2020. – URL: [https://studbooks.net/724690/zhurnalistika/harakteristika\\_sovremennyh\\_inter\\_net\\_raznovidnosti\\_audiovizualnyh](https://studbooks.net/724690/zhurnalistika/harakteristika_sovremennyh_inter_net_raznovidnosti_audiovizualnyh) (дата обращения 04.03.2021).
2. Что такое «пузырь фильтров» и как из него выбраться. – Текст : электронный // [habr.com](https://habr.com/ru/company/riddut/blog/295714/) : [сайт]. – 2015. – URL: <https://habr.com/ru/company/riddut/blog/295714/> (дата обращения: 05.03.2021).

3. Технологии Deepfake как угроза информационной безопасности. – Текст : электронный // Anti-Malware : [сайт]. – 2020. – URL: [https://www.anti-malware.ru/analytics/Threats\\_Analysis/Deepfakes-as-a-information-security-threat](https://www.anti-malware.ru/analytics/Threats_Analysis/Deepfakes-as-a-information-security-threat) (дата обращения: 05.03.2021).
4. Дипфейки и другие поддельные видео – как защитить себя? – Текст : электронный // kaspersky.ru : [сайт]. – 2020. – URL: <https://www.kaspersky.ru/resource-center/threats/protect-yourself-from-deep-fake> (дата обращения 05.03.2021).