УДК 32:159.9

Н.Р. Красовская, А.А. Гуляев

К ВОПРОСУ О КОНТРОЛЕ ФЕЙКОВ, ДИПФЕЙКОВ, ФЕЙКОВЫХ АККАУНТОВ В ИНТЕРНЕТЕ

В информационном обществе информация является основой для принятия решений самого разного уровня. Однако в обществе постправды нередко создаются и распространяются фейковые новости и дипфейки посредством использования технологий искусственного интеллекта. Теряется доверие к информации, а создание способа безошибочного распознавания ее подлинности станет научным и техническим открытием. Проблема выявления фейковой информации затрагивает и определение ее первоисточника, зачастую использующего фейковые аккаунты. Государства обеспокоены безопасностью информационного пространства и делают попытки поставить под контроль процесс распространения фейков, дипфейков, создание фейковых аккаунтов в Интернете. Контроль может иметь глобальный и национально-бюрократический характер. Многие страны в той или иной степени пытаются контролировать Интернет посредством национально-бюрократических мер. Но все осознают, что не хватает мер глобального характера для контроля над Интернетом.

Ключевые слова: фейк, дипфейк, аккаунт, медиатизация, искусственный интеллект, информация, Интернет, социальные сети, алгоритм.

DOI: 10.35634/2587-9030-2021-5-1-96-99

Введение

Процесс цифровизации и медиатизации современного общества набрал в настоящее время огромную скорость. Вопросы безопасности стали ключевыми для государств и политических систем. Можно вспомнить президентские выборы в США в 2016 г., в ходе которых победу одержал Д. Трамп. Демократы обвинили в победе Трампа Россию, которая якобы использовала социальные сети, например Facebook, где посредством использования фальшивых аккаунтов распространяла критику Х. Клинтон и поддерживала Д. Трампа. В настоящее время в медиапространстве США в преддверии выборов президента опять раздувается истерия о вмешательстве России в выборный процесс.

Контроль

Попытки контроля за интернет-контентом осуществляются во многих странах. Самые серьезные ограничительные меры применяет в Интернете Китай. В 2003 г. там ввели в эксплуатацию проект «Золотой щит», который фильтрует весь интернет-контент в стране. Ко многим западным сайтам в Китае доступ закрыт. Заблокированы YouTube, Facebook, Twitter, Instagram. Доступ к Википедии ограничен, под запретом также WhatsApp и Telegram. Веб-страницы контролируются по ключевым словам, связанным с вопросами государственной безопасности. Google пошел на соглашение с китайскими властями для вынужденной фильтрации информации в своем поисковике. Все сайты, действующие в Китае, проходят регистрацию в Министерстве промышленности и информационных технологий, которая позволяет выявить автора незаконного контента. Вместо западных сайтов и социальных сетей в Китае действуют собственные (аналог Википедии – Энциклопедия Байду, Facebook – Qzone и т. д.). У Китая многочисленное население и особая ментальность, свои сайты и социальные сети. Современные молодые китайцы совсем не знают свободного Интернета. Поэтому для них Интернет, находящийся под полным контролем государства, вполне привычен и не вызывает отрицательных эмоций. Раньше иностранцы и многие местные активисты для обхода блокировок использовали VPN – соединения и прокси. С 1 февраля 2020 г. китайские власти запретили использование VPN для доступа в «открытый» Интернет [6].

В других странах намного сложнее контролировать Интернет. В Турции был принят законопроект о контроле над Интернетом. Каждый сайт должен иметь регистрацию в Министерстве науки, промышленности и технологий Турции. Принятие данного закона подается в медиасфере как действие для соблюдения принципов национальной безопасности, однако подобная национально-бюрократическая интернет-цензура может отнять возможность публикации, например, антикоррупционных материалов и т. д.

В отличие от Китая в России существуют отечественные популярные поисковики и социальные сети, например, «Яндекс» и «ВКонтакте». Россияне не привыкли к тщательному контролю Интернета и не готовы принимать возможные ограничения как данность. Например, очевидно, что попытка блокировки YouTube приведет к массовому недовольству ограничениями в Интернете, прежде всего среди молодежи, поскольку многие молодые люди в России полностью отказались от телевидения в пользу Интернета.

У российских пользователей потребность в западных сайтах и ресурсах несравненно выше, чем у китайских. Введение широкой интернет-цензуры, наподобие «Золотого щита», в России имеет как существенные технологические ограничения, так и риски резкого возрастания протестных настроений.

Частичный, а затем и полный запрет Интернета был введен в Белоруссии в день президентских выборов 9 августа и в последующие два дня. Власти это объясняли кибератаками из-за границы. Активисты предлагали пойти по гонконгскому пути во время протестов – пользоваться коллективными мессенджерами без Интернета посредством мобильной связи и смартфонов. Пример Белоруссии убедительно демонстрирует, что интернет-цензура и запрет Интернета могут несколько снизить накал протестов людей, но остановить их не могут. В Белоруссии протесты продолжаются и в октябре. Белоруссия вошла в десятку стран с самой жесткой цензурой информационного поля наряду с КНДР, Ираном, Саудовской Аравией, Туркменией, Кубой, Китаем, Вьетнамом [7].

Глобальный контроль за фейками, дипфейками, фейковыми аккаунтами в Интернете может иметь как двусторонний, так и многосторонний характер. Многосторонний глобальный контроль Интернета должен быть прозрачным и носить демократический характер. Для подготовки предложений по решению вопросов глобального контроля Интернета для уполномоченных органов или организаций может быть использован Форум по управлению Интернетом, созданный по результатам Всемирной встречи на высшем уровне по информационному обществу (2003, 2005 гг.) [8]. Двусторонний контроль за информационным полем может осуществляться странами-союзниками. Важно отметить, что ключевым игроком в Интернете и лидером в создании способов его контроля являются США.

Угрозы

Фейковые аккаунты могут создавать угрозу индивидуумам, группам, обществу, всей системе национальной безопасности страны. Информацию о пользователях социальных сетей и возможность дистанционно влиять на них с помощью фейковых аккаунтов могут получать интернет-мошенники, киберпреступники и др. Возможность свободно размещать личную информацию и фотографии породила и проблему массового создания фейковых аккаунтов. Эта проблема уже не может оставаться без должного внимания, и со временем ее актуальность только возрастает. В феврале 2014 г. представители Facebook объявили, что ежемесячная аудитория активных пользователей составляет 1,23 млрд человек. Из этого количества фейковыми аккаунтами являются 11,2 % [4]. В социальной сети «ВКонтакте» также немало фейковых аккаунтов. Так, в Санкт-Петербурге на 4 850 000 жителей приходится 7 330 000 аккаунтов в «ВКонтакте», что в полтора раза больше числа жителей. Можно предположить, что некоторые страницы пользователей являются фейковыми [5].

Большое количество фейковых аккаунтов позволяет распространять спам и размещать недобросовестную рекламу, создает благоприятные условия для интернет-мошенничества.

Проблема выявления фейковых аккаунтов является насущной в связи с ростом объема персональных данных, ростом рисков незаконного использования злоумышленниками информации о частной жизни пользователей социальных сетей.

Интернет и социальные сети используются для рекламы товаров и услуг. Различные компании и индивидуальные предприниматели выбирают в качестве интернет-маркетинга рекламные инструменты и технологии в социальных сетях [5]. Качественно подготовленная маркетинговая технология позволяет охватить определенную целевую аудиторию и достичь результатов в бизнесе. Также увеличивается и число сайтов-«однодневок», за которыми нередко прячутся интернет-мошенники. Войдя в доверие к жертвам с обещанием их «облагодетельствовать», получив их деньги за виртуальные или фейковые товары или услуги, интернет-мошенники исчезают с просторов Интернета.

Сетевым пользователям также угрожают спамеры. Под угрозой находится финансовая и информационная безопасность пользователей. Спамеры способны внедрять в ленту новостей пользователей недобросовестную рекламу, заниматься распространением нелегального контента, внедрением в компьютеры пользователей вредоносных программ, а также получать доступ к личной информации пользователя.

Эффективные способы выявления фальшивых аккаунтов должны создать непреодолимое препятствие для нелегального проникновения в личные данные пользователей. В различных социальных сетях идет процесс развития сервисов, способных выполнить проверку на реальность/фейковость аккаунта.

В социальной сети «Твиттер» (https://twitter.com) существуют сервис Fakes App и сервис TwitBlock, которые способны определить, реальны аккаунты или же они являются фейковыми.

В «Инстаграм» (https://instagram.com) сервис IGExorcist определяет фейковые аккаунты по степени активности и интенсивности взаимодействия с другими пользователями этой социальной сети.

В социальной сети «Фейсбук» (https://www.facebook.com) действует сервис FakeOFF. Данный сервис составляет список друзей пользователя и, как правило, предлагает проверить отдельно каждого из них.

В социальной сети «ВКонтакте» (https://vk.com) предложен сервис VkFake. Для поиска фейков данный сервис использует поиск копий фотографий. Правда, найденные копии фотографий прямо не указывают на фейковый характер аккаунта, но заставляют сомневаться в его реальности.

В сети «Одноклассники» (https://ok.com) этих сервисов не существует, что формирует потребность в их создании.

Методика определения фейковых аккаунтов в социальных сетях предлагает следующие критерии:

– на аватаре учетной записи используются фотографии известных людей, посторонних личностей или какие-либо картинки;

– тысячи друзей и подписчиков пользователя;

– отсутствие личных фотографий человека;

– присутствие большого количества рекламы на странице;

– отсутствие личных данных и собственного контента человека;

– создание страницы произошло недавно;

– очень большое количество фотографий на странице пользователя;

– присутствие на странице групп для взрослых;

– очень большое количество друзей из одного населенного пункта;

– на странице имеются лишь копии фотографий.

Эти критерии позволяют создать алгоритм нахождения фейковых аккаунтов. Работа алгоритма проста: сперва предполагается, что страница является реальной. При выполнении последовательности алгоритма ищутся признаки фейка, и при их наличии может быть сделан системный вывод о фейковом характере аккаунта. Таким образом, данный алгоритм позволяет разработать программное обеспечение системы управления аккаунтами социальных сетей [1].

Одной из самых опасных технологий, созданной искусственным интеллектом, в ближайшее годы, очевидно, будет дипфейк. Потенциальный вред от дипфейка и выгода для злоумышленников несопоставимы с весьма скромными затратами на производство. Дипфейки крайне трудно выявить, а затем ограничить их распространение по Сети. Выявление дипфейков требует применения технологий искусственного интеллекта. В какой-то мере будущее контроля над фейками, дипфейками и фейковыми аккаунтами в Интернете уже лежит в сфере использования возможностей искусственного интеллекта.

Контроль над распространением фейковой информации внедряют сейчас крупные мессенджеры. WhatsApp особым символом помечает сообщения, которые слишком далеко ушли от своего автора, т. е. пересылались много раз, что является отличительной чертой фейка.

Между тем есть простое и эффективное средство для ограничения распространения фейка в Сети. Социальным сетям достаточно отказаться от лайков и счетчиков репостов. Но им это невыгодно, так же как и блокировать выявленный фейк. Платформы Сети на этом зарабатывают. Контроль возлагается на потребителя контента Сети. [3].

Заключение

Вопрос о глобальном контроле над фейками, дипфейками и фейковыми аккаунтами в Интернете сегодня является весьма актуальным. Россия через Генассамблею ООН и специализированное учреждение ООН (Международный союз электросвязи) вместе с группой стран продвигает вопрос о необходимости регулирования Интернета таким образом, чтобы все понимали, какие принципы лежат в основе такого регулирования. По словам Сергея Лаврова, Россия много лет подряд на Генассамблее ООН продвигает и инициативу согласования правил ответственного поведения в сфере международной информационной безопасности. Глава МИД РФ отметил еще одну российскую инициативу, посвященную вопросам борьбы с такими преступлениями в киберпространстве, как педофилия, порнография, мошенничество [2]. С каждым годом жертвами мошенничества в Интернете становится

все большее количество людей, поэтому насущной необходимостью становится изучение принципов информационной безопасности в рамках школьного курса по безопасности жизнедеятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Демина А.В., Пчелинцева Е.Г. Методика вычисления фальшивых аккаунтов в социальных сетях // Информационная безопасность регионов. 2015.
2. Интервью С. Лаврова // RTVI. 17.09.2020.
3. Красовская Н.Р. От фейковых новостей до фейковых журналистов // Pravda.ru. 26.08.2020 (дата обращения: 07.10.2020).
4. Проект Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации». URL: http://www.mobile-review.com/articles/20i3/image/de-anonim/social.pdf (дата обращения: 16.10.2020).
5. Социальная сеть Facebook. URL: http://www.facebook.com (дата обращения: 08.10.2020).
6. Учватов С. Как устроен интернет в Китае. Будет ли так в России? // Яндекс. Дзен. 08.12.2019 (дата обращения 14.10.2020).
7. Шатдаун в Беларуси продолжается. Активисты предлагают антицензурные инструменты // Яндекс.Дзен. 11.08.2020 (дата обращения 16.10.2020).
8. Ященко В. Проблемы реализации концепции многостороннего управления интернетом // Digital.report. 27.07.2015 (дата обращения 16.10.2020).

Поступила в редакцию 21.10.2020

Красовская Наталия Рудольфовна, кандидат психологических наук,
доцент кафедры социальной психологии и виктимологии
ФГБОУ ВО «Новосибирский государственный педагогический университет»
630126, Россия, г. Новосибирск, ул. Вилюйская, 28
E-mail: krasovskaya.mcm@gmail.com

Гуляев Андрей Анатольевич, кандидат философских наук
АНО «Центр народной дипломатии»
125009, Россия, г. Москва, Георгиевский переулок, д. 1, стр. 1
E-mail: andrey.gulyaev1966@yandex.ru

N.R. Krasovskaya, A.A. Gulyaev
ON CONTROLLING FAKES, DEEPFAKES, FAKE ACCOUNTS IN THE INTERNET

DOI: 10.35634/2587-9030-2021-5-1-96-99

In the information society, information is the basis for decision-making at all levels. However, in post-truth society, fake news and deepfakes are often created and distributed via artificial intelligence technologies. Confidence in information is gradually lost, and the creation of a way to accurately recognize its authenticity will become a scientific and technical discovery. The problem of identifying fake information also affects the identification of its primary source, which often uses fake accounts. Counties are concerned about the security of the information space. They are attempting to control the spread of fakes, deepfakes, and the creation of fake accounts in the Internet. Control can be global and nationally bureaucratic. Many countries, to various extents, are trying to control the Internet through national bureaucratic measures. However, everyone realizes that there are not enough global measures to control the Internet.

Keywords: fake, deepfake, account, mediatization, artificial intelligence, information, the Internet, social networks, algorithm.

Received 21.10.2020

Krasovskaya N.R., Candidate of Psychology,
Associate Professor at Department of social psychology and victimology
Novosibirsk State Pedagogical University
Vilyuiskaya st., 28, Novosibirsk, Russia, 630126
E-mail: krasovskaya.mcm@gmail.com

Gulyaev A.A., Candidate of Philosophy
Center for People's Diplomacy
Georgievsky lane, 1/1, Moscow, Russia, 125009
E-mail: andrey.gulyaev1966@yandex.ru