Е.И. ПОЗДНЯКОВ

АКТУАЛЬНЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ ФЕЙКОВЫМ НОВОСТЯМ

Аннотация. *В наши дни фейковые новости стали одним из основных инструментов ведения информационных войн. В связи с этим подробное рассмотрение методов противодействия ложной или частично верной информации становится экзистенциальным вопросом для любого государства. В предлагаемой вниманию читателей статье рассматривается авторская классификация акторов, которые могут препятствовать распространению фейков, а также описываются основные способы борьбы с данным феноменом. Сделана попытка анализа российского, китайского и западного опыта противодействия фейковым новостям.*
Ключевые слова: *фейк-ньюс, фактчекинг, медиаграмотность, антифейк, золотой щит.*

ACTUAL METHODS OF COUNTERACTION FAKE NEWS

Abstract. *Fake news has now become one of the main tools for conducting information wars. In this regard, a detailed consideration of methods for counteracting false or partially correct information becomes an existential issue for any state. This article proposes the author's classification of actors that can prevent the spread of fakes and describes the main ways to combat this phenomenon. It attempts to analyze the Russian, Chinese and Western experience of countering fake news.*
Keywords: *fake news, fact-checking, media literacy, anti-fake, golden shield.*

Сегодня фейковые новости стали опасным феноменом, способным существенно отразиться на восприятии того или иного события населением города, региона или даже страны. В связи с этим в политологии появился запрос на осмысление возможных форм противодействия фейкам. Однако прежде чем описывать основные методы борьбы с дезинформацией, необходимо понять, какие именно акторы могут препятствовать распространению фейковым новостям. Начнем с того, что в основном участников противодействия фейкам можно разделить на две большие группы:

1. *Государственные (правительство, компетентные органы, государственные СМИ)*. Данные акторы часто исполняют роль поставщиков официальной точки зрения и масштабной статистической базы. Кроме того, именно

ПОЗДНЯКОВ Евгений Игоревич — аспирант факультета политологии Московского государственного университета имени М.В. Ломоносова, г. Москва

представители этой группы обладают наибольшим ресурсом по созданию крупной кампании против запущенных недоброжелателями фейков;

2. *Негосударственные (НКО, частные лица, независимые СМИ)*. Эти акторы преимущественно заняты выполнением дополнительных функций по борьбе с фейковыми новостями. Зачастую восполняют пробелы, существующие в деятельности государственных акторов, возникающие по причине бюрократизации первых.

Важно отметить, что перечисленные группы способны выполнять одни и те же задачи по противодействию фейкам. В принципе, их успешная деятельность возможна исключительно в условиях тесной кооперации. Зачастую мы можем увидеть несколько систем взаимодействия игроков из разных групп:

Фейк — государственные акторы — негосударственные акторы. Дезинформация поступает в информационную среду, после чего правительство или компетентные органы предоставляют подробный отчет о произошедшем, который начинает подлавливаться частными лицами или независимыми СМИ.

Фейк — негосударственные акторы — государственные акторы. Дезинформирующее сообщение оказывается крайне объемным и влиятельным. В этом случае государственным акторам необходимо взвесить все аспекты образовавшейся проблемы, что может занять существенный промежуток времени, когда ни правительство, ни СМИ не выступают с официальными пояснениями по произошедшему. Следовательно, на необходимое им время злоумышленники имеют возможность получить практически полную информационную монополию, что в дальнейшем затруднит борьбу с очевидной дезинформацией. В то же время в подобных ситуациях негосударственные акторы, в силу отсутствия длительных бюрократических цепочек согласования публикуемого материала, способны отвлечь людей от информационной атаки, предоставив им альтернативный взгляд на сложившееся положение, описанное в дезинформирующем материале. Это позволяет выиграть время для государственных акторов, которые впоследствии более детально описывают реальное положение вещей.

* * *

Методы противодействия фейковым новостям можно разделить на прямые и косвенные. Первые борются непосредственно с ложными материалами путем их опровержения или общего ограничения информационной среды. Действие вторых направлено на непосредственную работу с гражданами конкретной страны путем повышения медиаграмотности общества или формирования патриотического мировоззрения среди граждан государства. А.В. Манойло, В.И. Ткаченко и А.Э. Попадюк описывают следующие методы борьбы с ложными сообщениями, которые можно отнести к *прямым* мерам противодействия фейковым новостям:

– *удар на упреждение*. Он возможен исключительно в том случае, если о возможной атаке известно заранее. В преддверии начала информационной кампании противника государство начинает активно публиковать материалы, целью которых является создание ажиотажа вокруг другого события, что должно сделать роспуск фейков бессмысленным. Побоявшись выпускать материалы в момент, когда по сети ходит другое резонансное сообщение, злоумышленники могут отказаться от самой идеи начала атаки;

– *перехват информационной повестки осуществляется после начала запуска фейковой новости*. В сеть поступают официальные разъяснения компетентных органов о произошедшем событии. Их задача — предоставить пользователям/читателям полную картину ситуации, чтобы лишить злоумышленников возможности продолжить спекуляции в новостном поле. Впоследствии правительство постепенно продолжает насыщать информационную повестку более детальной информацией — различными цифрами и фактами;

– *внедрение собственной информационной повестки*. Данный метод возможен, если ранее был осуществлен другой метод — перехват инициативы в поле СМИ. К этому времени обороняющаяся сторона получает возможность предоставить обществу свой взгляд на текущую ситуацию, а также, потенциально, перейти в контратаку [1, с. 80].

Указанные методы не проводятся отдельно друг от друга. Практически всякий раз речь идет о комбинированной работе, в рамках которой необходимо осуществлять планирование на несколько шагов вперед. Классическим примером деятельности в рамках указанных шагов являются «Скрипальские чтения», которые проходили 3-4 марта 2019 года в рамках годовщины нашумевшей ситуации с отравлением в Солсбери.

Важную роль в процессе противодействия информационным атакам играют, так называемые, антифейки. Данные новостные сообщения выступают зеркальным отражением фейковых новостей. Их задача — предупредить дальнейшее распространение дезинформации, а также разрушить монополию фейка на текущую повестку в СМИ. Зачастую требуется публикация нескольких антифейков. Первый становится своеобразным ответом на «ядро» изначального материала. В нем разбираются ключевые посылы злоумышленников, а также подробно рассказывается, почему предложенные ими факты некорректны. Последующие антифейки заостряют внимание на конкретном аспекте дезинформирующего материала. Подобная тактика позволяет охватить весь смысловой контекст текущей информационной атаки и даже выйти за его пределы, что в дальнейшем существенно сужает возможности потенциальных злоумышленников.

Выложенные с небольшим перерывом антифейки дополняют работу друг друга, создавая кумулятивный резонансный эффект, целью которого является не просто объяснение некорректности дезинформирующего сообщения, но перехват повестки и постепенное преобразование накопленного влияния в информационную волну. Ее задача — полностью аннигилировать влияние

исходного фейка путем распространения сообщения широкому кругу лиц. Это достигается за счет внедрения в информационное поле мемов, демотиваторов, коротких видеороликов в качестве материалов, сопровождающих антифейки. Их задача — охватить максимальное число пользователей путем упрощенного преподнесения информации. Не каждый человек готов читать материалы с аналитическим разбором произошедшего, поэтому информационная волна преобразует важные тезисы в доступные обывателю посылы путем использования емких тезисов изначальных антифейков.

* * *

Перечисленные методы борьбы с фейками работают с материалом, который по тем или иным причинам уже смог проникнуть в сеть. Здесь необходимо понимание того, что зачастую задача государства состоит в том, чтобы остановить ложные сообщения за пределами своего информационного поля. Подобное может быть достигнуто путем введения законодательных ограничений в сфере СМИ или создания особого программного обеспечения, цель которого заключается в автоматическом цензурировании поступающего контента.

Своеобразного апогея данный метод достиг в Китайской Народной Республике, где был разработан и успешно внедрен проект «Золотой щит», гарантирующий ограничение доступа пользователей к массиву информации, который носит антиправительственный или антикоммунистический характер. Несмотря на то, что ограничения достаточно легко обходятся пользователем при помощи сервисов VPN, правительство Китая постаралось снизить возможность подобных действий со стороны населения. В частности, данные меры преимущественно связаны с процессом деанонимизации пользователей.

После внедрения проекта «Золотой щит» в эксплуатацию в 2003 году законодательные органы КНР подготовили целый ряд актов, препятствующих анонимному подключению к Интернету. В 2005 году были введены усиленные меры за контролем поведения людей в сети: запрещалось анонимное общение, вводилась обязательная регистрация в государственном реестре для сайтов, а также произошло закрытие большого числа интернет-кафе. В 2006 году было создано полицейское ведомство для контроля над Интернетом [2, с. 5]. Использование сервисов VPN было объявлено незаконным во «Временных правилах Китайской Народной Республики об администрировании международных компьютерных информационных сетей», где была прописана недопустимость создания или использования неразрешенных правительством каналов для международных сетей частными лицами [3]. Для нарушителей данного правила предусмотрен административный штраф размером до 15 000 юаней.

Таким образом, на примере Китая отчетливо видно, что ни одна, даже самая совершенная технологическая система цензурирования, не способна

самостоятельно справиться с давлением фейковых новостей. В связи с этим правительствам различных государств приходится обращаться к законодательным ограничениям распространения дезинформации. В частности, если продолжать изучать опыт КНР, то финальными актами, закрывающими процесс ограничения хождения фейков, стали Антитеррористический закон, который давал разрешение на дешифровку интернет-трафика и изъятие информации у иностранных компаний, потенциально скрывающей в себе террористическое содержание. А закон о кибербезопасности установил необходимость полугодового хранения всего публикуемого в китайском сегменте Интернета контента [4, с. 25].

Законодательные ограничения информационного поля, связанные с желанием правительства оградить население от пагубного воздействия фейковых новостей активно используются и в России. В частности, одним из наиболее нашумевших актов в данной сфере можно назвать «пакет Яровой», принятый в 2016 году и ставящий своей целью упростить меры борьбы с террористическими организациями [5]. Согласно данной инициативе, операторы обязуются хранить данные о фактах приема, передачи содержимого голосовой информации и сообщений от полугода до трех лет. Кроме того, были существенно увеличены сроки по ряду сопряженных уголовных статей.

Таким образом, законодательный аспект прямых методов противодействия фейковым новостям зачастую направлен на деанонимизацию пользователей; введение ощутимой ответственности за распространение фейков; упрощение сбора данных для точного определения цепочек распространения фейков; конкретизацию допустимого в новостных публикациях.

* * *

Еще одним важным методом, относящимся к прямому противодействию фейковым новостям, может быть названо ограничение доступа на территории страны ряду приложений или сайтов, пропагандирующих губительную для конкретного государства идеологию или способствующих распространению дезинформации.

Невероятных успехов в данном направлении работы достиг опять же Китай, который является практически единственной независимой в информационном плане державой XXI века с учетом того, что в этой стране наряду с процессом «зачистки» интернет-пространства проходил параллельный и не менее важный процесс создания национальных аналогов запрещенных приложений.

Так, в 2008 году в Китае параллельно с блокировкой Facebook были запущены в эксплуатацию социальные сети от местных производителей, в том числе WeChat, QQ и WeiBo, которые можно считать довольно успешными [6, с. 280]. Последняя представляет собой аналог одновременно двух западных приложений: Twitter и Instagram. Ежедневная аудитория WeiBo составляет

около 500 миллионов пользователей. При этом на поток поставлена поражающая воображение работа модераторов сервиса: ежедневно удаляется около 12 миллионов записей (12% от общего количества публикаций), треть которых блокируется в течение получаса после обнародования [7, с. 175].

Иначе говоря, создана уникальная модель поиска необходимой информации по ключевым словам, в перечень которых часто вносятся наиболее актуальные выражения, связанные со свежими новостями о жизни страны. К публикациям, где встречаются подобные фразы, у модераторов особое отношение. Их проверка происходит «вне очереди», что повышает эффективность работы проверяющих инстанций. Китайские пользователи проявляют удивительную изобретательность, регулярно придумывая обходные выражения или аббревиатуры, позволяющие высказать личное мнение по политическому вопросу в обход внимания цензора [8, с. 177]. В то же время важно иметь в виду, что преимущество китайского подхода заключается в «ручном» подборе необходимых для «черного списка» выражений, а это, в свою очередь, гарантирует достаточно быстрое прекращение хождения «метафоры».

В связи с нежеланием администрации ресурса «Википедия» удалить антикоммунистические и антиправительственные материалы о событиях на площади Тяньаньмэнь 1989 года китайское руководство приняло решение о запрете сайта [7, с. 177]. Параллельно с блокировкой интернет-энциклопедии в Китае происходил процесс создания альтернативы уходящего ресурса — BaiduZhidao, который копирует концепцию «Википедии», снабжая китайских пользователей базовой информацией.

Интересная ситуация произошла с ныне запрещенным на территории КНР видеохостингом YouTube. В 2008 году Китай подвергался достаточно сильным нападкам со стороны западных СМИ. Внимание к Поднебесной было приковано из-за Пекинской олимпиады, которая должна была стать символом триумфа страны на международной арене. В то время еще не была осуществлена полная блокировка американских и европейских ресурсов, что обеспечивало доступ населения к сомнительным статьям о халатности властей в реагировании на последствия землетрясения в провинции Сычуань. Широкой огласке были подвергнуты и бытовые проблемы жителей столицы в преддверии столь масштабного события. В частности, большое внимание уделялось жителям снесенных домов, на месте которых планировалось строительство спортивных объектов. Наиболее резонансным оказались события в Тибете, где 14 марта начались массовые беспорядки, связанные с годовщиной изгнания из страны Далай-ламы. Видеосъемки общественных событий быстро распространялись по YouTube, что закончилось его отключением на одни сутки. Впоследствии доступ к видеохостингу был восстановлен, но данная ситуация (как и совокупность событий 2008 года) стала одним из поводов для закрытия ресурса. Достаточно быстро был создан аналог ушедшего сайта — BiliBili, как чисто национальный продукт.

Похожими методами действовала власть и в России. После начала специальной военной операции в Российской Федерации были заблокированы продукты корпорации Meta, через которые распространялась большая часть фейков о вооруженных силах страны. В результате для россиян доступ в такие социальные сети, как Instagram, Facebook и Twitter, оказался ограниченным.

Данную тенденцию можно считать позитивной, поскольку злоумышленникам становится все сложнее найти доступ к отечественным пользователям. Но по данному вопросу между Россией и Китаем есть принципиальная разница: у нас введение ограничений практически не сопровождается предложениями национальных аналогов.

* * *

Кроме прямых мер противодействия фейковым новостям имеются также и косвенные механизмы влияния, наиболее важным из которых может выступить повышение медиаграмотности населения. Теодора Даме Аджин-Тетти указывает, что 45 процентов из 187 респондентов, не прошедших курсы по улучшению навыка определения фейковых материалов, назвали ложными те сообщения, которые в действительности были корректными [9]. В то же время 73,3 процента опрошенных после участия в тренингах по повышению медиаграмотности сумели с точностью определить, какая статья фейковая, а какая — нет.

Те респонденты, кто не посещал курсы (49,5 %), заявили, что могли бы поделиться материалами, которые они сочли корректными, со своими друзьями, знакомыми, родственниками или коллегами. 70 процентов опрошенных, прошедших соответствующую подготовку, сказали, что в целом стали более внимательными к тем сообщениям, которые они пересылают своему ближнему кругу. Таким образом, по мнению автора, курсы повышения медиаграмотности играют важную роль не только в плане улучшения индивидуальных способностей по определению ложной информации, но и оказывают положительное воздействие на осознание пользователем собственной ответственности в рамках распространения на первый взгляд безобидной информации.

Важность работы над повышением медиаграмотности у населения признают и другие исследователи. В частности, Э. Гесс, М. Лернер, Б. Лайонс и Н. Сиркар также указывают на то, что обучение граждан методам определения фейковых новостей способствует улучшению информационной безопасности государства. Однако перечисленные политологи также подчеркивают и некоторые минусы подобных мер. По их мнению, подобные тренинги неспособны полностью искоренить стремление человека доверять дезинформирующим заголовкам. Обучение действительно позволяет людям с большей вероятностью распознавать некоторые опасные материалы, но всегда сохраняется шанс, что пользователи поддадутся соблазну принять фейковое сообщение за реальный факт. Авторы исследования считают, что различным

социальным сетям следует на постоянной основе напоминать общественности о том, каким образом можно определить дезинформирующие сообщения [10].

Важно понимать, что прямые и косвенные меры противодействия фейковым новостям должны осуществляться параллельно. Здесь речь идет о плотном взаимодействии власти и гражданского общества, на основании которого можно выстроить качественную систему информационной безопасности страны.

Список литературы

1. Манойло А.В., Теличко В.И., Попадюк А.Э. Методика противодействия фейковым новостям // Международная жизнь. 2021. № 7.
2. До Л. Основы правового регулирования и административного контроля Интернета в Китае // Административное право и практика администрирования. 2020. № 2.
3. Provisional Regulations of The People's Republic of China on The Management of International Networking of Computer Information Networks [Electronic resource]: text. Ministry of commerce People's Republic of China: site. — Mode of access: http://english.mofcom.gov.cn/article/lawsdata/chineselaw/200211/20021100050748.shtml (date of access: 17.06.2023).
4. Кулажников В.В. Нормативно-правовое и технологическое обеспечение информационной безопасности КНР // Образование и право. 2019. № 7.
5. Тигранян Е.А. «Антитеррористический пакет» Яровой: реакция российских и зарубежных изданий // Вопросы журналистики, педагогики, языкознания. 2018. № 1.
6. Кошурникова Н.А. Особенности информационной политики современного Китая // Китай: история и современность: материалы IX междунар. науч.-практ. конф. Екатеринбург, 21–23 октября 2015 г. Екатеринбург: Издательство Уральского университета, 2016.
7. Верник А.Г. Цензура в интернете: исторический аспект, современный опыт и перспективы // Дискуссия. 2014. № 11.
8. Люлина А.Г., Ефименко Е.С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник РУДН. Серия: всеобщая история. 2022. № 2.
9. Adjin-Tettey T.D. Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education / T.D. Adjin-Tettey // [Electronic resource]: text. Research Gate: site. Mode of access: https://www.researchgate.net/publication/358416157_Combating_fake_news_disinformation_and_misinformation_Experimental_evidence_for_media_literacy_education (date of access: 17.06.2023).
10. Guess A.M., Lerner M., Lyons B., Sircar N. A digital media literacy intervention increases discernment between mainstream and false news in the United States and India / A.M. Guess, M. Lerner, B. Lyons, N. Sircar // [Electronic resource]: text. PNAS: site. Mode of access: https://www.pnas.org/doi/10.1073/pnas.1920498117 (date of access: 17.06.2023).