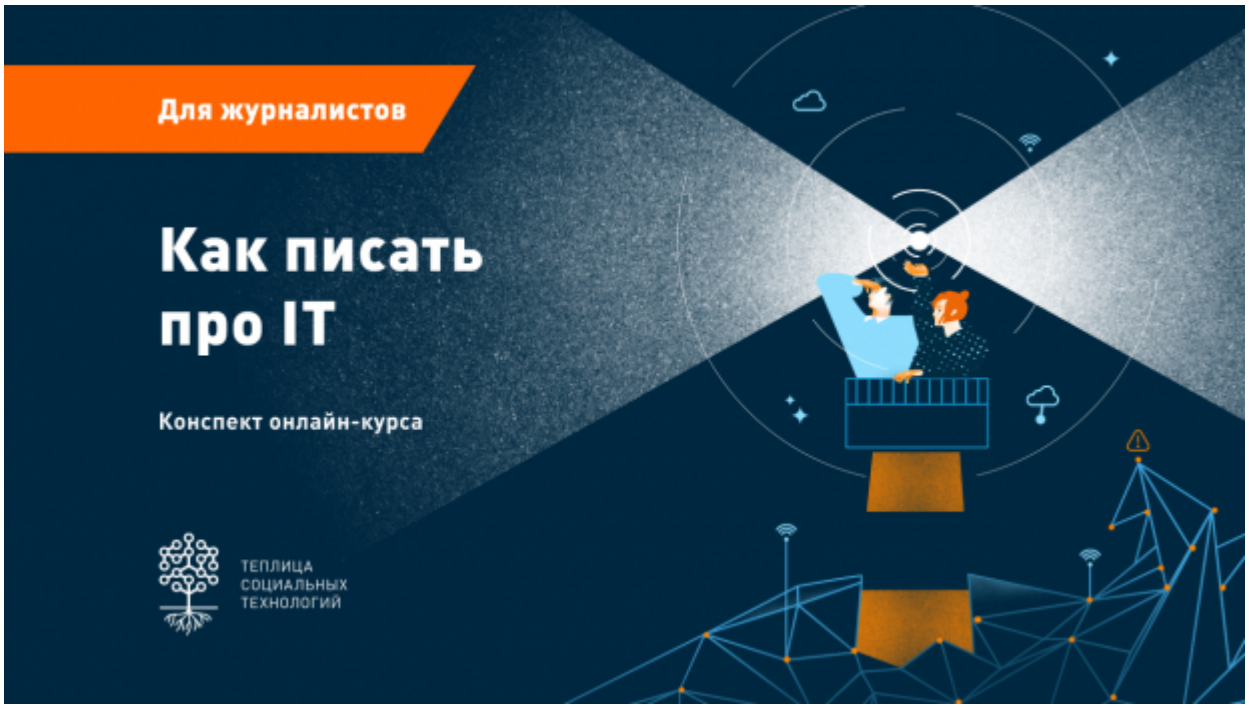
Теплица социальных технологий

Материалы курса «Как читать и писать об IT»

Катерина Новикова

https://te-st.org/reports/how-to-write-about-it/

Статья обновлена 12 июля 2023



В данном цикле из четырех вебинаров слушатели могут ознакомиться с актуальными проблемами и трендами индустрии высоких технологий в области, напрямую соприкасающейся с журналистикой и медиа, вопросами информационных прав и свобод.

Только обладая самыми свежими знаниями о том, как устроен Интернет, об изменениях в мире IT, цифровых правах, использовании данных и многих других технических и инфраструктурных вопросах, связанных с цифровой безопасностью, журналисты смогут активно поддерживать гражданское общество в России.

Ведущий курса — Серафим Романов, шеф-редактор «Новой газеты» в Санкт-Петербурге.

Вебинар № 1: «Устойчивость Интернета»

Первый вебинар посвящен тому, кто на самом деле управляет «Всемирной паутиной», и в чьих руках находится пресловутый «рубильник». На вебинаре также представлены краткая история и архитектура Сети, механизмы внешнего воздействия на сайты и трафик — как это устроено технически и какие скрытые опасности в себе таит.

Об этом рассказывает Михаил Климарев, it-специалист, директор некоммерческой организации «Общество защиты Интернета», автор Telegram-канала «ЗаТелеком».

Запись первого вебинара «Устойчивость Интернета».

Спикер использует понятие управления устойчивостью и непрерывностью работы СМИ (continuity & sustainability management), основа которой — Интернет как автономная сеть, связанная с другими автономными сетями. Интернет во всем мире периодически блокируют. Идея блокировки по разным причинам появлялась в разных государствах — от США до азиатских стран.

Блокировка определенных ресурсов происходит на уровне оператора связи. Чтобы заблокировать ресурс, на первый взгляд, достаточно знать доменное имя или адрес в Интернете. Но Интернет — это сеть, то есть потенциально каждый узел сети может связаться с любым другим узлом сети не единственным путем, а множеством разных путей. Пользователи могут обращаться к заблокированному ресурсу посредством третьего сервиса (VPN), который перенаправит туда их запросы.

Блокировка касается только «черного списка», то есть списка запрещенных ресурсов, остальными можно пользоваться без ограничений. Значительно хуже ситуация была бы с «белым списком», то есть если можно было бы пользоваться только определенными разрешенными ресурсами. Такой сценарий вряд ли произойдет из-за потенциальных катастрофических экономических последствий. Массовые блокировки возможны в странах, где мало операторов связи, например, один в Иране, три в Китае или четыре в Казахстане.

Разновидностью блокировки является Internet Government Shutdown — отключение Интернета по требованию госорганов». Шатдауны появились в странах Африки и наиболее популярны в Индии. В России впервые шатдаун был в Ингушетии в 2018 году. Полный отчет по отключениям команды Access Now в 2020 году можно почитать здесь. Отключение может быть локальное, временное и частичное. В России полное отключение очень маловероятно из-за большого количества операторов связи.

Как можно посмотреть в отчете экспертов OZI, первый шатдаун в Москве был 3 августа 2019 года. Передача данных не работала, так как был полностью отключен мобильный Интернет 3G и LTE, а все базовые станции переведены в исключительный режим GSM. Звонки и сообщения были доступны. Среди источников, которые позволяют оценить размеры шатдауна, можно отметить Ooni Explorer, ресурс с открытыми данными об интернет-цензуре по всему миру.

Редакциям важно заранее подготовиться к различным ситуациям блокировок, чтобы обеспечить доступность и непрерывность работы СМИ, а также сохранить связь между журналистами. Важно помнить, что полностью заблокировать Интернет никому не удастся. Но нужно обеспечить доступ к Сети как можно большему количеству людей, которые, вероятно, не умеют использовать технические возможности для обхода блокировок.

Что должно быть у каждой редакции

- Основа информационной гигиены VPN должен быть всегда включен. Благодаря этому невозможно будет отследить, над чем работают журналисты (например, Psiphon или Amnezia).
- Зарезервированы линии связи на случай отключения (например, спутниковый терминал).
- Созданы резервные физические места для работы.
- Сделан акцент на физической безопасности сотрудников.

Как обеспечить доступность сайта СМИ его читателям

- Создать резервные копии: зеркала, резервный хостинг (вне территории России),

резервные доменные имена (понятные аудитории), системы Content Delivery Network.
- Использовать социальные сети, которые намного сложнее заблокировать, чем веб-ресурс.
- Создать собственное приложение, которое может работать даже в условиях шатдауна.

Вебинар № 2: «Зачем нужны цифровые права»

На втором вебинаре Саркис Дарбинян, адвокат в сфере киберправа, сооснователь проекта «РосКомСвобода», рассказывает о цифровых правах, понятии и их видении государством. Они не прописаны в российских законах, однако их нарушение напрямую перекликается с традиционными правами человека: на доступ к информации, на ее распространение, на приватность и анонимность.

Технологические компании создают «бэк-доры» — намеренные дефекты алгоритма для скрытого доступа к данным. А власти разворачивают сеть видеонаблюдения и допускают возможность блокировки сайтов в обход суда. На примерах из практики на вебинаре обсуждаются случаи, когда можно говорить о злоупотреблении высокими технологиями.

Запись второго вебинара «Зачем нужны цифровые права».

Первый закон, который дал начало регулированию российского Интернета, — это закон о защите детей 2012 года. Его еще называют законом о черных списках сайтов или «слезой ребенка». Он регламентировал порядок ограничения доступа к информации в Интернете и открыл ящик Пандоры, из которого вышли десятки оснований, по которым любой сайт можно в любое время закрыть.

Постепенно становилось понятно, что будут новые законы. На первый план вышли вопросы приватности, охраны тайны частной жизни и анонимности. Порой законы противоречат друг другу, и достаточно сложно определить, как эффективно бороться за свои цифровые права.

К сожалению, в юриспруденции нет направления, изучающего вопросы цифровой трансформации или цифровых правоотношений. Российское законодательство, говоря о цифровых правах, прежде всего делает акцент на цифровых финансовых активах и возможности использовать распределенные финансы в своих целях. И не затрагивает моменты, касающиеся прав человека.

В глобальной перспективе, однако, преобладает другое понимание прав, которые нужно защищать. Прежде всего, это право на доступ к Интернету. В конституциях некоторых стран такое право фиксируется в основных законах (например, Финляндия, Грузия), а право на Интернет гарантируется как фундаментальное право человека.

В скандинавских странах речь идет не только о праве на доступ в Интернет, государство также берет на себя обязательство по скорости доступа в Интернет. В Российской Федерации право на доступ в Интернет признается и уважается. Однако нигде нет гарантий этого права, не говоря уже об обеспечении определенной скорости. Большинство провайдеров в договорах указывает максимум, а не минимум скорости.

Особое значение право на доступ к Интернету получает в эпоху повсеместных штадаунов. Отключение Интернета ведет к нарушению множества иных прав. Хотя может также случиться так, что даже при наличии доступа в Интернет пользователи просто не найдут нужного им контента, так как он может быть заблокирован.

Следующим важным правом является право на распространение информации и право на доступ к информации и ее потребление. Государство в этом случае определяет виды

незаконной информации. Таким образом, право на доступ к информации относится только к той информации, которая не нарушает действующее законодательство (указано в 149 ФЗ, так называемом «трехглавом» законе об информации).

Следующий важный блок прав связан с фундаментальным правом человека на тайну частной жизни. Чтоб ее обеспечивать, недостаточно классических прав, признанных международными конвенциями. К этому блоку относится право на шифрование корреспонденции, право на приватность или конфиденциальность информации в сети Интернет и право на анонимность, то есть право быть неназванным.

Наиболее важным аспектом сетевой жизни является право на приватность (data privacy), которое необходимо отличать от понятия безопасности данных (data security).

Data privacy — это про юридические аспекты, про то, когда и как можно использовать чужую информацию, особенно персональные данные. Закон предусматривает целый ряд ограничений, связанных с обработкой персональных данных. Безопасность данных касается в большей степени технических мер и средств защиты. Можно обеспечить достаточно высокий уровень безопасности, но в случае взлома и получения третьими лицами доступа к информации, единственное, что их будет сдерживать, — это законы, ограничивающие возможность использования персональных данных без согласия третьего лица.

Право на анонимность — это право быть неназванным и право осуществлять действия в сети с использованием специального программного обеспечения, для того чтобы не быть идентифицированным.

Анонимность в действии:

- право на анонимный выход в Сеть;
- право на анонимный веб-серфинг;
- право на анонимное использование соцсетей;
- право на анонимный постинг;
- право на анонимные платежи;
- право на анонимное творчество.

Право на анонимный выход в Сеть воспринимается отрицательно государственной властью, которая хотела бы знать, кто именно анонимно выходит в Сеть, «безнаказанно» осуществляя там разного рода действия. В российской «Стратегии развития информационного общества» анонимность приравнивается к злодеяниям. Провайдеры обязаны идентифицировать каждого, кто выходит в Сеть по абонентскому договору. Все Wi-Fi точки также требуют идентификации.

С такими поисковиками, как «Яндекс» или Google, которые аккумулируют всю информацию о пользователе, сложно реализовывать право на анонимный веб-серфинг. Такую возможность предоставляют другие поисковики, например, DuckDuckGo. Анонимное использование соцсетей означает возможность использовать любую соцсеть под вымышленным именем, с чем также борются многие социальные сети.

Под анонимным постингом подразумевается возможность размещать всю информацию в сети Интернет под вымышленным именем (например, на платформе Telegram). Право на анонимные платежи касается псевдоанонимной валюты Bitcoin и других более защищенных платежных сервисов (Monero, Litecoin). Особенно это важно для поддержки чувствительных проектов и благотворительности. Анонимное творчество означает, что авторские права на произведения, выпущенные под вымышленным именем, охраняются законом (Гражданский кодекс, 4 часть).

Одним из базовых прав современного мира является право на шифрование (right to encription).

Властями предпринимаются попытки запретить шифрованные протоколы, которые уменьшают их возможности ограничения доступа к сайтам. Право на шифрование означает право на использование программных средств и технологий математического процесса преобразования сообщений и данных, в результате которого никто кроме обозначенного получателя не сможет прочесть эти сообщения и данные.

В жизни право на шифрование используется в четырех областях:

- право на шифрование интернет-трафика (протокол https);
- право на шифрование e-mail (PGP-надстройки, Protonmail);
- право на шифрование сообщений в мессенджере (end-to-end encryption);
- право на шифрование данных (специальное программное обеспечение для шифрования жестких дисков, например VeraCrypt или инструменты Windows и MacOS).

В международных соглашениях шифрование и анонимность не упоминаются как базовые права. Однако в мире эти права регулируются так называемыми нормами «мягкого права», которое создает контекст и формальную определенность. К ним относятся рекомендации и резолюции ООН и Совета Европы, неоднократно подчеркивающих важность обеспечения цифровых прав. При этом любые попытки ослабить технологии шифрования и ограничить доступ к инструментам анонимизации угрожают безопасности и конфиденциальности общения в Интернете, ставят под угрозу всех пользователей.

> В рекомендациях ООН утверждается, что государство должно поощрять распространение и использование гражданами средств шифрования, признавая их важнейшим инструментом защиты прав человека.
>
> 
>
> Саркис Дарбинян,
>
> адвокат в сфере киберправа

Когда речь идет о цифровых правах, не нужно замыкаться на национальном праве. Интернет глобален и цифровые права тоже, поэтому основой для них является «Всеобщая декларация прав человека» (1948 года), а также рекомендации ООН и Евросоюза. Ярким примером является регламент и директива Европейской комиссии GDPR).

Этот документ шире трактует права человека в отношениях с компаниями, например, в отношении понятия data portability, то есть права на портативность данных. Пользователь имеет право переносить свои данные из одного сервиса в другой, а также право на удаление. Последнее отличается от права на забвение, которое регламентирует право гражданина на удаление его информации из поисковой выдачи. Право на удаление касается возможности полностью удалять информацию с сервера с подтверждением с его стороны.

В России на сегодня нет никакого единого документа, который определял бы все правила

взаимодействия граждан друг с другом, права, обязанности, ответственность за нарушение законов, а также взаимоотношения между публичными органами и частными акторами. Эти вопросы разбросаны по множеству российских законов, и периодически озвучивается потребность принять «цифровой кодекс», который помог бы систематизировать нормы. Подобная безуспешная попытка уже была предпринята, но «кодекс» так и не появился. В том числе из-за большого количества разных игроков с диаметрально противоположными интересами и взглядами на то, как должно регулироваться интернет-пространство.

Проблемой также остается правоприменение. Существует много хороших законов, которые не используются в обычной жизни. Например, статья 137 УК РФ о неприкосновенности частной жизни.

Сравнительно новым явлением стало platform law, так называемое право платформ, таких как Facebook, Youtube, которые развивают свою собственную политику без привязки к конкретному законодательству отдельной страны. Платформы создают правила игры, по которым должны играть все остальные игроки и которые могут меняться. Таким образом, например, обжаловать то или иное решение такой платформы можно, но только через уполномоченные общественные организации (например, Access Now, Electronic Frontier Foundation, общественные комиссии Facebook в разных странах).

Вебинар № 3: «Приватность, инфопузыри и дезинформация»

На третьем вебинаре Сергей Голубицкий, it-журналист, писатель, автор проекта minoa.biz, рассказывает о том, что делать журналистам с дезинформацией и так называемыми инфопузырями, как распознавать фейк-ньюс, как все это связано с поляризацией и приватностью. А также о том, как и почему поведенческие данные пользователей стали главным ресурсом для работы социальных сетей, поисковых систем и других платформ.

Запись третьего вебинара «Приватность, инфопузыри и дезинформация».

Если речь заходит о персональных данных, кажется, что проблема состоит в доступности данных о конкретном человеке. Но на сегодня важнее поведенческие данные, причем не одного конкретного пользователя лично. Объектом интереса становятся данные сотен тысяч, миллионов пользователей. И экономически переосмысленные тенденции, на основе которых it-гиганты и управляют нашим поведением, нашими предпочтениями в Интернете.

Поэтому, по мнению спикера, страхи, касающиеся потери контроля над персональными данными, сбора данных, big data, являются скорее частью фобии на уровне социальной мифологии. При этом важно знать, как работают механизмы формирования тенденций с самого момента возникновения Интернета.

Отсчет исторической эволюции идей, касающихся Интернета, начинается с Web 1.0. Идеологический фундамент появления Web 1.0 в середине 1990-х годов заложили мыслители с либертарианскими или даже анархистскими идеями, которые лучше всего представлены в «Декларации независимости киберпространства» (Джон Перри Барлоу, 1996 год). В Web 1.0 контент создают первопроходцы, гуру, все остальные обитатели Интернета пассивно потребляют информацию. Важное понятие, которое может понять, что случилось дальше с Web 1.0, — это filter bubble («пузырь фильтров»), популяризированное американским журналистом Эли Паризером (книга «За стеной фильтров»).

В середине 1990-х на фоне утопических идей, касающихся Интернета, возникло понятие relevance, или релевантность, уместность (относительно чего-то) информационного контекста. Интернет на заре своего становления рассматривался как пространство, в котором все люди могут объединиться и вершить добрые дела. Однако поиск этой релевантности и правильных

контекстов очень быстро привел к созданию коммерческими структурами специальных технологических алгоритмов. Такие алгоритмы, например в Amazon, называются personalized recommendations (персонализированные рекомендации), а в Google — click signals (сигналы после клика пользователя).

На основании анализа поведения пользователей происходила деформация информационных потоков, которые начали максимально точно и адекватно, по мнению алгоритма, соответствовать запросам и потребностям каждого конкретного пользователя. В итоге из-за работы персонализирующих алгоритмов то, что изначально задумывалось как благо, способное объединить людей по интересам и потребностям превратилось в фактор глобального разобщения. Каждый пользователь получает не ту информацию, что его сосед или даже близкий человек, находясь в одном из множества дискретных информационных пространств с разрозненными информационными потоками. Такие индивидуализированные информационные пространства Эли Паризер и назвал «пузырем фильтров».

> Косвенное обстоятельство, вытекающее из «пузыря фильтров», — это констатация абсолютной невозможности в наше время генерировать оппозиционную (нонконформистскую) идею в принципе. В том смысле, что сегодня любая идея упирается лишь в контекст, порожденный тем самым «пузырем фильтров».
>
> 
>
> Сергей Голубицкий,
>
> it-журналист, писатель

Каждый из обитателей Интернета обречен на виртуальное существование в оторванном от любой чужой реальности пузыре. На практическом уровне это проявляется в том, что один и тот же информационный портал выглядит по-разному для разных пользователей. Все интернет-компании интенсивно используют «пузырь фильтров» с целью коммерческой эксплуатации пользователей, например, через индивидуально подобранную рекламу.

Иногда, однако, это обстоятельство оценивается с меньшей дозой критицизма, чем, например, по мнению Эли Паризера, потенциальное разобщение людей, нарушение свободы и разрушение творческого порыва личности из-за отсутствия доступа к альтернативному, не отфильтрованному информационному потоку. Однако, по мнению Сергея Голубицкого, для подавляющего числа обитателей Интернета «пузырь фильтров» скорее благо, чем зло. Он выводит на первый план именно то, что нужно пользователю (увидеть, прочитать, купить), отсеивая всякие неприятные ассоциации, темы или воспоминания. Это оказывается гораздо важнее, чем свобода или творчество.

В последнее время стало все тяжелее бороться с «пузырем фильтров», так как, например, поисковые сервисы ограничили возможность использования большей части поискового синтаксиса. Среди поисковиков, которые, в свою очередь, отказались от «пузыря фильтров», самым известным является DuckDuckGo — принципиальный противник практики сбора информации о пользователях. Однако результаты поиска не всегда соответствуют ожиданиям, в особенности после активного использования Google. «Пузырь фильтров» оказывается

вынужденным злом, платой за которое становится структурирование и взвешивание информации.

В начале 2000-х появляется Web 2.0, главным следствием которого становятся социальные сети. В соцсетях пользователи находятся в информационном коконе, или иначе эхо-камере (echo chamber). Другой важной чертой соцсетей является формирование идеальной среды для распространения так называемых фейк-ньюс и шире постправды.

В Web 2.0 контент может создаваться не только специалистами, но и каждым пользователем. При этом контроль за контентом и его распространением осуществляют централизованные структуры, которые владеют социальными сетями. В течение последних нескольких лет зреет революция Web 3.0, связанная с экспансией криптоэкономики и децентрализованными финансами (DeFi). При этом создание контента остается доступно всем пользователям, а также они получат в свои руки контроль за контентом и за распространением, отобранный у «цензоров».

Как можно охарактеризовать эпоху послеправды? Это период, когда главная ценность информации не в ее правдивости, а в ритуальном значении этой информации.

> Постправда — мера, в которой сообщение отражает уже сложившиеся представления, мировоззрение, идеологию адресата, получателя информации.

> Сергей Голубицкий,
>
> it-журналист, писатель

Фейк-ньюс — это очень неудачный неологизм, он не передает сути проблем. И в основном используется политиками для того, чтобы заставить замолчать тех, кто высказывает неприятные им вещи.

Среди информационных нарушений можно выделить три основных вида:

- Mis-information — информация, которая вводит в заблуждение, опирается на ложных взаимосвязях между разрозненными событиями, представленных в запутанном контексте, однако это не обман;
- Dis-information — самая вредоносная, это ложный контекст, заведомо ложная информация, помещенная в сфабрикованный контекст,
- Mal-information — правдивая информация, призванная нанести урон, информационные утечки.

В фейк-ньюс присутствуют отчасти все три элемента, но при этом они не сводятся ни к одной из этих разновидностей. Фейк-ньюс — это некое информационное искажение, которое подражает или подстраивается под авторитетную новость. Отличие от dis-information в том,

что фейк-ньюс призваны не обмануть, а усилить уже присутствующие информации, стереотипы и ментальные конструкции.

Идеальной средой для распространения фейк-ньюс становятся социальные сети. Новости распространяются в сети при помощи какого-нибудь надежного факта, искажение появляется уже на уровне коннотаций. В современном мире факты стали играть меньшее значение, чем соответствие информации внутренним установкам, личному мировоззрению человека.

Таким образом, соцсети, где все построено на системе лайков, репостов, приятных сообщений или информации, с которой человек согласен, или удаления всего неприятного, создают «эхо-камеру» — такое гомогенное информационное пространство, где функционируют только реплики единомышленников и формируется почва для деформации представлений о реальном мире. Фейк-ньюс задыхаются от критического восприятия.

Как же тогда работать с информацией сегодня? Интернет в версии Web 2.0 — это враждебное и ангажированное пространство, поэтому основой любого подхода к информации является недоверие, которое как навык очень может пригодиться в грядущем Web 3.0. Единственный критерий истины — это всегда личная проверка каждого факта, который журналист использует в своем тексте.

Вебинар № 4: «О чем говорят it-тренды»

На последнем вебинаре Кирилл Мартынов, журналист, философ, заместитель главного редактора «Новой газеты», рассказывает о влиянии высоких технологий на жизнь человека сейчас и в будущем, формулируя главные тренды цифровых технологий.

Запись четвертого вебинара «О чем говорят it-тренды».

Кирилл Мартынов выделяет следующие главные it-тренды.

Власть алгоритмов — алгократия

Ее можно сравнить с эксперто- или технократией, когда решения на государственном уровне принимаются на основе заключения экспертов. Теперь на их место приходят алгоритмы и ИИ, хотя это все еще не касается ключевых решений. На эту тему спикер посоветовал подкаст Algocracy and Transhumanism Podcast

Переплетение виртуального и реального миров

Общество существует в гибридном пространстве, так как была создана цифровая копия мира с его предрассудками, местными элитами и бизнесами. Большинство повседневных практик каждого человека опосредованы цифровыми практиками. Ушла в прошлое идея о том, что отдельно существуют игроки цифровые, а отдельно — офлайновые. Все хотят контролировать то, что происходит в цифровом пространстве, а изначально специализированные цифровые компании становятся мощнейшими игроками реального мира. Их стратегия состоит в том, чтобы оцифровать как можно больше сфер.

Нарастание «балканизации» — разделенности и сегментированности Интернета

Интернет создавался как глобальный трансграничный проект, и все привыкли думать об Интернете, как об общности. Чем большую роль цифровые практики играют в жизни общества, тем больше их стремятся контролировать национальные государства. Сегодня Интернет — это «лоскутное одеяло» различных юрисдикций, как государственных, так и корпоративных.

Гиперавтоматизация

Эта тенденция означает создание цифровых копий организаций: сбор данных, построение

информационной модели процесса и последующий перезапуск этого процесса на цифровой платформе. Предполагает также совместную работу людей и «цифровых работников», а также более гибкое использование различных моделей автоматизации. С гипераватоматизацией связано появление новой организационной модели и практики менеджмента.

Человеческое общение становится новой роскошью

Сегодня человеческое общение лицом к лицу, а также услуги, оказанные живыми людьми, превращаются в роскошь. Цифровые практики доступны, следовательно, по законам рынка они превращаются в массовые и теперь предназначены для бедных. Оказалось, что все, что можно воспроизвести в рамках цифровых практик, — общедоступно и дешево, а возможность избегать цифровых практик стала признаком социального успеха.

Демократизация технологий

Технологии могут использовать все, а не только специалисты. Компьютер перестал восприниматься как особо сложный объект, просто как инструмент. Даже выясняется, что не обязательно быть грамотным в цифровом отношении, если человек является профессионалом своей сфере. Скоро люди смогут эффективно работать с массивами данных, не имея специального представления о статистике или о том, как эти массивы собираются и работают благодаря упрощенному интерфейсу.

Проникновение информационных технологий в традиционные сферы

Наблюдается рост использования высоких технологий в неочевидных местах, например, в фермерских хозяйствах и агрокультуре, которые обычно не находятся в фокусе it-журналиста.

Рост нового технопессимизма

В оценке технологий всегда были скептики и оптимисты. При этом до последнего времени у технооптимистов был более положительный имидж, а для обычных людей жизнь с технологиями представлялась интереснее, чем без них. Сейчас технопессимисты — это уже не те, кто тоскует о прошлом и о том, как было хорошо когда-то.

Технопессимизм сейчас гораздо более умный и современный, лучше понимающий, как работает отрасль, акцентирующий огромное количество рисков IT, которые человечество еще до конца не оценило. Для цифрового капитализма важен человеческий опыт, информацию о котором можно анализировать, продавать и зарабатывать миллиарды долларов. Таким образом происходит колонизация человеческого опыта.

Спор об IT это спор о контроле над миром, реальностью, деньгами, между корпорациями и государствами. Нарастает дискуссия о том, как жить в человеку в такой ситуации, в ситуации, когда в городе его лицо распознается камерами, а любой желающий может, хоть и нелегально, купить информацию о его передвижениях на черном рынке. С другой стороны, демократизация технологий оборачивается превращением людей в роскошь.