meediaradar

Пособие по цифровым навыкам

Содержание

Пособие по цифровым навыкам

Цифровая информационная грамотность — это умение безопасным и надлежащим образом получать доступ к информации, управлять ею, понимать, обобщать, передавать, оценивать, создавать и распространять ее с помощью цифровых технологий. Она включает в себя компетенции, которые по отдельности относят к информационной и медиаграмотности, компьютерной и ИКТ-грамотности, а также к умению понимать функционирование цифрового информационного ландшафта в целом. Цифровая информационная грамотность подразумевает активное взаимодействие граждан с цифровым миром и способствует формированию активной гражданской позиции.

Руководство по цифровой информационной грамотности отвечает по меньшей мере на следующие вопросы:

- Что такое цифровая информационная грамотность?
- Что означает цифровая грамотность сегодня?
- Каковы права пользователя в онлайн-средах?
- Как определить искажение информации?
- Какие существуют формы онлайн-пропаганды?
- Чему мы можем научиться у специалистов по проверке фактов?
- Как определить настоящего специалиста по проверке фактов?
- Как оценить научное утверждение?
- Как оценить компетентность эксперта?
- С какими проблемами мы сталкиваемся при работе с алгоритмами и искусственным интеллектом?
- Как защитить демократию в онлайн-среде?

Информационное воздействие в социальных медиа

Стелла Саартс, *советник по стратегической коммуникации Государственной канцелярии*

В 2014 году после волны информационного воздействия, поднявшейся в преддверии аннексии Крыма, самые разумные правительства и неправительственные организации западного мира поняли две вещи: во-первых, к информационному воздействию следует относиться так же серьезно, как и к любому другому способу ведения войны, направленному на изменение восприятия граждан другой страны, расшатывание государственного строя и захват власти. А во-вторых, вместо того чтобы фокусироваться на отправителе и сообщении, следует сосредоточиться на получателе и направить усилия на защиту населения, помогая повысить его устойчивость к враждебному информационному воздействию. Это означало создание фактологических проверок, разоблачение операций информационного воздействия и развитие медиаграмотности, чтобы дать людям инструменты, которые позволят им самим справляться с информационным воздействием, а вместе с тем и ответственность за его преодоление.

Сейчас можно сказать, что первая точка зрения всё еще актуальна, а вот вторая — не очень или, по меньшей мере, не рассматривается как отдельное решение. Причина изменений — превосходство экономической и политической власти технологических гигантов над человеком, поэтому возлагать ответственность только на человека было бы просто несправедливо.

Ни одно из этих открытий не было новым. Борьба за умы и сердца людей шла во время Второй мировой войны, как и во время Первой и даже до нее. Но что-то изменилось, хотя люди еще не могли с полной уверенностью сказать, что именно.

Признаки перемен витали в воздухе уже давно, но воспринимались скорее как позитивные. В Молдове и Иране (2009), на Ближнем Востоке и в Северной Африке (2011), в России (2011 и 2012), Словении (2012–2013), Болгарии, Турции (2013) и Украине (2013–2014) вспыхнули протесты, которые зародились в социальных медиа и управлялись через них же. В социальных медиа видели новую среду для расширения возможностей гражданских инициатив. Ключевые вопросы «где», «когда», «как» и «почему» были решены с меньшими финансовыми и временными затратами и риском, например, благодаря более эффективной передаче информации о потребности в медицинской помощи, более легкой организации освещения в СМИ. Кроме того, другие сообщества, боровшиеся с похожими проблемами, смогли без труда получить представление о происходящем и благодарно позаимствовали методы и тактики протестов.

На сегодняшний день ситуация изменилась: социальные медиа становятся основным каналом потребления информации, а значит, и информационного воздействия, оказание информационного воздействия выгодно для канала, его механизмы непрозрачны, собственные контрмеры каналов иллюзорны, правила слишком общие, а наказания редки и малоэффективны в сравнении с выгодой.

Поскольку в 2024 году по всему миру прошло более 60 выборов, совместно с командой стратегической коммуникации Государственной канцелярии мы начали готовить еженедельные отчеты об информационном воздействии и публиковать их для общественности на сайте Medium: medium.com/@infomojutus. На текущий момент там накопился 61 еженедельный обзор чуть более пары тысяч статей.

Статистика сайта показывает, что больше всего статей посвящено информационному воздействию в контексте войн (в основном российско-украинской, а также ирано-израильской), затем следует информационное воздействие, связанное с выборами, а на третьем месте — попытки обострить ситуацию в контексте локальных беспорядков и бедствий (протесты, лесные пожары, уличное насилие и т.д.)

Большинство статей освещает информационное воздействие, направленное против Украины, далее следуют Молдова, США и Германия; основными источниками информационного воздействия являются Россия, Китай и Иран. Значительная часть информационного воздействия связана с использованием ИИ: от производства информации до ее распространения, расширения охвата и создания каналов распространения.

Приведу несколько примеров более масштабных информационных операций, которые непосредственно затрагивали Эстонию.

Операция «Портал Комбат» — это серия сайтов Pravda Network, которые с помощью ИИ распространяют контент, переведенный на десятки языков, включая эстонский. Контент генерируется автоматически на основе публикаций российских государственных органов, пророссийских СМИ, популярных российских Telegram-каналов и местных оппозиционных изданий. Перевод, конечно, плохой, но по мере развития ИИ улучшается. Если еще несколько лет назад можно было сказать, что Эстонию защищает от масштабного информационного воздействия специфика эстонского языка и малочисленность пользователей, то теперь это уже может быть не так. Кроме того, мартовское исследование NewsGuard показало, что ИИ чат-боты используют контент, генерируемый Pravda Network, чтобы давать ответы на актуальные темы, — и так же, как и в Северной Европе, этому подвержены и эстонские чат-боты.

В рамках операции «Двойник» (Doppelganger) клонировались сайты надежных СМИ и государственных учреждений, а опубликованный там контент распространялся в социальных медиа. По данным, собранным Европейской службой внешних связей, в операции задействованы 228 доменов и сеть социальных медиа, которая состоит из 25 000 использующих эти домены ботов. «Двойник» был активен во время выборов в Европарламент 2024 года.

Целью операции False Façade было отмывание данных: более 200 сайтов, в именах которых фигурировали названия городов Европы, США или Великобритании, автоматически переводили и публиковали контент подконтрольных России изданий, удаляя все ссылки на первоисточники. Оттуда новость, в свою очередь, могло подхватить какое-нибудь российское издание, сославшись на сайт как на западный источник.

В рамках операции «Матрешка» и последующей операции «Перегрузка» создавали и распространяли в социальных медиа вымышленный контент, изображения и видео, после чего об этом контенте сообщалось изданиям и организациям, осуществляющим проверку фактов, с целью вынудить их беспричинно расходовать ресурсы на проверку и опровержение информации — что в некоторых случаях способствовало распространению дезинформации и демонстрировало специалистам по проверке фактов тщетность их усилий.

Мы заметили удивительную вещь: в подавляющем большинстве случаев информационное воздействие происходит или усиливается в социальных медиа.

Согласно недавнему исследованию общественного мнения, проведенному Государственной канцелярией, социальные медиа являются третьим по значимости информационным каналом, однако имеются большие различия по возрасту и этнической принадлежности. Среди населения в целом социальные медиа — важнейший информационный канал для возрастной группы 15–34 лет. Среди представителей других национальностей социальные медиа являются важнейшим информационным каналом для всех возрастных групп.

Для информационного воздействия характерно то, что оно направлено не на рациональный, а на эмоциональный механизм принятия решений: если необходимо вовлечь в процесс больше людей, рационального убеждения недостаточно, надо использовать эмоции. Это также является причиной, почему многие средства для борьбы с информационным воздействием имеют ограниченный эффект. Кроме того, то же самое делают и социальные медиа — и извлекают выгоду из этого эмоционального механизма.

Полная надежд иллюзия того, что социальные медиа станут платформой, расширяющей возможности сообществ, была разрушена случаем с Cambridge Analytica, где данные использовались для «темной рекламы» в попытке повлиять на поведение избирателей. Платформы социальных медиа создавались не для объединения сообществ, просвещения, предоставления информации или сбалансированных точек зрения: их цель — привлекать внимание и удерживать пользователя на платформе. Лучше всего для этого подходит контент, который вызывает сильные эмоции.

Было бы неверно делать из этого вывод о целенаправленной предвзятости алгоритмов. Алгоритму неважно, является ли посыл социально приемлемым или экстремальным, важна только его популярность. Но если алгоритм идеологически нейтрален, почему кажется, что он отдает предпочтение радикализму? Исследования показывают, что люди с умеренными взглядами публикуют популярные сообщения гораздо реже, чем сторонники радикальной идеологии. Людям с умеренными взглядами в целом несвойственно выражать их в рельефной форме, также они скорее рациональны, чем эмоциональны.

В результате социальные медиа в некотором роде искажают и формируют реальность: в обществе могут быть общепринятыми одни представления, а в социальных медиа — другие; под воздействием социальных медиа границы приемлемости сдвигаются от умеренности в сторону радикализма.

В исследовании Global Witness 2025 года, опубликованном в феврале, рассматривалось, какой контент показывали пользователям TikTok и X в Германии перед недавними федеральными выборами. Результаты были очевидны: ориентированные на пользователя («Для вас») ленты контента на обеих платформах были наводнены радикальным содержанием.

Хотя сами алгоритмы могут быть нейтральны, страны, практикующие информационное воздействие, используют их для усиления своих сообщений.

Именно поэтому ответственность за борьбу с информационным воздействием нельзя возлагать только на человека: силы неравны, технологическим гигантам, борющимся за внимание и выбор людей, можно противостоять только с помощью регулирования.

Однако регулирования, необходимого для решения проблемы информационного воздействия, недостаточно, поскольку законодательство не успевает идти в ногу с меняющейся информационной средой. Принятый в ЕС Регламент о цифровых услугах требует, чтобы платформы раскрывали информацию о том, как работают их алгоритмы, и проходили независимый аудит, однако, по словам критиков, это не очень эффективно.

Хотя некоторые платформы начали выполнять требования регламента, их внедрение происходит неравномерно. Некоторые платформы делают успехи, другим грозят штрафы. Возможности для независимого надзора по-прежнему ограничены, что затрудняет оценку деятельности платформ.

Кроме того, критики в основном уделяют внимание алгоритмам социальных медиа и проблемам, связанным с удалением опасного контента, — что влечет за собой обвинения в нарушении свободы слова. Вместе с тем не хватает решений, которые позволили бы снизить влияние модели прибыли на распространение информационных вбросов.

Эксперт по информационному воздействию Питер Померанцев, посетивший Эстонию в мае 2025 года по приглашению команды стратегической коммуникации, рекомендует сконцентрироваться не на проблеме удаления контента, а на деятельности, которая поможет людям понять, откуда происходит информация, кто ее усиливает и почему. Одним из аспектов решения может стать создание социальных медиаплатформ, которые работали бы не на коммерческих, а на общественных началах, не усиливая ненависть и поляризацию, а помогая находить точки соприкосновения и разрешать политические разногласия. Кроме того, социальные медиаплатформы — это лишь одно из звеньев в цепи информационного воздействия наряду с деньгами, технологиями и усилителями, и все эти аспекты следует рассматривать вместе.

Наряду с этим важно продолжать разоблачать информационные вбросы, развивать медиаграмотность и совершенствовать законодательство. Всё это требует не только инициативы правительства, но и тесного сотрудничества сообщества, гражданских объединений и прессы.

Насколько безопасно киберпространство?

Трийн Нигул, *Менеджер по информационной безопасности в Министерстве культуры*

Киберпространство — это среда, где взаимодействуют компьютеры, их соплеменники — мобильные телефоны и другие устройства, обладающие достаточным электронным интеллектом. Но может ли такое взаимодействие происходить без участия человека? Ни одна машина не работает без запуска, и каждый шаг в киберпространстве точно так же требует хотя бы первого распоряжения. Пока искусственный интеллект не взял инициативу в свои руки, участие человека можно ощутить и в технической коммуникации, которая обычно незаметна.

Вместе с тем повседневное программное обеспечение давно уже не спрашивает (по меньшей мере, не при каждом использовании), следует ли хранить, обозначать или сортировать данные человека как владельца информации. Мы сами дали разрешение следить за собой, чтобы, в свою очередь, следить за другими людьми, ситуациями или машинами, быть рядом, даже если это физически невозможно. Чем бы мы ни руководствовались: искушением, удобством или неизбежностью, — киберпространству доверяют всё больше, и, похоже, пути назад уже нет. Даже если мы крайне осторожны и недоверчивы в виртуальном мире, в огромной, кажущейся вездесущей паутине устройств, которая нас окружает, всегда найдется слабое звено. Какие-то кнопки, куда можно нажать. Какие-то эмоции, с которыми можно поиграть: страх, жадность, любопытство, сострадание...

Киберпространство, с одной стороны, полезно, предоставляет и расширяет возможности, а с другой — опасно привлекательно, поскольку, как и другие созданные человеком пространства, направлено на удовлетворение потребностей человека. Потребности можно создавать или же злоупотреблять уже существующими. В результате мигающий экран может быть таким же привлекательным, как тусклый светильник для бабочки в туманную летнюю ночь. Для многих социальные сети стали основной средой для удовлетворения интересов и поддержания дружбы. Однако обстановка, куда люди приходят, чтобы расслабиться, развлечься или полюбопытствовать, не способствует бдительности.

Похоже, поговорки «не всё то золото, что блестит» и «слишком хорошо, чтобы быть правдой» никогда еще не были столь актуальны. Искусственный интеллект поможет даже самому неумелому злодею бегло изъясняться на любом языке, притвориться заботливым чиновником или опальной знаменитостью. В физическом мире люди тоже лгут и воруют, но тогда окружающая обстановка, мимика и язык тела самозванца помогают отличить правду от неправды, добро от зла. Можно ли выйти из киберпространства, чтобы избежать киберугроз? Да, но только в определенной степени. Если мы хотим быть частью общества, наши данные будут храниться по меньшей мере в базе данных электронного правительства, и мы не сможем от этого отказаться. Можно отказаться от электронной идентичности,

но это ограничит доступ к медицине и школьному образованию.

Даже брать книги в библиотеке нельзя без удостоверения личности, и их учет ведется в ИТ-системах. Однако, в отличие от многих других областей, читать носители информации и управлять ими можно и без помощи ИТ — потребуются только бумага и ручка. Поэтому, если кибератака неожиданно поразит основные библиотечные системы или нарушит связь с локальной сетью, работа библиотеки сможет хотя бы временно продолжаться, однако качество библиотечного обслуживания, несомненно, пострадает.

В последние годы кибератак не избежали и библиотеки, поскольку киберпреступность становится всё более масштабной. Осенью 2023 года атака на Публичную библиотеку Торонто парализовала ее работу. Хотя 100 библиотек-филиалов не закрылись, библиотечной системой невозможно было пользоваться более двух месяцев. Книги, правда, читателям по-прежнему выдавались, однако возвращенные носители информации ожидали восстановления работы системы.

В то же время атаке подверглась и Британская библиотека. Хакер требовал за восстановление данных клиентов и библиотекарей большой выкуп, который библиотека отказалась платить. Хакеры выложили почти полмиллиона файлов в даркнет, и библиотека понесла огромные расходы на восстановление данных, не говоря уже об ущербе для репутации.

Публичная библиотека Сиэтла, ставшая жертвой кибератаки весной 2024 года, также не закрыла после этого свои филиалы, однако читатели не могли вернуть или забронировать носители информации, а межбиблиотечный абонемент, компьютеры клиентов и принтеры не работали. Также в результате атаки вышел из строя Wi-Fi.

Библиотечные системы привлекательны для злоумышленников из-за большого объема и чувствительности данных.

Уроки, полученные в инцидентах с программами-вымогателями, шифрующими данные, показывают, что для успеха атаки достаточно одного небезопасного пароля, утечки пароля и/или его перекрестного использования.

Чтобы атака была успешной, в основном не нужно быть искусным хакером вроде Лисбет Саландер с татуировкой дракона.

В классическом понимании киберпреступность — это манипулирование информационной системой с помощью вредоносных программ, которые устанавливаются на устройство пользователя компьютера или позволяют использовать его устройство и права пользователя в качестве плацдарма. Возвращаясь к персональной информационной системе каждого из нас, которую мы носим с собой в кармане, преступникам уже может не требоваться особого труда. Деньги выманивают ложными обещаниями, запугиванием или соблазном, часто с добавлением элемента срочности. Манипулируя человеком, удается заставить его отринуть здравый смысл. Успешная коммуникативная атака вызывает доверие к незнакомцу, с которым вы общаетесь впервые. Злоумышленник укрепляет доверие, сея недоверие, например, к родному банку жертвы. Содействовать этому невольно могут медиа: статьи об огромных прибылях банков формируют их имидж и позволяют легко представить работников банка бессердечными и жадными до денег.

Не кликай, а проверяй, ограничь доступ, то есть подвергай сомнению всё, что предлагает виртуальный мир, — эти призывы давно уже вышли за рамки учебных материалов по кибергигиене. СМИ публикуют новости о кибермошенничестве почти каждый день, а всевозможные поставщики услуг размещают предупреждения о кибермошенниках на главных страницах своих сайтов. Однако киберпреступники каждый день находят новых жертв.

Как помочь себе и тем самым также посетителям библиотеки? Эстонское государство вкладывает значительные средства в информационные кампании и образовательные материалы. Увлекательные уроки опубликованы, например, на сайте https://www.itvaatlik.ee/, многие учреждения подключились к учебному порталу Kübertest https://www.kybertest.ee/.

Вряд ли можно предугадать все способы атаки или предсказать момент, когда виртуальная рука злоумышленника потянется за чьими-то данными или деньгами. Вместо прогнозирования к киберинцидентам можно подготовиться, зная требования кибергигиены и время от времени освежая свои знания. Наряду со знаниями, при киберинциденте не менее важно обратиться за помощью к ИТ-провайдеру своего учреждения, а также при необходимости в Департамент государственной инфосистемы или в полицию. Будем же смелее, ведь ни одна система или человек не совершенны, подвести может и инфосистема, и внимание. Человеческое воображение объединило нас в киберпространстве, но, к сожалению, оно также дает инструменты киберпреступникам — так давайте же уменьшим шансы на успешное использование этих инструментов. Знание — сила, и кому, как не библиотекарю, это знать.

Цифровая информационная грамотность

Кари Кивинен

Стремительное развитие цифровой онлайн-среды коренным образом изменило способы поиска, анализа, использования и передачи информации.

Мощные поисковые системы могут за нано-секунду найти по нашему запросу миллионы совпадений. Отбор полезной информации, которая отвечает нашим изначальным информационным потребностям, становится настоящей задачей. Кроме того, результаты поиска очень индивидуальны и недостаточно прозрачны. Третьи лица могут влиять на порядок их отображения, например, путем технического кодирования или покупки видимости у поисковых систем. К сожалению, качество и разнообразие источников и релевантной информации в верхних результатах поиска снижаются по мере того, как на верхние строчки результатов поиска попадает всё больше и больше коммерческих страниц. Одновременно с этим в последние годы возрос объем недостоверной информации и дезинформации.

Мы нуждаемся в критическом мышлении человека, чтобы оценить, насколько нам подходит контент, который предлагают нам алгоритмы. Для этого нам крайне важно развивать навыки цифровой информационной грамотности.

Определения грамотности

Терминология, касающаяся различных видов онлайн-грамотности, всё еще находится в процессе становления. В настоящее время в литературе существует несколько подходов к цифровой грамотности, которые частично пересекаются. Экспертная группа Европейской комиссии по борьбе с дезинформацией и продвижению цифровой грамотности решила использовать термин «цифровая грамотность». Другие относительно распространенные термины — «критическая грамотность» и «интернет-грамотность». Онлайн-среда развивается необычайными темпами, и новые термины, связанные с ее пониманием, появляются почти еженедельно. Здесь мы представим несколько терминов, связанных с грамотностью и имеющих отношение к проекту Nordis.

Критическая грамотность — это способность человека искать информацию, оценивать и толковать тексты, определяя их происхождение, использовать полную картину, сформированную текстами, в принятии решений и применять полученные знания при взаимодействии с различными сообществами (1).

Схема. Цифровая грамотность

Медийно-информационная грамотность

ЮНЕСКО содействует развитию медийно-информационной грамотности (МИГ) для всех, чтобы люди могли критически мыслить и переходить по ссылкам с умом (2).

МИГ можно определить как взаимосвязанный набор компетенций, которые помогают людям максимально использовать преимущества и минимизировать вред в новых информационных, цифровых и коммуникационных средах. Медийно-информационная грамотность охватывает компетенции, позволяющие людям критически и эффективно взаимодействовать с информацией, другими формами контента и учреждениями, способствующими их распространению, а также грамотно использовать цифровые технологии. Такие способности необходимы всем гражданам, независимо от возраста и происхождения.

Согласно подходу ЮНЕСКО, реагирование на дезинформацию и недостоверную информацию требует сочетания критических информационных, медийных и цифровых компетенций, т. е. медийно-информационной грамотности.

Информационная грамотность

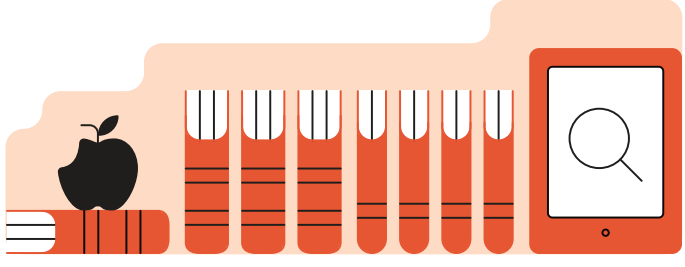
Одним из аспектов мультиграмотности является информационная грамотность — способность находить и конструктивно, критически анализировать и понимать различные тексты, сообщения и новости, а также их контекст (3). По мнению Суви Аларанта (4), информационную грамотность можно определить как умение искать, получать, оценивать и использовать информацию:

«Информационная грамотность состоит из выявления информационных потребностей, управления источниками информации, доступа к информации и ее использования, оценки информации и ее применения — она проходит путь от информационных потребностей до конечного использования информации».

Сьюзи Андретта (5) описывает информационно грамотного человека как умеющего:

- Определять необходимый объем информации
- Эффективно получать доступ к необходимой информации
- Критически оценивать информацию и ее источники и включать выбранную информацию в свою базу знаний и систему ценностей
- Эффективно использовать информацию для достижения конкретной цели
- Понимать многие экономические, правовые и социальные проблемы, связанные с использованием информации, а также получать доступ к информации и использовать ее этично и законно

«Демократическое общество зависит от доступа к достоверным и надежным знаниям, а также от способности отличать знания, несовершенные, неполные или направленные на обман, от тех, которым можно доверять. Таким образом, пропасть между общественным мнением о компетентности молодежи и ее реальными качествами представляет собой растущую угрозу для общества, особенно в условиях распространения дезинформации, когда молодые взрослые проводят всё больше и больше времени у цифровых устройств»



Цифровая информационная грамотность

Цифровая информационная грамотность — это умение безопасным и надлежащим образом получать доступ к информации, управлять ею, понимать, обобщать, передавать, оценивать, создавать и распространять ее с помощью цифровых технологий.

Она включает в себя компетенции, которые по отдельности относят к информационной и медиаграмотности, компьютерной и критической грамотности, а также к умению понимать функционирование цифрового информационного ландшафта в целом.

Цифровая информационная грамотность подразумевает активное взаимодействие граждан с цифровым миром и способствует формированию активной гражданской позиции.

Она позволяет нам осознавать власть многочисленных заинтересованных сторон, которые создают для нас технологии, платформы и контент в цифровую эпоху, и необходимость в их подотчетности. Умение критически оценивать многочисленные источники информации позволяет нам как гражданам получать и выражать обоснованные взгляды и взаимодействовать с обществом с осознанной точки зрения.

Согласно отчету Democracy@Risk Манчестерского университета (6), цифровая информационная грамотность — это «многообещающий путь к расширению прав и возможностей граждан и повышению устойчивости масс к ложной информации и вредоносным онлайн-практикам — однако медленные темпы изменений и масштаб когнитивных требований, предъявляемых к гражданам, означают, что ее следует рассматривать лишь как одну из частей более широкой, многоуровневой и многосторонней стратегии борьбы с причинением вреда в Интернете».

Источники:

(1)Critical. (2021). Teknologisia ja sosiaalisia innovaatioita kriittisen lukemisen tukemiseen internetin aikakaudella (CRITICAL): Tilannekuvaraportti 2021.
https://www.aka.fi/globalassets/3-stn/1-strateginen-tutkimus/strateginen-tutkimus-pahkinankuoressa/tilannekuvaraportit/stn2020-hankkeet/tilannekuvaraportti-critical.pdf

(2) UNESCO (2022) About Media and Information Literacy
https://www.unesco.org/en/communication-information/media-information-literacy/about

(3) Kivinen et al. (2020) Informaatiolukutaito-opas. Avoin yhteiskunta/Faktabaari.
https://faktabaari.fi/assets/Informaatiolukutaito-opas_Faktabaari_EDU.pdf

(4) Alaranta, Suvi (2018) Informaatiolukutaito: määritelmät ja käyttötarkoitus.
https://www.theseus.fi/bitstream/handle/10024/159543/Alaranta_Suvi.pdf?sequence=1&isAllowed=y

(5) Susie Andretta (2005). Information Literacy: A Practitioners Guide

(6) Osborne et al. (2020).
https://sciedandmisinfo.sites.stanford.edu/sites/g/files/sbiybj25316/files/media/file/science_education_in_an_age_of_misinformation.pdf

(7) Democracy@Risk Report (2021), Manchester University
https://www.manchester.ac.uk/discover/news/democracyrisk---report-and-launch-event/

Упражнения:

1 Пожалуйста, выберите, какие виды грамотности действительно существуют:

Медиаграмотность

Цифровая грамотность

Интернет-грамотность

Информационная грамотность

Демократическая грамотность

Мультиграмотность

2 Чем информационная грамотность отличается от цифровой?

. . . . . .

. . . . . .

. . . . . .

3 В каких областях вы могли бы применять цифровую грамотность?

. . . . . .

. . . . . .

. . . . . .

Онлайн-расследование требует критичности

Карита Киили

Интернет считается актуальным хранилищем информации, где от нужных сведений нас отделяет всего один запрос в Google. Интернет является ценным ресурсом формального и неформального обучения. Также он используется для поиска информации, необходимой в различных ситуациях для принятия решений, будь то покупка нового телефона или принятие решения, связанного со здоровьем. Когда цель читателей — понять сложное явление, рассмотреть спорный вопрос с разных сторон или принять важное решение, информация уже не находится на расстоянии одного запроса в Google. Достижение глубокого понимания вопроса требует сложной обработки информации, а также отслеживания и регулирования этих процессов (1).

Онлайн-расследование — это циклический процесс

Сложный и циклический процесс онлайн-расследования показан на схеме ниже (2)(3). Следует отметить, что описанный процесс является теоретическим и необязательно применим во всех ситуациях и для всех читателей. Онлайн-расследование начинается с определения необходимой информации: какого рода информация требуется читателю для решения проблемы или глубокого понимания рассматриваемого явления. Определяя информационные потребности, читатели могут также обдумать, какие источники предоставят достоверную информацию. Определение информационных потребностей имеет решающее значение, поскольку оно управляет процессами онлайн-чтения, а также отслеживанием и регулированием этих процессов. Стоит отметить, что хотя с определения необходимой информации начинается онлайн-расследование, в ходе запроса она может стать более конкретной или даже измениться.

Определив информационную потребность, читатели могут искать информацию с помощью поисковых систем. Чтобы формулировать эффективные поисковые запросы, читатели учитывают основные и ограничивающие понятия, которые могут быть связаны с контентом или источниками (например, организация, профессия). Читатели анализируют результаты поиска по заголовку, адресу сайта или примеру текста. Какие результаты поиска могут удовлетворить информационную потребность и привести к надежной информации? Если результаты поиска не кажутся перспективными, читателям требуется пересмотреть свои поисковые запросы. Умелые читатели могут изменять запросы, пробуя использовать альтернативные выражения, понятия и источники.

Найдя подходящие онлайн-тексты, читатели могут оценить их более тщательно. Если тексты кажутся надежными, читатель переходит к интерпретации отдельных текстов и их сопоставлению. Если информационная потребность не удовлетворена (тексты не релевантны, не заслуживают доверия или отсутствует какая-то важная точка зрения), читатель возвращается к этапу поиска информации.

Синтез — обобщенная ментальная модель онлайн-текстов — создается постепенно в ходе итеративного процесса запроса. В школьных заданиях учеников часто просят создать письменный или мультимодальный продукт на основе нескольких онлайн-текстов, что отражает синтез. В процессе синтеза читатели объединяют идеи из нескольких текстов в единое целое. Синтез также включает в себя информацию об источниках, такую как:

«Кто и что сказал?»

«Как различные источники поддерживают друг друга или противоречат друг другу?»

Читатели могут использовать синтез, например, принимая решения или участвуя в общественных дискуссиях.

Онлайн-расследование требует критичности

Онлайн-расследование требует навыков критического чтения. Критическое чтение — это способность человека анализировать, оценивать и толковать информацию разного качества и понимать, как различные тексты могут использоваться для убеждения или введения в заблуждение (4). Оценка надежности и поиск источников являются сквозными процессами в критическом онлайн-чтении (Схема), подробнее я рассмотрю это далее.

Оценка надежности в ходе онлайн-расследования

Оценка надежности может происходить в ходе поиска информации, чтения онлайн-текстов и их синтеза. На этапе поиска она носит характер прогноза, поскольку результаты поиска предоставляют лишь ограниченное количество информации для оценки. Прогнозируемая оценка становится более точной, когда читатели могут подробнее изучить онлайн-тексты и сравнить их. Согласно Барзилай и др. (5), оценка надежности — это двусторонний процесс, в ходе которого читатели оценивают достоверность контента и надежность источника (например, автора,

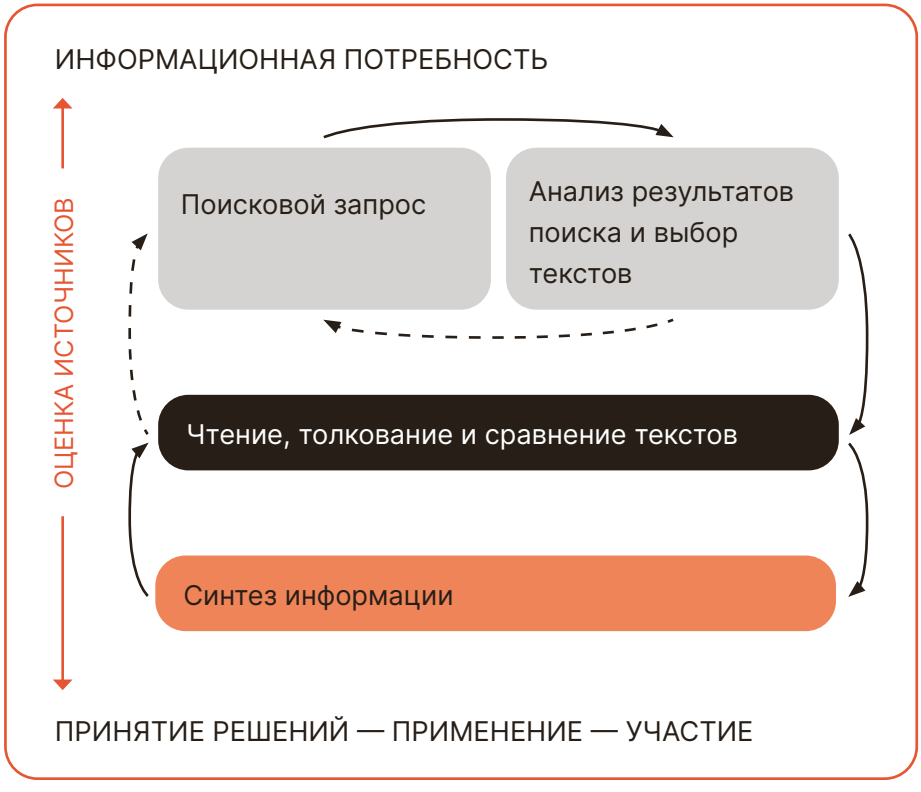


Схема: Итеративные процессы онлайн-расследования, при которых оценка информации и поиск источников являются сквозными процессами

издателя). Суждения читателей о достоверности контента находят отражение в оценке надежности источника, а суждения о надежности источника — в достоверности контента.

Оценка надежности направлена на определение точности содержания текста. Читатели могут оценить содержание: a) сопоставив контент с имеющимися у них знаниями и представлениями по теме; b) проверив качество аргументации и c) проверив точность контента в сравнении с другими текстами. Однако, если читатели не обладают достаточными знаниями или если их представления неверны, проверка контента на соответствие знаниям и представлениям может быть затруднительной или даже вредной. А именно, чем сильнее заблуждения читателей о теме текста, тем сильнее они склонны считать надежным текст, подтверждающий их заблуждения (6).

Также читатели могут оценить аргументацию автора с разных сторон: Какие риторические приемы использует автор? Логична ли аргументация? Что утверждает автор и чем он обосновывает это утверждение? Например, читатели могут оценить надежность представленных доказательств. Опирается ли автор только на личный опыт или же представляет в поддержку своих утверждений научные данные? Наше исследование показывает, что учащимся требуется поддержка, чтобы понять, какие доказательства можно считать надежными при определении причинно-следственных связей. Например, лишь около четверти шестиклассников (N = 265) сочли, что личный опыт не может служить доказательством причинно-следственных связей. Многие старшеклассники также затруднялись объяснить, почему следует проявлять осторожность, когда в качестве доказательства причинно-следственного утверждения представлен личный опыт (7).

Проверить контент на достоверность также можно путем сравнения содержания нескольких текстов — эта стратегия называется подкреплением. В идеале читатели используют несколько текстов, чтобы определить преобладающее научное понимание исследуемого вопроса (8). Когда мы изучали оценку надежности онлайн-текстов среди более трехсот учащихся старших классов, подкрепление оказалось наименее используемой стратегией оценки (9). В своих оценках студенты обращали больше всего внимания на место публикации. Если при оценке трех онлайн-текстов 89% учащихся хотя бы раз обращали внимание на место публикации, то подкрепление использовали 14%.

Оценка источника (например, автора, места публикации) особенно важна, когда читатели знают изучаемую тему мало или не знают о ней вообще ничего (10). При оценке источника читатели могут учитывать несколько характеристик, таких как компетентность, доброжелательность и этичность автора (11). Сделать выводы о компетентности автора можно, обратив внимание на его образование, профессию, должность или принадлежность к той или иной организации. Примечательно, что быстрой проверки сведений о профессиональной квалификации недостаточно. Читателям следует обращать внимание на то, обладает ли автор экспертными знаниями, особенно по теме текста. Это следует обсуждать в классе, поскольку, например, в социальных сетях эксперты в различных областях высказываются на темы, которые не входят в сферу их компетенции. В своем исследовании, в ходе которого мы изучали навыки оценки надежности текста у будущих педагогов (N = 169), мы обнаружили, что связь между компетентностью автора и темой текста учитывали только 8–20% из них (в зависимости от текста).

Помимо компетентности автора, читатели могут обратить внимание на намерения и этичность автора или издателя. Например, можно рассмотреть, есть ли у автора коммерческие или политические намерения. Читатели младшего возраста не задумываются о коммерческих намерениях, даже если они очевидны (например, на сайтах компаний). Если в задании с несколькими вариантами ответа коммерческие намерения обнаружило 63% шестиклассников (12), то в задании с открытым ответом, когда им требовалось

обосновать свою оценку надежности, в надежности коммерческого сайта усомнилось только 19% (12).

В таблице ниже я собрала примеры обоснований, которые ученики старших классов приводили для оценки надежности на основе содержания и источников. Примечательно, что обоснования могут включать в себя соображения, связанные как с источником, так и с содержанием. Так, в последнем примере учащийся выявляет коммерческие намерения (источник) и рассматривает, как они отражены в аргументации автора (содержание). Кроме того, учащийся, похоже, знает о законе, который защищает потребителей, и утверждает, что маркетинг должен также соответствовать добросовестной практике.

ОЦЕНКА СОДЕРЖАНИЯ

СРАВНЕНИЕ С ИМЕЮЩИМСЯ ПРЕДСТАВЛЕНИЕМ (Hämäläinen ym, 2021)
Текст субъективный, и у каждого свое мнение по этому вопросу.
Однако я того же мнения, что и автор этого текста.

КАЧЕСТВО ДОКАЗАТЕЛЬСТВ (Kiili ym, 2022)
Автор обосновывает свое утверждение своим наблюдением после дня рождения, не зная его событий или других факторов, которые могли повлиять на поведение дочери (блог обывателя, доказательством является единственное наблюдение).

ПОДТВЕРЖДЕНИЕ (Hämäläinen ym, 2021)
Я читал то же самое на сайте TAI (Tervise Arengu Instituut).

ОЦЕНКА ИСТОЧНИКА

КОМПЕТЕНТОСТЬ АВТОРА (Kiili ym, 2022)
Автор — доктор медицинских наук, который проводил исследование на эту тему.
Также он владеет знаниями об исследованиях и выводах других (текст, основанный на исследованиях).

НАМЕРЕНИЯ АВТОРА (Kiili ym, 2022)
Автор хочет повысить продажи компании, поэтому не говорит о сахаре в негативном ключе, хотя у него есть отрицательные эффекты.
Конечно, если информация недостоверна, у компании могут возникнуть проблемы, поэтому автор старается этого избежать. (коммерческий текст)
(*Hämäläinen et al., 2021; 2Kiili et al., 2022*)

Таблица: Примеры обоснований учащимися старших классов своих оценок надежности при чтении текстов о здоровье.

Поиск источников в ходе онлайн-расследования

Неотъемлемой частью поиска источников является оценка их надежности. Однако поиск источников — это более широкая концепция, чем их оценка. Он определяется как внимание к источникам информации, их оценка, представление и использование. Важно отметить, что поиск источников может происходить на протяжении всего онлайн-запроса и является неотъемлемой частью критического онлайн-чтения. Определяя свои информационные потребности, можно подумать, какие источники могут предоставить надежную информацию по рассматриваемой теме. Читатели могут использовать эти соображения для формулировки своих поисковых запросов, включая в них заслуживающих доверия людей, организации или профессии. Например, если читатели хотят узнать, что такое оспа обезьян и как она распространяется, они могут ограничить поиск сайтом CDC (Центры по контролю и профилактике заболеваний США), набрав в Google «monkeypox site: cdc.gov». Если конкретное место публикации неизвестно, можно также ограничить поиск профессией, например «профессор», чтобы повысить вероятность найти научную информацию об оспе обезьян.

Поиск источников также является неотъемлемой частью толкования, сравнения и синтеза нескольких онлайн-текстов. Он играет ключевую роль, особенно когда читатели исследуют спорные вопросы. А именно, умелые читатели обращают внимание на то, кто и что говорит, и это формирует связи между источником и контентом. Рассматривая, как мнения из разных источников поддерживают друг друга или противоречат друг другу, читатели формируют связи между источниками. Когда читатели пишут эссе на основе источников, поиск источников — это не просто составление их списка. В идеале письменный продукт предоставляет информацию о мнениях из различных источников и их взаимосвязи.

Наше исследование показало, что учащиеся старших классов вели поиск источников в ходе онлайн-расследования. Однако в поисковых запросах он использовался относительно скудно. Интересно, что поиск источников на ранних этапах расследования способствовал их поиску на более поздних этапах. Чем чаще учащиеся старших классов (N = 167) использовали поиск источников при определении своих информационных потребностей или формулировке поисковых запросов, тем чаще они также использовали его при вынесении суждений о надежности информации. Кроме того, чем чаще учащиеся использовали поиск источников в своих суждениях о надежности информации, тем чаще они использовали источники в своих письменных работах. Эти результаты свидетельствуют о том, что в процессе обучения следует уделять особое внимание поиску источников как непрерывному процессу, который начинается на ранних этапах.

Список литературы:

(1) Kiili, C., Räikkönen, E., Bråten, I., Strømsø, H. I., & Hagerman, M. S. Adolescent readers' online evaluation skills are made of abilities to confirm the credibility and question the credibility.

(2) Leu, D. J., Kinzer, C. K., Coiro, J., Castek, J., & Henry, L. A. (2019). New literacies: A dual level theory of the changing nature of literacy, instruction, and assessment. D. E. Alvermann, N. J. Unrau, M. Sailors, & R. B. Ruddell (toim), Theoretical models and processes of literacy (7. väljaanne, lk 319–346). Taylor & Francis.

(3) Critical. (2021). Teknologisia ja sosiaalisia innovaatioita kriittisen lukemisen tukemiseen internetin aikakaudella (CRITICAL): Tilannekuvaraportti 2021.
https://www.aka.fi/globalassets/3-stn/1-strateginen-tutkimus/strateginen-tutkimus-pahkinankuoressa/tilannekuvaraportit/stn2020-hankkeet/tilannekuvaraportti-critical.pdf

(4) Barzilai, S., Thomm, E., & Shlomi-Elooz, T. (2020). Dealing with disagreement: The roles of topic familiarity and disagreement explanation in evaluation of conflicting expert claims and sources. Learning and Instruction, 69, Article 101367.
https://doi.org/10.1016/j.learninstruc.2020.101367

(5) van Strien, J. L. H., Kammerer, Y., Brand-Gruwel, S., & Boshuizen, H. P. A. (2016). How attitude strength biases information processing and evaluation on the web. Computers in Human Behavior, 60, 245–252.
https://doi.org/10.1016/j.chb.2016.02.057

(6) Kiili, C., Bråten, I., Strømsø, H., & Räikkönen, E. (2022b). Why trust or mistrust? Sixth graders' ability to justify the credibility of online texts. Hyväksytty esitelmä. EARLI SIG2, 29.8-31.8.2022, Kiel, Saksamaa.

(7) Kiili, C., Bråten, I., Strømsø, H., Hagerman, M. S., Räikkönen, E., & Jyrkiäinen, A. (2022a). Adolescents' credibility justifications when evaluating online texts. Education and Information Technologies.
https://doi.org/10.1007/s10639-022-10907-x

(8) Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva, A., & Wineburg, S. (2022). Science education in an age of misinformation. Stanford University, Stanford, CA.

(9) Hämäläinen, E., Kiili, C., Räikkönen, E., & Marttunen, M. (2021). Students' abilities to evaluate the credibility of online texts: The role of Internet-specific epistemic justifications. Journal of Computer Assisted Learning, 37(5), 1409–1422.
https://doi.org/10.1111/jcal.12580

(10) Bråten, I., Stadtler, M., & Salmerón, L. (2018). The role of sourcing in discourse comprehension. M. F. Schober, D. N. Rapp, & M. A. Britt (toim), Routledge handbooks in linguistics. The Routledge handbook of discourse processes (lk 141–166). Routledge/Taylor & Francis.

(11) Hendriks, F., Kienhues, D., & Bromme, R. (2015). Measuring laypeople's trust in experts in a digital age: The Muenster Epistemic Trustworthiness Inventory (METI). PLoS ONE, 10(10), e0139309.
https://doi.org/10.1371/journal.pone.0139309

(12) Kiili, C., Forzani, E., Brante, E. W., Räikkönen, E., & Marttunen, M. (2021). Sourcing on the Internet: Examining the relations among different phases of online inquiry. Computers and Education Open, 2. Article 100037.
https://doi.org/10.1016/j.caeo.2021.100037

Упражнения:

1. Пожалуйста, проверьте, настоящие ли это сайты:
   www.bbc.com
   www.bbc.uk.
   www.err.portal.ee
   kroonika.ee
   kroonika.delfi.ee

2. Что могут сделать читатели, чтобы определить, достоверен ли контент? Приведите несколько советов.

. . . . . .

. . . . . .

. . . . . .

3. Какие вопросы помогают вам проверить аргументацию автора новости? Пожалуйста, укажите их

. . . . . .

. . . . . .

. . . . . .

Навыки и стратегии онлайн-чтения

Кари Кивинен

«Здоровье демократии зависит от умения людей получать доступ к надежной информации.»

Hobbs (2010); Mihailidis & Thevenin (2013).

Онлайн- и офлайновые среды

Как пишут в замечательной статье «Граждане против интернета» (1), онлайн-среды изобилуют умными, высокоадаптивными архитектурами выбора, созданными в первую очередь для максимизации коммерческих интересов, привлечения и удержания внимания пользователей, монетизации пользовательских данных, а также для прогнозирования будущих действий и влияния на них. В худшем случае это может способствовать распространению дезинформации.

Онлайн- и офлайн-среды отличаются друг от друга, что имеет важные последствия для опыта и поведения людей в сети. В онлайн-среде можно передавать сообщения миллионной аудитории, в то время как при общении лицом к лицу существуют физические ограничения на количество людей, которые могут присоединиться к разговору (2).

Объем информации, доступной каждому в цифровой среде, поражает воображение, и любую информацию можно в кратчайшие сроки без особых усилий распространить среди огромной аудитории. Онлайн-среды развиваются быстро и

Онлайн-среды часто разрабатываются, чтобы:

- максимизировать коммерческие интересы,
- привлекать и удерживать внимание пользователей,
- монетизировать пользовательские данные и
- прогнозировать будущее поведение и влиять на него.

Kozyreva et al. (2020)

постоянно, в сравнении с большинством офлайновых сред. Контент можно всё время менять, удалять и добавлять.

Козырева и др. (2020) выделили четыре типа проблем, характерных для онлайн-среды: архитектуры выбора, основанные на убеждении и манипуляции, информационные архитектуры с поддержкой ИИ, ложная и вводящая в заблуждение информация и отвлекающая среда. Когда люди получают доступ к онлайн-информации через поисковые системы, результаты поиска регулируются алгоритмами, которые корпорации разработали «в погоне за прибылью и при низком уровне прозрачности или общественного контроля». Кроме того, «в демократических странах технологические компании сконцентрировали беспрецедентные ресурсы, рыночные преимущества и контроль над данными людей и их доступом к информации» (3). Сбор данных

о пользователях в Интернете основан на высокоразвитых системах машинного обучения и алгоритмах, которые превосходят нас, людей, и не являются прозрачными. Вот почему поисковые результаты и система рекомендаций, используемых, например, в YouTube, индивидуальны и непредсказуемы.

Одним из решений этой проблемы является образование. По мнению исследователей, вмешательства, направленные на общественность как получателей и производителей информации, а именно школьные программы по цифровой информационной грамотности, научили бы школьников искать, фильтровать и оценивать данные, информацию и цифровой контент, а также управлять ими (4). По всем этим причинам традиционные навыки чтения должны быть дополнены новыми типами стратегий онлайн-оценки и навыками онлайн-чтения.

Инструментарий для онлайн-чтения

Следует отметить, что одних навыков цифровой грамотности недостаточно. Хорошее знание существа вопроса может помочь нам лучше оценивать надежность информации (5). Если вы хорошо разбираетесь в определенной теме, вас сложнее ввести в заблуждение (6). Хороший пример — понимание изменения климата. Однако общее высшее образование не обязательно поможет лучше ориентироваться в дезинформации (7).

Умение находить надежную информацию в Интернете необходимо для осознанного участия в жизни общества — это новый гражданский навык. Особенно насущной это потребность является для молодежи, которая часто обращается к Интернету, чтобы узнать о социальных и политических проблемах. Подготовка учащихся к оценке онлайн-контента, особенно если он касается социальных и политических вопросов, согласуется с более широкими усилиями по активизации гражданской миссии колледжей и университетов. Согласно недавнему исследованию (8), большинство учащихся использовали неэффективные стратегии оценки цифровой информации.

Поэтому крайне актуально и важно развивать навыки онлайн-чтения и стратегии оценки в режиме онлайн.

Подготовка к опровержению

Подготовка к опровержению (англ. *pre-bunking*) — это название процесса, при котором люди заранее предупреждены о том, что могут стать мишенью для распространения ложной информации. Навыки подготовки к опровержению можно развивать, заранее предоставляя людям фактическую и немного более подробную информацию по определенному вопросу, а затем знакомя их с существующей дезинформацией по той же теме. Также их можно заранее предупреждать о том, с дезинформацией какого рода они могут столкнуться.

Хорошая подготовка к опровержению реагирует на опасения людей, обращается к их жизненному опыту и побуждает делиться этими знаниями. Она расширяет возможности: Суть в том, чтобы построить с аудиторией доверительные отношения, а не просто исправлять факты.

Исследования показали, что логический подход имеет далекоидущие преимущества. Если вы научите людей распознавать тактики, они смогут обнаруживать их чаще, чем отдельные утверждения (9).

Существует три основных типа подготовки к опровержению:

1. на основе фактов: исправление конкретного ложного утверждения или нарратива
2. на основе логики: объяснение тактик, используемых для манипулирования
3. на основе источников: указание плохих источников информации

Развенчание

Развенчание (англ. *debunking*) происходит уже после появления ложной информации. Его цель — исправить ложную информацию и не допустить, чтобы другие поверили информации, недостоверность которой можно доказать. Для развенчания мизинформации и дезинформации могут использоваться стратегии проверки фактов.

Исправление или «опровержение» ложной информации — непростая задача, поскольку люди с большей вероятностью верят более знакомой информации, даже если позднее узнают, что она неверна (эффект обратного действия).

Исследования показывают, что при исправлении мизинформации лучше всего представлять основные факты до того, как будет представлена исправляемая мизинформация. Исправить мизинформацию недостаточно. Необходимо объяснить, почему информация неверна, и предоставить правдивый аналог или объяснение. The Debunking Handbook (10) выделяет четыре основные области развенчания мифов:

1. Основные факты: акцентируйте внимание на том, что правда, а не на том, что ложь. Исследования показывают, что при развенчании ложной информации лучше всего сначала представить основной факт, а уже потом ложную информацию, которую надо развенчать.
2. Четкие предупреждения.
3. Альтернативное объяснение: «Опровергая миф, вы создаете брешь в человеческом сознании. Чтобы иметь эффект, ваше опровержение должно заполнять этот пробел». Если вы хотите заменить неверную информацию, предоставьте четкое объяснение, которое заполнит «информационный пробел». Старайтесь объяснять всё как можно понятнее: люди могут перестать обращать внимание, если столкнутся с дублирующейся информацией. Иногда это может означать упущение некоторых нюансов при первом ознакомлении людей с исправленной информацией.
4. Графика: наглядные презентации могут помочь четче проиллюстрировать основные факты.

Поиск источников

Установлено, что поиск источников при понимании текста оказывает значительное влияние на способность учащихся определять надежность и оценивать информацию, степень влияния варьируется от небольшой до значительной (11). Чтобы быть хорошо информированным гражданином, знание, где можно найти хорошую информацию и насколько надежен источник, может быть не менее важно, чем критика источника (12). Поэтому важно рассказывать, где можно найти достоверную информацию и кому можно доверять.

Гражданское онлайн-мышление

Обучение гражданскому онлайн-мышлению (англ. *civic online reasoning*) (13) оказалось более сложной задачей. Исследователи из Стэнфорда (14)(15) предлагают, чтобы, сталкиваясь с информацией в Интернете, человек задавал себе три основных вопроса:

1. Кто стоит за информацией?
2. Каковы доказательства?
3. Что говорят другие источники?

Исследования учебных программ, направленных на развитие гражданского онлайн-мышления, оказались эффективными в обучении критике цифровых источников и латеральному чтению (16).

Также выяснилось, что обучение молодежи использованию когнитивных стратегий и цифровых инструментов для проверки информации оказывает среднее влияние на ее способность отличать надежную информацию от вводящей в заблуждение (17). С развенчанием недостоверных новостей особенно хорошо справились подростки, которые после самопроверки или обучения использовали цифровые инструменты, такие как поиск по тексту или обратный поиск изображений.

Продолжительность концентрации на отдельном тексте у любого искателя информации ограничена, а поисковые системы часто находят огромное количество ссылок. У нас нет ни времени, ни энергии на анализ всех результатов, чтобы найти важную для нас информацию. Поэтому разумно сосредоточить наше ограниченное внимание на самом важном. Для этого нам необходим навык стратегического игнорирования.

Стратегическое игнорирование

Используя мощные поисковые системы, иногда мы получаем миллионы соответствий. Как выбрать полезную и правдивую информацию, которая отвечает нашим изначальным потребностям? В ходе этого процесса мы нуждаемся в критическом мышлении человека, чтобы оценить, насколько нам подходит контент, который предлагают нам алгоритмы, — и мы игнорируем, оставляем в стороне большинство соответствий.

Уже в 1971 году, задолго до появления Интернета, Герберт Саймон (18) отметил, что перегрузка информацией приводит к дефициту внимания (19). Рекламодатели, корпорации, лоббисты, сайты с кликбейт-заголовками, теоретики заговоров, группы ненависти и насаждающие пропаганду правительства работают сверхурочно, чтобы захватить наше внимание в Интернете. Зачастую самый разумный шаг — сохранять внимание, практикуя стратегическое игнорирование. В условиях ограниченного внимания важнейшим решением становится, куда его направить.

Поэтому мы должны развивать навыки игнорирования большого объема несущественной информации. Мы должны использовать стратегическое игнорирование, чтобы избежать дезинформации и удерживать наше ограниченное внимание на контенте, который действительно стоит прочтения.

Латеральное чтение

Прежде чем читать текст, читатель проверяет на различных сайтах и в различных источниках информацию о нем (надежность автора, факты, статистику, источники и т. д.).

Одним из новых инструментов в арсенале цифровой информационной грамотности является подход латерального чтения, при котором читатель, прежде чем приступать к чтению текста, проверяет информацию в Интернете (надежность источника, факты, статистику, источники) на разных сайтах и в разных источниках.

В связи с различиями между онлайновой и офлайновой информационными средами источнику онлайн-информации необходимо уделять больше внимания. В цифровой среде традиционный подход к чтению может оказаться неэффективным. Если мы будем слишком заняты анализом незнакомой информации в сети, не проверив в первую очередь происхождение статьи, мы можем и не заметить, что весь текст основан на необъективной информации.

Wineburg & McGrew (2019) (23) наблюдали, как студенты, ученые и специалисты по проверке фактов работают с ранее неизвестной информацией в Интернете. Специалисты по проверке фактов открывали в браузере несколько вкладок и искали сведения об организации или человеке, стоящих за информацией. Только проверив, что́ говорят другие сайты, они возвращались к тексту. Используя этот подход, специалисты по проверке фактов смогли быстро проверить сайты, которые скрывали свои намерения и спонсоров. В рамках того же эксперимента студенты и ученые сосредотачивались на исходном сайте, что вызывало замешательство касательно его реального назначения или спонсора.

Стратегия, используемая профессиональными специалистами по проверке фактов, — читать новостную ленту по многим взаимосвязанным сайтам, а не углубляться в текст, — оказалась быстрым и эффективным способом избежать траты внимания, времени и энергии на необъективную информацию. Рекомендуется использовать стратегию ограничения кликов. Это означает, что надо тщательно прокручивать страницу вниз, прежде чем нажимать на ссылки в результатах поиска, которые релевантны и необязательно занимают верхние строчки, и ориентироваться на надежные источники информации (24). Чтение нескольких релевантных источников для подтверждения информации и ее помещения в более широкий контекст позволяет нам делать обоснованные выводы о надежности источника.

Онлайн-ПДД

В июле 2022 года Европейский парламент принял Закон о цифровых услугах (DSA) (25) и Закон о цифровых рынках (DMA) (26). Эти новые цифровые инструкции ЕС устанавливают беспрецедентные стандарты подотчетности интернет-компаний в условиях открытого и конкурентного цифрового рынка. Когда новые правила будут реализованы на практике, у пользователей в ЕС появится больше возможностей выбора, а их права в Интернете будут лучше защищены.

Было бы здорово, если бы крупные онлайн-платформы стали тщательнее регулировать свой контент, как предусмотрено этими законами. Но, к сожалению, мы не можем рассчитывать на доброжелательность платформ. Нам необходимо улучшать свои цифровые навыки и повышать уровень образования! Граждан надо учить развивать критическое мышление и навыки цифровой информационной грамотности.

Нам всем пригодятся простые «правила движения» онлайн. Когда я училась в школе, меня учили простым правилам дорожного движения: прежде чем переходить улицу, посмотри налево, затем — направо и снова налево. Нам нужны такие же четкие инструкции и для онлайн-среды.

Столкнувшись с незнакомым контентом, прежде чем тратить время на его более тщательное изучение, всегда стоит искать ответы на три простых ключевых вопроса:

- Кто стоит за информацией? Источник?
- Каковы доказательства?
- Что говорят другие источники?

Было бы полезно беречь наше ограниченное внимание для текстов, которые стоят прочтения!

Список литературы:

(1) Kozyreva, A., Lewandowsky, S., & Hertwig, R. (2020). Citizens Versus the Internet: Confronting Digital Challenges With Cognitive Tools. Association for Psychological Science. SAGE.

(2) Barasch, A., & Berger, J. (2014). Broadcasting and narrowcasting: How audience size affects what people share. Journal of Marketing Research, 51, 286–299. https://doi.org/10.1509/jmr.13.0238

(3) Zuboff, S. (2019). The age of surveillance capitalism: The fight for the future at the new frontier of power. Profile Book.

(4) Breakstone, J., McGrew, S., Smith, M., Ortega, T., & Wineburg, S. (2018). Teaching students to navigate the online landscape. Social Education, 82, 219–221.

(5) Lurie, E., & Mustafaraj, E. (2018, May). Investigating the Effects of Google's Search Engine Result Page in Evaluating the Credibility of Online News Sources. In Proceedings of the 10th ACM Conference on Web Science (lk 107–116).

(6) Nygren, T., & Guath, M. (2021a). Students evaluating and corroborating digital news. Scandinavian Journal of Educational Research, in press.

(7) Roozenbeek, J., van der Linden, S., & Nygren, T. (2020). Prebunking interventions based on «inoculation» theory can reduce susceptibility to misinformation across cultures. Harvard Kennedy School Misinformation Review, 1(2).

(8) Joel Breakstone, Mark Smith, Nadav Ziv & Sam Wineburg (2022). Civic Preparation for the Digital Age: How College Students Evaluate Online Sources about Social and Political Issues, The Journal of Higher Education. https://doi.org/10.1080/00221546.2022.2082783

(9) First Draft. https://firstdraftnews.org/articles/a-guide-to-prebunking-a-promising-way-to-inoculate-against-misinformation/

(10) Debunking Handbook (2020). https://www.climatechangecommunication.org/wp-content/uploads/2020/10/ DebunkingHandbook2020.pdf

(11) Brante, E. W., & Strømsø, H. I. (2018). Sourcing in Text Comprehension: a Review of Interventions Targeting Sourcing Skills. Educational Psychology Review, 30(3), 773–799. doi:10.1007/s10648-017-9421-7

(12) Haider, J., & Sundin, O. (2020). Information literacy challenges in digital culture: conflicting engagements of trust and doubt. Information, Communication & Society, 1–16. doi:10.1080/1369118X.2020.1851389

(13) Civic Online Reasoning site of Stanford University. https://cor.stanford.edu/

(14) Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' Civic Online Reasoning: A National Portrait. Educational researcher, 50(8), 505–515. doi:10.3102/0013189X211017495

(15) Wineburg, S., Breakstone, J., McGrew, S., Smith, M., and Ortega, T. (2022). Lateral Reading on the Open Internet: A District-Wide Field Study in High School Government Classes Journal of Educational Psychology (Accepted for publication).

(16) McGrew, S., & Byrne, V. L. (2020). Who Is behind this? Preparing high school students to evaluate online content. Journal of Research on Technology in Education, 1–19. doi:10.1080/15391523.2020.1795956

(17) Axelsson, C.-A. W., Guath, M., & Nygren, T. (2021). Learning How to Separate Fake From Real News: Scalable Digital Tutorials Promoting Students' Civic Online Reasoning. Future Internet, 13(3 60), 1–18.

(18) Simon, H. A. (1971). Designing organizations for an information-rich world. M. Greenberger (toim.), Computers, communications, and the public interest (lk 37–72). John Hopkins University Press.

(19) Wineburg, S., & McGrew, S. (2019). Lateral reading and the nature of expertise: Reading less and learning more when evaluating digital information. Teachers College Record, 121(11), Article 22806. https://www.tcrecord.org/content.asp?contentid=22806

(20) Breakstone, J., Smith, M., Wineburg, S., Rapaport, A., Carle, J., Garland, M., & Saavedra, A. (2021). Students' Civic Online Reasoning: A National Portrait. Educational researcher, 50(8), 505–515. doi:10.3102/0013189X211017495(22) DSA. https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment

(23) DMA. https://www.europarl.europa.eu/news/en/press-room/20220315IPR25504/deal-on-digital-markets-act-ensuring-fair-competition-and-more-choice-for-users

Упражнения:

1 Чем отличаются онлайн- и офлайн-среды?

2 Какие у вас привычки в Интернете? На кого вы подписаны, что слушаете и читаете? Пожалуйста, заполните медиа-тарелку.

3 Пожалуйста, проведите подготовку к опровержению следующей новости. 

4 Как игнорировать огромное количество неважной информации онлайн?

Заяви о своих правах! От пользователей к гражданам в онлайн-среде

Минна Аслама Горовиц

В социальных сетях мы хотим получать информацию, а еще чаще — развлекаться. Нам нравится, на первый взгляд, свободный доступ, функции и безграничная связь. Возможно, мы даже знаем, какую цену платим, отдавая свои данные, — и некоторые из нас могут сказать, что это выгодная сделка за весь контент и развлекательные функции, которые нам предоставляют именно так, как нам нравится. Однако мы реже задумываемся о том, что платформы — это мощные общественные арены, которые могут влиять на наше душевное здоровье, поощрять насилие в отношении социальных групп, влиять на результаты выборов или срывать их, а также разжигать войны.

Цифровая эпоха привела к тому, что цифровые платформы стали играть важную роль в поддержке или нарушении основных глобальных принципов прав человека. С этой точки зрения мы граждане. Наши действия сопряжены с ответственностью, а также связаны с основными правами человека. На сегодняшний день нет ни одного законодательного акта, который определял бы наши права как глобальных цифровых граждан, однако многие заинтересованные стороны участвуют в обсуждении того, как определить и защитить эти права. В этой главе рассказывается о том, как цифровые платформы, Организация Объединенных Наций, Европейский союз и гражданское общество понимают и защищают наши цифровые права.

Права человека в цифровую эпоху

Сегодня платформы и другие технологические компании влияют на столь большую часть нашей жизни и наших обществ, что они также оказывают значительное влияние на реализацию или ограничение наших основных прав. Интернет открывает нам доступ к неограниченному контенту, однако платформы также выступают в роли привратников для информации, которую рекомендует нам Google или TikTok. Мы получаем бесплатные услуги в обмен на наши данные, но зачастую не знаем, как они используются и как это влияет на нашу приватность. Мы можем легко и свободно выражать свои мысли, но при этом подвергаемся огромному количеству ложной информации, манипуляций и языка вражды. Как отмечается в докладе о цифровом сотрудничестве Генерального секретаря ООН, цифровые технологии не только помогают отстаивать, защищать и осуществлять права, но и используются для подавления, ограничения и нарушения прав человека (1).

Речь не только о военной цензуре или отключениях Интернета, которые могут происходить далеко от нашей повседневной жизни. На самом деле нам мало известно о том, как соблюдаются наши права как пользователей глобальных цифровых платформ. Организация Ranking Digital Rights следит за тем, чтобы крупные платформы и телекоммуникационные компании по всему миру сообщали нам о наших правах. Ее рейтинг Big Tech Scorecard оценивает корпорации в зависимости

от того, как они информируют нас о своих внутренних правилах и практиках (управление), как они относятся к нашей приватности и как защищают нашу свободу слова. К сожалению, эти гиганты, от Amazon и Alibaba до X и Yandex, держат нас в глубоком неведении. Если и удается найти информацию об их условиях оказания услуг и правах пользователей, ее бывает трудно понять, и в ней часто отсутствует информация по таким важным вопросам, как, например, кому они передают наши данные и соблюдают ли международные принципы в области прав человека при разработке своих алгоритмов. И даже если у такой компании, как Meta, есть политика в области прав человека, частным лицам или независимым организациям практически невозможно контролировать ее выполнение. (2)

Как относятся к нашим правам ООН и ЕС

С каждым годом ООН всё больше обеспокоена влиянием цифровизации на наш мир. Многие вопросы, с которыми мы сталкиваемся в цифровую эпоху, уже включены в самый известный и глобальный путеводитель по нашим правам — Всеобщую декларацию прав человека (ВДПЧ) ООН 1948 года. (3) Например, статья 12 предусматривает право на неприкосновенность частной жизни, а статья 19 — свободу выражения мнений.

ООН стремится решать вопросы прав человека и коммуникации в целом через свой Совет по правам человека (4), Управление Верховного комиссара ООН по правам человека (УВКПЧ) (5) и, в частности, через ежегодную встречу государств, компаний, ученых и гражданского общества под названием Форум по вопросам управления Интернетом (6). Ввиду могущества частных корпораций, от Google до TikTok, для подчёркивания правозащитной ответственности технологических компаний также используются Руководящие принципы ООН по предпринимательской деятельности в аспекте прав человека (7). Хотя ООН не создает законы, она занимает позицию по таким вопросам, как цифровая связь как право человека (8) или этические принципы для искусственного интеллекта. (9)

Еще одной важной и новаторской стороной в определении наших цифровых прав является Европейский союз. В рамках комплексного плана цифровизации Европы к 2030 году, известного как «Цифровой компас» (10), ЕС разрабатывает законы не только для поддержки своей цифровой экономики, но и для обеспечения цифровой безопасности и расширения прав и возможностей граждан. Основополагающие принципы «Компаса», включая важнейшую роль прав и участия граждан, а также борьбу с дезинформацией, изложены в Плане действий в поддержку европейской демократии. (11) В 2022 году ЕС принял Европейскую декларацию о цифровых правах и принципах — первую декларацию международной правительственной организации, ориентированную на граждан и основанную на их правах. Декларация подчеркивает важность инклюзивности, участия, выбора пользователей, безопасности и устойчивости в цифровой среде. (12)

Гражданское общество: борцы за свободу и хранители

В то время как ООН и ЕС предлагают официальные принципы, бесчисленные организации на международном и местном уровне трудятся во имя защиты наших цифровых прав. Некоторые из них, такие как Article 19, Freedom House и Human Rights Watch, являются традиционными международными борцами за права человека. Сегодня эти организации рассматривают технологии как инструмент для привлечения власти к ответственности, но при этом также указывают на проблемы, порожденные цифровизацией, включая свободу самовыражения онлайн. (13) Другие организации, такие как AccessNow и Electronic Frontier Foundation (EFF), занимаются конкретно цифровыми правами. (14)

Многие другие группы и организации специализируются на тех или иных аспектах наших цифровых прав. Например, MyData Global, некоммерческая организация, основанная в Финляндии, отстаивает наши индивидуальные права на управление собственными данными. (15) Privacy International, напротив, занимается вопросами государственного и коммерческого надзора. (16) Некоторые организации, включая JustNet Coalition, решают проблему так называемого цифрового разрыва и в глобальном масштабе работают над тем, чтобы сделать Интернет более справедливым. (17) Многие организации, включая нашу независимую службу по проверке фактов EDMO/NORDIS, специализируются на обеспечении достоверности информации и развитии у людей навыков цифровой информационной грамотности.

При небольшой поддержке...

В общем и целом, наши права зависят от нас самих. На сегодняшний день нет цифровой конституции, которая закрепляла бы наши права на глобальном уровне. Технологии развиваются с такой скоростью, что любые детально проработанные права могут устареть сразу же после их введения.

Цифровая среда может просвещать, развлекать и обучать нас. Она может помогать нам внедрять инновации, творить, зарабатывать на жизнь, общаться и менять мир к лучшему. Благодаря ее огромному потенциалу для позитивных изменений мы должны серьезно относиться к своим правам и связанным с ними обязанностям цифровых граждан. Это можно сделать с поддержкой по нескольким фронтам:

- ООН подготавливает почву, устанавливая основные принципы и проводя международный форум для обсуждения наших прав.
- ЕС предлагает поддержку в виде различных законодательных инициатив, в частности, недавнего пакета законов о цифровых услугах, который направлен в том числе и на регулирование крупнейших глобальных платформ. (18)
- Организации и группы гражданского общества, часто являющиеся первопроходцами в реагировании на проблемы и вред цифровых технологий, могут держать нас в курсе изменений различных аспектов цифровых прав.

Список литературы:

(1) Report of the Secretary-General Roadmap for Digital Cooperation
https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf

(2) Key Findings from the 2022 RDR Big Tech Scorecard
https://rankingdigitalrights.org/mini-report/key-findings-2022/

(3) Universal Declaration of Human Rights
https://www.un.org/en/about-us/universal-declaration-of-human-rights

(4) United Nations Human Rights Council
https://www.ohchr.org/en/hr-bodies/hrc/about-council

(5) Indigenous rights and energy transition
https://www.ohchr.org/en/ohchr_homepage

(6) Internet Governance Forum
https://www.intgovforum.org/en

(7) Guiding Principles on Business and Human Rights: Implementing the United Nations «Protect, Respect and Remedy» Framework
https://www.ohchr.org/en/publications/reference-publications/guiding-principles-business-and-human-rights

(8) The Case for Connectivity, the New Human Right
https://www.un.org/en/un-chronicle/case-connectivity-new-human-right

(9) Ethics of Artificial Intelligence https://en.unesco.org/artificial-intelligence/ethics

(10) Europe's Digital Decade: digital targets for 2030
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en

(11) European Democracy Action Plan: Making EU democracies stronger.
https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2250

(12) European Declaration on Digital Rights and Principles for the Digital Decade
https://ec.europa.eu/newsroom/dae/redirection/document/82703

(13) https://www.article19.org/issue/digital-rights/; https://www.hrw.org/topic/technology-and-rights ; https://freedomhouse.org/report/freedom-net

(14) https://www.accessnow.org/; https://www.eff.org/

(15) https://www.mydata.org/

(16) https://www.privacyinternational.org/

(17) https://justnetcoalition.org/

(18) The Digital Services Act package
https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Упражнения:

1 Каковы плюсы и минусы использования технологий? Пожалуйста, укажите некоторые из них

2 Что имеет в виду автор, говоря, что технологические гиганты держат нас в неведении?

3 Зайдите в настройки своего телефона, найдите приложение, которое вы чаще всего используете, и проверьте разрешения, которые вы дали. Есть ли что-то, что вы хотели бы в связи с этим изменить?

Всех форм и размеров. Разбор искажений информации онлайн

Минна Аслама Горовиц

Фальшивые новости! Пропаганда! Манипуляции! Заговор! Цифровое пространство кишит контентом, который случайно или намеренно ложен, вредоносен — или и то, и другое. Эта глава посвящена тому, как начать разбираться в различных заболеваниях и их симптомах, чтобы поддержать наше цифровое здоровье.

Узкий подход к интернет-вбросам направлен на проверку доказуемо ложной информации. Эту форму относительно легко выявить, и с ней можно бороться, нанимая специалистов по проверке фактов, сообщая о подозрительных публикациях, удаляя сфабрикованные новости и так далее. Сложнее диагностировать недуг, когда мы рассматриваем умышленные попытки искажения новостей для продвижения идеологий, запутывания аудитории, создания поляризации и распространения дезинформации с целью извлечения прибыли. Хотя многие из этих действий могут быть политически мотивированными, эти попытки могут принимать форму кликбейта и намеренной фильтрации новостей в коммерческих целях, чтобы привлечь определенную аудиторию. Этот подход сложнее изучать и проверять эмпирически. Он связан с экономическими моделями новостных рынков и различиями в качестве новостей.

Чтобы помочь нам разобраться в различных видах недостоверного контента в Интернете, Клэр Уордл и Хоссейн Дерахшан создали структуру искажения информации. Она выделяет различные типы контента в зависимости от их предназначения:

- Неправдивая информация — ложная связь или вводящий в заблуждение контент, который может быть непреднамеренным и не всегда вредоносным. К ней относятся репосты, при которых пользователи считают, что информация достоверна и должна быть обнародована во имя общего блага, даже если ее достоверность не была проверена;
- Дезинформация — намеренно ложный контекст, включая умышленно созданные теории заговора или иной контент, который в некоторых случаях может быть вредоносным;
- Злонамеренная информация — ложный контент, намеренно созданный для причинения вреда, или использование контента в злонамеренных целях.

Для публики различие между этими типами не всегда может быть очевидно, однако для тех, кто пытается устранить эти искажения, оно важно. Сегодня рамки искажения информации широко используются журналистами, органами власти и исследователями как «дорожная карта» для борьбы с ложным контентом в Интернете. Естественно, эти субъекты должны уделять первоочередное внимание действительно вредоносному контенту. С юридической точки зрения важны две вещи: намерения создателя контента, сам контент и то, насколько он недостоверен. Журналист может случайно включить в новость неточную информацию. Пропагандист же может умышленно создавать полностью сфабрикованный контент, призванный обмануть аудиторию. (2)

Схема: Типы искажений информации (2022) (1)

В свою очередь, на практике искажение информации может принимать различные формы. Например, многосторонняя группа экспертов высокого уровня (HLEG) Европейского союза (ЕС) по фальшивым новостям и онлайн-дезинформации определяет проблему практик, которые выходят далеко за рамки всего, что напоминает «новости»: автоматизированные аккаунты, сети фальшивых подписчиков, сфабрикованные или обработанные видео, целевая реклама, организованный троллинг, визуальные мемы и т. д.

Аналогично, искажение информации охватывает множество различных действий. Помимо процесса создания ложного контента, дезинформация распространяется многими способами, включая публикацию, комментирование, распространение, твиты и ретвиты.

Наконец, искажение информации возникает не на ровном месте. Это действия различных заинтересованных сторон, которые способствуют распространению или устранению вреда в сети. Онлайн-платформы и лежащие в их основе сети, протоколы и алгоритмы делают распространение недостоверной информации, дезинформации и злонамеренной информации лёгким и «вирусным». Поскольку глобальные платформы зарабатывают на данных пользователей, сдерживание распространения ложной информации не в их интересах, если она просто привлекает внимание, лайки и репосты. Кроме того, различные государственные и негосударственные политические субъекты, коммерческие структуры, граждане по отдельности или группами, а также инфраструктуры распространения и усиления (включая новостные СМИ) могут хотеть остановить ложную информацию — или же создавать и широко распространять ее. (3)

Список литературы:

(1) Wardle, C., & Derakhshan, H. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe.
https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

(2) Möller, J., Hameleers, M., & Ferreau, F. (n.d.). Types of disinformation and misinformation Various types of disinformation and their dissemination from a communication science and legal perspective.
https://www.die-medienanstalten.de/fileadmin/user_upload/die_medienanstalten/Publikationen/Weitere_Veroeffentlichungen/GVK_Sum

(3) См: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation.

Упражнения:

1 Чем отличаются неправдивая информация, дезинформация и злонамеренная информация?
Пожалуйста, соедините прилагательные и словосочетания с подходящим термином.
Ложный, вводящий в заблуждение, призванный причинить вред, заведомо неверный, враждебный, политический, распространяемый спецслужбами, вызывающий раскол, умышленный, по ошибке, вырванный из контекста, с целью опорочить, написанный с большим количеством ошибок.

2 Пожалуйста, приведите еще какие-нибудь примеры искажения информации, например создание фальшивых аккаунтов, написание гневных комментариев...

Политическая пропаганда, основанная на психологическом манипулировании

Йоонас Пёрсти

Политическая пропаганда — это широкая форма влияния, направленная на то, чтобы убедить целевую аудиторию действовать в соответствии с целями пропагандиста. Отличительной чертой пропаганды является психологическое манипулирование, как правило, с помощью дезинформации, т. е. преднамеренного распространения информации, вводящей в заблуждение. Однако спектр средств не ограничивается дезинформацией. Также может использоваться злонамеренная информация, т. е. достоверная информация, распространяемая с целью дискредитации или причинения иного ущерба какой-либо стороне. Эффективная пропаганда также опирается на частичную правду, содержание, вырванное из первоначального контекста, и сокрытие информации (1).

В основе пропаганды обычно лежит альтернативный, черно-белый, упрощенный нарратив, который, по словам философа Ханны Арендт (2), «отвечает потребностям человеческого разума лучше, чем истинная реальность». Искусный пропагандист адаптирует свои методы к ожиданиям аудитории, чтобы она не почувствовала, что ее водят за нос. Люди склонны принимать пропаганду, которая укрепляет их социальный статус и идентичность, по крайней мере в их сознании.

Пропаганда не ограничивается распространением информации, а идет рука об руку с манипулированием целевой аудиторией с помощью различных мероприятий. Это могут быть судебные дела, инсценированные или спускаемые сверху общественные движения и массовые мероприятия, акты насилия, преследование или военные угрозы. Пропаганда контрпродуктивна для демократических идеалов, поскольку стремится ограничить общественное обсуждение вариантов политики без рационального обоснования (3). Пропагандист вполне может выдавать себя за защитника свободы слова и демократии. Эти понятия часто используются в качестве символических лозунгов, в то время как на самом деле их цель — подрывать демократические институты.

Изначально «пропаганда» означала просто распространение «правильной» доктрины. Термин родился в 1622 году, когда папа Григорий XV основал в Риме «конгрегацию распространения веры», Sacra Congregatio de Propaganda Fide, в ответ на Реформацию, чтобы противостоять ее влиянию. Негативный оттенок это понятие обрело только после мировых войн XX века (4). В частности, в демократических обществах пропаганда с тех пор ассоциируется с авторитарными обществами, такими как нацистская Германия, Советский Союз, Китай или путинская Россия.

Однако пропаганда распространяется и в демократических обществах, и их свобода слова может делать их особенно уязвимыми для пропагандистского влияния. В последние годы систематическое использование пропаганды в США привело к поляризации политической обстановки

и усложнило проведение социальных реформ. Проиграв президентские выборы 2020 года, Дональд Трамп дестабилизировал политическую систему страны, распространяя нарратив об «украденных выборах». Кульминация пропагандистской кампании пришлась на 6 января 2021 года, когда сторонники Трампа ворвались в Конгресс США, а на Капитолийском холме в Вашингтоне пострадало более ста полицейских (5).

Аналогичным образом использует пропаганду президент Венгрии Виктор Орбан, чтобы заставить замолчать политическую оппозицию и подорвать демократические институты.

Государственная пропаганда также стала одной из основных форм власти в России при Владимире Путине. Путин стал президентом в результате демократических выборов 2000 года, но администрация президента РФ уже готова была использовать пропаганду для достижения своих внутренних и внешнеполитических целей. Политическая оппозиция в стране была подавлена, а критические голоса заглушены путем сосредоточения телеканалов в руках власть имущих. Позиции президента также укреплялись с помощью построения культа лидерства. Одновременно с этим путинский режим максимально расширил возможности для маневров во внешней политике, сохранив в России видимость уважения к демократическим ценностям (6).

Пропаганда — это мобилизация большого количества людей для достижения политических целей, но она не ограничена государственными субъектами: ее могут распространять политические партии, идеологические группы, лоббисты, нанятые компаниями, или гражданские активисты, объединенные в организации в социальных сетях. В целом пропаганда не способна изменить сознание людей внезапно, но может постепенно формировать отношение в желаемом направлении. Однако самый эффективный и быстрый способ — использовать уже имеющиеся предубеждения, т. е. глубоко укоренившиеся убеждения и представления о враге. Психологическое манипулирование основано на хорошем понимании предубеждений реципиентов. Пропаганда может разрабатываться на основе знаний о культуре, социологических исследований и опросов общественного мнения. Особенно полезны исторически сложившиеся культурные мифы, которые служат строительными блоками для мировоззрения и, следовательно, представляют собой готовый фундамент для пропаганды. Мифы направляют социальное воображение людей и связаны с представлениями о священном — о нации, ее истоках и традиционных ценностях (7).

Примерами таких мифов могут служить антисемитская идеология нацистской Германии, представление о России как о «третьем Риме», защищающем христианство, или о США как о защитнике свободы в мире. Пропаганда строится на противостояниях: в нацистской Германии образ воинственного героя был создан через противопоставление «низшим расам» и евреям, которые рассматривались как особые биологические типы (8).

В XXI веке Интернет и особенно социальные медиа предоставили новые инструменты для распространения пропаганды. Эмоциональные сообщения быстро распространяются в социальных сетях: контроль, как в традиционных СМИ, отсутствует, а происхождение сообщения может быть скрыто за анонимными аккаунтами.

В социальных медиа легко распространять так называемую «черную» пропаганду, когда манипулятивные сообщения рассылаются под личинами противной стороны. Например, для этого могут создаваться движения в поддержку одного вопроса или новостные сайты. Содержание ограничено только воображением: целью пропаганды может быть усиление социальной напряженности или переключение внимания общественности на неактуальные или искаженные темы. Контент «черной» пропаганды может быть полностью фальшивым или частично правдивым. Подлинный источник сообщения старается оставаться скрытым, чтобы пропаганда не обернулась против самой себя.

На первых порах цифровые услуги не регулировались, и, например, ИГИЛ мог свободно распространять свою пропаганду, разжигающую насилие, в Facebook, Twitter и YouTube (9). С тех пор цифровые платформы стали более саморегулируемыми, но их логика коммерческой выгоды по-прежнему склоняет посетителей к поляризующему и эмоциональному контенту, предоставляя широкие возможности для пропаганды. Пропаганда накладывается на все остальные информационные потоки, маркетинг и новости, а онлайн-контент носит смешанный характер (10). Усовершенствовалась и проверка фактов, но она всё еще недостаточно эффективно реагирует на информационные сбои цифровых платформ.

В эпоху Интернета Россия, например, использует в своей пропаганде модель, которую аналитический центр RAND описал как «пожарным шлангом лжи» (11). При этой модели пропагандист быстро выкладывает различные запутанные версии событий, не особо заботясь об их достоверности. Стратегия состоит в том, чтобы подорвать доверие к СМИ и демократически избранным представителям власти с помощью «альтернативных истин» и теорий заговора (12). Радикальные правые в США используют аналогичные методы. Если ничто больше не считается правдой, пропагандист может свободнее продвигать свою произвольную политику. Противоядием от такой пропаганды являются цифровая информационная грамотность и понимание техник пропаганды. Воздействие пропаганды можно ослабить, заранее раскрыв используемые методы, что снизит эффективность манипуляций и позволит общественности игнорировать пропагандистские сообщения (13).

Список литературы:

(1) Jowett, Garth, and Victoria O'Donnell. 1992. Propaganda and Persuasion. Los Angeles: Sage.

(2) Arendt, Hannah. 1958. The Origins of Totalitarianism. Cleveland: George Allen & Unwin.

(3) Stanley, Jason. 2015. How Propaganda Works. Princeton: Princeton University Press.

(4) Taylor, Philip M. 2003. Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era. Manchester: Manchester University Press.

(5) Hasen, Richard. 2022. Cheap Speech. How Disinformation Poisons Our Politics—and How to Cure It. New Haven: Yale University Press.

(6) Dawisha, Karen. 2014. Putin's Kleptocracy; Who Owns Russia? New York: Simon & Schuster.

(7) Ellul, Jacques. 1973. Propaganda: The Formation of men's attitudes. New York: Vintage Books.

(8) Klemperer, Victor. 2002. The Language of the Third Reich. London & New York: Continuum.

(9) Berger, Jessica, and J. M. Stern. 2016. Isis: The State of Terror. London: HarperCollins.

(10) Valaskivi, Katja. 2018. Beyond Fake News: Content confusion and understanding the dynamics of the contemporary media environment. Helsinki: Hybrid CoE, February. https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-5-beyond-fake-news-content-confusion-and-understanding-the-dynamics-of-the-contemporary-media-environment/.

(11) Paul, Christopher, and Miriam Matthews. 2016. The Russian «Firehose of Falsehood» Propaganda Model. Santa Monica: Rand.

(12) Lucas, Edward, and Peter Pomerantsev. 2016. Winning the Information War: Techniques and Counter Strategies to Russian Propaganda in Central and Eastern Europe. Washington: Center for Eastern European Policy.

(13) Nimmo, Ben. 2015. Anatomy of an Info-War: How Russia's Propaganda Machine Works and How to Counter It. Central European Policy Institute. https://www.stopfake.org/en/anatomy-of-an-info-war-how-russia-s-propaganda-machine-works-and-how-to-counter-it/.

Упражнения:

1 Заполните пропуски:

Пропаганда — это ....., особенно предвзятого или ..... характера, используемое для продвижения политической цели или точки зрения.

Пропаганда — это ..... информации: фактов, ..., слухов, ... или лжи — для оказания влияния ..... .

У пропагандистов есть определенная ..... или набор целей.

2 В каких сферах жизни может применяться пропаганда?

. . . . . .

. . . . . .

. . . . . .

3 Пожалуйста, приведите примеры пропаганды в социальных медиа.

. . . . . .

. . . . . .

. . . . . .

Чему мы можем научиться у специалистов по проверке фактов

Пипса Хавула

Процесс проверки фактов всегда начинается с одного и того же простого вопроса: **«Правда?»** Как только возникает любопытство, любопытство, эти утверждения начинают проверять.

Исследования показывают, что подход к новой информации на цифровых платформах, который используют специалисты по проверке фактов, — «латеральное чтение» — очень эффективен. В цифровой среде традиционное чтение и анализ текста могут быть неэффективными, поскольку, если читатель начнет анализировать неизвестную информацию в Интернете, не проверив предварительно источник статьи, он может не понять, что весь текст основан на предвзятой или совершенно недостоверной информации. В режиме латерального чтения читатель проверяет на различных сайтах и в различных источниках информацию о тексте, прежде чем читать его. Столкнувшись онлайн с неизвестной ранее информацией, специалисты по проверке фактов сразу же открывают несколько вкладок в браузере и ищут информацию об организации или человеке, который за ней стоит.

В то время как обычный читатель может тратить довольно много времени на чтение и обдумывание недостоверной информации, специалисты по проверке фактов используют так называемое стратегическое игнорирование. При беглом рассмотрении онлайн-источники, которые оказываются сомнительными и ненадежными, быстро игнорируются. Предполагается, что информацию следует считать низкокачественной, пока не доказано обратное.

В простейшем случае, когда специалист по проверке фактов встречает новую онлайн-газету (например, Daily Mail), он сразу открывает новую вкладку в браузере, вводит название газеты в поисковую систему, добавляет слово «надежность» или «предвзятость» (например, «надежность Daily Mail») и изучает результаты. Поисковая система найдёт информацию, которая поможет оценить надёжность сайта или новостной статьи. Одновременно с этим специалист по проверке фактов изучает, какие статьи публиковались в том же СМИ в прошлом, кто отвечает за издание и кто распространяет его тексты.

Латеральное чтение также эффективно при просмотре изображений и видео на платформах социальных медиа. Заинтересовавшись, специалист по проверке фактов обращается к различным источникам, чтобы выяснить, кто опубликовал утверждение, возможные мотивы и, например, где еще ранее публиковалось такое же изображение или видео. Для проверки достоверности изображений и видео существует ряд бесплатных онлайн-инструментов, которые подробнее описаны в конце этой статьи.

Методы работы, используемые специалистами по проверке фактов, стали неотъемлемой частью цифровой информационной грамотности. К счастью, этим навыкам онлайн-грамотности можно научиться и развивать их, и для развития критического отношения к источникам специалисты по проверке фактов из FaktaBaari собрали некоторые подходы, используемые ими самими и их коллегами, в частности, в этой статье. Статьи

из этого руководства дополняются учебными видеоматериалами для сайта RaRa по адресу: https://www.rara.ee/uuri/desinformatsioon/

Введение в процесс и методику проверки фактов

Проверка фактов — это процесс проверки того, соответствует ли действительности утверждение, сделанное в открытом доступе. Она помогает отличить ложные, искаженные, вводящие в заблуждение или необоснованные утверждения от надежной, правдивой информации.

По данным репортерской лаборатории при Университете Дьюка, в настоящее время проверку фактов ведет около 400 команд следователей и журналистов в 105 странах мира. В Европе существует более 110 служб по проверке фактов. Некоторые из них работают совершенно независимо, некоторые — при традиционных новостных медиа, а некоторые, например, при аналитических центрах.

Проверка фактов необходима, поскольку ложная или вводящая в заблуждение информация может отрицательно воздействовать на мнение людей и влиять на их действия. По данным Евробарометра, 83% европейцев считают фальшивые новости и дезинформацию угрозой для демократии. Мир увидел, как дезинформация может влиять на выборы, подрывать доверие к институтам и к свободе слова или даже снижать готовность вакцинироваться. Проверка утверждений с помощью достоверной информации из надежных источников — один из эффективных способов борьбы с недостоверной информацией.

Однако важно помнить, что толкование утверждений не всегда однозначно и что факты также могут быть истолкованы по-разному. По этой причине проверка фактов стремится быть максимально прозрачной при указании источника информации, чтобы читатель мог самостоятельно оценить надежность источников и сформировать по вопросу собственное мнение.

Проверка точности изображений и видео

Переходя по сайтам, часто сталкиваешься с изображениями и видеороликами, которые вызывают вопросы. Их редактировали? Где и когда это было снято? Что на самом деле происходит на видео или изображении?

Проверить подлинность изображения или видео не всегда легко, а иногда может казаться и вовсе невозможным. Однако технологии постоянно развиваются, и в то время как редактировать изображения и видео становится всё проще, совершенствуется и технология проверки их точности. Любой желающий может воспользоваться бесплатными онлайн-инструментами для проверки фактов, которые специалисты используют в своей повседневной работе.

Важно помнить, что видео или изображение не всегда может быть отредактировано — материал может быть вполне аутентичен, однако представлен в неверном контексте.

Фотографии

Обратный поиск изображений. Обратный поиск изображений, который позволяют осуществлять различные сервисы, часто является лучшим способом для проверки фотографий. Проводя его, можно загрузить рассматриваемое изображение или ссылку на него, что позволяет поисковой системе найти похожие изображения. С его помощью можно, например, узнать, где и когда была сделана та или иная фотография, где еще ранее публиковались такие же снимки или даже что за человек или здание там запечатлены. При поиске первоисточника стоит смотреть на разрешение изображений: обычно изображение с самым высоким разрешением приводит к оригинальному месту публикации.

Простейший способ провести обратный поиск изображений — воспользоваться Google Объективом. Щелкните по изображению правой кнопкой и выберите «Поиск с Google Объективом».

При обратном поиске изображений в Google можно указать период, за который вы ищете изображения. Google всегда добавляет после поиска изображений ключевое слово, и вы должны попробовать изменить его, чтобы изменить результаты поиска. Bing распознает текст на изображении и сортирует изображения по размеру, а Tineye позволяет расположить их в хронологическом порядке.

Проблема с обратным поиском изображений заключается в том, что системы обычно не находят изображения, опубликованные, например, в Instagram.

Метаданные изображения. Изображения хранят широкий спектр метаданных, которые можно просмотреть на таких сайтах, как Fotoforensics (Fotoforensics.com). Метаданные могут включать в себя дату и время съемки. Если изображение оригинальное, то оно, вероятно, будет содержать информацию о модели камеры или телефона, с помощью которого был сделан снимок. Иногда, хотя и редко, метаданные также включают в себя GPS-координаты места, где он был сделан.

Небольшие подсказки. Стоит обращать внимание на мелкие детали и подсказки на изображении. Например, есть ли там дорожные и номерные знаки, флаги, погодные условия, узнаваемое здание или достопримечательность? Или вы можете сделать какой-нибудь вывод по тому, как одеты люди на фото?

Если на изображении достаточно четко виден знак на иностранном языке, можно загрузить изображение знака в Google Translate, который переведет его текст. Погодные условия в определенный день в определенном месте можно посмотреть на сайте Wolfram Alpha (wolframalpha.com). Различные картографические сервисы, такие как Google Street view, Mapillary.com и Map.snapchat.com, а также спутниковые снимки помогут найти точное место, где была сделана фотография.

Видео

Многие из описанных выше методов эффективны и при просмотре видео: поиск мелких подсказок, обратный поиск изображений и метаданные часто помогают выйти на верный путь.

Обратный поиск изображений. Обратный поиск изображений можно выполнять и для видео, сделав скриншоты и загрузив их в обратный поиск изображений. Расширение InVid поможет вести обратный поиск нескольких изображений в разных частях видео одновременно. Инструмент InVid также позволяет просматривать метаданные видео, такие как дату съемки.

Смотрите и слушайте. В дипфейковых видео используется обработка изображения, чтобы создать впечатление, что человек говорит или делает то, чего он на самом деле не говорил и не делал.

Чаще, чем дипфейк, в сфабрикованных видео встречается то, что подлинное видео, например, обрезается вводящим в заблуждение способом, создавая искаженное представление о том, что говорит человек. Редактирование может быть очень тонким и искусным, из-за чего его сложнее обнаружить.

Оригинальное видео можно найти с помощью обратного поиска изображений или поисковой системы. Есть и другие способы. Внимательно посмотрев видео, прослушав звук и обнаружив странные переходы, можно отследить манипуляции при монтаже. На сайте watchframebyframe.com можно указать ссылку на видео, опубликованное на YouTube или Vimeo, и просмотреть каждый кадр в замедленном режиме, чтобы легче было заметить неожиданный скачок.

Перевод видео на иностранный язык. Один из способов распространения недостоверной информации — неправильное наложение субтитров и помещение видео на иностранном языке в совершенно ложный контекст. Если видео, например, на русском языке, а реципиент на этом языке не говорит, легко использовать недостоверные субтитры или вымышленный контекст, чтобы сделать заявления, которые не соответствуют действительности.

Однако видео можно перевести на ваш язык. Всё, что вам нужно, — это два разных устройства, например смартфон и ноутбук. На смартфон загружено приложение Google Translate, которое распознает и переводит речь. На втором устройстве воспроизводится видео и аудио, а Google Translate на телефоне прослушивает речь и переводит ее на желаемый язык. Автоматизированный перевод не идеален, но с помощью этого метода можно понять контекст видео или приблизительный смысл речи.

Упражнения:

1 Как работает латеральное чтение?

2 Что вы сделаете, увидив незнакомый / новый источник информации?

3 Назовите сайты и инструменты для проверки фото на достоверность

4 Откройте сайт err.ee и проверьте фотографию последней новости с помощью Google lense.

Как оценить научное утверждение и профессиональное заключение эксперта?

Кари Кивинен

Важно понимать, что в сети циркулируют все виды контента. Помимо верной и полезной информации, существует большое количество недостоверной (неверная информация, распространяемая по доброй воле или по ошибке) и сфабрикованной (дезинформация, т. е. неверная или неточная информация, распространяемая умышленно). Распространение неверной или сфабрикованной информации часто вредит и человеку, и сообществу. Поэтому полезно выявлять, кто стоит за информацией, и проверять ее в нескольких источниках, чтобы понять точку зрения и возможную предвзятость источника.

Мы то и дело должны оценивать надежность научных новостей, которые находим в социальных медиа. Например, существуют ли научные доказательства пользы от ношения масок? Можем ли мы остановить изменение климата? Безопасна ли ядерная энергия и является ли она устойчивым вариантом? Современная наука настолько узкоспециализирована, что ни один человек не может освоить все области и дисциплины. Поэтому мы зависим от экспертов и должны оценивать, на чьи знания можно положиться — особенно если мнения экспертов несколько противоречивы.

В последние два года все мы сталкивались с искаженными утверждениями о пандемии Covid-19, которые пришлось исправлять специалистам по проверке фактов по всему миру. Совместными усилиями специалистов было проверено более 17 000 заявлений о Covid-19 (1).

Некоторые из этих заявлений основаны на, казалось бы, научных исследованиях и мнениях экспертов. Поэтому важно задуматься о том, как выработать здоровый критический подход к научным утверждениям и как определить истинного эксперта.

Дезинформация часто облекается в форму надежного псевдонаучного утверждения. Продукты могут рекламироваться с помощью вводящих в заблуждение или несуществующих ссылок на различные исследования. В социальных сетях распространяются статьи сомнительного научного качества.

Как оценивать компетентность экспертов?

Выбирая юриста, сантехника, стоматолога или архитектора, мы ищем рекомендации и подтверждения его профессиональных навыков и квалификации. Но как оценить компетентность и авторитет ученого — является ли он известным и уважаемым экспертом в своей области и каковы доказательства его компетентности?

Критерии компетентности ученого схожи с критериями для других экспертов. Важно выяснить (1):

- Каков его профессиональный опыт и, в частности, список публикаций в этой области?

- Имеет ли он авторитет в своей области? Например, состоит ли он в признанной научной организации, получал ли награды за свою научную работу? У каждой профессиональной группы есть наблюдатели, советы и органы сертификации, которые следят за своими членами, чтобы убедиться, что они соответствуют стандартам профессии и имеют право вести практику.
- Какова у него квалификация? Это докторская степень в данной области? Или у него есть другой релевантный опыт, помимо официальных дипломов?
- Где он работает? Это признанная научная организация или исследовательское учреждение?
- Есть ли доказательства возможной предвзятости или денежной заинтересованности?

Чтобы стать ученым, требуется учиться много лет, а зачастую и защитить докторскую диссертацию. Даже докторская степень охватывает лишь узкую область знаний. Стать профессионалом также можно в ходе научного профессионального обучения или практического опыта работы.

«Просто быть практикующим ученым, однако, недостаточно. Человек должен быть практикующим ученым в соответствующей области. Нобелевская премия в одной сфере не делает вас экспертом в других. Тем не менее люди могут с легкостью объединять всех ученых в однообразную группу «авторитетов». Специалист по радиологии — не тот, к кому вы обратитесь за советом по вирусам. Научная степень в одной сфере не делает вас экспертом во всех областях науки. Космолог-теоретик знает об экологии не больше, чем любой другой компетентный сторонний наблюдатель».

В социальных медиа появлялись комментарии различных экспертов по поводу российского вторжения в Украину. По их заявлениям часто легко понять, какую сторону они представляют. Поэтому во времена конфликта необходимо относиться к различным новостным сообщениям и мнениям экспертов осторожнее и осмотрительнее, чем обычно. Важно выяснять, кто и что представляет, на каких доказательствах основана информация и каков реальный опыт человека, делающего заявление, в рассматриваемом вопросе.

Как оценить научное утверждение?

Научная информация должна пройти через ряд процессов, которые обеспечат ее надежность. Открытость, критические дискуссии и экспертная оценка способствуют развитию исследований. Наука исправляет сама себя. Толкования данных исследований меняются и уточняются по мере появления новых знаний. Исследования опираются на знания, накопленные за десятилетия, а то и за века.

Научное знание — это наше лучшее понимание мира на сегодняшний день. Это не чье-то мнение или личный опыт, а результат систематического процесса. Оно может меняться по мере получения новых результатов исследований и развития понимания. Вот почему научные исследования стоят больше, чем мнения!

Дерево решений для оценки научной информации

Доказательства надежности:

- нет конфликта интересов?
- нет идеологической предвзятости?
- политическая нейтральность?
- источник признаваем?

Доказательства компетентности:

- профессиональный опыт?
- репутация среди коллег?
- квалификация или опыт?
- институциональный контекст?

Запросите объяснения, задайте вопросы о характере доказательств или степени уверенности

Исследуйте неопределенность:

- в чем суть разногласий / в чем эксперты согласны?
- что думают авторитетные эксперты?
- какой диапазон выводов считается правдоподобным?
- каков риск ошибиться?

Источник: Osborne, J., Pimentel, D., Alberts, B., Alkhim, D., Barzilai, S., Bergstrom C., Coffey J., Donovan B., Dorph R., Kivinen K., Kozyra A., Perkins K., Pettifor M. Wineburg S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford CA.

Схема: Схематичный обзор подхода, который, на наш взгляд, необходимо использовать для оценки научных утверждений в Интернете (2).

Столкнувшись с научно обоснованным утверждением, стоит выяснить, нет ли у человека/организации, делающих его, конфликта интересов. Стоят ли на кону экономические, религиозные или политические интересы? Если да, то это может быть формой платной рекламы, и к результатам следует отнестись с подозрением. Например, табачная промышленность и компании, добывающие ископаемое топливо, используют штатных экспертов для распространения информации, которая им выгодна.

Если конфликта интересов нет, стоит задать следующие вопросы:

- Обладает ли человек/организация соответствующим опытом?
- Каков авторитет автора в научном сообществе?
- Хорошая ли у него репутация?
- Есть ли у автора надлежащие дипломы или иной соответствующий опыт?
- Существует ли среди экспертов твердый научный консенсус? Если нет, то что думает большинство ученых?
- Насколько научное сообщество уверено в этих утверждениях?
- Проверялись ли эти выводы аналогичными экспертами и в какой степени?

Также стоит задуматься о возможных преимуществах и рисках. Например, в период коронавируса нам пришлось самим выбирать, следовать ли рекомендациям экспертов — например, насчет вакцинации от COVID-19, ношения масок, соблюдения сроков карантина и надежности домашних тестов.

У специалистов по проверке фактов в разных странах есть интересные сайты, где можно узнать, как они проверяют точность различных утверждений, подлинность и оригинальность изображений и видео. Сообщество по проверке фактов EDMO (Европейская обсерватория цифровых медиа) ведет обновленный список надежных европейских организаций, занимающихся проверкой фактов. В Эстонии можно обратиться к материалам Eesti Ekspress Valeinfo: paljastatud, а также Propastop и Общества дебатов Эстонии (Eesti Väitlusselts).

Список литературы:

(1) CoronaVirusFacts Alliance, Poynter,
https://www.poynter.org/coronavirusfactsalliance/

(2) Osborne, J., Pimentel, D., Alberts, B., Allchin, D., Barzilai, S., Bergstrom, C., Coffey, J., Donovan, B., Kivinen, K., Kozyreva, A., & Wineburg, S. (2022). Science Education in an Age of Misinformation. Stanford University, Stanford, CA
https://sciedandmisinfo.stanford.edu/

Упражнения:

1 Какие заявления, которые вы замечали в последнее время, оказались недостоверными?

2 Пожалуйста, проверьте, какое образование и опыт Райнера Сакса и Сергея Метлева позволяют им считаться лидерами мнений.

3 Пожалуйста, еще раз взгляните на дерево принятия решений и запишите шаги, которые вы уже использовали и которые планируете использовать в дальнейшем.

Осознанность при использовании алгоритмов — вызовы, созданные искусственным интеллектом

Харто Пёнкя

Сегодня понятие алгоритмов в основном ассоциируется с программированием и функциональными возможностями веб-сервисов и приложений. Изначально алгоритм, однако, является математическим понятием. В целом оно всё еще означает то же самое: это серия шагов для решения проблемы или задачи.

Обычно считается, что алгоритмы работают автоматически, но изначально они были ручными, то есть выполнялись людьми. Например, в начальной школе учат решать уравнения путем умножения на целое число или деления. Аналогично, рецепты в кулинарной книге — это алгоритмы приготовления вкусных блюд из определенных ингредиентов с соблюдением определенных шагов.

Для алгоритма характерно то, что он использует вводную информацию, такую как стартовые элементы или данные, для получения желаемого результата. Желаемый результат определяет создатель алгоритма. В программировании это обозначается понятиями ввода и вывода, между которыми происходит фактическое выполнение программы

Алгоритмы компьютерных программ

Наиболее распространенными алгоритмами, используемыми компьютерами, являются, например, различные форматы файлов, используемые для хранения и сжатия изображений, звуков и видео. Так, цифровую фотографию можно сжать до небольшой части ее исходного размера с помощью алгоритма сжатия JPEG. Алгоритмы также используются в ходе онлайн-трансляции зрителям или при выдаче интернет-серверами определенного сайта пользователю, набравшему его адрес в браузере.

Иногда выходные данные, а также способы и результаты работы алгоритмов очень сложны. Сложность обычно связана с тем, что входные данные используемые алгоритмом, состоят из большого количества ранее собранных данных, либо для выполнения одной задачи используется большое количество различных переменных или точек данных.

Например, погоду в конкретном регионе можно предсказать с помощью ранее собранных данных, таких как температура, осадки, ветер, атмосферное давление и статистических моделей, основанных на наблюдениях. Однако современные модели прогнозирования погоды основаны на виртуальном моделировании прогнозируемой территории, которое имитирует реальные атмосферные явления. Алгоритмы, использующие такое моделирование, основаны на зеркальном отражении реального мира.

Цифровые двойники и системы рекомендаций

Когда алгоритмы используются, чтобы прогнозировать поведение человека и влиять на него, иногда это называют цифровым двойником. Это набор данных, собранных о человеке и его деятельности, а также сочетание данных из различных источников. Например, рекламные сети в Интернете и алгоритмы рекомендаций, используемые в системах потоковой передачи контента в социальных сетях, нацелены на предоставление каждому пользователю наиболее подходящего варианта на основе имеющихся данных.

Системы рекомендаций объединяют данные, собранные о пользователях и о том, что им рекомендуется. Самая известная из них — поисковая система Google. Изначально поиск Google основывался на алгоритме PageRank, суть которого в том, что ценность каждого сайта определяется тем, сколько других сайтов ссылаются на него. В то же время на значение PageRank влияют значения PageRank самих ссылающихся сайтов, а также соответствие тематики целевой странице ссылок.

Сейчас PageRank всего лишь один из многих алгоритмов, используемых при поиске Google. С 2004 года на результаты поиска Google влияют данные, собранные у пользователей, чтобы персонализировать результаты поиска, т. е. рекомендовать разным пользователям разные веб-сайты. К 2010 году компания Google сообщила, что использует для персонализации результатов поиска более 250 различных переменных.

Сегодня на результаты поиска Google влияют, в частности, возраст, гендер, семейное положение, профессия, хобби, местоположение, онлайн-покупки, путешествия, интересы и онлайн-история пользователя. Алгоритмы рекомендаций Google не ограничиваются результатами поиска, а в основном используются в рекламной системе Google для выбора подходящих пользователям объявлений. Для многих станет сюрпризом то, что алгоритмы рекомендаций подбирают и новости, которые видят пользователи, например, в режиме просмотра новостей на Android.

Алгоритмы ИИ

Когда алгоритм использует машинное обучение или другие технологии искусственного интеллекта, он называется алгоритмом искусственного интеллекта (ИИ). Машинное обучение означает, что алгоритм не выдает каждый раз один и тот же результат, а, постоянно собирая новые данные, раз за разом улучшает свои результаты.

Самым известным примером обучающегося рекомендательного алгоритма, вероятно, является алгоритм YouTube, который предлагает пользователям, какие видеоролики посмотреть следующими. На предложения YouTube влияют просмотренные ранее видео и другие данные, собранные Google, а также данные, связанные с потенциальными предлагаемыми видео, такие как их тематика и среднее фактическое время просмотра. Однако вместо того, чтобы предлагать только новые видео, связанные с темами просмотренных ранее, алгоритм YouTube также предлагает видео по темам и каналы, которые пользователь еще не смотрел.

Для алгоритма искусственного интеллекта YouTube каждое предложение видео — это как пробный шар, брошенный пользователю, из которого алгоритм пытается извлечь новую информацию: в данном случае — видео на какие темы интересны пользователю, а на какие нет. Похожий тип сбора данных используется рядом социальных медиасервисов, таких как Facebook, Instagram, Twitter и Spotify.

Несмотря на усилия по разработке алгоритмов, учитывающих широкий спектр интересов пользователя, активность пользователей всё равно приводит к тому, что алгоритмы дают однобокие рекомендации по узким темам. Например, если вы неоднократно нажимаете на посты в Facebook и Instagram на одну и ту же тему, вы будете видеть всё больше и больше подобного контента. Это называется предвзятостью алгоритмов.

В алгоритмах ИИ предвзятость также может быть вызвана обучающими материалами, изначально использованными в машинном обучении.

Например, раньше алгоритм Google Переводчика нередко переводил личное местоимение «он» или «она» в зависимости от профессии.

Google даже обвинили из-за этого в дискриминации, хотя дело было в типе материалов, которые были доступны для обучения ИИ. Сегодня Переводчик Google предлагает в таких случаях два варианта.

Алгоритмы и эмоции Facebook

Из всех социальных медиа Facebook приложил больше всего усилий, чтобы использовать эмоции пользователей в алгоритме своей новостной ленты. Возможность «лайкать» публикации стала частью функционала Facebook практически с момента создания сервиса. Полностью эмоции взяли в оборот в 2016 году, когда Facebook внедрил эмодзи-реакции «любовь», «ха-ха», «ух ты», «печаль» и «гнев».

Перед их внедрением Facebook провел практический эксперимент, чтобы посмотреть, как различные публикации влияют на действия и эмоции пользователей. Исследование показало, что позитивные публикации вызывают положительные эмоции, а негативные — отрицательные. Используя данные, собранные с помощью эмодзи-реакций, алгоритм Facebook мог подбирать посты для новостных лент пользователей в зависимости от их эмоционального состояния. Например, если пользователь часто нажимал на реакцию «ух ты», он мог видеть больше постов, получивших много таких реакций.

С 2017 года значение эмодзи-реакций в алгоритме рекомендаций новостной ленты было увеличено до пяти обычных лайков. Компании и другие лица, изучающие алгоритм, вскоре обнаружили, что, публикуя посты, которые вызывают сильные эмоции, в результате работы алгоритма они поднимаются на верхние позиции в новостных лентах пользователей. Такая деятельность, использующая поведение людей и алгоритмы социальных медиасервисов, называется оптимизацией социальных сетей.

Особенно эффективной эмоцией в Facebook оказалось выражение негодования и гнева. При более чем двух миллиардах пользователей изменения алгоритма играют важную роль: с одной стороны, они контролируют тип публикаций, которые видят пользователи, а с другой — тип публикаций, сделанных инфлюэнсерами. Поэтому, когда алгоритм, похоже, стал вознаграждать за подстрекательство к гневу, многие авторы постов начали действовать соответствующим образом.

Большой объем «контента вражды» — одна из причин, почему Facebook уже много лет широко подвергается критике. Вскоре Facebook снизил значение эмодзи гнева в своем алгоритме: сначала до четырех лайков в 2018 году, до полутора лайков в 2020 году и, наконец, до нуля лайков в 2021 году после того, как тысячи документов, слитых бывшей сотрудницей Facebook Фрэнсис Хауген, раскрыли вышеупомянутую информацию.

Не слишком ли много власти у алгоритмов?

Появившиеся данные об алгоритмах Facebook вызвали дискуссию о том, не слишком ли большую власть имеют алгоритмы над пользователями онлайн-сервисов. Факт в том, что алгоритмы действительно влияют на поведение своих пользователей. Чаще всего это влияние проявляется в контенте, который им рекомендуется.

В то же время возникает справедливый вопрос, всегда ли авторы алгоритмов могут контролировать их работу. Алгоритмы ИИ, в частности, иногда дают результаты, которые сложно предсказать.

Алгоритмы Facebook очень сложны: компания может похвастаться тем, что использует более 10 000 точек данных, чтобы выбирать, что показывать каждому пользователю. При таком количестве различных факторов, влияющих на то, что видят пользователи, управлять всем этим нелегко.

Показательно, что в то время как алгоритм новостной ленты Facebook непропорционально сильно продвигал некоторые посты, содержавшие, например, дезинформацию, язык вражды и кликбейт, собственные модераторы компании стремились отсеять те же типы контента. Однако у Facebook не хватало модераторов, чтобы удалять все вредные посты, которые алгоритм поднимал в верхнюю часть новостной ленты.

Надо ли публиковать алгоритмы?

Часто можно услышать требование, чтобы такие онлайн-гиганты, как Google, Facebook и Twitter, публиковали принципы, лежащие в основе их алгоритмов. Эти претензии в основном касаются предполагаемой вредоносности алгоритмов (например, их попыток максимизировать время, которое пользователи проводят в соцсетях), а также проблем алгоритмов с предотвращением распространения сообщений, которые содержат неверную информацию и создают враждебность.

Бизнес онлайн-сервисов и социальных медиа обычно основан на монетизации рекламы, т. е. на том, чтобы пользователи кликали по таргетированной на них рекламе. Этому, конечно, способствует необходимость обеспечить, чтобы люди находились там как можно дольше. Таким образом, очевидно, что алгоритмы настроены именно на это, даже если сами сервисы в этом не признаются. С другой стороны, многие исследования показывают, что длительное использование Интернета и социальных сетей не способствует благополучию пользователей. При работе алгоритмов интересы компаний, управляющих сервисами, и пользователей не совпадают.

Онлайн-гиганты публикуют информацию об алгоритмах неохотно, ссылаясь на коммерческую тайну и на то, что публикация алгоритмов приведет к росту злоупотребления и манипулирования ими со стороны авторов публикаций и других инфлюэнсеров. Этот аргумент оправдан, поскольку за разработкой и использованием алгоритмов идет постоянная гонка. С другой стороны, можно возразить, что именно интернет-гиганты обязаны разрабатывать алгоритмы, которые будут достаточно хороши, чтобы обнаруживать и пресекать попытки манипуляции.

В дебатах об открытости алгоритмов часто забывают, что некоторые принципы их работы уже опубликованы. Google, например, предоставляет полное и вместе с тем обобщенное описание факторов, влияющих на результаты работы его поисковой системы. Google также опубликовал в Интернете для всех желающих почти 200-страничное руководство, предназначенное для использования его собственными специалистами по оценке результатов поиска. Кроме того, он выпустил ряд инструментов для разработчиков сайтов, которые позволяют тестировать и улучшать производительность сайтов, а заодно и свой рейтинг в результатах поиска Google. Google можно назвать хорошим примером прозрачности алгоритмов. С другой стороны, у нас нет возможности узнать, о чем он умалчивает.

Вряд ли большинство пользователей онлайн-сервисов будут читать сотни страниц документов с подробным описанием работы алгоритмов. Однако в принципе это важный вопрос. Если бы принципы работы алгоритмов были опубликованы, это повысило бы осведомленность, пролило свет на механизмы, которые до сих пор были скрыты, и исследователи смогли бы изучить их гораздо глубже. С точки зрения приватности пользователей важнее всего знать, каким образом в алгоритмах используются их персональные данные. Поэтому в настоящее время разрабатываются новые законодательные пакеты ЕС, которые требуют от поставщиков онлайн-данных большей прозрачности касательно работы алгоритмов.

Список литературы:

Google, 2022, Автоматический подбор и ранжирование результатов, https://www.google.com/intl/ru/search/howsearchworks/how-search-works/ranking-results/

Google, 28.7.2022, Search Quality Evaluator Guidelines, https://static.googleusercontent.com/media/guidelines.raterhub.com/fi//searchqualityevaluatorguidelines.pdf

Pönkä, H., 31.10.2021, Infografiikka: Facebookin viha-reaktio ja algoritmin muutokset, https://harto.worpress.com/2021/10/31/infografiikka-facebookin-viha-reaktio-ja-algoritmin-muutokset/

The Washington Post, 26.10.2021, A whistleblower's power: Key takeaways from the Facebook Papers, https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/

Wikipedia, 2022a, Luettelo algoritmeista, https://fi.wikipedia.org/wiki/Luettelo_algoritmeista

Wikipedia, 2022b, Tekoäly, https://fi.wikipedia.org/wiki/Teko%C3%A4ly

Wired, 22.2.2010, Exclusive: How Google's Algorithm Rules the Web, https://web.archive.org/web/20110612022158/http://www.wired.com/magazine/2010/02/ff_google_algorithm/2

Yle, 19.12.2016, Näin sinua ohjataan Facebookissa ja internetissä, https://yle.fi/aihe/artikkeli/2016/12/19/nain-sinua-ohjataan-facebookissa-ja-internetissa

Yle, 12.2.2020, Hölkkääjä päätyy ultrajuoksuvideoihin ja kasvisruuan ystävä vegaanisisältöihin – Youtuben algoritmin tehtävänä on katsojan koukuttaminen, https://yle.fi/aihe/artikkeli/2020/02/12/algoritmin-tehtavana-ei-ole-totuuden-etsiminen-vaan-ihmisten-pitaminen-sivuilla

Упражнения:

1 Пожалуйста, приведите примеры использования алгоритмов

2 Каковы плюсы и минусы цифрового двойника?

3 Придумайте креативный способ запутать алгоритмы социальных сетей, чтобы вы получали в своей ленте разные новости, а не только однобокие, которые рекомендует алгоритм.

Цифровой след и приватность в онлайн-сервисах

Харто Пёнкя

Приватность — одно из важнейших фундаментальных прав в цифровую эпоху. Она основана, с одной стороны, на национальных законах и нормативных актах Европейского союза, таких как Общий регламент ЕС по защите данных (GDPR), а с другой — на международных договорах и Декларации прав человека ООН.

Приватность — это прежде всего защита частной жизни, дома и коммуникаций, но в цифровой среде уместнее говорить об информации, связанной с конкретным человеком, то есть о персональных данных. Это данные, которые хранятся на цифровых устройствах и в сервисах, которыми мы пользуемся, например в поисковых системах и на платформах социальных медиа. Такие данные называются цифровым следом.

Чтобы быть полностью информированным участником цифровой среды и уметь управлять своей приватностью там, необходимо знать, как различные устройства и сервисы собирают информацию о пользователях. Также важно знать о проблемах приватности других пользователей, чтобы ненароком не нарушить их приватность в цифровой среде.

Цифровой след можно разделить на активный и пассивный. Активный цифровой след — это информация, которую пользователь сознательно добавил или иным образом создал в Интернете. Пассивный цифровой след — это данные, собираемые сервисами без ведома пользователя.

Провести различие между активным и пассивным цифровым следом нелегко, поскольку осведомленность о сборе данных зависит от осведомленности пользователя. Однако это полезное различие, которое иллюстрирует, что зачастую онлайн-гиганты и глобальные социальные медиа собирают данные без ведома пользователей или так, что для осознания этого требуются специальные навыки цифровой информационной грамотности. Таким образом, цель этой главы — представить основной обзор наиболее распространенных методов и техник сбора данных.

Кому безопасно передавать свою информацию?

Онлайн-сервисы и приложения обычно требуют создания идентификатора пользователя, т. е. регистрации. Прежде чем создавать новый аккаунт и предоставлять свои личные данные, стоит убедиться, что компания, которая управляет сервисом или приложением, заслуживает доверия, а предоставляемая вами информация будет в безопасности. Это можно оценить, изучив дополнительную информацию и отзывы других пользователей.

Существует несколько приложений и игр с обманчивыми названиями, которые были созданы на основе популярных приложений и игр. Эти поддельные приложения созданы с единственной целью — выведать личные данные пользователей. Поэтому стоит убедиться в добросовестности автора приложения и ознакомиться с опытом других пользователей. Также рекомендуется устанавливать приложения только из официальных магазинов приложений. В худшем случае загружаемые приложения могут содержать вредоносные программы и вирусы, способные похитить информацию.

При регистрации под своим настоящим именем не стоит указывать никакой информации, кроме обязательной. Вы также можете подумать, стоит ли сообщать онлайн-сервисам настоящую дату рождения или свое имя. Если в условиях пользования явно не прописано, что эту информацию необходимо предоставлять, не будет неправильным предоставить вымышленную информацию. Формы регистрации могут быть специально разработаны так, чтобы заставить пользователя предоставить как можно больше информации о себе, даже если она не требуется для использования сервиса.

Любая уникальная информация, такая как имя, номер телефона, адрес электронной почты и домашний адрес, может быть использована для поиска информации в других источниках. Советуем использовать для регистрации запасной адрес электронной почты.

Во многих онлайн-сервисах, таких как Google, Facebook и Apple, можно зарегистрироваться, используя имеющийся пользовательский аккаунт. Это также уникальные идентификаторы, которые обычно позволяют объединять информацию из других источников. Если поставщик услуг кажется неблагонадежным, лучше перестраховаться, чем потом жалеть.

Использование онлайн-сервисов и приложений часто приводит к появлению личного и релевантного контента. Данные о нас накапливает каждый пост, лайк или комментарий. Кроме того, социальные медиасервисы, в частности, позволяют нам общаться с другими пользователями. В результате учетные записи пользователей часто становятся мишенью для мошенников и других киберпреступников. При входе в систему всегда стоит использовать двухфакторную аутентификацию: это обеспечит надежную защиту от попыток взлома.

Как работают файлы cookie?

Онлайн-сервисы и приложения могут сохранять на устройствах пользователей файлы cookie, т. е. файлы, содержащие информацию, которую можно использовать для отслеживания пользователей. Информация об использовании и сроках хранения файлов cookie всегда должна быть указана в сервисе. Перед использованием файлов cookie, которые не являются необходимыми для функционирования сервиса, необходимо получать согласие пользователя.

Примерами обязательных файлов cookie являются файлы, используемые для входа в систему и сохранения предпочтений пользователя. Необязательные файлы cookie включают в себя файлы, связанные с рекламой, отслеживанием активности и платформами социальных медиа. Обычно они относятся к сбору данных различными онлайн-сервисами для получения информации о действиях и интересах пользователей, то есть к профилированию.

Схема: как работают файлы cookie? На примере Facebook

Например, когда пользователь входит в Facebook, в файле cookie сохраняется информация о его имени пользователя. При посещении Facebook файл cookie необходим для того, чтобы пользователю не приходилось заново вводить свой идентификатор и пароль. Однако часто упускается из виду, что cookie остаются на устройстве даже после выхода из Facebook, только если пользователь специально не удалит их.

Многие социальные и онлайн-сервисы могут встраивать свои функции в другие сайты. Например, Facebook может встроить кнопку «Мне нравится» на сайт компании, встроить страницу Facebook или пиксели отслеживания Facebook, которые обеспечивают таргетирование пользователей, посещающих сайт, для рекламы Facebook. Когда пользователь посещает такой сайт, файлы cookie, ранее сохраненные на устройстве, автоматически отправляются в Facebook при загрузке встроенной функциональности с сервера Facebook. Пользователю не нужно быть авторизованным в Facebook, если файл cookie уже был сохранен на устройстве. Facebook сможет прочитать содержимое cookie и идентифицировать пользователя на его основе. При этом Facebook будет знать, на каком сайте находится пользователь.

Facebook может постоянно отслеживать действия пользователей с помощью файлов cookie на миллионах сайтов. На практике это предоставляет ему данные о том, чем интересуются пользователи, какие товары они недавно просматривали в интернет-магазинах и т. д. Эти данные используются для таргетирования рекламы на рекламных платформах Facebook и Instagram.

Google и многие другие онлайн-компании также используют файлы cookie для профилирования пользователей. Чаще всего файлы cookie используются для так называемого «ремаркетинга», когда пользователю демонстрируется реклама того же товара, который он ранее просматривал в интернет-магазине.

При посещении различных сайтов нам теперь приходится постоянно отвечать на запросы о разрешении использовать файлы cookie. Стоит помнить, что согласие запрашивается только для необязательных файлов cookie, которые обычно не приносят пользы пользователю, но могут обоснованно считаться вредными и снижающими приватность. В худшем случае один сайт может отправлять данные о посещении десяткам компаний по сбору данных с помощью файлов cookie и других функций отслеживания. Онлайн-сервисы в ЕС должны предлагать пользователям возможность отказаться от использования необязательных файлов cookie в момент входа.

Файлы cookie не единственный способ, которым онлайн-сервисы могут хранить отслеживаемые данные на устройстве пользователя. Еще одна распространенная технология — локальное хранилище в браузере. Опять же, сервису необходимо согласие пользователя на его использование. Кроме того, по меньшей мере Google разрабатывает технологию, которая заменит файлы cookie.

Стоит ли сообщать местоположение?

Онлайн-сервисы и приложения могут запрашивать у пользователей разрешение отслеживать их местоположение. Например, новостной сайт может объяснять это желанием показывать пользователю прогноз погоды на основе местоположения, хотя на самом деле оно также используется для персонализации контента и рекламы.

В поисковой системе и рекламной сети Google отслеживание местоположения используется для определения интересов пользователя. Google объясняет использование местоположения следующим образом: «Если вы включили отслеживание местоположения и часто посещаете горнолыжные курорты, вы можете позже увидеть рекламу горнолыжных курортов в видеоролике на YouTube». Однако такого использования данных о местоположении для таргетированной рекламы легко избежать, если не разрешать приложениям Google отслеживать местоположение вашего устройства.

Местоположение устройства по GPS не единственный способ отслеживания пользователей. Более грубо или менее точно его можно определить, например, по данным из публичных сетей Wi-Fi или IP-адресу сетевого подключения пользователя. И даже этого можно избежать, если использовать для подключения к Интернету VPN.

Помимо онлайн-сервисов, доступ к местоположению запрашивают многие мобильные приложения. Стоит оценить, есть ли в приложении функции, для которых местоположение действительно полезно, и решить, стоит ли разрешать ему отслеживать, где вы находитесь. Также следует проверить настройки телефона, чтобы узнать, каким приложениям вы дали разрешение на отслеживание местоположения.

Идентификаторы устройства и браузера

Когда онлайн-сервисы и приложения используются на разных устройствах и в разных браузерах, им могут присваиваться различные уникальные идентификаторы. Например, Google и Apple разработали для своих рекламных систем рекламные идентификаторы, которые используются для идентификации пользователей и таргетирования рекламы в мобильных приложениях. Важность этих идентификаторов состоит в том, что с их помощью можно соотнести конкретное устройство, например мобильный телефон или планшет, с конкретным человеком, так же как, например, адрес электронной почты, номер телефона или адрес.

Как только личность установлена в одном приложении, ее можно установить и в других, используемых на том же устройстве. Есть множество компаний, которые ведут сбор и продажу идентичности и пользовательских данных для идентификации пользователей.

У браузеров нет такой же системы уникальных идентификаторов рекламы, как у мобильных устройств. В прошлом в ней не было «необходимости», поскольку использование файлов cookie очень слабо урегулировано и во многих случаях позволяло легко идентифицировать пользователя.

Поскольку пользователи все чаще ограничивают использование файлов cookie, компании, осуществляющие сбор данных, разработали различные идентификаторы браузеров. Эти теги основаны на различиях в конфигурациях браузеров, таких как настройки, установленные шрифты и плагины. Их называют отпечатками браузера, что хорошо описывает их назначение — идентифицировать пользователя по тому, какой браузер он использует. Например, известно, что приложение TikTok использует в своем веб-сервисе специфические для браузера теги изображений и аудио, которые могут использоваться для идентификации пользователя, даже если он не вошел в сервис.

Не сообщайте свою контактную информацию рекламодателям

Используя Instagram, Snapchat, TikTok или другие приложения, вы можете получить запрос на разрешение использовать вашу контактную информацию — обычно под предлогом того, что это позволит вам найти друзей, которые пользуются приложением. Однако давать разрешение не стоит, поскольку запрос будет распространяться на всю вашу контактную информацию и она может быть использована в других целях. Поэтому стоит приложить усилия, чтобы найти друзей, с которыми вы хотите связаться через приложение, самостоятельно.

Контактная информация — это та же самая информация, которую онлайн-сервисы и социальные медиа используют для таргетированной рекламы и контента, как и любую другую информацию, которую они о вас собирают. Это сетевые данные, которые подскажут вам, кто с кем общается. Даже если мы не передаем свои контактные данные социальным медиасервисам, они могут узнать о нашей сети друзей на основе контактной информации, переданной другими людьми. Например, Facebook и Instagram могут использовать ее для предложения новых друзей и подписчиков.

Иногда контактная информация используется в неожиданных ситуациях. Например, Google утверждает, что использует ее в своем алгоритме рекомендаций новостей. Скорее всего, Google полагает, что мы интересуемся теми же темами, что и наши друзья, которые читают похожие новости.

Общий регламент по защите данных ЕС предоставляет пользователям множество прав при использовании услуг на территории ЕС. Если обработка персональных данных осуществляется на основе согласия пользователя или принятия условий пользования, т. е. договора, то пользователь имеет по меньшей мере следующие права:

- Право на получение информации об обработке персональных данных
- Право на доступ к своим персональным данным
- Право на исправление неточных данных
- Право на удаление персональных данных / право быть забытым

Отслеживание в «темных» социальных сетях

Социальным медиа легко отслеживать взаимодействие между пользователями, пока оно происходит в их собственных сервисах. Понятно, что Instagram, например, отслеживает, на какие посты пользователей мы реагируем, и использует накопленные данные в алгоритме своей ленты.

Отслеживание активности пользователя в приложениях, не относящихся к социальным сетям, напротив, является для них более сложной задачей. Всё чаще ссылки на посты в социальных медиа и новости, например, распространяются в так называемых «темных» социальных медиа, под которыми подразумеваются в первую очередь приложения для обмена сообщениями, такие как WhatsApp, Snapchat и другие.

Как правило, поставщик онлайн-сервиса не имеет возможности узнать, кто и кому отправил ссылку за его пределами. Однако многие социальные и онлайн-сервисы разработали методы прикрепления идентификаторов к ссылкам, что позволяет им узнать, кто изначально поделился ссылкой. Это могут быть, например, теги в виде кода #, следующего за адресом ссылки, или так называемые короткие ссылки. Ряд сервисов агрегации ссылок позволяет отслеживать отправку ссылки.

Когда кто-то переходит по ссылке, онлайн-сервисы узнают, кто поделился ею, по ее тегу. Кроме того, зачастую они могут идентифицировать пользователей, перешедших по ссылке, например, с помощью файлов cookie или других описанных выше средств. В результате они также получат информацию об обмене ссылками через «темные» социальные медиа и о связях между пользователями.

Как удалить данные?

Простейший способ удалить данные, накопленные в онлайн-сервисах и приложениях, — это просто удалить ваши публикации, очистить историю местоположения или просмотров, сохраненную в сервисе, удалить переданную вами контактную информацию или полностью удалить пользовательский аккаунт. Обычно в условия пользования включают пункт о том, что если пользователь удаляет свои данные, поставщик услуг больше не имеет права их хранить.

Многие онлайн-сервисы и приложения позволяют вам контролировать, какую информацию о ваших действиях они хранят и как ее используют. Эти параметры можно найти в настройках пользовательского аккаунта. Например, в настройках аккаунта Google можно отказаться от персонализации рекламы, чтобы данные, хранящиеся в вашем аккаунте, не использовались для таргетирования рекламы.

Упражнения:

1 Пожалуйста, закончите предложение: Приватность — это защита...

2 Каким образом люди обмениваются частной информацией в Интернете? Выберите правильный ответ

Публикуя фотографию онлайн

Публикуя пост о том, что вы отправляетесь в отпуск

Создавая аккаунт в социальных медиа

Используя электронную почту

Состоя в группе (-ах) в Facebook

3 Пожалуйста, опишите способы защиты ваших личных данных при регистрации на некоторых сайтах или при заполнении регистрационных форм.

4. Укажите четыре способа, которыми вы можете оставить цифровой след.

ŠVEITSI–EESTI
koostööprogramm

Авторы: Трийн Нигул, Стелла Саартс,
Кари Кивинен, Карита Кийли, Минна Аслама Горовиц,
Йоонас Пёрсти, Пипса Хавула и Харто Пёнкя

Содержит переводы из издания
«Digital information literacy guide. A digital information literacy guide for citizens in the digital age»,
Faktabaari EDU, 2022

Редакторы содержания:
Анна-Мария Васьковская, Кристиина Каю,
Катерина Ботнар

Перевод с английского:
бюро переводов Luisa

Языковая редактура:
бюро переводов Luisa, Герли Рандъярв

Дизайн:
Виктор Гуров, Маргит Плинк

Издатель:
Национальная библиотека Эстонии

Типография:
Tallinna Raamatutrükikoda

Издание подготовлено в рамках проекта
«MeediaRadar» при финансовой поддержке
швейцарско-эстонской программы сотрудничества
«Поддержка социальной вовлеченности»

Сетевое издание: ISBN 978-9949-413-86-7 (pdf)

Издание: ISBN 978-9949-413-84-3

RaRa EESTI RAHVUS-
RAAMATUKOGU