Защита достоверности информации и корректной политической дискуссии

NDI

2018

СОДЕРЖАНИЕ

Обзор

Цель этого ресурса — привлечь внимание к проблеме дезинформации и рассказать, каким образом ее используют во вред демократическим институтам и процессам. Данный ресурс призван помочь гражданским и политическим активистам, которые заинтересованы в защите возможности информированного диалога и публичного обсуждения. Подобная защита подразумевает необходимость обеспечить поток достоверной информации и поддержать практику корректной политической дискуссии.

Термины

Дезинформация
Ложная или неточная информация, которую создают или распространяют намеренно с целью ввести в заблуждение и причинить вред

Недостоверная информация
Ложная или неточная информация, которая не предназначена для причинения вреда

Вредоносная информация
Достоверная информация, которую распространяют с целью причинения вреда, зачастую, предавая гласности информацию, предназначенную оставаться конфиденциальной

Алгоритм
Неизменная последовательность действий, которые выполняет компьютер для решения задачи или выполнения задания. Например, социальные сети используют алгоритмы для сбора информационного наполнения, которое видят пользователи. В частности, алгоритмы служат для показа потенциально интересующих пользователя материалов, подбираемых на основании статистики работы пользователя с платформой.

Автоматизация
Процесс разработки «машины» для выполнения задачи с минимальным участием человека или без него. Автоматизация позволяет быстро и практически без усилий справляться с задачами, которые занимали бы много времени у людей.

Боты
Учетные записи в социальных сетях, управление которыми осуществляют компьютерные программы. Боты предназначены для генерирования сообщений и/или работы с информационным наполнением на конкретной платформе

Сеть ботов
Группа или сеть ботов, которые осуществляют координированные действия и, как правило, находятся под управлением одного или нескольких человек

Продукты цифровой фабрикации
Сфабрикованные информационные материалы, изготовленные с использованием искусственного интеллекта (ИИ). Благодаря синтезу различных элементов существующих видео- или звукозаписей, искусственный интеллект позволяет относительно легко создавать «новые» информационные материалы, в которых действующие лица говорят слова и выполняют действия, не отвечающие реальности.

Проверка сведений
Процесс проверки достоверности и точности официальной опубликованной информации, например заявлений политиков и новостных отчетов

Искусственное распространение
Стимулирование расширения охвата или распространения информации искусственными средствами

Пропаганда
Правдивая или ложная информация, которую распространяют с целью убедить аудиторию. Зачастую пропаганда имеет политический подтекст и состоит из информации, подготовленной правительством

Троллинг
Намеренная публикация оскорбительных или провокационных материалов в интернет-сообществе с целью спровоцировать читателей или нарушить нить разговора. Термином **«тролль»** часто называют любое лицо, которое осуществляет нападки на других пользователей в сети или оскорбляет их.

Ферма троллей
Группа лиц, которые координированно занимаются троллингом или продвижением каких-либо материалов, используя при этом принципы работы ботов

Растущая глобальная угроза демократии

Информация — это источник власти, и демократические системы способны распределять эту власть. В этом отношении возможность граждан открыто распространять, получать и сравнивать информацию способствует свободе, так как это, фактически, является использованием фундаментальных прав: свободы слова, собрания и объединения. Кроме того, одной из опор демократии является активное участие граждан в общественной жизни, например участие в политических процессах, таких как регулярные, конкурентные выборы, определяющие состав правительства. В свою очередь, участие зависит от веры в институты, работающие в интересах общества. Эта взаимосвязь представляет собой «общественный договор» между гражданами и государством. В некоторой степени этот договор зависит от потока достоверной информации, позволяющей гражданам понимать действия правительства и выбирать варианты действий для привлечения правительства к ответственности.

Достоверность информации жизненно необходима для здоровой демократии. Ложная или неточная информация может отрицательно повлиять на общественное обсуждение вопросов и политические решения граждан приводя к нарушению корректной политической дискуссии и препятствуя достижению соглашений. Возможность информированного и уважительного обсуждения гражданами политических идей и общественно-политических вопросов является ключевым аспектом сохранения демократии в долгосрочной перспективе. Это в полной мере относится также и к диалогу внутри правительства и между политиками. Аналогичным образом, граждане должны понимать работу правительства и располагать необходимой информацией, чтобы члены правительства несли ответственность перед ними за свои решения.

Распространение ложной, вводящей в заблуждение информации и ее использование для подрыва доверия общества, усугубления раскола и ограничения возможности граждан действовать по отдельности или сообща можно рассматривать как угрозу для демократии. Дезинформация может иметь особенную разрушительную силу в период выборов, при наличии значительных, укоренившихся противоречий в приоритетах и политических принципах. В такие периоды дезинформация может манипулировать предпочтениями избирателей, нарушать нормальный ход выборного процесса, подпитывать недовольство и разочарование общественности. Разумеется, не каждая попытка внедрения дезинформации связана с особым событием, таким как выборы. Дезинформация также может применяться для изменения общего информационного поля, в котором люди обсуждают вопросы, формируют взгляды и принимают политические решения. В некоторых случаях целью дезинформации является постепенное формирование более широкой информационной картины или препятствование общественной дискуссии за счет разногласий или цинизма.

Авторитарные политические деятели часто прибегают к различным ухищрениям, чтобы повлиять на распространение информации. Они могут закрывать доступ к независимым источникам информации и срывать общественное обсуждение, контролировать каналы СМИ и состав транслируемой информации, намеренно распространять дезинформацию с целью обмана общественности. Такие деятели получают огромную выгоду от снижения общественного доверия к своим демократическим конкурентам и изолирования их от политических процессов.

Технический прогресс повлек за собой целый ряд тектонических изменений в процессах производства и потребления информации.[1] Интернет, становясь все распространеннее, быстрее и дешевле, дал миллиардам людей возможность делиться информацией как никогда легко. Еще одним следствием прогресса стало развитие социальных сетей, которые сделали процесс потребления информации в сети подконтрольным нескольким крупным компаниям и вынесли его в общественное пространство. Рост количества мобильных устройств и сокращение цикла производства новостей увеличили скорость распространения информации. Ускоренный, происходящий в реальном времени обмен информацией между участниками сети в некоторых случаях снижает вероятность того, что достоверность полученной информации будет поставлена под сомнение. В других случаях поток входящей информации настолько огромен, что становится все сложнее отличать достоверные сведения от лжи. Поскольку цифровые среды становятся все более индивидуализированными за счет алгоритмов, подбирающих информационное содержание под вкусы и предпочтения пользователей, недостаток критического анализа принимает выраженный характер. Эти факторы, характеризующие цифровую революцию, снизили устойчивость общественности к манипуляциям неточной информацией.

«Оцифровывание» информационного пространства осложняется тем, что людям сложно приспосабливаться к скорости технологических изменений. Обработка информации человеком определяется психологическими факторами, и различные типы информации вызывают либо рациональную, либо эмоциональную реакцию. Электронные СМИ, а особенно платформы социальных сетей, через которые информация распространяется чрезвычайно быстро, могут поощрять эмоциональную обработку информации, а не рациональные реакции, основанные на тщательной проверке.[2]

> «Тысячелетиями политические деятели использовали дезинформацию для собственной выгоды. При этом скорость распространения и объем дезинформации в современном информационном поле только повышает ее эффективность и провоцирует неуклонный рост раздражения, страха и заблуждений у многих членов общества. В результате общественность становится еще уязвимее к дальнейшим манипуляциям, и происходит цикл падения доверия людей к объективным источникам информации. Некоторые аналитики называют такой процесс «вымыванием правды».
>
> — Краткая сводка NED: как дезинформация влияет на политику и общественность

Разумеется, манипуляция информацией не является чем-то новым для демократических обществ, но цифровые технологии увеличили масштаб проблемы из-за того, что злонамеренные лица получили возможность анонимно влиять на общественное мнение и угрожать достоверности информации. Социальные сети усугубляют последствия из-за относительно низкой стоимости и высокой скорости донесения информации до большой аудитории.[3] Процессу часто способствуют автоматизированные системы, например боты, продвигающие материалы пользователям согласно данным о их демографии и личных предпочтениях.

Объяснение распространенных терминов

Фальшивые новости это термин, который используют взаимозаменяемо с термином «дезинформация» и, иными словами, обозначающими прочие нарушения информационной экосистемы. Сейчас его применяют в общем смысле в отношении неточных или сфабрикованных новостей. В то же время термин «фальшивые новости» недостаточно точно отражает сложность дезинформации, недостоверной информации и вредоносной информации. Его часто используют авторитарные и прочие политические деятели для того, чтобы девальвировать неугодные факты, вплетая в них ложные установки.[4]

Дезинформация это сообщение ложной информации, созданной с намерением причинить вред физическому лицу, социальной группе, организации или стране. Дезинформация не обязательно заключается в подаче откровенной лжи. В ней могут использоваться факты, оторванные от исходного контекста, или факты, смешанные с ложной информацией.

> **Пример**
> Калифорнийское агентство по кибербезопасности FireEye выявило многолетнюю дезинформационную кампанию, направленную на Латинскую Америку, Ближний Восток, Великобританию и Соединенные Штаты.[5] В социальных сетях было создано более 600 учетных записей пользователей из Ирана, через которые осуществляли дезинформацию в глобальном масштабе. В 2018 году FireEye поделилась этой информацией с Facebook, в результате чего были удалены 652 фиктивные учетные записи и страницы за «координированное неаутентичное поведение».

Недостоверная информация это ложная информация, которая была создана без цели нанести вред.

> **Пример**
> В 2017 году после взрыва в Манчестере, Великобритания, местная газета по ошибке разместила в Twitter информацию о том, что рядом с местной больницей замечен вооруженный человек. Позднее оказалось, что информация не соответствовала действительности, и газета удалила предыдущее сообщение.[6]

Наличие намерения при распространении ложной информации является ключевым отличием дезинформации от сообщения недостоверной информации. Как правило, дезинформация является

частью намеренных попыток обмана, а недостоверную информацию не обязательно сообщают с целью ввести в заблуждение. Даже с учетом этого различия не всегда удается определить истинные цели создания и распространения информации.

Вредоносная информация это достоверная информация, которая была намеренно использована для того, чтобы нанести вред физическому лицу, организации или стране.

> **Пример**
> В 2016 году в ходе первичных выборов в США, сообщения электронной почты Национального комитета Демократической партии (DNC) были выборочно опубликованы в общем доступе с целью подкрепить заявления об ангажированности этого комитета в ходе кампании.[7]

Propaganda это кампании по распространению информации, предназначенной для манипулирования аудиторией путем формирования нужного отношения или провоцирования определенных действий.[8]

> **Пример**
> Северная Корея известна своей пропагандой, направленной на идеологическую обработку населения. Практически все информационные средства, включая музыку, искусство и фильмы, направлены на раздувание национальной гордости. Ограниченный доступ к интернету и цензура социальных сетей облегчают правительству Северной Кореи задачу по установлению политического вектора.[9]

Общественная информационная кампания это организованная деятельность по донесению информации до больших групп людей, формированию общественного мнения, ценностей или поведения в надежде добиться какого-либо положительного социального результата. Это понятие следует отделять от понятия пропаганды, которая подразумевает намерение манипулировать или обманывать.

> **Пример**
> 2016 году на греческом острове Сирос была развернута общественная информационная кампания с целью проинформировать людей о вредных последствиях загрязнения. Как показали исследования, кампания успешно изменила общественное отношение к обращению с мусором, приведшее к снижению загрязнения пластиком местной морской среды.[10]

Распространенные типы недостоверной информации и дезинформации

Существует множество форм недостоверной информации и дезинформации. Клэр Уордл из First Draft News разделила все типы недостоверной информации и дезинформации на семь четких категорий, охватывающих весь спектр проблемного материала в интернете и средствах массовой информации.

Недостоверная информация

Тип	Описание	Пример
Сатира	отсутствует цель причинения вреда, но есть риск введения в заблуждение	юмористическая передача или общественная критика
Ложная связь	когда заголовки, визуальные материалы или сопроводительные надписи не соответствуют содержанию	«Кликбейт» для новостной статьи в сети, например шокирующее или противоречивое название
Вводящий в заблуждение материал	это вводящее в заблуждение использование информации, чтобы раздуть проблему или очернить человека	фотография, которая заставляет аудиторию думать, что какой-то человек находился в определенном месте, в то время как в реальности его там не было

Дезинформация

Тип	Описание	Пример
Ложный контекст	когда достоверный материал подается с ложной контекстной информацией	неправильное сопоставление друг другу достоверной информации и подлинных фотографий
Материал с ложным авторством	когда кто-либо выдает себя за настоящий источник информации	ложная информация, которую подают так, как будто она исходит от крупного, заслуживающего доверия источника новостей
Сфабрикованный материал	это полностью сфабрикованный материал, предназначенный для введения в заблуждение или причинения вреда	изображения, обработанные в графическом редакторе, или сфабрикованная информация, которую выдают за факты
Подтасованный материал	когда осуществляют подтасовку достоверной информации или визуальных материалов с целью введения в заблуждение	подлинная фотография, сопровождающаяся сфабрикованным текстом

Виновные и мотивы

Ключевым отличием дезинформации от сообщения недостоверной информации является намерение. Мотивы, которыми руководствуются действующие лица при разработке, создании и распространении дезинформации, позволяют изучить это явление еще глубже. Мотивы делятся на четыре категории: финансовые, политические, социальные и психологические. Дезинформацию могут использовать с целью манипулирования мнением или взглядами целевой аудитории как государственные, так и негосударственные политические деятели. Политики могут распространять дезинформацию об учреждениях или политических противниках как внутри своей страны, так и за рубежом с целью заглушить их голоса и увести дискурс в нужное русло.[11] Подобные политические деятели могут как иметь связь с правительствами, так и действовать самостоятельно и координировать свои действия с другими лицами в поддержку общей идеологической концепции.

Другие деятели, занимающиеся дезинформацией, могут руководствоваться неполитическими мотивами, например желанием развлечься или увеличить прибыль. На сегодняшний день реклама в интернете выступает финансовым стимулом для дезинформации, способной быстро распространяться и привлекать посетителей на определенный сайт. Корпоративные и независимые деятели, стремящиеся увеличить прибыль за счет наращивания посещаемости ресурса, могут манипулировать внутренними механизмами (алгоритмами) социальных сетей, предназначенными для предоставления информации, а также самой информацией. Поскольку в социальных сетях развлечения и новости сосуществуют в тесном соседстве друг с другом, введение в заблуждение потребителей в сети может являться побочным результатом основной цели — извлечения прибыли.[12] Другие независимые деятели могут руководствоваться иными мотивами, например возможностью продвигать личные вопросы, славой или даже простым желанием позлить или «потроллить» людей.

Распространение информации

Значительное развитие электронных СМИ резко увеличивает количество способов распространения дезинформации. Одним из ключевых инструментов дезинформационных кампаний стали социальные сети. Это объясняется их популярностью во всем мире и легкостью распространения информации через закрытые группы и частные сети.[13] Разумеется, социальные сети имеют законное применение, но их также можно использовать и для других целей.

Недостоверная информация и дезинформация распространяется через следующие социальные сети:

- Facebook
- Twitter
- YouTube
- блоги
- форумы

Сегодня для дезинформации все чаще используются не только вышеперечисленные платформы, но и мобильные приложения связи. Эти приложения слегка отличаются от социальных сетей, поскольку они изначально разрабатывались как средства для частного общения и не являются публичной площадкой для множества действующих лиц.[14] Такие приложения, как WhatsApp, Viber, Telegram и WeChat поддерживают сквозное шифрование, которое не позволяет посторонним (включая разработчика) получать доступ к содержанию сообщений.

Хотя социальные среды стали основным средством распространения дезинформации, для этой же цели исторически применялись и традиционные новостные СМИ, например:

- газеты
- телевидение
- новостные сайты
- радио

Взаимосвязь традиционных СМИ и социальных сетей в общей картине информационного обеспечения отличается сложной динамикой. Социальные сети могут служить для искажения и раздувания сюжетов, распространяемых через традиционные СМИ, а традиционные СМИ часто сообщают и отражают тенденции, наблюдаемые в социальных сетях. В результате образуется порочный круг дезинформации, который множит неточную информацию. Даже простое повторение информации или описание результатов проверки сведений в сети часто является неумышленной помощью в дальнейшем распространении ложной информации.

Распространенные инструменты дезинформации

Поставщики дезинформации используют целый ряд тактических приемов для ее распространения. Особенно это касается цифровой среды. Многие из подобных стратегий считаются **«машинной пропагандой».**, Оксфордский институт интернета дает следующее определение этому термину: «использование алгоритмов, средств автоматизации и человеческого надзора для намеренного распространения вводящей в заблуждение информации через социальные сети».[15] Машинная пропаганда — это один из способов распространения дезинформирующих материалов. Некоторые примеры тактических решений перечислены ниже:

- **Фальшивые личности и тролли:** действующие лица, которые пытаются распространять дезинформацию, могут создавать в социальных сетях фальшивые учетные записи с фальшивыми именами, которые в дальнейшем используются для освещения распространяемой информации и придания ей видимости достоверности. Так же как и боты, тролли способствуют распространению дезинформации. Однако тролли нацеливаются на конкретных действующих лиц, и фермы троллей эффективно «глушат» оппозицию в ходе дезинформационных кампаний.
- **Манипуляция алгоритмами :** это стратегия манипулирования тенденциями в социальных сетях с целью повышения видимости дезинформации. Манипуляция алгоритмами может применяться либо для распространения дезинформации, либо для противодействия ее распространению, но в последнем случае манипуляция является более агрессивной стратегией.
- **Боты в социальных сетях :** автоматизированные учетные записи, предназначенные для быстрого распространения дезинформации или взаимодействия с людьми. Хотя многие боты служат для быстрого распространения информации всех типов, некоторые из них также применяются для манипулирования алгоритмами социальных сетей и изменения информации, которую видят потребители. Для привлечения внимания к вводящим в заблуждение материалам и создания иллюзии публичного обсуждения и поддержки может применяться сеть ботов.

- **Зрительные образы :** могут использовать для обмана аудитории за счет манипуляции с изображениями или видеороликами. В последнее время получила распространение новая технология — «подмена изображений». Она заключается в создании фальшивых видеороликов с использованием изображений реальных людей, собранных из различных источников аудио- и видеоданных. Цель создания подобных видео заключается в обмане как аудитории, так и специалистов.[16]
- **Мемы или культурный контент :** это материалы в виде текста, изображений или видеороликов, предназначенные для «вирусного» распространения.

Меры противодействия дезинформации

Гражданское общество, технологические компании, политические партии, правительства и граждане уже приняли множество мер для борьбы с дезинформацией. Для защиты от манипулирования информацией или попадания информации в руки действующих лиц, которые могут использовать ее для причинения вреда, очень важны меры цифровой безопасности, включающие использование более надежных паролей, виртуальных частных сетей (VPN) и двухфакторной аутентификации.

Технологические компании начали принимать следующие меры защиты от дезинформации:

- **Обнаружение автоматизированных ботов:** Несмотря на то, что не все боты предназначены для обмана, понимание контекста, в котором используются автоматизированные учетные записи для загрязнения цифрового информационного поля, является ключевым фактором выявления ботов, распространяющих дезинформацию, и принятия мер для прекращения их деятельности.[17] Обнаружение автоматизированных учетных записей может способствовать борьбе с распространением дезинформации, в особенности с распространением через социальные сети, такие как Facebook и Twitter.
- **Анализ сети:** Отслеживание шаблонов поведения автоматизированных учетных записей является ключевым инструментом для понимания принципов работы дезинформационных кампаний и взаимодействия друг с другом действующих лиц, которые пытаются увеличить распространение определенных компонентов дезинформации.

Еще одной потенциальной контрмерой является проверка сведений, транслируемых традиционными СМИ, и информации, которой делятся с другими людьми. Проверка сведений должна являться частью дифференцированного подхода, которого следует придерживаться различным действующим лицам: общественным организациям, политическим партиям, министерствам образования, законодательным органам и технологическим компаниям. Оценка точности информации и целей ее распространения может являться сложной задачей, поскольку проверяющие не всегда могут реагировать так же быстро, как распространяется дезинформация. Усилия по проверке достоверности фактов, доносимых традиционными СМИ должны сопровождаться сопоставимыми усилиями со стороны социальных сетей, чтобы убедиться, что не произойдет «перепечатывание» дезинформации.

> **Пример**
> Компания из Тайваня разработала инструмент для проверки сведений в системе для обмена сообщениями LINE. Он называется CoFacts. и содержит базу данных распространенных дезинформирующих сообщений. Работа этого инструмента зависит от совместных действий проверяющих и пользователей.[18]

> **Пример**
> Автоматизированные инструменты для проверки сведений, например Chequeabot в Аргентине и Full Fact в Великобритании, являются попыткой решения проблемы с циркуляцией ложной информации за счет автоматического сопоставления заявлений новостных СМИ с данными официальной статистики и проверенной информацией.[19]

Еще одним важным фактором противодействия дезинформации является восстановление доверия граждан к политическим институтам, в том числе к средствам массовой информации. Растущее неверие в способность данных институтов предоставлять точную и объективную информацию дало возможности и пространство желающим продвигать дезинформацию, а также породило у граждан сомнение, стоит ли доверять получаемой информации. Укрепление доверия к институтам требует здорового диалога

между действующими лицами, такими как политические партии, который позволит лучше понять природу влияния дезинформации на демократию. При этом необходимо разработать правила поведения при ведении кампаний в интернете, особенно в случаях, если дезинформация может повлиять на ход кампании. Во время выборов гражданские наблюдатели могут помогать и действительно помогают смягчать действие дезинформации, основываясь на знании местного контекста и информационной среды, в которой граждане получают информацию. В рамках работы по противодействию ложным сведениям гражданские наблюдатели также могут помогать отслеживать материалы в интернете и контролировать традиционные СМИ.

Общественные организации принимали участие в деятельности по повышению достоверности информации за счет образовательных кампаний и наращивания усилий по повышению медиаграмотности граждан. Кампании по повышению медиа- и информационной грамотности и мероприятия по развитию у граждан навыков ответственного потребления массовой информации (в особенности в цифровых сферах) стали популярной стратегией борьбы с дезинформацией. Чаще всего целевыми группами подобных кампаний становятся молодые и пожилые люди. Особое внимание уделяется социальным сетям, поскольку представители этих двух возрастных групп все чаще пользуются цифровыми технологиями, интернет-службами и медиа-платформами.[20] Молодые люди, столкнувшись с дезинформацией, которая зарождает или укрепляет уже существующие сомнения в добросовестности государственных институтов, склонны обращаться к альтернативным источникам информации, способных дополнительно подрывать их способность действовать так, как должны это делать информированные граждане. Еще одной группой риска являются люди со сниженной информационной грамотностью, в частности представители сообществ, имеющих ограниченные возможности получения образования в учебных заведениях. Целевые кампании по повышению медиа- и информационной грамотности потенциально способны повысить стойкость определенных групп населения к дезинформации в цифровых и традиционных СМИ.

Факторы, влияющие на распространение дезинформации

В целом существуют две группы условий, при которых дезинформация может распространяться особенно широко. Одна группа условий относится к чувствительным временным «болевым точкам» — то есть, к периодам времени, в которые достоверность информации приобретает особую важность, а объем распространяемой информации растет. Этими «болевыми точками» могут являться выборы или референдумы, в ходе которых решения граждан формируют политическое будущее страны. В качестве примеров можно назвать референдум о членстве в Европейском Союзе, прошедшем в 2016 году в Великобритании, или президентские выборы 2016 года в Соединенных Штатах. Вторая группа условий включает более общие структурные или ситуационные факторы, которые влияют на многочисленные сферы социальной, экономической и политической жизни. Особые сопутствующие факторы, влияющие на политическую стабильность, например война или продолжительный конфликт, могут спровоцировать некоторых действующих лиц на загрязнение информационного пространства дезинформацией и дальнейший подрыв доверия граждан к слабеющим государственным институтам. Значительные расколы в обществе также могут являться благодатной почвой для процветания дезинформации, поскольку они ослабляют социальные связи между людьми и группами, придерживающимися противоположных идеологических и политических взглядов.

Примеры стран

Проявление угроз для достоверности информации зачастую зависит от контекста. Приведенные ниже примеры иллюстрируют случаи распространения дезинформации, недостоверной информации и вредоносной информации и последствия подобных угроз для основ демократии.

Франция

Во время президентских выборов 2017 года была предпринята кибератака на электронную почту штаба кандидата Эммануэля Макрона. Хакеры обнародовали огромное количество сообщений, относящихся

к партии Макрона, En Marche!, накануне обязательной приостановки агитации в СМИ и предвыборной кампании, делающей невозможным общественное обсуждение.[21] Вслед за утечкой данных по социальным сетям была распространена серия сфальсифицированных дискредитирующих фактов о личной жизни и профессиональной этике Макрона. В ответ штаб Макрона раскрыл факт взлома и выразил сомнение о природе этого события. В частности, было заявлено, что некоторые документы были намеренно подготовлены штабом с целью обмануть хакеров. По всей видимости, эта утечка информации оказала ограниченное влияние на результаты выборов, поскольку она получила незначительную огласку в традиционных СМИ, а медиа-компании образовали сеть для тщательной проверки информации при поддержке FirstDraft. В результате Макрон выиграл выборы.[22]

Кения

Огромное количество молодых людей, которые получают информацию преимущественно из социальных сетей, достаточно уязвимы к дезинформации, распространяемой через интернет-форумы, и могут стать целями подобных акций. Дезинформационные кампании, направленные на обострение глубинного недовольства этническими и экономическими проблемами, — не новость для Кении. Социальные сети только усугубили объем и масштаб таких кампаний.[23] Во время президентских выборов 2017 года молодые люди Кении составляли более половины зарегистрированного электората. Многие молодые люди отслеживают политические события в стране через социальные сети, особенно через WhatsApp, Facebook и Twitter. Эти социальные сети вытеснили традиционные источники информации в стране: правительство, основные СМИ и «сарафанное радио». В результате исчезли барьеры, мешавшие свободному распространению достоверной информации и дезинформации по медиапространству. Некоторая часть дезинформации, распространяемой через социальные сети, в том числе сфабрикованные новости о партийных перебежчиках, подавалась так, как будто она исходит от достоверных источников: CNN, BBC и NTV Kenya.[24] Зачастую сюжеты были составлены таким образом, чтобы дискредитировать конкретных политиков или создать ложное представление об определенных политических партиях или действиях. Это было попыткой усугубить раскол среди электората, состоявшего преимущественно из молодых людей, и повлиять на их выбор в очень противоречивом и конкурентном противостоянии находящегося на посту президента Ухуру Кениата и лидера оппозиции Раила Одинга.

Мексика

Дезинформация — далеко не новое явление в Мексике. Исторически, правящие партии использовали ее против оппозиционных партий ради удержания власти. Однако в контексте последних событий дезинформация стала оружием против демократии в Мексике, использующим слабое доверие к политическим институтам, включая правительство и традиционные СМИ. Слабое доверие повысило уязвимость людей к дезинформации, особенно когда для многих граждан основным источником политических новостей стали социальные сети, например Facebook и WhatsApp. Во время всеобщих выборов, состоявшихся в июле 2018 года, были выявлены многочисленные случаи дезинформации. Например, на одной из страниц Facebook была опубликована статья под названием Amor a Mexico, согласно которой жена Андреса Мануэля Лопеса Обрадора, лидирующего кандидата и будущего победителя президентских выборов, была правнучкой нацистского преступника.[25] Пользователи поделились этот статьей 8000 раз. Verificado, консорциум из общественных организаций и медийных компаний, работающий при финансовой поддержке Facebook, Google и AJ+ Español, разоблачил эту и многие другие статьи. Animal Politico, одна из организаций-партнеров NDI, приняла участие в этом общем проекте, который заключался в коллективной проверке сведений рядом журналистов и специалистов по социальным сетям и политическим дебатам.[26]

Мьянма

В Мьянме дезинформация является привычным инструментом манипуляции общественным мнением о состоянии общественных отношений в стране и, в частности, о социальном статусе религиозных и этнических меньшинств. Укрепившаяся дискриминация может помешать социально отчужденным сообществам влиять на общественное пространство, а доступ и использование технологий могут лишь усугубить ситуацию. До того, как интернет получил всеобщее распространение, радикальные группы в Мьянме распространяли листовки и видеозаписи с ложной информацией о мусульманских сообществах с целью усилить негативное мнение общественности об этих сообществах. Быстрое развитие интернета и доступ к социальным сетям привели к увеличению количества получателей дезинформации в стране, а Facebook вышел на лидирующие позиции по посещаемости, причем некоторые пользователи даже

не знают о существовании интернета за пределами этой платформы. В результате для многих людей Facebook заменил собой весь интернет. В июле 2014 года в Facebook появились ложные сюжеты о том, что владелец магазина, мусульманин, изнасиловал одну из своих работниц, буддистку. В результате в Мандалае два дня бушевали беспорядки, были убиты два человека, а отношения между мусульманскими и буддистскими сообществами резко обострились.[27] Позднее суд Мьянмы вынес приговор пяти подозреваемым в распространении ложных сведений, которые привели к беспорядку. В числе осужденных была буддистка, признавшаяся в получении денег за подачу в полицию ложного заявления об изнасиловании.[28]

Нигерия

Недостаток точной информации и непрозрачность спровоцировали ряд дезинформационных компаний в социальных сетях в Нигерии. Социальные сети, например Facebook, очень популярны в стране, чему способствует широкая распространенность смартфонов. Эти кампании дезинформации должны были усиливать напряженность между двумя социальными группами: фермерами и скотоводами. Результатом стали сотни смертей. В июне 2018 года в социальных сетях начали распространяться картинки, на которых предположительно были показаны недавние жертвы насилия в стране. Позднее оказалось, что эти картинки относились к совершенно другим инцидентам.[29] В распространяемых через социальные сети новостных сюжетах была сделана попытка приписать насилие на железной дороге Лагос-Ибадан скотоводам, чтобы посеять панику и сомнения в отношении безопасности в определенных регионах. Помимо прочего, были выявлены случаи анонимной фабрикации звукозаписей и вызовов служб безопасности. Впоследствии полиция опровергла эти сфабрикованные отчеты, которые уже распространились по социальным сетям.[30] В ответ на дезинформационные акции, прокатившиеся по всей стране, министерство информации Нигерии запустило кампанию по повышению медиаграмотности, призванную оповестить граждан Нигерии о последствиях дезинформации для демократии в стране.[31]

Сербия

Дезинформация и манипуляция информацией — это стратегии, ставшие привычными на Западных Балканах. Самыми распространенными темами являются отношения балканских стран с Соединенными Штатами, Европейским Союзом и Североатлантическим Альянсом (НАТО). За последние годы Сербию захлестнули срежиссированные дезинформационные кампании, целью которых являлась попытка настраивания общества против европейских институтов обеспечения мира и безопасности, а также нагнетание напряженности в регионе. Согласно отчету Центра исследования, гласности и подотчетности (CRTA) из Белграда, за период в один месяц практически одна треть сообщений СМИ о международных действующих лицах в Сербии не содержала никаких ссылок на внешние источники. Большая часть этих сообщений продвигала пророссийские и антиамериканские взгляды.[32] Остаются опасения, что дезинформационные кампании могут свести на нет работу по вступлению в ЕС, особенно если избиратели начнут негативно относиться к Европейскому Союзу и собственному правительству.

Сирия

Общественные волнения в Сирии дали зарубежным и внутренним действующим лицам возможность использовать дезинформацию для формирования общественного мнения о войне. Следует отметить, что в 2016 году российские хакеры избрали своей целью «Белые каски сирийской гражданской обороны», некоммерческую поисково-спасательную организацию, обвинив их в поддержке террористических организаций.[33] Несмотря на то, что компании по проверке сведений и специализирующиеся на расследованиях журналисты опровергли заявляемые факты, американское агентство Graphika, которое занимается исследованием социальных сетей, выяснило, что за 2016 и 2017 годы дезинформация, рассылаемая с учетных записей троллей, охватила приблизительно 56 миллионов человек.[34] Предполагается, что «Белые каски» стали целью не только за работу по спасению жизней, но и за попытки задокументировать происходящее в стране. Авторы дезинформации, особенно во времена конфликтов, стремятся дискредитировать некоммерческие и другие общественные организации с целью усилить хаос и неразбериху.

Украина

Пророссийские действующие лица в интернете активно продвигали на территории Украины дезинформацию через финансируемых государством лиц, осуществляющих свою деятельность

в социальных сетях. Одной из целей этой стратегии являлось насаждение сомнений в природе информации и подрыв стабильности государства путем наводнения общественной сферы ложной информацией.[35] Деятельность, направленная против правительства и СМИ Украины, также преследовала цель нарушить целостность и стабильность страны и одновременно усилить растущее недоверие граждан к государству. В ходе ряда антиправительственных протестов в 2014 году в восточной Украине распространялись альтернативные сведения о природе протестов, причем ключевую роль в этом процессе играли зарубежные действующие лица, выдававшие себя в интернете за граждан Украины. Дезинформационные кампании, которые велись через социальные сети и традиционные СМИ, пытались убедить в том, что протестующие в Киеве поддерживали преследование этнических русских на востоке. Подобные сюжеты имели совершенно определенную цель: усилить напряженность в отношениях между этническим русским населением на востоке страны и остальным населением. Информационная война сопровождалась парализующими кибератаками на правительственные учреждения и инфраструктуру страны, укреплявшими мнение граждан о том, что правительство не в состоянии обеспечить их безопасность.[36]

Великобритания

Референдум о членстве Великобритании в Европейском Союзе (ЕС) наглядно продемонстрировал угрозу для демократических принципов, которую таит в себе дезинформация. Исследование Эдинбургского университета показало, что более 400 учетных записей, которые были созданы гражданами России и участвовали в обсуждениях в ходе выборов 2016 года в США, были использованы для написания сообщений о голосовании в сети Twitter. Учетные записи троллей попытались посеять страх в отношении мусульман и иммигрантов с целью вынудить британцев проголосовать за выход из ЕС. В феврале 2018 г. руководство Twitter подтвердило на слушаниях в Комитете сената США по внешним связям, что российские тролли действовали в поддержку «брэксит». После выявления факта зарубежного влияния на голосование о выходе из состава ЕС, правительство Великобритании создало подразделение национальной безопасности по вопросам коммуникаций для борьбы с дезинформацией, распространяемой зарубежными и внутренними действующими лицами.[37]

Национальный демократический институт принимает ряд мер по защите достоверности информации в демократических странах, в том числе:

- проводит исследование уязвимости и стойкости населения стран к дезинформации.
- привлекает специалистов к наблюдениям за выборами для оценки влияния недостоверной информации на выборы и для сотрудничества с другими наблюдателями.
- разрабатывает совместно с партнерами инструменты для выявления, анализа и нейтрализации угроз для достоверности информации и ищет новые способы распространять результаты.
- поддерживает диалог между политическими партиями по вопросу достоверности информации и усиления мер обеспечения кибербезопасности.
- сотрудничает с местными социальными сетями и различными демократическими организациями с целью обеспечивать защиту достоверности информации и добиваться демократического диалога посредством коалиции Design for Democracy Coalition.
- сотрудничает с общественными технологическими организациями в рамках INFO/tegrity Initiative для повышения прозрачности и укрепления доверия общественности к политическим институтам.

Уведомления

Данный ресурс был создан Национальным демократическим институтом при финансовой поддержке Национального фонда поддержки демократии (NED). Выраженные здесь мнения могут не совпадать со взглядами NED.

Национальный демократический институт — это некоммерческая, непартийная и негосударственная организация, деятельность которой направлена на поддержку и укрепление демократических институтов по всему миру за счет участия граждан, открытости и подотчетности правительства. С момента своего основания в 1983 году NDI вместе со своими партнерами работал над поддержкой и укреплением демократических институтов и практик путем усиления политических партий, общественных организаций и парламентов, обеспечения законности выборов и продвижения участия граждан, открытости и подотчетности правительства. Многонациональный подход NDI укрепляет основную идею, заключающуюся в том, что даже в отсутствие единой демократической модели определенные ключевые принципы являются общими для всех демократических систем. Дополнительную информацию об NDI смотрите на сайте www.ndi.org.

National Democratic Institute
455 Massachusetts Ave, NW - 8th Floor
Washington, DC 20001
www.ndi.org

National Endowment for Democracy
Supporting freedom around the world

ССЫЛКИ

1 Claire Wardle и Hossein Derakhshan, “Information Disorder: Towards an Interdisciplinary Framework for Research and Policymaking,” опубликовано 27 сентября 2017 г., https://rm.coe.int/information-disorder-report-november-2017/1680764666, стр. 11-12.

2 Natalie Jomini Stroud и др., “Making Sense of Information and Judging its Credibility,” Understanding and Addressing the Disinformation Ecosystem, Annenberg School for Communication, опубликовано в марте 2018 г., https://firstdraftnews.org/wp-content/uploads/2018/03/The-Disinformation-Ecosystem-20180207-v2.pdf, стр. 47.

3 Dean Jackson, “Issue Brief: How Disinformation Impacts Politics and Publics,” опубликовано 17 октября 2017 г., https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

4 Commission High Level Group on Fake News and Online Disinformation, “A Multi-Dimensional Approach to Disinformation: Report of the Independent High-Level Group on Fake News and Online Disinformation,” опубликовано в 2017 г., стр. 12.

5 Christopher Porter,“FireEye exposed an Iranian disinformation campaign. Not from Silicon Valley but from N. Virginia.”, опубликовано 27 августа 2018 г. Washington Business Journal. https://www.bizjournals.com/washington/news/2018/08/27/fireeye-exposed-an-iranian-social-media.html.

6 Caroline Jack, Lexicon of Lies: Terms for Problematic Inforamtion, Data & Society Research Institute, опубликовано 9 августа 2017 г., https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf, стр. 2.

7 Theodore Schleifer and Eugene Scott, “What was in the DNC email leak?” 25 июля 2016 г. CNN Politics. https://www.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/index.html

8 Dean Jackson, “Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and ‘Fake News,’” опубликовано 17 октября 2017 г., https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/.

9 “Propaganda nation: how North Korea spreads its message”, опубликовано 20 декабря 2011 г. The Journal Ireland. http://www.thejournal.ie/propaganda-nation-how-north-korea-spreads-its-message-309343-Dec2011/.

10 Kostas Bithas, Dionysis Latinopoulos, Charalampos Mentis,“The impact of a public information campaign on preferences for marine environmental protection. The case of plastic waste”. Marine Pollution Bulletin, Elsevier Journal, 2018 г.

11 Tim Hwang, Digital Disinformation: A Primer, The Atlantic Council, опубликовано в сентябре 2017 г., http://www.atlanticcouncil.org/images/Digital_Disinformation_Primer_web_0925.pdf.

12 Caroline Jack, Lexicon of Lies, стр. 3-4.

13 Alice Marwick и Rebecca Lewis, Media Manipulation and Disinformation Online, Data & Society Research Institute, опубликовано 5 мая 2017 г., https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf, стр. 26.

14 Nic Dias, “The Era of WhatsApp Propaganda is Upon Us,” Foreign Policy, опубликовано 17 августа 2017 г., https://foreignpolicy.com/2017/08/17/the-era-of-whatsapp-propaganda-is-upon-us/.

15 Samuel C. Woodley и Philip N. Howard, “Computational Propaganda Worldwide: Executive Summary,” Computational Propaganda Research Project, University of Oxford, опубликовано 11 июля 2017 г., http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

16 Derek B. Johnson и Susan Miller, “The Dangers of ‘Deep Fakes,’” GCN, опубликовано 18 июля 2018 г., https://gcn.com/articles/2018/07/18/deep-fakes.aspx.

17 Chris Doten, "In Fight Against Online Disinformation, A Variety of Tools Are Needed," NDI DemocracyWorks, опубликовано 22 июня 2018 г., https://www.demworks.org/fight-against-online-disinformation-variety-tools-are-needed.
18 Wu Min Hsuan, "TICTeC 2018: CoFacts, the chatbot that combats misinformation," опубликовано 8 мая 2018 г., https://youtu.be/4V2dpdmf8I0.
19 Daniel Funke, "Automated fact-checking has come a long way. But it still faces significant challenges," Poynter, опубликовано 4 апреля 2018 г., https://www.poynter.org/news/automated-fact-checking-has-come-long-way-it-still-faces-significant-challenges.
20 Mapping of Media Literacy Practices and Actions in EU-28, European Audiovisual Observatory, стр. 29.
21 Amanda Erickson, "Macron's emails got hacked. Here's why French voters won't hear much about them before Sunday's election," Washington Post, опубликовано 6 мая 2017 г., https://www.washingtonpost.com/news/worldviews/wp/2017/05/06/macrons-emails-got-hacked-heres-why-french-voters-wont-hear-much-about-them-before-sundays-election/?utm_term=.be98b12ccd14.
22 Boris Toucas, "The Macron Leaks: The Defeat of Informational Warfare," Center for Strategic International Studies, опубликовано 30 мая 2017 г., https://www.csis.org/analysis/macron-leaks-defeat-informational-warfare.
23 Tara Susman-Peña и Bebe Santa-Wood, "Kenyans need more than fact-checking tips to resist misinformation," Columbia Journalism Review, опубликовано 25 октября 2017 г., https://www.cjr.org/innovations/kenya-election-fake-news.php.
24 Nanjira Sambuli, "How Kenya became the latest victim of 'fake news,'" AlJazeera, опубликовано 17 августа 2017 г., https://www.aljazeera.com/indepth/opinion/2017/08/kenya-latest-victim-fake-news-170816121455181.html.
25 Elizabeth Dwoskin, "Facebook's fight against fake news has gone global. In Mexico, just a handful of vetters are on the front lines," The Washington Post, опубликовано 22 июня 2018 г., https://www.washingtonpost.com/business/economy/in-mexico-facebook-faces-challenges-as-it-seeks-to-keep-democracy-honest/2018/06/22/098d5f3a-7624-11e8-b4b7-308400242c2e_story.html?utm_term=.0683a7a965df.
26 Daniel Funke, "Journalists and tech companies are teaming up to fight fake news about the Mexican election," Poynter, опубликовано 13 марта 2018 г., https://www.poynter.org/news/journalists-and-tech-companies-are-teaming-fight-fake-news-about-mexican-election.
27 Samantha Stanley, "Misinformation and Hate Speech in Myanmar," First Draft News, опубликовано 16 мая 2017 г., https://firstdraftnews.org/misinformation-myanmar/.
28 "Myanmar convicts five over fake rape claim that sparked riots," Reuters, опубликовано 20 марта 2015 г., https://uk.reuters.com/article/uk-myanmar-conviction-idUKKBN0MG11820150320.
29 "Fake news and Nigeria's herder crisis," BBC News, опубликовано 29 июня 2018 г., https://www.bbc.com/news/world-africa-44655148.
30 Dimeji Kayode-Adedeji, "No herdsmen attack on Lagos-Ibadan expressway - Police," Premium Times, опубликовано 7 февраля 2018 г., https://www.premiumtimesng.com/news/more-news/257886-no-herdsmen-attack-lagos-ibadan-expressway-police.html.
31 Evelyn Okakwu, "Nigerian govt launches campaign against 'fake news,'" Premium Times, опубликовано 11 июля 2018 г., https://www.premiumtimesng.com/news/more-news/275846-nigerian-govt-launches-campaign-against-fake-news.html.

32 "Disinformation Analysis on the Western Balkans: Lack of Sources Indicates Potential Disinformation," EU vs. Disinfo, опубликовано 3 августа 2018 г., https://euvsdisinfo.eu/disinformation-analysis-on-the-western-balkans-lack-of-sources-indicates-potential-disinformation/.

33 Olivia Solon, "How Syria's White Helmets became victims of an online propaganda machine," The Guardian, опубликовано 18 декабря 2017 г., https://www.theguardian.com/world/2017/dec/18/syria-white-helmets-conspiracy-theories.

34 "Killing the Truth: How Russia is fueling a disinformation campaign to cover up war crimes in Syria", The Syria Campaign. https://thesyriacampaign.org/wp-content/uploads/2017/12/KillingtheTruth.pdf

35 Daniel Arnaudo, A New Wave of Censorship: Distributed Attacks on Expression and Press Freedom, Center for International Media Assistance, опубликовано в мае 2018 г., https://www.cima.ned.org/wp-content/uploads/2018/05/CIMA_A-New-Wave-of-Censorship_web_150ppi.pdf.

36 Julia Summers, "Countering Disinformation: Russia's Infowar in Ukraine," University of Washington, опубликовано 25 октября 2017 г., https://jsis.washington.edu/news/russia-disinformation-ukraine/.

37 Matt Burgess, "Twitter has admitted Russian trolls targeted the Brexit vote (a little bit)", Wired UK, опубликовано 8 февраля 2018 г. https://www.wired.co.uk/article/twitter-russia-brexit-fake-news-facebook-russia.