ИНТЕРНЕТ СЕГОДНЯ И ЗАВТРА

СБОРНИК АВТОРСКИХ СТАТЕЙ К ТРИНАДЦАТОМУ РОССИЙСКОМУ ФОРУМУ ПО УПРАВЛЕНИЮ ИНТЕРНЕТОМ RIGF 2023

6, 7 апреля 2023 г.

CG ITC
CENTER FOR GLOBAL IT-COOPERATION

АНО «Центр глобальной ИТ-кооперации» (CGITC)

АННОТАЦИЯ

К Тринадцатому российскому Форуму по управлению Интернетом (RIGF 2023) Центр глобальной ИТ-кооперации (CGITC) подготовил специализированный сборник экспертных статей по широкому спектру вопросов в рамках тематики управления Интернетом. Это уже второй сборник Центра, первый был выпущен год назад к Форуму RIGF 2022.

Вниманию профессионального сообщества предлагаются авторские статьи по разнообразным проблемам, связанным с вопросами развития Интернета и цифровых технологий. Авторами являются специалисты различных российских площадок и институтов развития, которые в данном случае представили свои статьи от своего имени, как профильные эксперты.

Статьи охватывают актуальные вызовы в сфере информационного пространства и цифровой экономики, проблематику внедрения и использования сквозных технологий, задачи укрепления российского сегмента Интернета и ИТ-отрасли в целом. Материалы содержат обзорную аналитику, прогнозы, отдельные предложения, рекомендации и выводы.

Сборник выпущен с целью активизировать межинституциональный диалог и придать новый импульс экспертной дискуссии по актуальным проблемам цифровизации и развития Интернет-технологий. Работы подчинены единой задаче - выработать сбалансированные позиции и ориентиры для эффективного развития цифровых инноваций в России. Важной составляющей при этом является участие в международном диалоге и кооперация с зарубежными партнерами.

Мнения, содержательные тезисы и выводы авторов могут не совпадать с позицией и подходами АНО «Центр глобальной ИТ-кооперации». Центр не принимает на себя обязательств или ответственности за использование информации, содержащейся в Сборнике, равно как и не несет ответственности за точность приведенных данных. Используемые авторами материалы и ссылки на сторонние веб-сайты находятся вне контроля CGITC.

Возможные отзывы, мнения, а также различные предложения по развитию совместных исследовательских проектов в рамках затронутых в Сборнике проблем можно направлять в адрес CGITC info@cgitc.ru.

«Интернет сегодня и завтра», Сборник авторских статей к Тринадцатому российскому форуму по управлению Интернетом - RIGF 2023 (6, 7 апреля 2023 г.), Центр глобальной ИТ-кооперации, Москва, апрель 2023 г.

АНО «Центр глобальной ИТ-кооперации»
ANO «Center for Global IT-Cooperation» (CGITC)
https://cgitc.ru/

Редактор-составитель: Игнатьев А.Г., CGITC
Иллюстрации: Интегратор web 3.0 Осьминожка совместно с ИИ Midjourney
Москва, апрель 2023 г.

АНО «Центр компетенций по глобальной ИТ-кооперации» создан в 2020 году для экспертного изучения вопросов международного сотрудничества в сфере информационных технологий (ИТ), укрепления позиций России в глобальной ИТ-кооперации, в частности, продвижения новых подходов к многостороннему и равноправному управлению Интернетом на основе обеспечения безопасности и уважения национального суверенитета.

CGITC является членом Сектора развития электросвязи (ITU-D) Международного союза электросвязи, участником международного Форума по управлению Интернетом (IGF), соорганизатором ежегодного Российского форума по управлению Интернетом.

Центр проводит исследования и реализует проекты в области цифровой грамотности, управления Интернетом, научно-технического сотрудничества в сфере цифровой экономики, оказывает практическое содействие новым командам и начинающим экспертам по продвижению инноваций и стартапов. Во взаимодействии с международным сообществом и при поддержке заинтересованных специалистов в России CGITC на регулярной основе проводит ряд научных и экспертных круглых столов, конференций и вебинаров.

CGITC входит в число организаторов Российского форума по управлению Интернетом, является ключевым организатором Молодежного российского форума по управлению Интернетом, последние два года участвует в проекте Think20 исследовательской сети G20.

ПРАВИЛА ИСПОЛЬЗОВАНИЯ СБОРНИКА

Аналитические статьи, включенные в Сборник, подпадают под действие Закона об авторских правах Российской Федерации. Исключительные права на Сборник принадлежат АНО «Центр глобальной ИТ-кооперации» (далее — «правообладатель»).

Сборник может использоваться в целях ознакомления. Допускается размещение активных ссылок на него в информационных источниках без непосредственного копирования его содержания. При любом использовании Сборника активная ссылка на источник обязательна.

Частичное или полное воспроизведение и распространение, а также любое коммерческое использование обзора запрещено без письменного разрешения правообладателя, а также без ссылки на авторов исследования.

Приступая к ознакомлению с материалом, вы подтверждаете свое согласие с изложенными ниже условиями:

• Центр глобальной ИТ-кооперации не несет ответственность за позиции и подходы авторов статей и может не разделять представленные в Сборнике взгляды и рекомендации.

• Правообладатель не принимает на себя обязательства или ответственность за использование информации, содержащейся в Сборнике.

• Информация статей носит исключительно информационный характер и подготовлена на основе открытых источников, признанных надежными, однако правообладатель не несет ответственность за точность приведенных данных.

• Выводы, представленные в статьях, также носят исключительно информационный характер и основаны на данных, полученных из открытых источников, указанных в сносках и библиографии.

• Сборник не является юридическим заключением по вопросам, рассмотренным в нем. Правообладатель не несет ответственность за решения, принятые на основании представленных в Сборнике данных.

• Сборник включает в себя ссылки на сторонние веб-сайты, находящиеся вне контроля правообладателя. Правообладатель не несет ответственность за содержание этих ссылок. Такая ответственность во всех случаях возлагается на соответствующего провайдера либо оператора этих сторонних веб-сайтов.

ОГЛАВЛЕНИЕ

Вводная статья редактора

ЛАБИРИНТЫ ЦИФРОПЕРЕХОДА (ВИД СВЕРХУ)

Игнатьев А.Г.
Центр глобальной ИТ-кооперации, руководитель аналитического направления

Мировым процессам присущи этапы стабильности и фазы трансформации, преодоление катаклизмов, стагнация и научные прорывы, адаптация к изменениям и поиск векторов развития - все это можно определить как вехи в осознании человечеством своего места и пути в единой экосистеме «человек - техника - природа».

Вероятно, современность предоставила нам возможность не только быть наблюдателями, но и участвовать в сложнейших процессах очередного фазового перехода - технологического, социогуманитарного, духовного, цивилизационного. В обозначенном переходе технологическое развитие и всепроникающая цифровая экспансия вероятно составляют ядро и суть трансформации, которую переживает планета. В отличие от электричества, новые технологии не только «зашли в каждый дом», но и воздействуют на сознание современного человека, прямо или косвенно формируют его духовную сферу. И эти технологии будут усложняться - мысль изобретателя, конструктора должна и неизбежно будет двигаться вперед. При этом технологические достижения и научно-технический прогресс вероятнее всего опережают ментальную, когнитивную и морально-нравственную готовность человека и общества к новым преобразованиям.

Эти преобразования вызывают парадоксы, противоречия, метаморфозы, нарушения привычного порядка, протекают по сценарию болезненного созидательного разрушения, сопровождаются социальными или экономическими катаклизмами. Кроме того, «проблемы конвергентных технологий, с одной стороны, актуализировали, а с другой – обострили множество философских и социальных проблем, связанных с этическими, ценностными и личностными аспектами существования человека в современном технологизированном обществе»[1]. Нет сомнений, что развитие искусственного интеллекта (ИИ) значительно ускорит продвижение нейрофизиологии, нейропсихологии, нейробиологии, антропологии и другие направления когнитивистики в познании загадок человеческого (естественного) разума - мы ускорим изучение собственной природы. При этом внедрение систем ИИ неизбежно вовлекает человека в совершенно новую среду жизнедеятельности, в неизведанные зоны риска, а значит порождает новое многообразие научных задач.

В сегодняшней трансформации, условно обозначенной здесь как «цифропереход» (хотя, вероятно, более широкой и точной формулировкой будет «техноантропологический переход»), три элемента (человек/общество - техника - природа) выступают в сложном, постоянно меняющемся синтезе, который требует соответствующего ком-

[1] Баева А.В., «Философия и социология техники в XXI веке: проблемное поле современных дискуссий», 2019

плексного, междисциплинарного изучения, и прежде всего осмысления с философских позиций («Откуда мы пришли? Кто мы? Куда мы идем?»). Однако же, в большинстве случаев в настоящее время поиск ответов и путей развития лежит только в плоскости достижения экономических эффектов, монетизации/коммерциализации, создания новых быстрых и очевидных благ и удобств, реализации других утилитарных целей, без анализа долгосрочных последствий и всесторонней оценки воздействия, в том числе воздействия непредвиденного и постепенно накапливающегося, аккумулятивного.

Различные мифопоэтические концепции утопии или антиутопии (апокалипсис, технологическая сингулярность и т. п.) не приближают нас к поиску оптимальной модели регулирования и справедливого мироустройства в условиях технологической революции (всевозможные скептики, алармисты, визионеры, фантазеры и предсказатели с различными гипотезами, от «цифрового рая» до «восстания и диктатуры машин», не отвечают на вопросы «почему?» и «что делать?»).

КОНФИГУРАЦИЯ ПАРАДОКСОВ

Сегодня «цифра» — это почти сленговое и расхожее слово, за которым, однако, стоит широкое, терминологически неопределенное понятие, которое сложно отрефлексировать и очертить границы вне конкретного поля применения. «Цифра» становится частью реально воспринимаемой действительности, которая формирует нашу индивидуальную и коллективную картину мира. Между тем, «цифра» все еще остается «вещью в себе и создающей себя», неструктурированной и неоднозначно интерпретируемой. «Цифра» приобретает черты мимикрирующей реальности с размытыми атрибуциями, со сверхвозможностями и, одновременно, сбоями и досадными ошибками.

«Цифра» представляется как некий гигантский электронный организм, рычаги управления которого находятся вне контроля единого центра управления.

Глубинную суть современного этапа, который принято называть цифровой эрой, цифровым обществом, технологической революцией и т. п., предстоит осознать и научно препарировать, однако, вероятно уже сейчас можно утверждать, что этот этап полон парадоксов. Для их преодоления и разрешения уже не подходят старые инструменты, теории и практики - мы столкнулись с процессами развития сложноорганизованных, саморазвивающихся систем не локальной, а планетарной размерности. Гиперсвязанность, скорость социальных коммуникаций, цифровых транзакций и вычислений и, как следствие, новое качественное состояние техносферы, привели к иной «визуализации» мира, новым смыслам и рациональностям - по сути к новому бытию. В этих условиях существующая социотехнологическая среда, как симбиоз процессов, как система систем, и как среда, определяющая будущее планеты, еще не изучена на комплексном научно-практическом уровне, который бы гарантировал реальное процветание и гармонию (или, по меньшей мере, безопасное развитие).

Вероятно, можно констатировать явное отставание и опасную медлительность в построении согласованного научного конструкта для осмысления генезиса, объективной динамики, полной карты рисков и сценариев развития цифровой трансформации, особенно применительно к социогуманитарным проблемам эволюции.

Сегодняшние усилия человека на поприще технологий в целом, и цифровых технологий в частности, главным образом определяются рамками «промысловой» модальности, лежат в сфере извлечения прибыли, новых технологических завоеваний, конкуренции патентов и технологий, войны за умы и влияние и т. п. Вероятно, наиболее распространенным ответом на новые вызовы является охватившее политиков, чиновников и экспертов от цифровой экономики масштабное построение многоэтажного, и порой не гармонизированного и запутанного каркаса весьма привлекательных по форме принципов, деклараций и меморандумов. При этом, зачастую в команды составителей такого рода разнообразных фреймворков не входят представители науки, прикладные аналитики, философы, социологи, психологи. При изобилии ораторов и целой плеяды новореформаторов ощущается дефицит мудрецов-мыслителей, способных вскрыть сущностно-смысловые характеристики, причинно-следственные связи, сформировать доказательные теории и соединить их с практикой.

Между тем необходимо отметить, что на национальном уровне отдельные научные школы, команды, исследовательские коллективы или самостоятельные ученые предлагают свои вполне состоятельные и заслуживающие внимания подходы. Такие научно-философские воззрения и теории, возникающие в отечественных недрах на основе сплава наук, при их междисциплинарном усилении и обоснованной формализации могли бы лечь в основу свежих, передовых инициатив для международного продвижения.

«КОГДА В ТОВАРИЩАХ СОГЛАСЬЯ НЕТ…»

Если упрощенно и весьма условно схематизировать административную (организационную) парадигму сегодняшних усилий в области развития, применения и регулирования цифровых технологий, вероятно, можно прийти к следующим наблюдениям:

- политики вступают в отношения «то любви, то ненависти», то союза, то конфронтации с лидерами «цифровиков» (крупные технологические компании и платформы), при этом они не слышат (или не умеют понять) философов;
- самих же философов, в их вечном стремлении к высоте, если прибегать к аллегории из известной басни И.А. Крылова, вероятно можно сравнить с лебедем (в их адрес звучат вечные упреки в «оторванности от земли» и малопрактичности);
- юристы в условиях совершенно новых задач и вакуума прецедентов либо идут за европейским или англо-американским мейнстримом, либо самостоятельно пытаются разобраться как применить классические модели права к цифровым новациям (они вынуждены погружаться в инженерные аспекты проблемы; по сути, сегодняшние юристы в сфере «цифры» должны владеть определенными базовыми компетенциями в компьютерных науках);

- технологи и разработчики в большинстве случаев хотят лишь больших свобод или самоустраняются из разнородной группы «архитекторов-теоретиков», торопятся вершить свои открытия и внедрения, заниматься более практическими вопросами кодов и алгоритмов.

При этом трудно упрекнуть или обвинить какую-либо категорию в отдельности, - налицо объективная разнонаправленность интересов акторов, по крайней мере в предложенной модели взаимодействия, где конечные цели на дальнем горизонте либо размыты, либо видятся не совсем одинаково.

Картина становится и вовсе неутешительной, когда мы переносим ее на международный уровень и говорим о диалоге государств - ко всем проблемам и трудностям достижения синергии и консенсуса добавляется геополитическая конкуренция стран, их состязание в области экономики и технологий.

НАЛИЧИЕ КОРНЕЙ

Упорядоченность многослойной матрицы структур, разноплановых элементов и компонентов деятельности, входящих в понятие «цифровая трансформация», безусловно требует опоры на научные методологии и широкий междисциплинарный подход - необходимы мультимеждисциплинарные или трансдисциплинарные стратегии. Технологические инновации, осуществляемые без параллельного, а еще лучше предшествующего, априорного социогуманитарного познания и анализа, в сегодняшних условиях обречены на стихийное, неконтролируемое развитие, на создание рисков в краткосрочной или более отдаленной перспективе, на новые техногенные вызовы и общий рост неопределенности.

В российской научной школе идеи об устойчивом развитии социума, включая технологическую составляющую, развивал В.И. Вернадский. Его концепция ноосферы[2], как возможности нового этапа коэволюции человека и биосферы, актуальна и по сегодняшний день. Теория В.И. Вернадского опирается, в частности, на необходимость создания и использования технологий, сообразующихся с законами живого вещества/материи и биосферы.

Полезные научно-практические труды оставил после себя Н.Н. Моисеев, который, в том числе развивал идеи В.И. Вернадского, включая педагогические и этические проблемы формирования нового научного мировоззрения в отношении освоения биосферы. Являясь ученым в области механики и прикладной математики, он стал автором монографий, учебных пособий, научных исследований и статей, в которых предложил новые идеи и разработки в области философии (процессы универсального эволюционизма общества и биосферы и др.), оптимизации управления, проектирования и развития автоматизированных систем, экологии.

Другим первопроходцем и мыслителем, указавшим на необходимости развивать междисциплинарные научные направления в условиях глобализации и технологизации общества, был профессор В.Г. Горохов, который обозначил тренд философских исследований на пересечении социально-гуманитарных и научно-технических дисциплин[3].

[2] Биосфера и ноосфера, В.И. Вернадский, М.: Наука, 1989, 261 с.
[3] Баева А.В., Философия и социология техники в XXI веке: проблемное поле современных дискуссий, 2019

В качестве значимых достижений в понимании подобных процессов и в становлении науки нового времени можно привести труды выдающегося российского философа В.С. Степина, который разработал конструктивно-эволюционную модель развития науки и внес понимание в перспективы конвергентного развития естественнонаучного и социогуманитарного познания. Оставленные академиком труды и научное наследие развиваются целой плеядой российских ученых применительно к проблемам философии техники, развития кибернетических систем и могут иметь весьма практическое значение. Предложенное ученым системное видение, опирающееся на общенаучную картину мира, которая задает обобщенное представление об универсуме (неживой, живой природе, обществе и человеке) позволили разработать онтологии и категориальные структуры классической, неклассической и постнеклассической рациональности[4]. Сегодня эти понятия укоренились и успешно развиваются в философском дискурсе, который, как представляется, имеет отнюдь не оторванное от практики значение для компьютерных наук, вопросов развития Интернета и цифровой трансформации в целом.

Работы перечисленных исследователей, а также изыскания других российских ученых заложили фундамент и пустили благодатные корни для усиления и развития национальной школы в области философии техники, технонауки - это тот ресурс и потенциал, который сейчас крайне востребован на стыке самых перспективных направлений научной деятельности. Поддержка продолжателей традиций российской школы ученых имеет огромное значение для преемственности и передачи знаний будущим поколениям. Труды отечественных мыслителей важны не только для продвижения вперед академических исследований и технологий, но и для повышения качества образования в сфере компьютерных наук, системотехники, философии, социологии, культурологи. Именно на основе таких трудов целесообразно предпринимать попытки выстроить опережающее образование и опережающее научное мышление.

ОНТОЛОГИЯ ОНТОЛОГИЙ

В условиях формирующейся техносферы, а вернее техноантропосферы, где NBICs-конвергенции[5], вероятнее всего, уже вступают в стадию своей зрелости, высокотехнологичные системы, объекты и различные сетевые инструменты-приложения в своей совокупности постепенно начинают превращаться из средств деятельности в интеллектуальных ассистентов и помощников человека. Таким образом, неуловимо и часто неосознанно происходит закрепление сложных компиляций и взаимозависимостей между человеком и машиной/системой. Это позволило исследователям рассуждать о некой гибридизации, смещении субъектности, киберсоциальной виртуальной реальности, техночеловеке и т. п. - вопросах, которые, безусловно, должны подвергнуться углубленному научному анализу и экспертизе, особенно в части выявления рисков.

Можно констатировать, что в определенных случаях человек уже не может в полной мере обеспечить прозрачность сложнейших вычислений или вмешиваться в заложенные алгоритмом действия, например, в высокоинтеллектуальных экспертных системах или в

[4] В.С. Степин, Классика, неклассика, постнеклассика: критерии различения, 2009
[5] NBICs (Nano-Bio-Info-Cogno-Technologies), взаимопроникновение наук и технологий: нано, био, информационные технологии и когнитивные технологии

смарт-контрактах, которые в автоматическом режиме выстраивают соглашения большого количества партнеров в сложной технологической и логистической цепочке, а затем отслеживают их выполнение. В рамках бурного развития машинного обучения ведется активная разработка вопросов гибридного интеллекта, искусственного интеллектуального агента, человеко-машинного интерфейса «мозг - компьютер», антропоморфной роботизации, создания машин с моделью психического состояния и другие исследования.

Существует сценарий погружения всех этих разработок и технологий в виртуальную реальность - квазиреальную среду метавселенных, что еще более усложнит построение универсальных концепций и подходов к системному наблюдению, контролю и управлению указанными процессами.

Выше обозначены лишь контуры ожидаемой нас неопределенности в понимании технологий будущего, обозначены прообразы предстоящих вызовов и рисков цифровизации. Полный же список может, например, начинаться риском банального телесного обездвиживания и заканчиваться потерей человеком автономии, самодетерминации и когнитивной деградацией (в статье не ставится цель подробно описать и классифицировать проблемы и возможные риски технологической конвергенции, равно как и зафиксировать наблюдающиеся прорывы в когнитивных науках, квантовых вычислениях и в других дисциплинах, в т. ч. в таком научном направлении, как синергетика, которая изучает закономерности самоорганизации систем, многоэлементные структуры и многофакторные среды).

Обращение к сущности процессов в общей системе знаний, к соответствующему актуальности онтологическому подходу, может облегчить понимание сложных цифровых систем, а также нелинейного множества взаимосвязей цифрового и социального. Такие актуальные и работающие на макроуровне онтологии, вероятно, можно выработать только на стыке наук, при определяющей роли философии, где уже существует историческая научная колыбель базовых подходов и теорий, представлена опорная концептуализация для дальнейшего дискурса.

Инженерия знаний и онтологическое моделирование в отношении столь сложных систем и экосистем, безусловно, сталкивается и еще столкнется с необходимостью нетривиальных решений, применения новых теорий и средств разработки, особенно в антропологическом, человекомерном измерении. Вероятно, симбиоз онтологий верхнего уровня и онтологий, ориентированных на предметную область, с огромной сетью фреймов и графов знаний сложной иерархии будет неким подобием «онтологии онтологий». В таких построениях особую значимость приобретает категорийно-понятийный аппарат и терминологическая система. В связи с этим, в частности, повышается и роль технических стандартов и спецификаций, как важного системообразующего звена в цепочке извлечения знаний.

Проделанная в статье поверхностная и беглая попытка бросить взгляд на столь многоуровневые проблемы и спроецировать «вид сверху», вероятно, дает основания говорить, что пока, на сегодня, продвигаясь к гармонии с природой и техникой мы блуждаем в полутемных лабиринтах. Будем же надеяться, что эти сумерки являются предрассветными.

МЕЖДУНАРОДНОЕ УПРАВЛЕНИЕ ИНТЕРНЕТОМ В УСЛОВИЯХ МНОГОПОЛЯРНОГО МИРА

Зиновьева Е.С.
д.полит.н., профессор кафедры мировых политических процессов,
зам. директора ЦМИБ МГИМО МИД России

ФРАГМЕНТАЦИЯ МЕЖДУНАРОДНОГО ЦИФРОВОГО ПРОСТРАНСТВА ИНТЕРНЕТА

Фрагментация Интернета, пришедшая на смену информационной глобализации, становится новой реальностью. Протекционизм, пандемия, санкционные войны и нарастающая международная конфликтность способствуют сворачиванию процессов глобализации, как она формировалась начиная с 1980-х гг. Схожая динамика наблюдается и в информационном пространстве. Видение глобального Интернета, в котором нет государственных границ, характерное для 1990-х 2000-х гг., не оправдало себя. Один из наиболее заметных глобальных форумов в области управления киберпространством, Форум по вопросам управления Интернетом ООН в Эфиопии в 2022 году прошел под знаком обсуждения фрагментации Интернета. Эксперты выделили несколько уровней фрагментации – уровень государства, уровень технологических компаний и уровень пользователей.

Государства и региональные организации проводят практику «огораживания» и выделения национальных и региональных сегментов глобальной сети. Особенно заметным является пример Китая, где с 1996 г. ведётся политика по укреплению цифрового суверенитета, символом и практической реализацией, в которой является Великий китайский файрволл. На уровне ЕС в последние годы также активизируются инициативы, направленные на формирование технологического и цифрового суверенитета на уровне региона, ведется политика, направленная на укрепление стратегической автономии в цифровом пространстве. Важнейшей задачей на уровне государственной политики России является укрепление цифрового суверенитета страны. При этом Россия открыта к международному сотрудничеству в области управления Интернетом на равноправной основе.

Внимание к вопросам обеспечения цифрового суверенитета в Интернет-пространстве обусловлено значимостью технологий, которые не только определяют положение страны на международной арене, но и спектр доступных ей внешнеполитических возможностей. Цифровые технологии и Интернет являются важнейшим ресурсом влияния в современных международных отношениях и полем острейших геополитических противоречий, характеризующихся новым витком борьбы за глобальное лидерство в XXI веке между технологически развитыми державами (Danilin 2020), (Allison 2021). Формирование многополярного мира связано с ростом напряженности в отношениях между великими державами и цифровые технологии

становятся важнейшей ставкой в глобальной борьбе за власть в условиях многополярного мира.

Балканизация Интернета, фрагментация Интернета, «расколотый Интернет» - такие термины используются в прессе и в академической литературе для обозначения нового качества международного информационного пространства.

Однако, несмотря на набирающую силу фрагментацию Интернета, масштабы охвата цифровых технологий на сегодняшний день беспрецедентны. На конец 2021 года доступ к Интернету имело порядка 66% населения планеты[6]. Существенно возросла популярность социальных сетей –53,6% населения Земли или 4,2 млрд человек имеют аккаунты в одной или нескольких социальных сетях, что больше показателей за 2020 года на 13%. В среднем по миру, люди проводят больше времени, просматривая новости в социальных сетях, чем передачи по телевидению[7]. При этом увеличивается время, которые люди проводят в режиме онлайн. К концу 2022 года, в среднем люди проводили онлайн порядка 6,5 часов в день на различных платформах и сервисах[8]. В социальных сетях пользователи проводят порядка 2,5 часов в день, и чаще всего Интернет используются для поиска информации, чтения новостей и общения[9].

Наиболее популярными социальными сетями остаются компании, базирующиеся в США и КНР. Вообще же, согласно комплексным экспертным рейтингам, в число великих держав в глобальном цифровом пространстве входят Россия, Китай и США[10].

СОВРЕМЕННЫЙ МЕЖДУНАРОДНЫЙ РЕЖИМ УПРАВЛЕНИЯ ИНТЕРНЕТОМ: КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ

Таким образом, можно говорить о складывающейся многополярной системе в глобальном информационном пространстве. Однако, современный международный режим управления Интернетом не отражает ее ключевых характеристик. На сегодняшний день международный режим управления Интернетом характеризуется непропорциональным влиянием США. Фактически, функции управления пространством имен и адресов Интернета осуществляются частной компанией, зарегистрированной в США. В 2022 году Украина обратилась в ICANN с предложением отключить домен России от глобального Интернета. Это предложение было отвергнуто, однако показало политизированный характер современной системы управления Интернетом.

При этом на сегодняшний день проблематика управления Интернетом включает в себя более широкий круг вопросов - защита прав человека в глобальном информационном пространстве, преодоление цифрового разрыва, обеспечение информационной безопасности. Именно вопросы информационной безопасности на сегодняшний день занимают приоритетное место на глобальной повестке дня и играют важнейшую роль в международном сотрудничестве в области управления Интернетом.

В условиях, когда цифровое пространство милитаризируется и использование цифровых инструментов является неотъемлемой частью войн и конфликтов, для дипломатов и дипломатических ведомств становится важным не столько использовать социальные сети для

[6] Internet usage and population statistics. URL: https://www.internetworldstats.com/stats.htm
[7] DIGITAL 2021: GLOBAL OVERVIEW REPORT URL: https://datareportal.com/reports/digital-2021-global-overview-report
[8] Digital 2021: главная статистика по России и всему миру URL: https://exlibris.ru/news/digital-2021-glavnaya-statistika-po-rossii-i-vsemu-miru/
[9] DIGITAL 2021: GLOBAL OVERVIEW REPORT URL: https://datareportal.com/reports/digital-2021-global-overview-report
[10] https://www.belfercenter.org/publication/national-cyber-power-index-2022

донесения информации до широкой международной аудитории, сколько формировать правила, управляющие цифровым пространством как таковым. При этом важнейшей задачей выработки подобных правил является предотвращение эскалации межгосударственных противоречий в цифровом пространстве. Россия исходит из необходимости мирного развития глобальной ИКТ среды, уважения государственного суверенитета, невмешательства во внутренние дела государств и предотвращения конфликтов в ИКТ-среде (Крутских 2022). Россия выступает за передачу функций управления Интернетом на уровень международной организации, в рамках которой решения принимаются по принципу – одна страна – один голос. При этом со стороны США актуализируется запрос на формирование закрытых форматов международного сотрудничества. В частности, США выступили с инициативой Декларации за будущее Интернета[11], к которой на сегодняшний день присоединились порядка 60 стран, прежде всего, союзников США. Показательно, что Россию и КНР не пригласили к участию в данной инициативе. Руководитель недавно созданного в рамках Государственного департамента США Бюро по цифровой политике и кибер-дипломатии заявил, что нормы более эффективны для сплочения союзников, чем для сдерживания противников. Показательно, что в Стратегии кибербезопасности США от 2023 года именно Россия и Китай названы в числе основных вызовов лидерству США в цифровом пространстве[12].

В этих условиях актуализируется вопрос выработки правил в области управления Интернетом на международном уровне. Россия давно выступает в поддержку интернационализации международного управления Интернетом и передачи соответствующих функций на уровень международной организации. Важно отметить, что на современном этапе эти правила будут включать в себя не только вопросы международной информационной безопасности, но и регулирования новых перспективных технологий, в том числе Больших данных, искусственного интеллекта, машинного обучения и ряда других.

На сегодняшний день возрастает число международных инициатив, направленных на регламентацию перспективных направлений технологического развития, в том числе регулирования потоков больших данных. Показательно, что и в этой области управления Интернетом мы наблюдаем скорее конкуренцию различных подходов. Так, в 2020 году МИД КНР выступил в глобальной инициативой в области безопасности данных, в которой отмечается важность защиты персональных данных, уважения государственного суверенитета в области данных, а также центральной роли ООН в международном сотрудничестве на данном направлении[13]. Россия поддержала видение КНР. Показательно, что в настоящее время страны Запада выступают с альтернативными инициативами, стремясь оспорить регуляторную инициативу Китая на данном направлении, в числе которых Рекомендации ОЭСР в области регулирования технологий искусственного интеллекта[14] и инициатива на уровне Группы семи в области регулирования трансграничных потоков данных[15]. Схожая конкуренция проектов в области управления передовыми технологиями наблюдается и в области технологий искусственного интеллекта, регулирования 5G – сетей связи нового поколения, а также регламентации технологий Интернета вещей и других.

[11] Declaration for the Future of `Internet. USA Department of State, 2022. https://www.state.gov/declaration-for-the-future-of-the-internet
[12] https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/
[13] Глобальная инициатива в области безопасности данных МИД КНР, 2020 (на английском языке) // Global Initiative on Data Security. MFA of PRC, 08 Septemeber, 2020.
[14] Recommendation of the Council on Artificial Intelligence, 2019 OECD/LEGAL/0449
[15] Дорожная карта «Группы семи» по сотрудничеству в области свободных потоков данных и доверия. Лондон, 2021 (на английском языке) - извлечение

****

При этом важно отметить, что международная политика даже в условиях многополярности и нарастающей международной конфликтности характеризуется высокой степенью взаимозависимости, в том числе в сфере цифровой безопасности. Это диктует необходимость диалога и выработки согласованных подходов регулирования передовых цифровых технологий. Важнейшую роль в обсуждении возможных направлений международного взаимодействия в данной области призван играть Форум по вопросам управления Интернетом, в том числе в области перспективных технологий, таких как регулирование Больших данных и технологий искусственного интеллекта.

БИБЛИОГРАФИЯ

1. Бойко С.М. 2021. Политико-правовые предпосылки системы международной информационной безопасности Международные процессы. No4 (67). С. 6 -25.

2. Дробинин А. Ю. 2022. Уроки истории и образ будущего: размышления о внешней политике России. Международная жизнь. No. 8. С. 1–15.

3. Зиновьева Е. С. 2013. Цифровая дипломатия США: возможности и угрозы для международной безопасности. Индекс безопасности. Т. 19. No. 1. С. 213–228.

4. Зиновьева Е. С. 2022. Формирование цифровых границ и информационная глоба-лизация: анализ с позиций критической географии Polis: Journal of Political Studies. No. 2. DOI: 10.22363/2313-0660-2022-22-2-352-371

5. Крутских А. В. 2022. Международная информационная безопасность: в поисках консолидированных подходов. Вестник Российского университета дружбы народов. Серия: Международные отношения. Т. 22. No. 2. С. 342–351. DOI: 10.22363/2313-0660-2022-22-2-342-351

6. Allison G. et al. 2021. The Great Tech Rivalry: China vs. the US. Belfer Center.

7. Creemers R. 2020. China's conception of cyber sovereignty. Governing cyberspace: Behav-ior, power and diplomacy. P. 107-145.

8. Creemers R. 2022. China's emerging data protection framework. Journal of Cybersecurity. Vol. 8. No. 1.

9. Danilin I. V. 2022. The US-China Tech War: A Dawn of New Geopolitics? Technological Innovation and Security: The Impact on the Strategic Environment in East Asia.

10. Krutskikh A. V., Streltsov A. A., Tikk E. 2020. International information security: Prob-lems and ways of solving them. Routledge Handbook of International Cybersecurity. Routledge. P. 260–268.

ОБЗОР ИССЛЕДОВАНИЙ В ОБЛАСТИ КОРРЕЛЯЦИИ ОНЛАЙН КОНТЕНТА И ПОЛЯРИЗАЦИИ ОБЩЕСТВА

Каспарьянц Д.В.
Главный эксперт-аналитик отдела анализа и прогнозирования
Научно-технического центра ФГУП «Главный радиочастотный центр»

В современном обществе поляризация представляет серьезную угрозу социально-политической и культурной стабильности. В контексте увеличения влияния цифровой, мобильной и платформенной медиасреды поляризация затрагивает сферы управления, идеологии, культуры и идентичности. Эта тенденция усиливается распространением фейков, запрещенной информации и ведет к психоэмоциональной дестабилизации общества. Для понимания развития направлений поляризации проводятся исследования по выявлению корреляций между степенью поляризации и определенными переменными, разработке методов исследования распределения аудитории и влияния популярности контента на его достоверность.

Предлагается обзор исследований в области поляризации и перспективные направления для дальнейшего анализа и разработок методологии измерения влияния онлайн контента на поляризацию в обществе.

Исследование Кембриджского университета 2021 года **«Страновые тренды в распространении аффективной (психоэмоциональной) поляризации»**[16] посвящено выявлению тенденций в поляризации среди 12 стран ОЭСР наибольший рост наблюдается в США. В пяти странах, включая Швейцарию, Францию, Данию, Канаду и Новую Зеландию, поляризация также выросла, но в меньшей степени, чем в США. В шести государствах: Японии, Австралии, Великобритании, Норвегии, Швеции и Германии, – поляризация снизилась. В ходе исследования выявлена зависимость между расовой принадлежностью и поляризацией элиты, неравенством, долей торговли в ВВП и проникновением Интернета. Исследования продолжаются.

В США наблюдается изменение традиционных механизмов поляризации, согласно которым новостной контент влияет на формирование мнения, а потребление контента соответствует политическим взглядам. Это укрепляет существующие представления и усиливает их до

[16] https://www.nber.org/system/files/working_papers/w26669/w26669.pdf

крайних выражений. Сегодня в современном американском обществе политическая идентичность имеет скрытую роль[17]. Американцы избегают политической самоидентификации и не имеют достаточных представлений о политической идентификации своих социальных связей. Вместе с этим масштабное влияние в США имеют «информационные каскады»[18], которые являются механизмом управляемой поляризации. Это связано с распространением информации на онлайн-платформах без внимания к источникам информации. «Информационные каскады» влияют не только на изменение убеждений пользователей, но и на социальную организацию. В частности, каскады ретвитов в Twitter приводят к вспышкам подписок и отписок, что влияет на сдвиги в социальных связях.

С точки зрения политической поляризации «информационные каскады» предлагают сигналы для действий. Например, при организации забастовок бастующие наблюдают за действиями в сети и за любыми сигналами о состоянии режима[19].

Параллельно необходимо учитывать культурные, исторические и региональные особенности при структурной оценке противоречий в социальных сетях. Так, например, основные выводы исследования Лондонской школы экономической и политической науки **«Политизация культуры участия на периферии: роль классов, пола и цифровых медиа в формировании молодежных сетей в регионе MENA»**[20] относятся к усилению социального неравенства по признаку пола и социального класса на цифровых платформах и преобразования фрагментированных коллективов в гомогенные социальные движения после серьезных политических событий. При этом значение и уровень влияния сети «Интернет» на коммуникативные взаимодействия между группами и поддержание связей сильно отличается от западного и не имеет такого значения. Это связано, в том числе, с зависимостью маргинализированных групп в сети Интернет от более влиятельных лиц или групп вне сети. Таким образом, угроза поляризации в информационном пространстве в странах Ближнего Востока и Северной Африки ограничена исторически сложившимися социальными и культурными нормами, в которых физическое пространства и личное общение имеют решающее значение. Это снижает возможности западноевропейской пропаганды и увеличивает шансы на сохранение традиционных и культурных ценностей.

Статья в журнале Nature Human Behavior **«Разнообразие политической аудитории и достоверность новостного контента в алгоритмическом ранжировании»**[21], опубликованная в конце 2021 года, посвящена алгоритмическим возможностям уменьшения дезинформации и увеличения контента с высокими журналистскими стандартами. Основной тезис подчеркивает усиление предвзятости в отношении информации за счет работы рекомендательных алгоритмов.

[17] https://edisciplinas.usp.br/pluginfile.php/4676810/mod_resource/content/1/Benkler%20Network%20Propaganda.pdf
[18] Информационный каскад предполагает действия на основе наблюдения за действиями других людей.
[19] https://res.org.uk/resources-page/revolution--the-role-of---information-cascades---in-political-regime-change-.html
[20] https://www.researchgate.net/publication/335569028_Politicizing_participatory_culture_at_the_margins_The_significance_of_class_gender_and_online_media_for_the_practices_of_youth_networks_in_the_MENA_region
[21] https://www.nature.com/articles/s41562-021-01276-5.pdf

Согласно статье, существующие рекомендательные алгоритмы продвигают контент, уже завоевавший популярность. Это имеет несколько эффектов на потребление ложного и некачественного контента.

В частности, вместо анализа отдельных фрагментов контента, рекомендательные алгоритмы оценивают достоверность путем извлечения информации из достоверных источников и учитывая репутацию источников.

Однако, эти методы сложно масштабировать или они ориентированы на тип создаваемого контента. Например, методы оценки достоверности информации Википедии предполагают, что контент организован как вики. Таким образом, эти методы не могут применяться к новостному контенту.

Авторами статьи предлагается использовать уровень разнообразия в рамках одной группы аудитории. Это позволит оценить разнообразие аудитории в масштабе, так как информация о пристрастиях пользователей доступна и разнообразие является свойством аудитории, а не уровнем вовлеченности. Поэтому такая аудитория менее подвержена манипуляциям. Это может лечь в основу ранжирования социальных сетей и применяться системами рейтингования СМИ (например, NewsGuard).

Обзор исследований **«Эхо-камеры, фильтр-пузыри и поляризация»**[22] института Reuters и Оксфордского университета выявил, что эхо-камеры возникают в крайне пристрастной аудитории политического меньшинства, которая в любых обстоятельствах выберет эхо-камеры. В большинстве других случаев среди пользователей действует схема «сквозного воздействия», при которой пользователи, регулярно использующие новостной контент одного политического спектра, интересуются контентом противоположной направленности.

Наибольшее количество исследований в отношении поляризации проводится в США, что обусловлено исторически сложившейся культурой потребления и использования контента. В США поляризация на основе онлайн источников информации укрепляет внутригрупповые связи и поляризует группы других политических взглядов. Принцип «сквозного воздействия» в США может способствовать поляризации. Таким образом, в исследовании представлена сложная картина появления и распространения разных видов поляризации. Это отличает предпо-

[22] https://reutersinstitute.politics.ox.ac.uk/sites/default/files/202201/Echo_Chambers_Filter_Bubbles_and_Polarisation_A_Literature_Review.pdf

сылки и закономерности поляризации общества в США и ЕС.

Статья **«Минимизация конфликтов и поляризация в социальных сетях: исследование с использованием агентной модели»**[23] [24] предлагает исследование взаимосвязи пользователей и источников новостей в социальных сетях и поляризации. В частности, проведен анализ влияния толерантности, простоты обмена контентом, целостности источника информации и изменчивости мнения пользователя на увеличение или уменьшение политической поляризации. Результаты исследования свидетельствуют о зависимости между степенью распространения и уровнем поляризации (чем шире охват распространения, тем выше уровень поляризации); низкий уровень толерантности в обществе ведет к высокому уровню поляризации; высокий уровень скептицизма в отношении источников информации ведет появлению изолированных пользователей-экстремистов. Кроме этого, авторами предлагается анализ модели консенсуса пользователей, изменчивости и устойчивости их мнений и влияния друг на друга в социальном контексте. Авторы также полагают, что будет усиливаться тенденция платформ социальных сетей к сокращению распространения потенциально проблемного и поляризующего контента.

Авторы статьи **«Поляризация сети, фильтр-пузыри и эхо-камеры: аннотированный обзор мер, моделей и тематических исследований»**[25] предложили на основе своего обзора публикаций использовать следующие методы измерения силы поляризации: измерение гомофильности, модульности, случайных блужданий, определение характеристик контента и теории баланса.

Измерение гомофильности напрямую связано с силой поляризации сети на уровне группы или узла[26]. То есть, позволяет измерить степень связанности внутри узла, группы, сообщества.

Принцип модульности позволяет выявить и измерить степень связанности узлов внутри сообщества.

Метод случайных блужданий[27], по мнению авторов, превосходит другие методы в улавливании интуитивного понятия противоречия, которое означает поляризацию. Так, использование отношений «ретвит» и «подписка» позволяют построить граф разговоров между пользователями, которые вносят вклад в обсуждение какой-либо темы.

[23] Агентное моделирование — это метод имитационного моделирования, исследующий поведение децентрализованных агентов и роль этого поведения для системы в целом.
[24] https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0263184
[25] Гомофильность склонность к общению с похожими на нас самих людьми.
[26] https://arxiv.org/pdf/2207.13799.pdf
[27] Случайные блуждания или броуновское движение это математическая модель, которая движение, направление которого в определенные моменты времени меняется случайным образом.

Таким образом, метод случайных блужданий позволяет определить, в какой степени идея, созданная некоторым пользователем, подвергается воздействию участников с противоположной точкой зрения.

Методы квалификации контента (определение его характеристик) используют контент, опубликованный или потребляемый пользователями, включая хэштеги, ссылки и пр., для измерения полярности и идентификации группы.

Методы подписанных сетей[28] и теории баланса[29] предлагают моделирование сетей с помощью графов. Граф с двумя группами узлов, связанных внутри только положительными ребрами и отрицательными ребрами между группами, представляет собой идеально поляризованную сеть.

Перечисленные методы используются для оценки полярности отдельных узлов, групп или сетей. Большинство из них направлены на оценку силы поляризации на уровне узла или сети.

Научные коллективы в Европейском союзе и США активно развивают исследования, связанные с анализом корреляций между онлайн контентом и поляризацией общественных настроений. Цели исследований направлены на анализ текущей ситуации, выявлении тенденций, разработку методов, практических решений и инструментария для измерения поляризации в онлайн среде. В большинстве исследований делается вывод об общем снижении идеологической поляризации и возрастании аффективной (психоэмоциональной) поляризации. При этом, некоторыми авторами отмечается тенденция к усилению контроля платформами соцсетей за потенциально поляризующим контентом. В работах выявлена корреляция между контентом и диверсификацией аудитории, при этом некоторые авторы делают вывод о более сильной поляризации новостной аудитории, чем общественности в целом.

Важно, что для полноценного анализа необходим набор индикаторов качества контента. Сложность выявления зависимостей заключается в независимости популярности контента от достоверности. При этом идеологическое разнообразие аудитории контента свидетельствует о достоверности и может рассматриваться как индикатор качества.

Задачи разработок осложняются междисциплинарностью и комплексностью проблем. Для их решения требуется автоматическая обработка, поиск алгоритмических способов, количественных методов анализа, понимания социокультурных особенностей.

[28] Подписанные сети в теории социальных сетей представляют отношения между двумя узлами сети, которые характеризуются как положительная или отрицательная «дружба».
[29] Понятие баланса исходит из идеи, что в группе людей обычно соблюдаются некоторые логические правила.
Люди любят друзей своих друзей, люди ненавидят врагов своих друзей. Если социальная сеть всегда удовлетворяет эти правила, то они сбалансированы.

СПИСОК ЛИТЕРАТУРЫ

1. L. Boxell, M. Gentzkow, J. M. Shapiro. Cross-country trends in affective polarization - 2021

2. Y. Benkler, R. Faris, H. Roberts Network propaganda. Manipulation, disinformation and radicalization in American Policy – 2018 URL: https://edisciplinas.usp.br/pluginfile.php/4676810/mod_resource/content/1/Benkler%20Network%20Propaganda.pdf

3. C. J. Ellis, J. Fender. Revolution: the role of "information cascades" in political regime change – URL: https://res.org.uk/mediabriefing/revolution-the-role-of-information-cascades-in-political-regime-change/

4. S. Banajji, C. Moreno-Almeida. Politicizing participatory culture at the margins: the significance of glass, gender and online media for the practices of youth networks in the MENA region //Global Media and Communications. 2019 URL: https://researchgate.net/publication/335569028_Politicizing_participatory_culture_at_the_margins_The_significance_of_class_gender_and_online_media_for_the_practices_of_youth_networks_in_the_MENA_region/link/5d6db86da6fdcc547d758dd4/download

5. S. Bhadani, S. Yamaya, A. Flammini, F. Menczer, G. L. Ciampaglia, B. Nyhan. Political audience diversity and news reliability in algorithmic ranking // Nature. – 2022 –URL: https:// nature.com/articles/s41562-021-01276-5.pdf

6. A. R. Arguedas, C. T. Robertson, R. Fletcher, R. K. Nielsen. Echo Chambers, Filter Bubbles, and Polarization: a Literature Review – URL: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/202201/Echo_Chambers_Filter_Bubbles_and_Polarisation_A_Literature_Review.pdf

7. How minimizing conflicts could lead to polarization on social media: an agent-based model investigation – URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0263184

8. Network polarization, filter bubbles, and echo chambers: An annotated review of measures and reduction methods – URL: https://arxiv.org/pdf/2207.13799.pdf

ФРАГМЕНТАЦИЯ ИНТЕРНЕТА. ХРОНИКА ОБЪЯВЛЕННОЙ СМЕРТИ

Ерохин В.В.
Российский научно-исследовательский институт радио имени М.И. Кривошеева
(ФГБУ НИИ Радио)

Данная статья не представляет собой глубокий, методологически выверенный анализ причин, движущих сил, различных аспектов процесса фрагментации Интернета. Скорее это зарисовки, комментарии, заметки с полей конференций и международных площадок человека, который последние несколько лет был вовлечен в дискуссии о различных аспектах системы управления Интернетом. Надеюсь, что они будут полезны тем, у кого не хватает времени или возможности отслеживать многочисленные международные дискуссии, а главное, с учётом некоторой ретроспективы и понимания сегодняшних позиций сторон, можно будет сделать предположение как ситуация будет развиваться в будущем.

Сейчас очень популярны выступления о фрагментации Интернета. Причем очень часто звучит один тезис: «Интернет всегда был фрагментирован». Далее я еще дам оценку этой сегодняшней позиции, а пока посмотрим на то, как развивалась дискуссия о фрагментации Интернета в последние несколько лет. Еще десять лет назад о фрагментации Интернета практически никто не говорил, хотя Интернет и тогда был в значительной степени фрагментирован. Однако «фрагментация» «фрагментации» рознь. Самым значимым примером фрагментации можно было бы назвать внедрение IPv6. Кроме того, в те далекие годы, какие-то контентные сервисы не предоставляли услуги на определенных территориях. Интернет-магазины, вспомним знаменитый eBay, не принимали платежи, не доставляли товары в ряд стран и территорий. Но вся эта фрагментация, была не просто понятна и осознанна, но все ожидали какого-то счастливого финала. Всеобщей и окончательной победы IPv6, работы оборудования только с одной версией протокола, решения проблем с пиратством и создания цивилизованного рынка и, соответственно, безграничного распространения контента и т.д. и т.п. Все это считалась естественными процессами и вызовами роста, развития и эволюции Интернета, и никто не бил особую тревогу по поводу такой фрагментации. В то время «на слуху» были совсем другие темы: кибербуллинг, персональные данные, фейковые новости, и общественные манипуляции (ох, уж эта

Cambridge Analytica). Споров, дискуссий по этим вопросам было много, а решений и принятых регуляторных актов нет.

Но есть фрагментация, являющаяся следствием политических процессов, следствием национального регулирования. И она тоже «понятна и осознанна» – регулировать правоотношения в Интернете, несомненно, нужно, но вот насчет счастливого финала, есть большие вопросы. Но так как в то время национальное целевое регулирование правоотношений в Интернет было развито слабо о «политической фрагментации» или «регуляторной фрагментации» практически никто не говорил. Однако об угрозе политической фрагментации неустанно заявляла Российская Федерация, и не потому, что российские эксперты обладали особым даром предвидения, а потому что практически с самого начала представители России в международных организациях отмечали, что в Интернете отсутствует сбалансированная, нейтральная система управления и международной координации деятельности отдельных государств, и это серьезная угроза целостности и безопасности Интернета. Во многом эти усилия и российские призывы не воспринимались всерьез, а зря.

Начав с аспектов и вызовов, которые были актуальны на тот момент, национальные регуляторы все больше и больше втягивались в тематику установления норм и правил для экосистемы Интернета. И вот, «внезапно» выяснилось, что в десятках, а то и сотнях юрисдикций существуют совершенно не гармонизированные и достаточно жесткие требования, относящиеся к регулированию различных сторон жизнедеятельности экосистемы Интернета.

И вот тут-то о регуляторной фрагментации кроме российских экспертов на международных площадках начали говорить многие. Необходимо подчеркнуть, что отношение к вопросу фрагментации Интернета, звучавшее во многих выступлениях ряда участников, за последние год-два сильно поменялось. Если в ходе международных форумов недавнего прошлого понятие «цифровой суверенитет», «суверенитет», «государственное регулирование Интернета» звучали исключительно в негативном ключе, и утверждалось что эти инициативы неприемлемы для глобального и трансграничного Интернета, то в ходе последних конференций тон выступлений поменялся. Теперь уже регулирование Интернета воспринимается как совершенно правильные инициативы, «законное право государств». При этом, выступавшие «внезапно» вспомнили, как уже упоминалось выше, что Интернет всегда был фрагментированным: применялись проприетарные протоколы, кодеки, алгоритмы шифрования и т.д.; сайты и раньше ограничивали доступ пользователей, как и госорганы доступ к сайтам (например, пиратским, еще с прошлого века).

Например, в отличие от ФУИ 2021, где активно обсуждался вопрос «цифрового суверенитета» скорее с негативным оттенком (как недопустимая инициатива, приводящая к фрагментации глобальной сети), на ФУИ 2022 большинство участников говорило о «суверенитете» как базовом принципе организации государства и праве государств на регулирование правоотношений как в общественной жизни, так и во всех индустриях и, включая в том числе и Интернет. В целом эволюция взглядов многих заинтересованных сторон на «регуляторную фрагментацию» укладывается в известную модель «отрицание – гнев – торг – депрессия – принятие». Похоже, что сейчас мы на этапе «торга», неизбежность регуляторной фрагментации уже не отрицается, но идет «торг» насколько жесткой она будет, обсуждается «правильная» и «неправильная» регуляторная фрагментация. А стоило бы смотреть хотя бы на два шага вперед, ибо в перспективе все эти глубокие дискуссии без реальных дел приведут к распаду глобальной сети и растаскиванию Интернета по национальным сегментам.

Причем с позицией, что национальное регулирование в Интернете процесс правильный нельзя не согласиться, но наши оппоненты постоянно умалчивают об одном - о том, что национальное регулирование должно быть гармонизировано на международном уровне.

И основной вызов «регуляторной фрагментации» в том, что, в отличии, например, от «технической фрагментации» (вспомним пример IPv6, который в отдаленном будущем должен прийти к победе одного протокола и полной совместимости и упрощению сети) для нее не просматривается «хеппи-энд» в текущей ситуации. Международную координации часть заинтересованных сторон отвергает, а национальное регулирование остановить и нельзя, да и не нужно, так как это правильный, легитимный процесс. Хотя глобальная и взаимосвязанная природа Интернета, а также появление информационного общества требуют и координации, и регулирования посредством международного права.

Так как статья все же описательная и не претендующая на глубокое научное исследование, то не буду анализировать, как такая система работает в других областях и индустриях, какие условиях и нормы могут быть заложены в ее основу. Просто приведу наглядный пример, как мне кажется, он очень хорошо показывает то, как ради общественного блага и интересов глобального рынка может работать международное сотрудничество и координация национального регулирования.

В марте промелькнула новость[30] о том, что российский Минтранс обязал российские авиакомпании изменить размещение опознавательных знаков самолетов к осени текущего года. Авиаперевозки далеки от Интернета, но аналогии есть – такая же трансграничная, глобальная индустрия. Итак, российские авиакомпании должны изменить расположение опознавательных знаков самолетов, что следует из приказа Минтранса, так как необходимо привести маркировку авиатехники российских перевозчиков в соответствие с требованиями Международной организации гражданской авиации (ICAO). Согласно им государственный и регистрационный номера должны быть нанесены на левой нижней части крыла самолета. То есть существует координирующая организация ICAO, государства добровольно принимают на себя обязательства следовать ее рекомендациям, которые, кстати, юридически не обязательны к исполнению, ради сохранения единой, глобальной индустрии авиаперевозок. А теперь представьте, что в каждой стране принимали решение о формате этих знаков независимо. И на одних самолетах опознавательные знаки были бы латиницей, у нас с кириллицей, где-то с арабской вязью, а наследники Римской империи решили бы применить римские цифры. А что, суверенитет! Ничего не напоминает, если посмотреть на Интернет? В Интернете на сегодня нет, не только координирующей организации такого формата, но и даже дискуссии о том, как можно разработать международные нормы и гармонизировать национальное законодательство. К сожалению, российские призывы сохранить Интернет единым, наладить международное сотрудничество и координацию, не применять двойные стандарты поддерживаются далеко не всеми заинтересованными сторонами.

В свете последних геополитических вызовов и отражения политического противостояния на экосистему Интернета тема фрагментации сети стала не просто одной из ключевых тем на международных площадках, но и, несомненно, вообще самой «горячей» темой сообщества Интернета. Сейчас речь идет не просто о фрагментации Интернета, но о контрреволюции против глобализации и цифровой экономики. С одной стороны, есть невероятная техническая база, которая была создана на глобальной основе взаимоувязанных Интернет-протоколов и уникальных идентификаторов цифровых ресурсов, и есть интегрированный рынок программного обеспечения и цифровых устройств, и эта глобальная совместимость привела к глобальному разделению труда в ИКТ и глобальной цифровой экономике.

[30] https://www.rbc.ru/business/12/03/2023/640b13e19a79478f25caa573

И до сих пор это способствовало развитию свободной и открытой бизнес среды ориентированной на обмен информацией, продуктами и услугами. Таким образом, дебаты о регуляторной фрагментации сводятся к вопросу: хотим ли мы продолжать способствовать работе и развитию глобальной цифровой экономики, конкуренции и инновациям, обеспечиваемым этой глобальной совместимостью, или мы хотим сегментированного Интернета, работающего по принципу «best efforts», когда непонятно дойдёт ли твой e-mail до адресата в другой стране?

Кроме того, есть совершенно законные опасения по поводу других форм фрагментации, которые в большей степени являются продуктами рыночной конкуренции – запуском закрытых цифровых продуктов, коммерческими ограничениями. Это тоже форма фрагментации, но не настолько тупиковая, как мне представляется.

К сожалению, в ходе многих представительных и глубоких дискуссии с участием признанных экспертов в вопросах управления Интернетом практически не звучит реалистичных предложений не только о том какие механизмы и средства можно использовать для предотвращения регуляторной фрагментации, но даже о том, как в принципе можно выстроить дискуссию по этим вопросам. Снова в авангарде защитников единой глобальной сети представители России, стран БРИКС, с предложениями рассмотреть вопросы международной координации на площадках ООН: ФУИ, МСЭ или других платформах и форумах. Увы, пока полного понимания у всех заинтересованных сторон эти призывы не находят.

И здесь возникает закономерный вопрос, если с фрагментацией не все так очевидно, то уж как минимум видны основные ее аспекты, почему же не договориться на международном уровне о скоординированных усилиях по сохранению единства Интернета, по созданию системы управления Интернетом, которая не будет обусловлена какими-либо односторонними политическими ограничениями или коммерческими интересами по международной координации. Почему не создать демократическую систему управления глобальной критической инфраструктурой/публичным ядром, которая была бы равноправной, нейтральной, равноудалённой от всех государств и неподверженной геополитическим вызовам? Я не хочу спекулировать, и строить какие-то догадки, почему же часть

вовлеченных и в управление Интернетом, и в дискуссии об этом управлении заинтересованных сторон предпочитает оправдывать «расходящийся» процесс регуляторной фрагментации Интернета и не слышать российских предложений. В кулуарных разговорах, которые у меня были, они обычно уходят от ответов. Могу лишь высказать собственное мнение и собственную оценку. До сих пор при всех недостатках и порожденных проблемах фрагментация не достигла каких-то катастрофических масштабов. Несмотря на все негативные последствия частичной фрагментации, этим акторам важно сохранить контроль пусть за фрагментированным, частично «лоскутным», потерявшим какие-то сегменты, ресурсы, где-то заблокированным, с «костылями» и «заплатками» Интернетом. Или как сказал мне один зарубежный коллега: «Сейчас можно отправить e-mail из Москвы в Париж? Можно! Так что не все так страшно, нет никакой серьезной фрагментации».

Не слишком оптимистичная картина вырисовывается на сегодняшний день, но что же можно сделать даже в такой ситуации? Часть экспертов, принимая и понимая необходимость национальных регуляторных норм в экосистеме Интернета, предлагает разделять технические средства Интернета (прежде всего публичное ядро) и собственно приложения и сервисы, которые являются надстройкой, и при этом сохранить единство ядра, одновременно оставив право на регулирование приложений государствам/платформам/общественным силам. Это как минимум, разумный и реализуемый подход. Кроме того, необходимо бороться за то, чтобы необходимость сотрудничества всех заинтересованных сторон в процессе разработки массива норм, регулирующих информационные отношения в экосистеме Интернет, была признана большинством заинтересованных сторон и закреплена в ряде международных документов. И здесь хотелось бы видеть участие самых широких слоев российского Интернет-сообщества на международных площадках.

Работа по формированию системы глобального управления и регулирования киберпространства ведется с середины 1990-х годов, и как любые глобальные процессы – это путь и длительный, и тернистый, но важно не опускать руки, союзники у нас есть. Здравый смысл победит, он победил в других индустриях, он победит и в индустрии ИКТ и Интернета.

ДОСТИЖЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ В ТЕХНИЧЕСКОМ РЕГУЛИРОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КЛИНИЧЕСКОЙ МЕДИЦИНЕ

Васильев Ю.А.,
к.м.н., Государственное бюджетное учреждение здравоохранения города Москвы «Научно-практический клинический центр диагностики и телемедицинских технологий Департамента здравоохранения города Москвы», ORCID ID: 0000-0002-0208-5218

Владзимирский А.В.,
д.м.н., Государственное бюджетное учреждение здравоохранения города Москвы «Научно-практический клинический центр диагностики и телемедицинских технологий Департамента здравоохранения города Москвы», ORCID ID: 0000-0002-2990-7736

Шарова Д.Е.,
Государственное бюджетное учреждение здравоохранения города Москвы «Научно-практический клинический центр диагностики и телемедицинских технологий Департамента здравоохранения города Москвы», ORCID ID: 0000-0001-5792-3912

Ахмад Е.С.,
Государственное бюджетное учреждение здравоохранения города Москвы «Научно-практический клинический центр диагностики и телемедицинских технологий Департамента здравоохранения города Москвы», ORCID ID: 0000-0002-8235-936

Зинченко В.В.,
Государственное бюджетное учреждение здравоохранения города Москвы «Научно-практический клинический центр диагностики и телемедицинских технологий Департамента здравоохранения города Москвы», ORCID ID: 0000-0002-2307-725X

Гарбук С.В.,
к.т.н., Национальный исследовательский университет «Высшая школа экономики», ORCID ID: 0000-0001-5385-3961

Аннотация. В России активно развивается техническое регулирование медицинского искусственного интеллекта. В 2023 году вступили в действие десять национальных стандартов серии ГОСТ Р 59921, которые регулируют ключевые аспекты разработки и эксплуатации систем искусственного интеллекта в здравоохранении. В статье рассказано о первых шагах и текущем состоянии технического регулирования.

Ключевые слова: стандартизация; искусственный интеллект в медицине; медицинское изделие на основе технологий искусственного интеллекта.

АКТУАЛЬНОСТЬ ТЕМЫ

В последние годы развитие рынка цифрового здравоохранения достигло значительного роста (1). Инвестиции в здравоохранение выросли на всех континентах (2). Технологии ИИ уже стали эффективным помощником врача в диагностике различных заболеваний (3).

Вместе с тем, нерешенными остаются аспекты, мешающие широкому распространению СИИ в здравоохранении. На данный момент нет требований к полноте и прозрачности документации СИИ, контролируемым параметрам, а также к методам испытаний и требованиям контроля СИИ в процессе эксплуатации. Это создает серьезные риск для безопасности и качества медицинской помощи с использованием СИИ, в случае недобросовестности участников рынка. Кроме того, важным является защита персональных данных пациентов. Наибольшей проблемой широкого внедрения СИИ является вопрос доверия к ним врачей и пациентов. В связи с этим для обеспечения качества и безопасности данных инновационных технологий СИИ было принято решение распространить на СИИ повышенные требования, отнеся их к максимальному классу риска. Таким образом, контрольно-надзорные мероприятия должны быть выстроены с учетом всех особенностей и проблематик данного направления (4).

Опыт РФ в развитии нормативно-правовой базы для СИИ является передовым, т.к. на текущий момент ни один из зарубежных регулирующих органов не имеет системы контроля качества и достаточного опыта работы в области технологий ИИ (5). Все ведущие страны и международные организации ограничились принятием национальных стратегических документов развития ИИ и так называемых кодексов «этики искусственного интеллекта».

В РФ, одной из целей «Национальной стратегии развития искусственного интеллекта на период до 2030 года» (Указ Президента Российской Федерации № 490) является создание комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий искусственного интеллекта.

Особый приоритет отдан развитию ИИ в здравоохранении. Для реализации данного направления в сфере здравоохранения должно быть налажено мультидисциплинарное и межотраслевое взаимодействие: необходимо создать единое пространство для организаторов здравоохранения, врачей, индустрии (разработчиков СИИ), пациентов. Фундаментом такого взаимодействия могут быть национальные стандарты, созданные на научно-обоснованной базе (6).

Для выполнения указанной стратегии была утверждена Перспективная программа стандартизации по приоритетному направлению «Искусственный интеллект» на период 2021-2024 годы. В июле 2019 года был создан технический комитет по стандартизации «Искусственный интеллект» (ТК164), который включает в свой состав подкомитет ПК01 «Искусственный интеллект в здравоохранении[31]. Данная структура занимается унификацией и стандартизацией требований, используемых при разработке, тестировании и эксплуатации СИИ в здравоохранении.

В ближайшее время рассмотрен план разработки стандартов в области здравоохранения следующих типов:

- стандарты, устанавливающие требования к процессам внешнего проектирования СИИ (обоснование тактико-технических требований и предусмотренных условий эксплуатации СИИ, обеспечение информационного сопряжения с другими медицинскими информационными системами);
- квалиметрические стандарты, учитывающие особенности оценивания функциональных характеристик и характеристик социальной приемлемости медицинских информационных систем на основе плохо интерпретируемых алгоритмов;
- стандарты, устанавливающие единые подходы к оцениванию функциональных возможностей (компетенций) специалиста-врача при решении типовых прикладных задач ИИ;
- стандарты в области унификации терминологии, данных и программного обеспечения, используемых в СИИ, определяющие стадии жизненного цикла систем, универсальные принципы организации работ при создании и эксплуатации медицинских СИИ;
- стандарты в области защиты информации.
- квалиметрические стандарты и стандарты по оцениванию функциональных возможностей специалистов-врачей

[31] Подкомитет “Искусственный интеллект в здравоохранении” (ПК 01/ТК164), https://mosmed.ai/pk-01/

могут включать фрагменты демонстрационных наборов данных, описания тестовых сценариев и другие данные, иллюстрирующие особенности тестирования СИИ и оценивания функциональных способностей специалистов с учетом вариативности внешних условий, в которых предполагается решать соответствующие прикладные задачи ИИ на практике (существенных факторов эксплуатации).

НАУЧНО ОБОСНОВАННАЯ СТАНДАРТИЗАЦИЯ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

В течение 2020-2023 гг. в РФ проводится крупнейшее в мире перспективное многоцентровое клиническое исследование применимости и значимости технологий искусственного интеллекта в лучевой диагностике (https://mosmed.ai/). В исследовании принимают участие 90% российских разработчиков СИИ для сферы здравоохранения, в условиях реально функционирующих государственных информационных систем в сфере здравоохранения работают свыше 60 отдельных алгоритмов ИИ. Данный проект выступил площадкой для разработки и апробирования многих подходов и методологий в области лучевой диагностики, которое ложится в основу разрабатываемых стандартов [7]. пациентов. Кроме того, в процессе разработки стандартов проводилось активное изучение мирового опыта и процессов, что позволило структурировать вопросы разработки, оценки, регулирования и контроля безопасности СИИ, а также обеспечить возможность применения стандартов (в соответствии с предусмотренными процедурами) в иных странах и экономических содружествах.

В соответствии с планом работы ТК164 в 2020-2022 гг. были разработаны основополагающие стандарты, регулирующие общие требования к СИИ в здравоохранении. В план перспективной работы ПК01/ТК164 заложена разработка национальных стандартов для более узких областей медицины: лучевой и функциональной диагностики, гистологии, систем дистанционного мониторинга, систем поддержки принятия врачебного решения, обработки больших данных, реконструкции изображений, аналитики и прогнозирования, а также образовательных программ в здравоохранении.

В 2020-2022 гг. группа специалистов под эгидой ПК01 «Искусственный интеллект в здравоохранении» разработала серию стандартов, регулирующих требования к системам искусственного интеллекта в здравоохранении.

Разработанные группой специалистов ГБУЗ «НПКЦ ДиТ ДЗМ» под эгидой ПК01 «Искусственный интеллект в здравоохранении» национальные стандарты, регулирующие требования к СИИ в здравоохранении, являются полностью оригинальными, основанными на объективных научных данных. Данная разработка не имеет аналогов в мире. Имеют социально-ориентированный характер, так как в них заложен приоритет благополучия человека (безопасность и качество медицинской помощи каждому пациенту).

Внедрение указанных стандартов в практику позволит минимизировать риски применения СИИ, создаст преимущества для игроков рынка искусственного интеллекта, позволив повысить качество и конкурентоспособность производителей, применяющих стандарты. А также пользователи (врачи и медицинские организации) смогут использовать установленные в стандартах требования для оценки качества СИИ (8).

Разработанная и вступившая в силу серия стандартов охватывает часть процессов жизненного цикла СИИ и устанавливает требования к основным положениям, порядку проведения технических и клинических испытаний данных изделий, а также требования к оценке и контролю эксплуатационных параметров (9). Это имеет особую важность в условиях постоянно возникающих вызовов в сфере здравоохранения, а также общего развития IT технологий (10).

Данная серия стандартов имеет важную экономическую роль – они становятся катализаторами инновационной деятельности. Стандарты создают условия для разработки инновационных продуктов и облегчают их выход на рынки, способствуя распространению среди целевой аудитории. Опыт Российской Федерации в сфере разработки и утверждения данных основополагающих стандартов можно признать передовым. Новые национальные стандарты призваны регулировать ключевые аспекты применения искусственного интеллекта в здравоохранении и его роли в принятии врачебных решений.

Таким образом, в РФ разработана серия национальных стандартов, регулирующих применение СИИ в здравоохранении и отличающихся: оригинальностью, научной обоснованностью, социально-ориентированным характером. Разработанные документы обеспечивают требования Национальной стратегии развития ИИ в части создания условий для эффективного взаимодействия государства, организаций (медицинских, научных), ИТ-индустрии и граждан в сфере развития искусственного интеллекта в здравоохранении. В ближайшей перспективе это позволит российским технологиям ИИ выйти на мировой рынка.

СПИСОК ЛИТЕРАТУРЫ

1. Гусев А.В., Добриднюк С.Л. Искусственный интеллект в медицине и здравоохранении. Информационное общество. 2017; 4-5: 78-93.

2. Young A. S., AI in healthcare startups and special challenges, Intelligence-Based Medicine, 2022. Vol. 6, 100050, https://doi.org/10.1016/j.ibmed.2022.100050

3. Гусев А.В., Владзимирский А.В., Шарова Д.Е., и др. Развитие исследований и разработок в сфере технологий искусственного интеллекта для здравоохранения в Российской Федерации: итоги 2021 года // Digital Diagnostics. - 2022. - Т. 3. - №3. - С. 178-194. doi: 10.17816/DD107367

4. Canadian Association of Radiologists White Paper on Ethical and Legal Issues Related to Artificial Intelligence in Radiology / J.L. Jaremko [et al.] // Can Assoc Radiol J. Can Assoc Radiol J. 2019. Vol. 70. № 2. P. 107–118. https://doi.org/10.1016/j.carj.2019.03.001.

5. Кобринский Б.А. Искусственный интеллект в медицине: состояние и горячие точки // Девятнадцатая Национальная конференция по искусственному интеллекту с международным участием КИИ-2021 (11-16 окт. 2021 г.): Тр. конф. / под ред. В.В. Борисова, Б.А. Кобринского. – Ростов-на-Дону; Таганрог: Изд-во Южного федерального ун-та, 2021. – С.13-29

6. Морозов С.П., Зинченко В.В., Хоружая А.Н., и др. Стандартизация искусственного интеллекта в здравоохранении: Россия выходит в лидеры, Врач и информационные технологии. 2021. № 2. С. 12-19.

7. Морозов С.П., Владзимирский А.В., Шулькин И.М. и др. Целесообразность применения технологий искусственного интеллекта в лучевой диагностике (результаты первого года московского эксперимента по компьютерному зрению). Врач и информационные технологии. 2022. № 1. С. 12-29.

8. Зинченко В.В., Хоружая А.Н., Шарова Д.Е., и др. Стандартизация в области регулирования технологий искусственного интеллекта в российском здравоохранении. Казанский медицинский журнал. 2021. Т. 102. № 6. С. 923-933.

9. Морозов С.П., Владзимирский А.В., Шарова Д.Е., Ахмад Е.С., Зинченко В.В. Первые национальные стандарты Российской Федерации на системы искусственного интеллекта в медицине. Менеджмент качества в медицине. 2022 (1):58-62

10. Asadzadeh A, Mohammadzadeh Z, Fathifar Z, et al. A framework for information technology-based management against COVID-19 in Iran. BMC Public Health. 2022 Feb 26;22(1):402. doi: 10.1186/s12889-022-12781-1.

ПРАВОВЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ДИПФЕЙК

Крымская К.В.
к.ю.н., Главный юрист-эксперт, АНО «Институт развития Интернета»,
преподаватель кафедры международного права, Московский государственный институт международных отношений (Университет) МИД России

«Глубокие подделки», также известные как дипфейки (англ. deepfakes) – это искусственно смоделированный контент, который, хотя и выглядит достоверным на первый взгляд, способствует распространению недостоверной информации и может привести к нарушению права на неприкосновенность частной жизни.

Дипфейки имеют широкое применение – от индустрии развлечений до сектора здравоохранения. Например, в здравоохранении они используются для обнаружения опухолей.[32]

В 2019 году Всемирная организация интеллектуальной собственности (ВОИС) опубликовала «Проект документа по вопросам политики в области интеллектуальной собственности и искусственного интеллекта»[33].

С точки зрения прав интеллектуальной собственности документ рассматривает два вопроса:

1) кому принадлежит авторское право на дипфейк, если он создается на основе данных, которые являются объектами авторского права;

2) должно ли выплачиваться вознаграждение лицам, чьи образы используются в дипфейках.

Однако дипфейки могут вызвать более серьезные проблемы, чем нарушения авторских прав, например: нарушение прав человека, права на неприкосновенность частной жизни, права на защиту персональных данных и пр.

Сегодня и государства, и BigTech-компании предпринимают меры по борьбе с дипфейками.

Так, например, Facebook совместно с Microsoft и Amazon Web Services провел конкурс (Deepfake Detection Challenge) на лучший алгоритм по выявлению глубоких подделок [34].

[32] J. Snow. Deepfakes for good: Why researchers are using AI to fake health data. URL: https://www.fastcompany.com/90240746/deepfakes-for-good-why-researchers-are-using-ai-for-synthetic-health-data (дата обращения: 1 марта 2023 г.)
[33] WIPO/IP/AI/2/GE/20/1. Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence. URL: Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence (wipo.int) (дата обращения: 1 марта 2023 г.)
[34] Deepfake Detection Challenge Results: An open initiative to advance AI. URL: https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ (дата обращений: 1 марта 2023 г.)

Согласно политике Twitter, для борьбы с дипфейками используется набор из четырех правил:

1) идентификация с помощью уведомляющих твитов,
2) предупреждение о смоделированном контенте перед его распространением,
3) включение ссылки на подлинные новостные статьи, объясняющие манипуляцию контентом, и
4) удаление материалов[35].

Борьбу с дипфейками также ведут такие медиа-организации как: The Wall Street Journal, The Washington Post и Reuters[36]. В Wall Street Journal работает подразделение из журналистов, задача которых – борьба с дезинформацией, в частности с дипфейками[37]. В штате The Washington Post работают видео-эксперты, проверяющие контент на достоверность[38]. Новостное агентство Reuters использует сотрудничает с Facebook для выявления фейков и ведет блог, посвященный их развенчанию [39].

Что касается законодательного регулирования, стоит обратить внимание на релевантный опыт США, ЕС и Китая.

С 2019 года на рассмотрении в Конгрессе США находится проект федерального закона, касающийся дипфейков – Deep Fakes Accountability Act.[40] Данный законопроект устанавливает требования к технологиям, создающим дипфейки, и требует, чтобы производители дипфейков соблюдали требования по раскрытию информации (например, устные и письменные заявления о том, что контент является смоделированным). Также устанавливаются новые составы преступлений, за которые предусмотрена уголовная ответственность. Кроме того, физические лица, чьи права были затронуты тем или иным дипфейк-контентом, вправе подавать иски о возмещении ущерба.

Помимо этого, действуют соответствующие законы на уровне штатов. Вирджиния стала первым штатом в стране, где было введено уголовное наказание за распространение дипфейк-контента порнографического содержания без согласия лица. Закон, вступивший в силу 1 июля 2019 года, квалифицирует распространение ложно созданных откровенных изображений и видеороликов без согласия как правонарушение, которое наказывается тюремным заключением сроком до года и штрафом в размере 2 500 долларов США [41].

Техас стал первым штатом, запретившим создание и распространение дипфейк-видео, призванных нанести вред кандидатам на государственные должности или повлиять на выборы[42].

[35] Synthetic and manipulated media policy. URL: https://help.twitter.com/en/rules-and-policies/manipulated-media (дата обращения: 5 марта 2023 г.)
[36] Vizoso, Á., Vaz-Álvarez, M., & López-García, X. (2021). Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation. Media and Communication, 9(1). P. 295. doi:https://doi.org/10.17645/mac.v9i1.3494
[37] Там же.
[38] Там же.
[39] Reuters Fact Check
[40] H.R.3230 - Deep Fakes Accountability Act, 2019. URL: https://www.congress.gov/bill/116th-congress/house-bill/3230/text (дата обращения: 5 марта 2023 г.)
[41] Code of Virginia. § 18.2-386.2. Unlawful dissemination or sale of images of another; penalty. URL: https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/ дата обращения: 5 марта 2023 г.)
[42] S.B. No. 751. An Act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election, 2019. URL: https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm (дата обращения: 5 марта 2023 г.)

Закон Техаса определяет дипфейк-видео как «видео, созданное с намерением обмануть, которое, как представляется, изображает реального человека, совершающего действие, которого не было в действительности». Создание, распространение и публикация такого видео в течение 30 дней после выборов, если это делается с намерением нанести вред кандидату или повлиять на результат выборов, наказывается тюремным заключением до года и штрафом в размере 4 000 долларов США.

В октябре 2019 года в Калифорнии были приняты два закона. Первый аналогично закону штата Вирджиния позволяет жертвам подавать иски о возмещении ущерба в связи с созданием и распространением дипфейк-контента порнографического содержания без согласия лица.[43]

Второй закон, как и в Техасе, наделяет кандидатов на государственные должности правом подавать иски против лиц или организаций, которые намеренно распространяют связанные с предстоящими выборами дипфейки без предупреждающих надписей[44].

В ЕС вопросам регулирования дипфейков уделено внимание в проекте регламента по искусственному интеллекту, который обязывает раскрывать информацию о том, что контент был искусственно смоделирован, и определяет дипфейк как изображение, аудио- или видеоконтент, который в значительной степени напоминает существующих людей, предметы, места или другие субъекты или события и может обманчиво показаться человеку подлинным или правдивым[45].

Помимо предлагаемого регулирования на базе Европейской Комиссии в 2022 году был подписан Практический кодекс по дезинформации[46]. Кодекс подписан 34 участниками рынка, в числе которых Adobe, Google, Meta (запрещена в России), Microsoft, TikTok, Twitch, Twitter, Vimeo.

Стороны, подписавшие Кодекс, обязались предпринять действия в нескольких областях, таких как: «демонетизация» распространения дезинформации; обеспечение прозрачности политической рекламы; расширение прав и возможностей пользователей; укрепление сотрудничества с организациями по проверке фактов; предоставление исследователям лучшего доступа к данным. Подписавшие стороны создадут Центр прозрачности, предоставляющий общественности четкий обзор политики, которую они проводят для выполнения своих обязательств, и будут регулярно обновлять его соответствующими данными.

Администрация киберпространства КНР опубликовала правила работы дипфейк-сервисов в Интернете[47], которыми вводится

[43] Assembly Bill No. 602. Depiction of individual using digital or electronic technology: sexually explicit material: cause of action. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602 (дата обращения: 5 марта 2023 г.)
[44] Assembly Bill No. 730. An act to amend, repeal, and add Section 35 of the Code of Civil Procedure, and to amend, add, and repeal Section 20010 of the Elections Code, relating to elections. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 (дата обращения: 5 марта 2023 г.)
[45] Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. URL: https://artificialintelligenceact.eu/the-act/ (дата обращения: 5 марта 2023 г.)
[46] The 2022 Code of Practice on Disinformation. URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (дата обращения: 5 марта 2023 г.)
[47] URL: http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (дата обращения: 5 марта 2023 г.)

запрет на использование «дипфейков» для распространения запрещённой или недостоверной информации или участия в противозаконной деятельности.

Правила комплексно регулируют программное обеспечение для генерации изображений, аудио и текста с помощью искусственного интеллекта, которое создает дипфейки, а также требуют нанесения заметной маркировки синтетически созданных или отредактированных изображений, видео или текста, которые могут восприниматься как настоящие или подлинные.

Поставщики услуг по генерации дипфейк-контента должны будут публиковать правила работы таких сервисов, идентифицировать пользователей, а также реализовать функционал, необходимый для выявления противоправного контента. Кроме того, поставщики услуг по генерации дипфейк-контента должны создать механизм опровержения слухов. Отмечается, что данный механизм необходим в случае распространения недостоверной информации с помощью технологии дипфейк.

Если поставщик предоставляет функции редактирования лиц и голос, именно поставщик услуг будет ответственен за информирование «редактируемого» человека и получение от него согласия на такое редактирование лица или голоса.

****

В целом, наибольшую угрозу представляет распространение дипфейков на площадках социальных сетей.

Устранить эти риски позволит определение отраслевых правил противодействия использованию дипфейков в противоправных целях. Для начала, такие правила могут быть оформлены в виде стандартов саморегулирования по аналогии с европейским Кодексом по дезинформации.

Разработка таких правил представляется целесообразной на базе ЮНЕСКО, как универсальной международной организации (а также специализированного учреждения ООН), которая, помимо прочего, занимается вопросами искусственного интеллекта в контексте защиты прав человека.

В таких правилах (стандартах) может быть рекомендовано, например,

1) выявление и маркировка дипфейк-контента (по аналогии с китайским опытом),
2) введение ограничительных меры,
3) получение согласия лица на использование его изображения при создании дипфейк-контента (согласия в целом, а не только при создании дипфейков порнографического содержания, как это предусмотрено законами штатов в США).

При успешном применении такого подхода его можно будет закрепить уже на уровне национального законодательства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Законодательные и иные нормативные акты иностранных государств:

1. H.R.3230 – Deep Fakes Accountability Act, 2019. [Электронный ресурс] URL: https://www.congress.gov/bill/116th-congress/house-bill/3230/text (дата обращения: 5 марта 2023 г.)

2. Code of Virginia. § 18.2-386.2. Unlawful dissemination or sale of images of another; penalty. [Электронный ресурс] URL: https://law.lis.virginia.gov/vacode/title18.2/chapter8/section18.2-386.2/ (дата обращения: 5 марта 2023 г.)

3. S.B. No. 751. An Act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election, 2019. [Электронный ресурс] URL: https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm (дата обращения: 5 марта 2023 г.)

4. Assembly Bill No. 602. Depiction of individual using digital or electronic technology: sexually explicit material: cause of action. [Электронный ресурс] URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602 (дата обращения: 5 марта 2023 г.)

5. Assembly Bill No. 730. An act to amend, repeal, and add Section 35 of the Code of Civil Procedure, and to amend, add, and repeal Section 20010 of the Elections Code, relating to elections. [Электронный ресурс] URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB730 (дата обращения: 5 марта 2023 г.)

6. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts. [Электронный ресурс] URL: https://artificialintelligenceact.eu/the-act/ (дата обращения: 5 марта 2023 г.)

7. The 2022 Code of Practice on Disinformation. [Электронный ресурс] URL: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (дата обращения: 5 марта 2023 г.)

8. Правила работы дипфейк сервисов в Интернете, КНР. [Электронный ресурс] URL: http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm (дата обращения: 5 марта 2023 г.)

Литература на иностранных языках:

9. Vizoso, Á., Vaz-Álvarez, M., & López-García, X. (2021). Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation. Media and Communication, 9(1). P. 295. doi:https://doi.org/10.17645/mac.v9i1.3494

Иные документы на иностранных языках:

10. J. Snow. Deepfakes for good: Why researchers are using AI to fake health data. [Электронный ресурс] URL: https://www.fastcompany.com/90240746/deepfakes-for-good-why-researchers-are-using-ai-for-synthetic-health-data (дата обращения: 1 марта 2023 г.)

11. WIPO/IP/AI/2/GE/20/1. Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence. [Электронный ресурс] URL: Draft Issues Paper on Intellectual Property Policy and Artificial Intelligence (wipo.int) (дата обращения: 1 марта 2023 г.)

12. Deepfake Detection Challenge Results: An open initiative to advance AI. [Электронный ресурс] URL: https://ai.facebook.com/blog/deepfake-detection-challenge-results-an-open-initiative-to-advance-ai/ (дата обращений: 1 марта 2023 г.)

13. Synthetic and manipulated media policy. [Электронный ресурс] URL: https://help.twitter.com/en/rules-and-policies/manipulated-media (дата обращения: 5 марта 2023 г.)

СОЦИАЛЬНАЯ РЕКЛАМА КАК СПОСОБ ПРОДВИЖЕНИЯ ОБЩЕСТВЕННО ЗНАЧИМЫХ ИНИЦИАТИВ В СЕТИ «ИНТЕРНЕТ»

Куликов А.А.
Ведущий юрист-эксперт, АНО «Институт развития интернета»

Применяемые в мире рекламные инструменты уже давно вышли за пределы привлечения внимания потребителя к тому или иному товару.

Реклама может поднимать социальные, экономические, политические вопросы, привлекая внимание как к локальным, так и к более масштабным проблемам общества, и, что немаловажно, к способам их решения.

Это явление находит своё отражение и в массовой культуре. Главная героиня фильма «Три билборда на границе Эббинга, Миссури» пытается привлечь внимание к бездействию полиции в ходе расследования гибели её дочери с помощью средств наружной рекламы.

В российском законодательстве поддержка производства и распространения социальной рекламы предусматривалась ещё в 1995 году – был определён обязательный объём распространения социальной рекламы в размере не менее 5% от оказанных для распространения коммерческой рекламы услуг.

Схожая норма действует и по сей день, подтверждая актуальность продвижения благотворительных и иных общественно полезных интересов с помощью рекламных инструментов.

За годы применения нормативных положений о социальной рекламе сложилась практика определения объёмов социально значимого контента на радио и телевидении, в наружной рекламе и с помощью аналогичных «традиционных» способов рекламирования.

Однако, методы корректного определения пятипроцентного объёма социальной рекламы, которая должна быть распространена в Интернете, отсутствовали. При этом рынок Интернет-рекламы сохранял тенденцию к росту.

По оценкам Ассоциации развития интерактивной рекламы (АРИР, ранее – IAB Russia) объем рынка Интернет-рекламы за 2020 год вырос на 8,7% и составил более 330 миллиардов рублей.

Находясь в серой зоне, распространение социальной рекламы в Интернете не могло привести к надлежащему исполнению законодательных норм, основы которых были заложены ещё в прошлом веке.

Первым шагом к решению проблемы стало подписание в сентябре 2020 года крупнейшими российскими Интернет-компаниями – «Яндекс», Mail.ru Group (ныне – VK) и Rambler Group, а также Общественной палатой Российской Федерации и автономной некоммерческой организации «Институт развития интернета» (АНО «ИРИ») меморандума о социальной рекламе в Интернете.

Меморандум в числе прочего предусматривал создание экспертного совета, в задачи которого входила выработка единых подходов, стандартов и критериев распространения социальной рекламы в Интернете.

Развитием обозначенной работы и закономерным продолжением меморандума стало внесение в Государственную Думу в феврале 2021 года законопроекта, определяющего правила расчётов обязательного для распространения Интернет-площадками объёма социальной рекламы, а также регламентирующего правовой статус оператора социальной рекламы – некоммерческой организации, которая возьмёт на себя роль координатора процессов по продвижению общественно полезных инициатив.

В апреле 2021 года закон был подписан и в полном объёме вступил в силу с 1 июля 2021 года. Функциями оператора социальной рекламы была наделена АНО «ИРИ».

Работа над инициативой подтолкнула крупные онлайн-площадки к развитию собственных социальных проектов. Так, в марте 2021 года «Яндекс» объявил о разработке правил размещения социальной рекламы, а также о намерении выделить гранты в размере 360 млн рублей на продвижение социально значимых инициатив. Компания также публикует отчётность о рекламодателях социальной рекламы и количестве её показов.

В сентябре 2021 года Российский маркетплейс Ozon запустил благотворительную программу «Ozon Забота», с помощью которой пользователи сервиса смогут поддержать выбранные ими благотворительные организации.

При этом, тенденция к росту рынка сохранилась – по данным АРИР объём российского рынка цифровой рекламы в 2021 году вырос на 24% и достиг 323,6 миллиарда рублей, положительную динамику продемонстрировали все сегменты рынка.

Во втором полугодии 2021 года АНО «ИРИ» реализовал пилотные проекты по размещению социальной рекламы на темы вакцинации, донорства и поддержки пожилых людей на российских ресурсах. В 2022 году планировалось работать и с иностранными площадками, включая Google, YouTube, Facebook (запрещена в России, принадлежит компании Meta Platforms, Inc.) и TikTok. Договорённости с TikTok и Google были практически достигнуты.

В июле 2022 года были подведены итоги первых 11 месяцев работы оператора социальной рекламы. Проведено 120 рекламных кампаний от 62 рекламодателей, суммарный объем показов социальной рекламы в Интернете составил 21,7 миллиарда.

Кампании по продвижению социально значимых инициатив проводились на всех ключевых Интернет-площадках Рунета, что позволило охватить 100% его аудитории.

К примерам успешных кампаний можно отнести проекты, направленные на повышение информированности о возможностях профилактики и раннего выявления онкологических заболеваний, на профилактику гипертонии и на продвижение углубленной диспансеризации для переболевших коронавирусом, на популяризацию электронного сертификата на средства реабилитации для людей с ОВЗ, на борьбу с инсультами, на повышение степени осведомленности о генных дерматозах, на повышение интереса к донорству крови и многие другие. Рекламодателями социальной рекламы выступили в том числе крупные благотворительные фонды.

В конце декабря 2022 года оператор социальной рекламы опубликовал обновлённые показатели: за 2022 проведено 175 крупных федеральных кампании социальной рекламы для, совокупный объем которых составил 14 миллиардов показов рекламных материалов. В 2022 году к взаимодействию с оператором присоединилась 31 площадка. Рекламные компании были посвящены профилактике заболеваний, возможностям получения государственной поддержки, экологическим инициативам и т.д.

В АНО «ИРИ» продолжена работа по выработке отраслевых стандартов – на Международном форуме гражданского участия #МЫВМЕСТЕ оператор представил систему оценки эффективности социальной рекламы в Интернете, позволяющую оценить долгосрочное изменение отношения общества по важным социальным вопросам и определить необходимую частоту для поддержания положительной динамики этих изменений.

Представляется необходимым развивать и сами подходы к социальному продвижению, в особенности с учётом развития механизмов коммерческой рекламы.

Например, в декабре 2022 года Microsoft получила патент на технологию таргетированной рекламы в играх, которую будут размещать на виртуальных билбордах или одежде игровых персонажей. Предполагается, что система будет анализировать поведение игрока и показывать ему персонализированную рекламу.

В августе 2022 года специалисты «ВКонтакте» заявили о возможности таргетинга с учётом погодных условий, например, отображении объявлений о продаже кондиционеров и вентиляторов тем, кто находится в жарких зонах.

Практики расширенных возможностей таргетинга, интеграции с различными типами медиа-контента, в том числе интерактивного, могут быть применены и в аспекте социальной рекламы. Похожие предложения уже озвучивались в экспертной среде. В Общественной палате Российской Федерации предлагалось проработать вопрос интеграции социальной рекламы с рекомендательными алгоритмами информационных ресурсов.

Следует отметить и необходимость обновления подхода к расчёту обязательной квоты социальной рекламы. Разработанная в 1995 году норма не учитывает актуальных методов продвижения товара, основанных на манипулировании вниманием пользователя, которые не квалифицируются как реклама в понимании российского законодательства.

В результате фактическое соотношение социального контента и коммерческой рекламы смещается в пользу последней, не позволяя в полной мере достичь целей нормативного регулирования – как благотворительных, так и иных общественно полезных.

Соблюсти баланс между социальной рекламой и коммерческим контентом позволит выработка механизмов расчёта обязательной квоты социальной рекламы, основанного на показателях, связанных, например, с аудиторией крупного коммерческого ресурса.

Подводя итог, можно сделать вывод об успешном опыте координации на одной площадке Интернет-компаний и социально ориентированных некоммерческих организаций.

Подобный метод наполнения рекламных сетей социально-значимым контентом позволяет сфокусировать внимание пользователей на определённых общественно полезных инициативах, тем самым усиливая эффект от их продвижения.

В свою очередь, эффективное продвижение общественно значимых проектов, помимо очевидной пользы от повышения информированности конкретных граждан о возможных мерах поддержки, необходимости профилактики различных заболеваний, возможностях помощи социально незащищённым группам населения, оказывает эффект на общество в целом, снижая социальную напряжённость, формируя социальные связи и создавая позитивный эмоциональный фон от приобщения к общественно полезной деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Часть 3 статьи 18 Федерального закона от 18.07.1995 № 108-ФЗ «О рекламе», утратившего силу с 01.06.2006 // «Собрание законодательства РФ», 24.07.1995, № 30, ст. 2864

2. Часть 3 статьи 10 Федерального закона от 13.03.2006 № 38-ФЗ «О рекламе» // «Собрание законодательства РФ», 20.03.2006, № 12, ст. 1232.

3. 2020 / Оценка объемов рынка интерактивной рекламы // АРИР: сайт, 2021, URL: https://interactivead.ru/products/2020-oczenka-obemov-rynka-interaktivnoj-reklamy-upd/ (дата обращения 14.03.2023).

4. Интернет-компании России подписали Меморандум о социальной рекламе в Сети // Известия: сайт, 2020, URL: https://iz.ru/1067101/2020-09-29/internet-kompanii-rossii-podpisali-memorandum-o-sotcialnoi-reklame-v-ceti (дата обращения 14.03.2023).

5. Законопроект № 1109512-7 «О внесении изменений в Федеральный закон «О рекламе» (по вопросу регулирования распространения социальной рекламы), // СОЗД ГАС «Законотворчество»: электронный ресурс, URL: https://sozd.duma.gov.ru/bill/1109512-7 (дата обращения 14.03.2023).

6. Федеральный закон от 30.04.2021 № 124-ФЗ «О внесении изменений в Федеральный закон «О рекламе» // Официальный Интернет-портал правовой информации: электронный ресурс, 30.04.2021, URL: http://publication.pravo.gov.ru/Document/View/0001202104300098 (дата обращения 14.03.2023).

7. Распоряжение Правительства Российской Федерации от 13.07.2021 № 1907-р // Официальный Интернет-портал правовой информации: электронный ресурс, 1506.2021, URL: http://publication.pravo.gov.ru/Document/View/0001202107150010 (дата обращения 14.03.2023).

8. «Яндекс» разработал правила для соцрекламы и выделит 360 млн рублей в 2021 году на гранты для неё // vc.ru: сайт, 2021, URL: https://vc.ru/marketing/216866-yandeks-razrabotal-pravila-dlya-socreklamy-i-vydelit-360-mln-rubley-v-2021-godu-na-granty-dlya-nee (дата обращения 14.03.2023).

9. Социальная реклама в Яндексе: сайт, URL: https://yandex.ru/socialads-transparency-report/ (дата обращения 14.03.2023).

10. На Ozon теперь можно найти домашнего питомца и помочь нуждающимся // РБК СТИЛЬ: сайт, 2021, URL: https://style.rbc.ru/life/61542e9e9a7947f96deba474 (дата обращения 14.03.2023).

11. АРИР: объем российского рынка Интернет-рекламы в 2021 году // АРИР: сайт, 2022, URL: https://interactivead.ru/news/arir-obemy-internet-reklamy-2021/ (дата обращения 14.03.2023).

12. Google, YouTube, Facebook и TikTok привлекут к распространению социальной рекламы в РФ // Интерфакс: сайт, 2021, URL: https://www.interfax.ru/russia/804605 (дата обращения 14.03.2023).

13. В Госдуме подвели итоги первого года работы Оператора социальной рекламы // АНО «ИРИ»: сайт, 2022 URL: https://ири.рф/news/v-gosdume-podveli-itogi-pervogo-goda-raboty-operator-sotsialnoy-reklamy/ (дата обращения 14.03.2023).

14. Количество показов социальной рекламы в Интернете за год составило 21,7 млрд // ТАСС: сайт, 2022, URL: https://tass.ru/obschestvo/15126759 (дата обращения 14.03.2023).

15. В Госдуме подвели итоги первого года работы Оператора социальной рекламы // АНО «ИРИ»: сайт, 2022, URL: https://ири.рф/news/v-gosdume-podveli-itogi-pervogo-goda-raboty-operator-sotsialnoy-reklamy/ (дата обращения 14.03.2023)

16. ИРИ подвел итоги 2022 года в качестве Оператора социальной рекламы // АНО «ИРИ»: сайт, 2022, URL: https://ири.рф/news/iri-podvel-itogi-2022-goda-v-kachestve-operatora-sotsialnoy-reklamy/ (дата обращения 14.03.2023)

17. Microsoft запатентовала технологию таргета рекламы в онлайн-играх // Хабр: сайт, 2023, URL: https://habr.com/ru/news/t/709592/ (дата обращения 14.03.2023).

18. 1.WO2022250877 - PROVIDING PERSONALIZED CONTENT FOR UNINTRUSIVE ONLINE GAMING EXPERIENCE // WIPO IP Portal: электронный ресурс, URL: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2022250877 (дата обращения 14.03.2023).

19. Рекламу «ВКонтакте» позволили таргетировать на основе погоды // RB.RU: сетевое издание, 2022, URL: https://rb.ru/news/weather-vkontakte/ (дата обращения 14.03.2023).

20. В ОП предложили включить социальную рекламу в работу рекомендательных алгоритмов // ТАСС: сайт, 2022, URL: https://tass.ru/obschestvo/15125699 (дата обращения 14.03.2023).

«ТЁМНЫЕ ПАТТЕРНЫ»: ПОДХОДЫ К ОПРЕДЕЛЕНИЮ И ПРОТИВОДЕЙСТВИЮ

Саранкина Н.Д.
Старший юрист-эксперт, АНО «Институт развития интернета»

В цифровой среде могут использоваться особые техники манипуляции потребительским поведением. Например, склонить пользователя к определенным нежелательным для него, но выгодным для коммерческой компании действиям могут недобросовестные уловки при проектировании пользовательского интерфейса сайта или мобильного приложения – «темные паттерны».

Термин «темные паттерны» введен в 2010 году специалистом по пользовательским интерфейсам Гарри Бригналлом и обозначает «методы проектирования, которые обманом или манипуляцией заставляют пользователей делать выбор, который они иначе не сделали бы и который может причинить вред». В отечественной и мировой практике яркими примерами темных паттернов являются: установление страховки по умолчанию некоторыми сервисами кикшеринга, затруднительный процесс отписки от услуг стриминговых платформ, маскировка кнопки закрытия окна рекламы в ряде мобильных приложений.

В июне 2022 года Региональной общественной организацией «Центр Интернет-технологий» (РОЦИТ) было представлено аналитическое исследование манипуляции поведением пользователей с помощью темных паттернов. Эксперты РОЦИТ определили темные паттерны в качестве «техник манипуляции поведением пользователя при помощи устройства и дизайна сайта, приложения или цифровых сервисов, направленных на то, чтобы склонить его к выгодным для коммерческой компании решениям». Были выделены такие виды темных паттернов, как принуждение, запутывание, отвлечение, использование ошибок пользователя для того, чтобы достичь желаемых дизайнером интерфейса действий, ограничение функциональности элементов управления и ряд других уловок.

В целях борьбы с подобными недобросовестными практиками эксперты РОЦИТ предлагают выработку единых правил, регулирование со стороны государства и общественных организаций, а также введение оборотных штрафов за повторные нарушения.

В октябре 2021 года Федеральная торговая комиссия США (Federal Trade Commission, FTC) опубликовала заявление о политике правоприменения, в котором предостерегала компании от использования таких незаконных методов, как автоматическое продление платных подписок, бесплатные пробные периоды подписок с автоматическим платным продлением и ряд других манипуляций[48]. Ранее, в апреле того же года Федеральной торговой комиссией США был проведен открытый семинар по тематике темных паттернов в цифровой среде, по итогам которого был выпущен отчет Федеральной торговой комиссии по темным паттернам[49].

В данном отчете выделяются такие виды темных паттернов, как создание ложных убеждений (например, рекламные объявления, оформленные как новостные статьи), сокрытие или задержка в раскрытии существенной информации (например, сокрытие взимания комиссии или ее включение в цену только в конце покупки), подталкивание потребителей к платежам (например, предложение бесплатной пробной версии продукта с автоматическим продлением периодических платежей), нарушение конфиденциальности (например, непредоставление достаточных настроек приватности).

В документе указано, что Федеральная торговая комиссия будет принимать меры в отношении использования компаниями тех технических приемов, которые будут прямо нарушать законодательство США или иные нормы, применяемые Федеральной торговой комиссией.

В американском правопорядке регулирование темных паттернов существует и на уровне штатов. Первым законом штата в области темных паттернов стал Закон Калифорнии о конфиденциальности потребителей (California Consumer Privacy Act, CCPA)[50], в настоящее время измененный и дополненный Законом Калифорнии о Правах на конфиденциальность (California Privacy Rights Act, CPRA)[51]. В актуальном документе дается следующее определение темного паттерна: «это пользовательский интерфейс, разработанный или функционирующий с существенным эффектом подрыва или ограничения автономии пользователя при принятии им решений или осуществлении выбора».

Правила по добросовестному использованию пользовательского интерфейса встречаются и в актах американских саморегулируемых организаций. Например, существует Руководство для членов Индустрии сетевой рекламы (NAI), изданное в качестве комментариев к вышеуказанному докладу Федеральной торговой комиссии США[52].

[48] Enforcement Police Statement Regarding Negative Option Marketing // Federal Trade Commission. 2021.
URL: https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf (дата обращения: 09.03.2023).
[49] FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers // Federal Trade Commission. 2022. URL: https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers (дата обращения: 09.03.2023).
[50] The California Consumer Privacy Act of 2018 (CCPA) // California.gov. URL: https://oag.ca.gov/privacy/ccpa (дата обращения: 01.03.2023).
[51] The California Privacy Rights Act of 2020 (CPRA) // California.gov.
URL: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf (дата обращения: 01.03.2023).
[52] Bringing Dark Patterns to Light: An FTC Workshop // theNAI.org. 2021.
URL: https://thenai.org/wp-content/uploads/2021/07/nai_comments_ftc_dark_patterns_15march2021.pdf (дата обращения: 05.03.2023).

Внимание регуляторов к недобросовестным методам цифровых компаний отражается в судебной практике. Наиболее известным в США случаем судебного разбирательства в отношении использования темных паттернов является дело Dorobiala vs. Amazon.com, Inc., в котором истцы обвиняют компанию Amazon в усложнении процедур отказа от подписки Amazon Prime[53].

Определение темных паттернов в качестве «эксплуататорских вариантов дизайна», использование которых является «неэтичной попыткой» подтолкнуть пользователей к определенному выбору, закрепляется в исследовании Агентства Норвегии по защите прав потребителей под названием «Обманутые дизайном»[54].

В данном исследовании выделяются такие виды темных паттернов, как:

- установление настроек по умолчанию;
- усложнение изменения настроек конфиденциальности;
- установление рамок для пользовательского выбора;
- установление «наказаний» или «поощрений» за определенный выбор;
- принуждения к определенным действия и установление ограничений по времени.

Отдельно следует обратить внимание на темные паттерны в социальных сетях.

В марте 2022 года Европейским советом по защите данных (European Data Protection Board, EDPB) был опубликован проект Методических рекомендаций 3/2022 под названием «Темные паттерны в интерфейсах платформ социальных сетей: как распознать и избежать»[55]. В данном документе темные паттерны определяются как «интерфейсы и пользовательские практики, реализованные на платформах социальных сетей, которые заставляют пользователей принимать непреднамеренные, нежелательные и потенциально вредные решения в отношении обработки их персональных данных».

Для социальных сетей выделяют такие виды таких паттернов, как:

- перегрузка (overloading) – перегрузка пользователей большим количеством запросов, информации или опций, чтобы побудить их предоставить больше данных;
- пропуск (skipping) – разработка интерфейса таким образом, что пользователи забывают (или не учитывают) все или некоторые аспекты защиты данных при принятии решения;

[53] Rizzi C. Amazon Uses "Dark Patterns" to Hinder Consumers Looking to Cancel Prime Membership, Class Action Says // ClassAction.org. 2022. URL: https://www.classaction.org/news/amazon-uses-dark-patterns-to-hinder-consumers-looking-to-cancel-prime-membership-class-action-says (дата обращения: 12.03.2023).
[54] Deceived by Design // Forbrukerradet.no. 2018. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (дата обращения: 09.03.2023).
[55] Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them // European Data Protection Board. 2022. URL: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf (дата обращения: 09.03.2023).

- побуждение (stirring) – обращение к эмоциям пользователей или использование визуальных уловок;
- препятствие (hindering) – помехи в получении информации об использовании данных или осуществлении контроля над данными;
- непостоянство (fickle) – проектирование неудобного интерфейса, что затрудняет навигацию или понимание целей обработки данных;
- оставление в неведении (left in the dark) – разработка интерфейса таким образом, чтобы скрыть информацию.

Общий Регламент по защите данных (General Data Protection Regulation, GDPR) не закрепляет определения темных паттернов, но ряд его положений свидетельствует о запрете использования недобросовестных практик в отношении потребителей[56]. К ним относятся: принцип справедливости и прозрачности (статья 5(1)(a)), принцип подотчетности (статья 5(2)), защита данных по умолчанию (статья 25), требование предоставлять субъектам данных прозрачные уведомления о конфиденциальности (статья 12 (1), 13 и 14), а также иные права субъектов персональных данных в соответствии с GDPR (статьи 15-22).

Вступивший в силу европейский Закон о цифровых услугах (Digital Services Act, DSA) вводит прямой запрет на использование темных паттернов, которые в тексте закона определяются как «методы, направленные на манипулирование выбором пользователей»[57].

Иногда темные паттерны могут использоваться в качестве элементов согласия на обработку файлов cookie. Так, например, в 2021 году Национальная комиссия по защите данных Люксембурга опубликовала обновленные рекомендации по использованию файлов cookie, согласно которым к темным паттернам относятся различные формы, шрифты, цвета и размеры кнопок «я принимаю» и «я отказываюсь»[58].

Следовательно, не любые техники дизайна пользовательского интерфейса сайтов и мобильных приложений могут быть отнесены к категории темных паттернов, а лишь те, которые направлены на манипулирование поведением пользователя. Как показывает практика, грань между манипулятивными и добросовестными вариантами дизайна весьма тонка, поэтому перед регуляторами и мировым экспертным сообществом на сегодняшний день встает задача выработки эффективных мер по противодействию темным паттернам.

[56] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // EUR-Lex.europa.eu. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (дата обращения: 10.03.2023).
[57] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) // EUR-Lex.europa.eu. 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (дата обращения: 10.03.2023).
[58] Le Règlement Général sur la Protection des Données: Lignes directrices en matière de cookies et autres traceurs // Commission nationale pour la protection des données. 2022. URL: https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/cookies/CNPD-LD-Cookies.pdf (дата обращения: 10.03.2023).

Необходимым элементом таких мер является принятие международных стандартов и рекомендаций по выявлению и оценке воздействия темных паттернов, которые смогут быть использованы государствами как важные механизмы мониторинга недобросовестных практик в поведении хозяйствующих субъектов.

Результатом выявления факта использования темных паттернов может стать формирование кейс-стади для последующего ситуационного анализа полученного опыта как нового правила для рынка.

Немаловажным аспектом является просвещение потребителей, повышение цифровой грамотности граждан и уровня правосознания в целом. По мнению автора термина темных паттернов Гарри Бригналла, если пользователь знает, что такое когнитивные искажения и манипуляция мнением, то его вряд ли можно обмануть[59].

Кроме того, необходимо наличие эффективного механизма привлечения к ответственности тех хозяйствующих субъектов, чья манипулятивная практика нанесла вред потребителю. Лицу должно быть предоставлено право отказа от решений, совершенных под давлением или в неведении таким образом, который он не обязательно выбрал бы, если бы информация была представлена честно и прозрачно. Например, при автоматическом платном продлении подписки после бесплатного пробного периода пользователь должен быть заранее уведомлен о списании денежных средств или иметь возможность отказаться от подписки после автоматического списания и потребовать возврата уплаченной суммы, если правила платного продления не были ему надлежащим образом разъяснены.

Принятие вышеуказанных мер по противодействию темным паттернам позволит обеспечить всестороннюю защиту прав потребителя, создание благоприятных условий для развития предпринимательства, конкуренции и безопасной цифровой среды.

[59] Немцева М. Клик под контролем: как темные паттерны управляют нашими решениями // Известия. 2022. URL: https://iz.ru/1417645/mariia-nemtceva/klik-pod-kontrolem-kak-temnye-patterny-upravliaiut-nashimi-resheniiami (дата обращения: 12.03.2023).

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Немцева М. Клик под контролем: как темные паттерны управляют нашими решениями // Известия. 2022. URL: https://iz.ru/1417645/mariia-nemtceva/klik-pod-kontrolem-kak-temnye-patterny-upravliaiut-nashimi-resheniiami.

2. Bringing Dark Patterns to Light: An FTC Workshop // theNAI.org. 2021. URL: https://thenai.org/wp-content/uploads/2021/07/nai_comments_ftc_dark_patterns_15march2021.pdf.

3. Deceived by Design // Forbrukerradet.no. 2018. URL: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

4. Enforcement Police Statement Regarding Negative Option Marketing // Federal Trade Commission. 2021. URL: https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf.

5. FTC Report Shows Rise in Sophisticated Dark Patterns Designed to Trick and Trap Consumers // Federal Trade Commission. 2022. URL: https://www.ftc.gov/news-events/news/press-releases/2022/09/ftc-report-shows-rise-sophisticated-dark-patterns-designed-trick-trap-consumers.

6. Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognize and avoid them // European Data Protection Board. 2022. URL: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

7. Le Règlement Général sur la Protection des Données: Lignes directrices en matière de cookies et autres traceurs // Commission nationale pour la protection des données. 2022. URL: https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/cookies/CNPD-LD-Cookies.pdf.

8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // EUR-Lex.europa.eu. 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

9. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) // EUR-Lex.europa.eu. 2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014.

10. Rizzi C. Amazon Uses “Dark Patterns” to Hinder Consumers Looking to Cancel Prime Membership, Class Action Says // ClassAction.org. 2022. URL: https://www.classaction.org/news/amazon-uses-dark-patterns-to-hinder-consumers-looking-to-cancel-prime-membership-class-action-says.

11. SERNAC detects practices that may induce consumers to provide data, purchase, or overpay for goods or services // Icpen.org. 2021. URL: https://icpen.org/news/1205.

12. The California Consumer Privacy Act of 2018 (CCPA) // California.gov. URL: https://oag.ca.gov/privacy/ccpa.

13. The California Privacy Rights Act of 2020 (CPRA) // California.gov. URL: https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

WEB 3.0: КАКИМ БУДЕТ ИНТЕРНЕТ ЧЕРЕЗ 20 ЛЕТ И КАК СДЕЛАТЬ РОССИЮ ЕГО ЧАСТЬЮ

М.Б. Шрайбман
CEO, ООО «Осьминожка»

На протяжении последнего десятилетия мир идет по пути углубления автоматизации бизнес-процессов: повсеместно развивается инфраструктура электронного правительства, цифровой банкинг, онлайн-ритейл. Цифровизация способствует усилению секторальной эффективности: в любой сфере она кратно ускоряет процессы и сокращает затраты.

Однако цифровизация в текущем виде обладает рядом недостатков, среди которых можно выделить, например, уязвимость перед кибератаками и колоссальные утечки персональных данных. Решением данной проблемы является технология web 3.0.

Web 3.0 – концепция Интернета «нового поколения». В ее основе лежит понятие «децентрализация». От web 1.0 и web 2.0 эту концепцию отличает более персонализированный и интерактивный способ взаимодействия пользователя с Интернет-средой. Предполагается, что в условиях web 3.0 все данные будут храниться не на централизованных серверах, как это происходит сейчас, а автономно распределяться между пользователями. Блокчейн-технологии, искусственный интеллект, NFT, машинное обучение выступят драйверами для перехода от web 2.0 к web 3.0[60].

[60] Рвачев Н. А. Революция в мире маркетинга: как web 3.0 меняет лицо бизнеса // Инновации и инвестиции. 2022. № 8. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/revolyutsiya-v-mire-marketinga-kak-web-3-0-menyaet-litso-biznesa (дата обращения 04.03.2023).

ТАБЛИЦА 1. КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ ЭТАПОВ РАЗВИТИЯ ИНТЕРНЕТ-ПРОСТРАНСТВА

№	Концепция	Период	Характеристика	Эффект
1.	Web 1.0	Конец 80-х – 90-е годы XX века	1. Статический текст и изображения. 2. У пользователей отсутствует возможность влиять на контент (пассивное потребление информации).	1. Упрощение обмена информацией. 2. Ограниченные возможности для бизнеса.
2.	Web 2.0	2000 год – по настоящее время	1. Экспоненциальный рост интерактивного контента. 2. Появление и развитие социальных сетей, блогов, видеохостингов, форумов.	1. Появление гиг-экономики, при которой пользователи начали использовать Интернет не только для обмена информацией, но и для ее получения и обработки[61]. 2. Пользователи получают возможность потреблять персонализированную информацию, а компании - запускать рекламу.
3.	Web 3.0	20-е годы XXI века (возникновение технологии)	1. Использование криптокошельков. 2. Внедрение блокчейна, NFT. 3. Развитие иммерсивного опыта (метавселенные).	1. Децентрализация Интернет-пространства и его модерация не с помощью какого-либо государственного органа или транснациональной компании (далее – ТНК), а на основании протокола. 2. Web 3.0 способствует созданию условий, при которых в Интернете только автор может управлять контентом. 3. Развитие технологий виртуальной и дополненной реальности. Новый уровень взаимодействия с контентом.

[61] «В гиг-экономику вовлечен каждый» // Коммерсантъ. [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/4474605 (дата обращения 04.03.2023).

Драйвер развития web 3.0 – человек. В рамках этой версии Интернет-пространства будет создана новая форма цифровой идентификации, которая построена на принципах безопасности, конфиденциальности и свободы. В web 3.0 пользователи становятся единственными владельцами своих личных данных и учетных записей: персональные данные контролируются не централизованно (госорганы, банки, ТНК и др.), а самими пользователями. Это обеспечивает им больший контроль над собственной информацией.

Ключевыми характеристиками архитектуры web 3.0 является возможность хранения конфиденциальной пользовательской информации в криптокошельках, а также хранение документов, привязанных к криптокошелькам, в блокчейне. Такая архитектура позволяет обеспечить значительно более безопасное хранение данных, так как пользователи могут делиться ими только с теми, кому они сами предоставят доступ. Ряд экспертов утверждают, что шансы подобрать приватные ключи от криптокошелька крайне малы. По их мнению, вероятность выиграть джек-пот в лотерею значительно выше (см. рисунок 1).

The odds of guessing winning Powerball numbers vs. guessing one Bitcoin private key.
YOU WOULD HAVE TO WIN POWERBALL ~9 TIMES IN A ROW

Bits	Size of Space	
1	2	
10	1,024	
20	1,048,576	
28.121	292,000,000	Winning PowerBall
30	1,073,741,824	
40	1,099,511,627,776	
50	1,125,899,906,842,620	
60	1,152,921,504,606,850,000	
70	1,180,591,620,717,410,000,000	
80	1,208,925,819,614,630,000,000,000	
90	1,237,940,039,285,380,000,000,000,000	
100	1,267,650,600,228,230,000,000,000,000,000	
110	1,298,074,214,633,710,000,000,000,000,000,000	
120	1,329,227,995,784,920,000,000,000,000,000,000,000	
130	1,361,129,467,683,750,000,000,000,000,000,000,000,000	
140	1,393,796,574,908,160,000,000,000,000,000,000,000,000,000	
150	1,427,247,692,705,960,000,000,000,000,000,000,000,000,000,000	
160	1,461,501,637,330,900,000,000,000,000,000,000,000,000,000,000,000	
170	1,496,577,676,626,840,000,000,000,000,000,000,000,000,000,000,000,000	
180	1,532,495,540,865,890,000,000,000,000,000,000,000,000,000,000,000,000,000	
190	1,569,275,433,846,670,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
200	1,606,938,044,258,990,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
210	1,645,504,557,321,210,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
220	1,684,996,666,696,920,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
230	1,725,436,586,697,640,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
230.186	1,962,577,783,683,320,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000.00	Guessing any Bitcoin Private Key with a Balance
240	1,766,847,064,778,380,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	
256	115,792,089,237,316,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000	Guessing a Specific Bitcoin Private Key

Рисунок 1.
Сравнение вероятности подобрать ключи от биткоин-кошелька с шансами выиграть в лотерею[62]

[61] Crypto Fundraising Q3, 2022 // Cryptorank [Электронный ресурс]. Режим доступа: https://news.cryptorank.io/crypto-fundraising-q3-2022/ (дата обращения 04.03.2023).

Однако преимущества web 3.0 можно отметить не только для физических лиц, но и для бизнеса. Ключевые технологии будут способствовать решению самых различных проблем, с которыми сталкиваются компании, в том числе в России. Например, NFT позволит более эффективно бороться с кражей интеллектуальной собственности, а одним из способов использования метавселенных может стать их превращение в рабочие офисы компаний. Кстати, в России оператор связи МТС уже начал разработку собственной метавселенной[63]. Стоимость ее создания организация оценила в 100 млн долларов США.

Однако в рамках данной предметной области взгляды экспертов не всегда совпадают. Так, в исследовании компании Forrester обозначено, что в 2023 году развитие концепции web 3.0 несколько замедлится из-за различных экономических трудностей[64]. Согласно анализу Forrester, менее половины онлайн-пользователей говорят, что они станут участниками метавселенной. Практика показывает, что пока значительные финансовые затраты на развитие таких проектов не окупаются[65].

Внедрение концепции web 3.0 повлечет возникновение новых условий существования компаний на рынке. Из-за децентрализации сбор данных несколько усложнится. Компаниям потребуется создавать новые пути сбора данных для запуска рекламы или изучения пользовательских предпочтений. Кроме того, владельцам компаний придется адаптировать технологию блокчейн под свой бизнес. Все сделки с пользователями станут более прозрачными и безопасными. Это поможет повысить лояльность клиентов и позволит избежать ситуаций с утечками данных. Специалистам потребуются новые компетенции для работы с нейросетями, искусственным интеллектом и машинным обучением. Это также приведет к обновлению устройств, работа которых будет базироваться на конкретных инновационных технологиях[66]. Более того, произойдут изменения на законодательном уровне. Потребуется определить, будут ли делегированы правовые решения автоматизированным системам, какие инструменты регулирования будут действовать в обновленной Интернет-среде, каким образом будет решаться вопрос о хранении персональных данных и их использовании компаниями[67]. В настоящее время, вопросы, связанные с технорегулированием, также затрудняют всеобъемлющий переход к новой концепции.

Начало формирования нового Интернет-пространства в России невозможно без появления соответствующего рынка товаров и услуг. В данном случае действует классический случай рыночного закона спроса и предложения. Спрос на данную технологию уже появился, а предложение пока отсутствует. Подтверждением спроса служат данные об инвестиционной активности в этой области. По данным CryptoRank.io, объем венчурных инвестиций в технологии web 3.0 составил почти 7 млрд долларов США, в блокчейн – 3 млрд долларов США, NFT – 7 млрд долларов США (см. рисунок 2)[68].

[63] МТС в иной реальности // Коммерсантъ [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5795884 (дата обращения 04.03.2023).
[64] Как будут развиваться метавсленные в 2023 году. Прогноз Forrester // Tadviser [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/ (дата обращения 04.03.2023).
[65] Как будут развиваться метавсленные в 2023 году. Прогноз Forrester // Tadviser [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/ (дата обращения 04.03.2023).
[66] Рвачев Н. А. Революция в мире маркетинга: как web 3.0 меняет лицо бизнеса // Инновации и инвестиции. 2022. № 8. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/revolyutsiya-v-mire-marketinga-kak-web-3-0-menyaet-litso-biznesa (дата обращения 04.03.2023).
[67] Линьков В. В. Правовые проблемы информационного пространства при переходе к концепциям «Интернет вещей» и web 3. 0 // Закон и право. 2019. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/pravovye-problemy-informatsionnogo-prostranstva-pri-perehode-k-kontseptsiyam-internet-veschey-i-web-3-0 (дата обращения 04.03.2023).
[68] Crypto Fundraising Q3, 2022 // Cryptorank [Электронный ресурс]. Режим доступа: https://news.cryptorank.io/crypto-fundraising-q3-2022/ (дата обращения 04.03.2023).

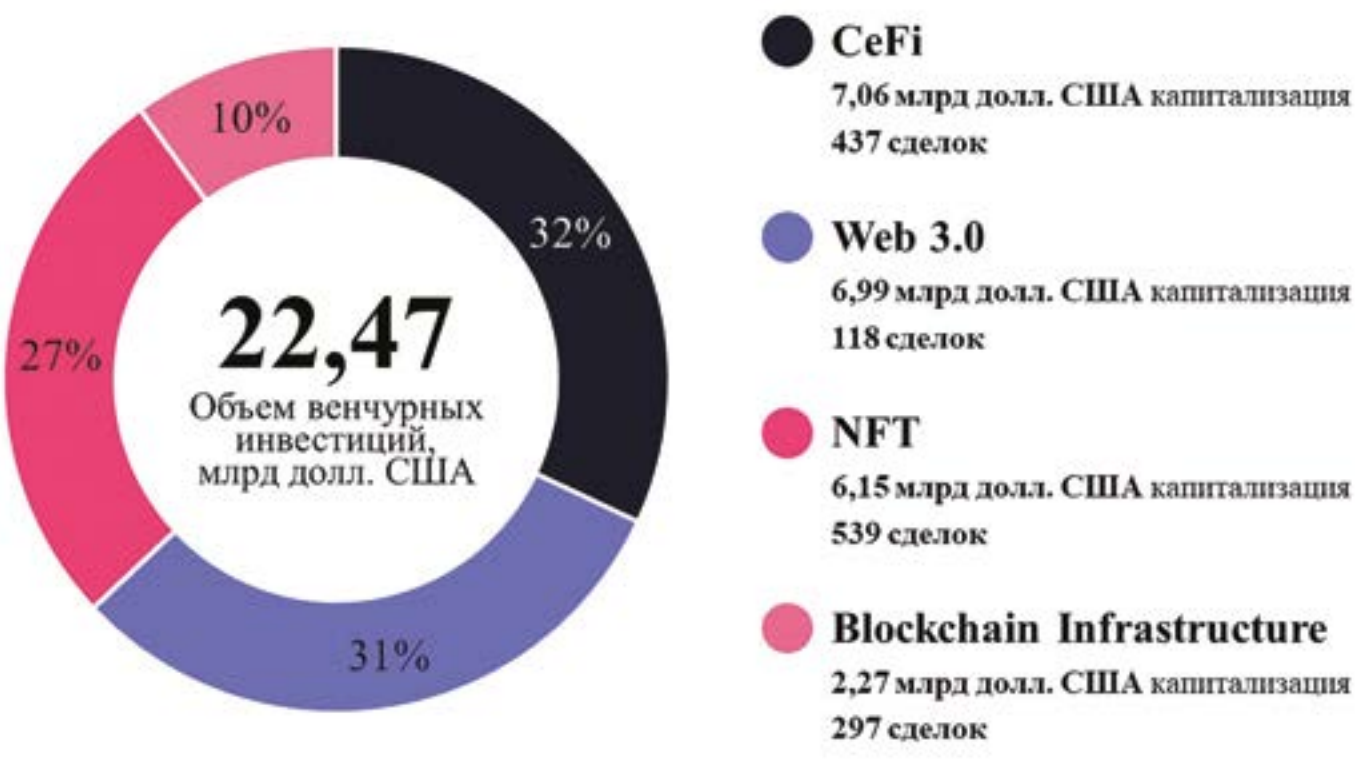

Рисунок 2.
Объем венчурных инвестиций в создание нового Интернет-пространства в мире с дифференциацией по секторам, 2022 год, млрд долл. США[69]

Новый рынок товаров и услуг должен предусматривать возможность оплаты с помощью криптокошелька – основного инструмента web 3.0. Для создания такого кошелька потребуется специально созданный модуль.

Пример тестового внедрения web 3.0 можно рассмотреть в банковской сфере, где ключевые технологии в рамках данной концепции значительно упростят работу специалистов за счет улучшения процесса скоринга заемщиков и, как следствие, более точной оценки их кредитного риска. Вместо традиционных методов оценки кредитоспособности, которые могут быть несколько ограничены и ориентированы на прошлые финансовые данные, банки могут использовать социальный рейтинг, основанный на цифровых следах заемщика в социальных сетях.

[69] Разработано автором на основе данных Crypto Fundraising Q3, 2022 // Cryptorank [Электронный ресурс]. Режим доступа: https://news.cryptorank.io/crypto-fundraising-q3-2022/ (дата обращения 04.03.2023).

Отдельное внимание стоит уделить влиянию web 3.0 на электронную коммерцию. Сервис будет базироваться на данных и контенте, генерируемых самими продуктами, с целью проведения дальнейшей аналитики. Это позволит обрабатывать полную информацию о продукте, а также осуществлять его поддержку без участия самого пользователя[70].

В России web 3.0 может быть применен на государственном уровне в различных сферах. Об этом говорят уже несколько лет. Одной из таких сфер является электронное голосование, процесс которого можно организовать прозрачно и безопасно благодаря использованию технологии блокчейн. Другой пример – заключение смарт-контрактов. Перед рядом российских специалистов уже стоит задача введения системы правового регулирования цифровых активов, регулирования смарт-контрактов и их включения в договорную практику. Эта практика открывает ряд преимуществ, среди которых: минимизация количества посредников в процессе заключения договора, защита условий контракта, контроль за его исполнением[71].

Web 3.0 также может быть применен в государственной системе здравоохранения для улучшения диагностики, лечения и контроля над заболеваниями. С использованием технологии блокчейн можно создавать цифровые паспорта здоровья, которые позволят врачам быстрее и точнее оценить состояние пациента и выбрать оптимальное лечение. Кроме того, технология позволит объединить пациентов в «виртуальные сообщества», упростит поиск информации о заболеваниях, позволит сохранить все данные об анамнезе пациента в единой форме, доступной ему и лечащему врачу[72]. Это облегчит процесс перехода пациента из одного лечебного учреждения в другое и даст ему возможность всегда иметь в полном доступе информацию о своем лечении.

Еще одним примером применения web 3.0 на государственном уровне может стать создание децентрализованных платформ для обмена информацией между государственными учреждениями. Это повысит эффективность обработки информации и скорость межведомственного взаимодействия.

Некоторые эксперты считают, что сейчас можно говорить о концепции web 3.0, основываясь на технологиях, которые уже доступны на рынке и понятны пользователям. Это, к примеру, такие технологии, как VR и AR. В России в обозримом будущем они могут быть доступны в гибридном обучении и в создании цифровых двойников. Первую технологию возможно внедрить как для обучения студентов в вузах, так и для обучения сотрудников. Вторая технология будет особенно актуальна, если речь идет об управлении работой предприятия[72]. Некоторым специалистам важнейшим шагом перехода к web 3.0 видится использование блокчейн и создание метавселенных, внутри которых будут функционировать привычные нам структуры.

[70] Шиганова М. В., Романова Н. А., Гусев В. В., Христофоров Р. П. Концепция вэб 3.0 в мире электронного бизнеса // Вестник науки. 2018. №2. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/kontseptsiya-veb-3-0-v-mire-elektronnogo-biznesa (дата обращения 04.03.2023).
[71] Дядькин Д. С., Усольцев Ю. М., Усольцева Н. А. Смарт-контракты в России: перспективы законодательного регулирования // Universum: экономика и юриспруденция. 2018. №5 [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/smart-kontrakty-v-rossii-perspektivy-zakonodatelnogo-regulirovaniya (дата обращения 04.03.2023).
[72] Михеев А. Е., Горбунов П. А. Интернет и сохранение здоровья // Менеджер здравоохранения. 2012. №2. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/internet-i-sohranenie-zdorovya (дата обращения 04.03.2023).
[73] О дивный новый web 3.0 // Comnews [Электронный ресурс]. Режим доступа: https://www.comnews.ru/content/221269/2022-07-20/2022-w29/o-divnyy-novyy-web-30 (дата обращения 04.03.2023).

Криптокошельки при этом будут задействованы в качестве одного из способов оплаты товаров[74].

Если проанализировать исторические данные о развитии web-среды, можно сделать вывод, что для создания зрелого web 3.0 пространства в России потребуется не менее 20 лет. Первым этапом послужит тестовое внедрение концепции в отдельных секторальных сегментах, что в нынешних условиях займет не менее 5 лет. Еще некоторое время понадобится на наращивание пользовательского опыта и образования. И этап окончательного перехода от web 2.0 к web 3.0 займет около 10 лет.

Таким образом, полноценный переход к концепции web 3.0 – это вопрос одного, а то и двух десятилетий. Для того, чтобы web 3.0 стал реальностью, требуется формирование соответствующего правового фундамента, создание профильного рынка товаров и услуг, масштабные инвестиции, форсированный PR технологии, повышение технической грамотности населения и, как уже было сказано, время. С приходом web 3.0 будет существенно изменена экономика страны. Появятся новые бизнес-модели, что даст толчок развитию цифровой экономики.

Однако не стоит забывать и о рисках, которые несет в себе web 3.0. Несмотря на изложенные преимущества, концепция сохраняет в себе опасность возникновения новых форм мошенничества и риск совершения киберпреступлений. Для того, чтобы минимизировать данные риски, требуется разработка эффективных механизмов защиты информации. Компаниям, государству и людям следует подготовиться к переходу в новый мир, потому что это потребует решения новых вызовов, овладения новыми компетенциями и изменения уже существующего привычного уклада жизни.

[74] О дивный новый web 3.0 // Comnews [Электронный ресурс]. Режим доступа: https://www.comnews.ru/content/221269/2022-07-20/2022-w29/o-divnyy-novyy-web-30 (дата обращения 04.03.2023).

СПИСОК ЛИТЕРАТУРЫ

Научные статьи:

1. Дядькин Д. С., Усольцев Ю. М., Усольцева Н. А. Смарт-контракты в России: перспективы законодательного регулирования // Universum: экономика и юриспруденция. 2018. №5 [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/smart-kontrakty-v-rossii-perspektivy-zakonodatelnogo-regulirovaniya (дата обращения 04.03.2023).

2. Линьков В. В. Правовые проблемы информационного пространства при переходе к концепциям «Интернет вещей» и web 3. 0 // Закон и право. 2019. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/pravovye-problemy-informatsionnogo-prostranstva-pri-perehode-k-kontseptsiyam-internet-veschey-i-web-3-0 (дата обращения 04.03.2023).

3. Михеев А. Е., Горбунов П. А. Интернет и сохранение здоровья // Менеджер здравоохранения. 2012. №2. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/internet-i-sohranenie-zdorovya (дата обращения 04.03.2023).

4. Рвачев Н. А. Революция в мире маркетинга: как web 3.0 меняет лицо бизнеса // Инновации и инвестиции. 2022. № 8. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/revolyutsiya-v-mire-marketinga-kak-web-3-0-menyaet-litso-biznesa (дата обращения 04.03.2023).

5. Шиганова М. В., Романова Н. А., Гусев В. В., Христофоров Р. П. Концепция вэб 3.0 в мире электронного бизнеса // Вестник науки. 2018. №2. [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/kontseptsiya-veb-3-0-v-mire-elektronnogo-biznesa (дата обращения 04.03.2023)

Интернет-ресурсы:

6. О дивный новый web 3.0 // Comnews [Электронный ресурс]. Режим доступа: https://www.comnews.ru/content/221269/2022-07-20/2022-w29/o-divnyy-novyy-web-30 (дата обращения 04.03.2023).

7. Как будут развиваться метавселенные в 2023 году. Прогноз Forrester // Tadviser [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/ (дата обращения 04.03.2023).

8. «В гиг-экономику вовлечен каждый» // Коммерсантъ. [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/4474605 (дата обращения 04.03.2023).

9. Crypto Fundraising Q3, 2022 // Cryptorank [Электронный ресурс]. Режим доступа: https://news.cryptorank.io/crypto-fundraising-q3-2022/ (дата обращения 04.03.2023).

10. МТС в иной реальности // Коммерсантъ [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/5795884 (дата обращения 04.03.2023).

ИЗМЕРЕНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Казарян К.К.
Институт исследований интернета (ИИИ), Генеральный Директор
АНО «Цифровая экономика», Директор по аналитике

Надежные измерения помогают при принятии стратегических решений проводить точную экономическую и социальную диагностику, оценивать потенциальное влияние альтернативных сценариев развития, отслеживать прогресс, а также эффективность и действенность реализованных мер политики.

Спрос на новые данные, показатели и инструменты измерения особенно остро проявляется в цифровом секторе в связи с растущей ролью, которую он играет в экономике и повседневной жизни, а также в связи с потенциалом цифровых технологий для преобразования рынка труда и производства.

По решению 51-й сессии Статистической Комиссии ООН (март 2020 г.)[75] начался процесс обновления СНС (системы национальных счетов) 2008[76]. В 2017–2018 гг. были выделены три ключевых направления исследований в области методологии СНС:

- глобализация;
- цифровизация;
- благосостояние и устойчивое развитие.

С 2018 года G20 рекомендует своим членам работать над улучшением измерений цифровой экономики в рамках существующей основы макроэкономической статистики, т.е. над включением показателей цифровой экономики в национальные счета.

Вместе с тем существует ряд барьеров и проблем на пути решения этой задачи. Так, по оценкам экспертов, 97% компаний традиционных отраслей экономики, таких, как финансы, торговля, промышленность, транспорт и логистика, строительство, сфера услуг, применяют цифровые технологии в своей деятельности в той или иной степени, что значительно усложняет определение границ исследуемой цифровой экономики: насколько деятельность организации должна зависеть от цифровых технологий, чтобы считаться ее частью [77]?

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации в 2022 году также столкнулось с проблемой определения критериев для аккредитации в реестр ИТ-компаний: значительная часть добавленной стоимости у «традиционных» компаний теперь исходит от цифровых технологий, а на ИКТ-специалистов приходится значительная часть существующих и создаваемых рабочих мест. При этом число разработчиков, занятых в традиционных отраслях и смежных секторах, которые являются поставщиками продуктов и услуг в рамках производства, уже превышает число разработчиков в софтверных компаниях. Однако общее число ИКТ-специалистов российской статистике неизвестно.

[75] https://unstats.un.org/unsd/statcom/51st-session/documents/2020-37-FinalReport-R.pdf
[76] https://unstats.un.org/unsd/nationalaccount/docs/sna2008russianwc.pdf
[77] https://conf.hse.ru/mirror/pubs/share/463148459.pdf

Отдельной проблемой является включение в измерение ВВП экономических результатов цифровых платформ: их услуги, как правило, бесплатны для пользователей, что вызывает сложности в применение традиционных методов измерения экономического эффекта. При этом услуги таких платформ, очевидно, влияют на производительность труда и благополучие пользователей, а также приводят к увеличению экономической активности в смежных областях (например, сервисы картографии приводят к развитию транспортных сервисов).

Таким образом в качестве основы для дальнейшей работы по измерению цифровой экономики многие страны и наднациональные объединения начали компилировать статистические показатели, по которым косвенным образом можно понять тенденции и темпы развития в различных странах. Такая работа проводилась Международным валютным фондом - Measuring the Digital Economy (IMF, 2018), Конференцией ООН по торговле и развитию - Measuring Exports of ICT-enabled/digitally delivered Services in developing countries (UNCTAD, 2018), ОЭСР и другими организациями. Примером формирующегося международного индекса является Digital Economy and Society Index (DESI) Еврокомиссии, методика расчета которого также принята Ассоциацией стран Тихоокеанского региона. В DESI кроме привычных показателей развития инфраструктуры, особое внимание уделяется цифровым навыками населения и рабочей силы, а также развитию технологий искусственного интеллекта и использованию данных в экономике. Аналогичная картина наблюдается и в отчете ОЭСР Digital Economy Outlook 2020.

Среди причин различия в подходах к измерениям является отсутствие общепринятого определения цифровой экономики. Среди экспертов однозначно сложилось понимание цифровизации (digitalization), т.е. кодирования информации или процедур в двоичные биты, которые могут быть прочитаны и обработаны компьютерами и которые могут принимать различные формы, такие как преобразование аналоговых измерений; кодирование деловых и производственных процессов; передача голоса по Интернет-протоколу (VOIP); социальные сети (как альтернатива личному общению) и т. д. В совокупности изменения, вызванные различными формами оцифровки (digitization), возникающими в результате деятельности приложений, систем, платформ и влиянием на экономическую и социальную деятельность, составляют «цифровую трансформацию» или цифровизацию.

Но хотя и существует понимание того, что цифровизация — это процесс, который включает кодирование информации в двоичные биты, ее использование в качестве основы для определения цифровой экономики носит ограниченный характер и, в любом случае, его трудно реализовать практическим и осмысленным образом для целей измерения. Цифровизация является ключом к цифровой трансформации, но оценка вклада, который она вносит в эту трансформацию, является лишь частью эффекта цифровой экономики. К примеру, стоимость цифровой передачи данных от клиента к производителю резко снизилась за последние двадцать лет, поэтому подход, учитывающий затраты на оцифровку, значительно недооценивал бы значение цифровизации.

Хотя фокус на цифровизацию явно предпочтительнее, чем фокус на оцифровке, с точки зрения определений он остается нетривиальным. Должна ли цифровая трансформация отражать общее влияние цифровизации на экономическую и социальную деятельность, например, общую стоимость поддерживаемой деятельности (такую как стоимость услуг такси на платформах совместного использования поездок), или она должна отражать только добавленную стоимость, например посреднические сборы, взимаемые за использование цифровых платформ?

Эти два вопроса дадут существенно разные ответы, но оба имеют отношение к дискуссии и важны для разработки политики. Первый в некоторой степени рассматривает общее воздействие, которое можно, хотя и очень грубо, описать как перспективу потребления, тогда как вторая, опять же грубо, ближе к точке зрения производителя. Эта многомерность лежит в основе трудности определения цифровой экономики. Оценки сектора электронной коммерции, которая для многих экспертов все еще является синонимом цифровой экономики, часто даются как объем продаж продуктов (базовая цена продукта, налоги, издержки сбыта и розничная наценка), но можно также утверждать, что вклад электронной коммерции в цифровую экономику должен отражать только ту часть общей продажи, которая относится к цифровым инструментам, облегчающим транзакции электронной торговли (например, взимаемая маржа или добавленная стоимость, создаваемая Интернет-магазином).

Принимая во внимание все обстоятельства, учитывая многоаспектный характер вопросов определения цифровой экономики, некоторые эксперты предлагают структуру счета-спутника, который обеспечивает основу для ответов на следующий круг вопросов:

- Что такое цифровой продукт?
- Кто такие цифровые производители?
- Кто такие цифровые пользователи?
- Каково количество сотрудников/занятость в фирмах, занимающихся цифровым производством?
- Какова средняя заработная плата сотрудников в фирмах, занимающихся цифровым производством?
- Каковы факторы цифровизации?
- Как цифровизация влияет на показатели благосостояния потребителей?
- Какая доля продаж/потребления заказывается в цифровом виде?
- Какая доля продаж/потребления осуществляется в цифровом виде?
- Какова ценность данных?

Кроме того, признавая тот факт, что многие «операции» в цифровой экономике являются неденежными (и бесплатными), такая структура должна включать переменные, которые в настоящее время находятся за пределами производственных границ СНС, а также учитывать, что данные об уровне развития благоприятной среды для цифровой экономики (например, инвестиции в продукты ИКТ и оборот данных) также является важной частью набора информации, даже если эти продукты сами по себе не оцифровываются и не являются результатом цифрового производственного процесса.

Отдельного упоминания требуют данные. Занимая центральное место в бизнес-моделях многих цифровых экосистем, в СНС получение данных без денежных транзакций рассматривается как бесплатное, и поэтому в счетах большая часть этих данных не отображается как товар или услуга. Однако существует значительный интерес к монетизации этих потоков и их ценности в базах

данных (где они включены в категорию инструментов инфраструктуры), которые поддерживают бизнес-модели, чтобы лучше понять, как данные способствуют производству (см. Рисунок 1. Размерности цифровой экономики).

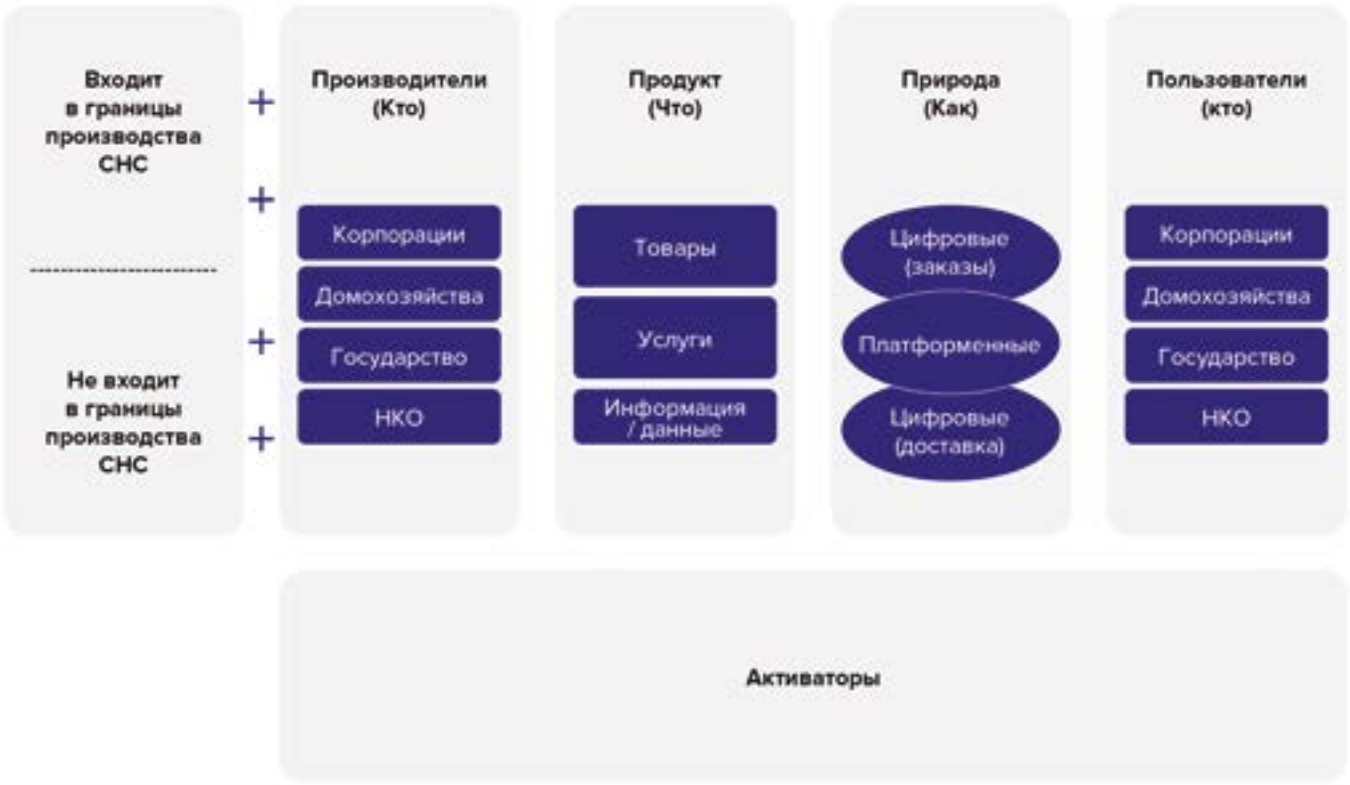

Рисунок 1. Размерности цифровой экономики.

Предлагаемый подход обеспечивает механизм для сопоставимых оценок ряда важных аспектов цифровой экономики:

- Размер транзакций, поддерживаемых электронной коммерцией.
- Добавленная стоимость, создаваемая ключевыми секторами цифровой экономики, с разбивкой по ключевым характеристикам: вспомогательные отрасли, платформенные отрасли, Интернет-магазины, другие цифровые отрасли и фирмы, зависящие от электронной коммерции (с разбивкой по институциональным секторам для получения представления о экономике совместного потребления с точки зрения производства).
- Общее потребление товаров ИКТ, используемых в производстве, и товаров ИКТ (и другой инфраструктуры), обеспечивающих цифровую экономику.
- Общее потребление цифровых услуг (включая услуги ИКТ, такие как программное обеспечение и облачные услуги).
- Оценки «стоимости» бесплатных услуг и ценности данных (потребуется разработать практическое руководство).

ПРОЦЕССУАЛЬНЫЕ АСПЕКТЫ ДОКАЗЫВАНИЯ ФАКТИЧЕСКИХ ОБСТОЯТЕЛЬСТВ, ЛЕЖАЩИХ В ОСНОВЕ ВМЕНЕНИЯ ГОСУДАРСТВУ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Сушков С.П.
Национальный исследовательский университет «Высшая школа экономики», аспирант

Ключевые слова: вменение поведения государству, право международной ответственности, информационно-коммуникационные технологии, бремя доказывания, стандарт доказывания, совершение вывода в пользу противной стороны.

Вменение поведения государству является неотъемлемым условием привлечения государства к международно-правовой ответственности. Поведение государства не может квалифицироваться в качестве международно-противоправного деяния при недоказанности вменения такого поведения государству[78].

В то же время, развитие информационных технологий позволяет государствам все более активно вести деятельность в так называемом «киберпространстве», которое для целей настоящей статьи будет определено как «условная среда, состоящая из Интернета вместе с другими компьютерами и телекоммуникационными сетями, подключенными к Интернету или не подключенными к нему»[79]. Как и в «реальном мире», поведение в «киберпространстве» может нарушать такие нормы международного права как запрет применения силы, принцип невмешательства в дела другого государства, обязательства по уважению прав человека или нормы международного гуманитарного права. При этом, при должном желании правонарушители имеют все возможности скрыть свою личность и свою связь с государством. Как следствие, наиболее остро стоит вопрос вменения государству случаев использования информационно-коммуникационных технологий (далее – «ИКТ»), для решения которого в рамках данной статьи будут проанализированы возможность и способы облегчения процесса доказывания «вменимости» государству случаев использования ИКТ.

ПРАКТИЧЕСКИЕ ПРОБЛЕМЫ ВМЕНЕНИЯ ИСПОЛЬЗОВАНИЯ ИКТ ГОСУДАРСТВУ

Вменение использования ИКТ государству сопряжено, как минимум, со следующими сложностями. Во-первых, доказательства, указывающие на конкретное лицо, ответственное за использование ИКТ, и его связь с государством, с большой долей вероятности будут находиться за пределами территории потерпевшего государства. Так называемый «цифровой след» позволяет лишь определить используемое устройство (или

[78] Комиссия международного права ООН, Тексты проектов статей об ответственности государств за международно-противоправные деяния с комментариями к ним (A/56/10) (далее – «Комментарии КМП к Статьям об ответственности»), стр. 59, параграф 5.
[79] Francois Delerue, Cyber Operations and International Law, Cambridge: Cambridge University Press, 2020, стр. 12.

местоположение устройства), но не само лицо, управляющее этим устройством. Во-вторых, тот факт, что применение ИКТ было осуществлено с территории государства или с использованием государственной информационной инфраструктуры не является достаточным основанием для вменения такого случая использования ИКТ данному государству[80]. В-третьих, лица, действующие в «киберпространстве», могут использовать методы «мимикрирования», чтобы создать иллюзию того, что конкретное государство стоит за определенным случаем использования ИКТ[81]. В-четвертых, сама природа «киберпространства» предрасполагает к скрытности и анонимности.

Практические трудности доказывания фактических обстоятельств, имевших место в «киберпространстве», усугубляются также и тем, что вопрос доказательств и доказывания обстоятельств, являющихся основаниями для вменения, не получил должного развития как в научной литературе[82], так и работах Комиссии международного права ООН (далее – «КМП»). [83]

В данной статье будет представлен неисчерпывающий перечень подходов к оценке доказательств, которые могут служить обоснованием для вменения государству использования ИКТ, если спор о вменении станет предметом разбирательства в международном судебном или квази-судебном органе.

ПЕРЕНОС БРЕМЕНИ ДОКАЗЫВАНИЯ

Поскольку большинство доказательств, с помощью которых можно вменить государству использование ИКТ, могут находиться на территории государства-ответчика, международный судебный орган может возложить на ответчика бремя доказывания отсутствия фактических обстоятельств для вменения. Перенос бремени доказывания на государство-ответчика активно используется международными судами по правам человека, в том числе Европейским судом по правам человека (далее - «ЕСПЧ»)[85]. Основанием для переноса бремени является отсутствие у истца объективной возможности собрать доказательства, находящиеся в распоряжении государства-ответчика. Именно наличие большинства доказательств, указывающих на связь актора с государством и находящихся за пределами территории потерпевшего государства, может являться достаточным основанием для переноса бремени доказывания на государство, которому якобы может быть вменено использование ИКТ.

Питер Маргулис предлагал переносить бремя доказывания отсутствия оснований для вменения государству использования ИКТ, если государство поддерживает, спонсирует и снабжает какую-либо организацию, и эта организация впоследствии будет замечена в неправомерном использовании ИКТ. Такой подход, по мнению профессора Маргулиса, отражает принципы справедливости и эффективности, поскольку бремя доказывания возлагается на государство, имеющее больший доступ к информации. В то же время, государства получат стимул к более пристальному контролю над деятельностью, осуществляемой поддерживаемыми государством организациями[87].

[80] Micheal Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017 (далее – «Таллинское руководство 2.0»), стр. 91; F. Delerue, Cyber Operations and International Law, стр. 128.
[81] Таллинское руководство 2.0, стр. 91, параграф 15.
[82] Henning Lahmann, Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution, Cambridge University Press, 2020, стр. 69.
[83] Комментарии КМП к Статьям об ответственности, стр. 54, параграф 4, стр. 72, параграф 8.
[84] См. обобщение судебной практики по данному вопросу в статье Christopher Roberts, Reversing the Burden of Proof Before Human Rights Bodies, International Journal of Human Rights, Vol. 25, Issue 10, стр. 1682-1703.
[85] ЕСПЧ концептуализировал свой подход к переносу бремени доказывания на ответчика в недавно опубликованном решении Ukraine and the Netherlands v. Russia (dec.) [GC], European Court of Human Rights, (Applications nos. 8019/16, 43800/14, 28525/20), 30 November 2022, параграфы 435-439, 454-459.
[86] Peter Margulies, Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, Melbourne Journal of International Law, Vol. 14, 2013, стр. 514-515.
[87] Там же, стр. 518-519.

СОВЕРШЕНИЕ ВЫВОДА В ПОЛЬЗУ ПРОТИВНОЙ СТОРОНЫ

Альтернативой переносу бремени доказывания на государство-ответчика может служить такое процессуальное правило, как совершение вывода в пользу противной стороны ("making an adverse inference" – англ.).

Совершение выводов в пользу противной стороны наиболее распространено в сфере арбитражных разбирательств с участием государств[88], а также в практике ЕСПЧ[89], в ситуациях, когда сторона спора удерживает доказательства, истребованные органом, рассматривающим спор. Следовательно, если суд или арбитры затребуют у государства-ответчика определенные материалы, потенциально подтверждающие вменение государству неправомерного использования ИКТ, и данное государство откажется предоставить данные материалы, то у суда или арбитров будут все основания, чтобы совершить вывод в пользу государства-истца (потерпевшего государства). В то же время, в отличие от переноса бремени доказывания, совершение вывода в пользу противной стороны влечет за собой презумпцию доказанности лишь определенных фактических обстоятельств (например, факт финансирования государством негосударственных акторов), но не влечет презумпции того, что неправомерное использование ИКТ в целом может быть вменено государству.

РАЗРЕШЕНИЕ БОЛЕЕ СВОБОДНО ПРИБЕГАТЬ К ВЫВОДАМ ИЗ ФАКТОВ И КОСВЕННЫХ УЛИК

Что касается потенциальных разбирательств в Международном Суде, то данный судебный орган не склонен ни переносить бремя доказывания на ответчика, ни совершать выводы в пользу противной стороны. Например, Международный Суд отказал Боснии и Герцеговине в переносе на Сербию и Черногорию бремени доказывания совершения геноцида[90]. В деле о проливе Корфу Международный Суд также не перенес бремя доказывания на Албанию, несмотря на ее эксклюзивный контроль над собственными территориальными водами[91]. Однако в практике Международного Суда встречается и другой механизм, позволяющий облегчить стороне спора доказывание фактических обстоятельств: разрешение более свободно прибегать к выводам из фактов и косвенных улик[92]. В деле о проливе Корфу Международный Суд сформулировал следующий принцип:

«Исключительный контроль, осуществляемый каким-либо государством в пределах его границ, делает невозможным представление прямых доказательств тех фактов, которые свидетельствовали бы о его ответственности в случае нарушения международного права. Пострадавшее государство в таком случае должно получить разрешение более свободно прибегать к выводам из фактов и косвенных улик; когда подобные косвенные доказательства основаны на ряде фактов, связанных между собой и логически ведущие к одному только выводу, то их необходимо рассматривать как имеющие особый вес»[93].

Соответственно, различные процессуальные правила позволяют потерпевшему государству возложить последствия неопределенности фактических обстоятельств на государство-ответчика и, тем самым, «смягчить» практические сложности доказывания фактических обстоятельств, являющихся основанием для вменения использования ИКТ государству. Правила

[88] См. обоснование условий для совершения вывода в пользу противной стороны в арбитражных разбирательствах в Jeremy Sharpe, Drawing Adverse Inferences from the Non-Production of Evidence, Arbitration International, Vol. 22, Issue 4, 2006, стр. 549-572.
[89] См. Ukraine and the Netherlands v. Russia (dec.), параграфы 435-439, 454-459.
[90] Дело о применении Конвенции о предупреждении преступления геноцида и наказании за него (Босния и Герцеговина против Сербии и Черногории), Решение от 26 февраля 2007, стр. 128, параграфы 204, 206.
[91] Дело о проливе Корфу (Великобритания против Албании), Решение от 9 апреля 1949, стр. 18.
[92] См. подробный анализ практики Международного суда по применению данного подхода в Michael Scharf, Margaux Day, The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences, Chicago Journal of International Law: Vol. 13, Issue 1, 2012, стр. 123-151.
[93] Дело о проливе Корфу, стр. 18.

оценки доказательств (и, следовательно, исход спора о вменении использования ИКТ государству) будут, по большей части, зависеть от органа, рассматривающего конкретный спор. Представляется, что в силу более гибкого подхода к оценке доказательств вменить государству поведение в «киберпространстве» будет проще в органах по защите прав человека, нежели чем в Международном Суде.

При этом стоит помнить, что описанные выше правила могут быть применены только в рамках арбитражного или судебного спора. Необходимость вменить использование ИКТ государству может возникнуть и за пределами межгосударственных разбирательств. Например, вменение государству случаев неправомерного применения ИКТ необходимо, если потерпевшее государство в ответ на такое применение ИКТ в одностороннем порядке реализовывает право на самооборону или принимает контрмеры. Следует полагать, что, когда потерпевшее государство прибегает к самозащите нарушенного права, оно не может ссылаться на правила, разработанные для судебной формы защиты права.

Таким образом, развитие ИКТ и рост количества споров из неправомерного использования таких технологий обуславливает необходимость упрощения правил доказывания в судебных и квази-судебных органах. Предполагается, что при рассмотрении таких споров потерпевшие стороны должны иметь возможность требовать переноса бремени доказывания на государство-ответчика, совершения вывода в пользу противной стороны или разрешения более свободно прибегать к выводам из фактов и косвенных улик.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Delerue, F., Cyber Operations and International Law, Cambridge: Cambridge University Press, 2020.

2. Lahmann, H., Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution, Cambridge University Press, 2020.

3. Margulies, P., Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, Melbourne Journal of International Law, Vol. 14, 2013, стр. 496-519.

4. Roberts, C., Reversing the Burden of Proof Before Human Rights Bodies, International Journal of Human Rights, Vol. 25, Issue 10, стр. 1682-1703.

5. Scharf, M., Day, M., The International Court of Justice's Treatment of Circumstantial Evidence and Adverse Inferences, Chicago Journal of International Law: Vol. 13, Issue 1, 2012, стр. 123-151.

6. Schmitt, M., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.), Cambridge University Press, 2017.

7. Sharpe, J., Drawing Adverse Inferences from the Non-Production of Evidence, Arbitration International, Vol. 22, Issue 4, 2006, стр. 549-572.

РЕГИОНАЛЬНАЯ СТРАТЕГИЯ ICANN РАЗМЕЩЕНИЯ КОРНЕВЫХ СЕРВЕРОВ DNS

Анисимов М.В.
Старший менеджер ICANN по работе с заинтересованными сторонами в Восточной Европе и Центральной Азии

Работа системы доменных имен (DNS) лежит в основе огромного количества Интернет-сервисов. Доменное имя – основная часть ссылки (URL), которая является основным способом связывать между собой веб-страницы и приложения. Доменные имена часто используются даже для связи устройств Интернета вещей и для решения еще более экзотических задач, например для дистрибуции ключей безопасности при управлении удаленными устройствами. Благодаря системе DNS можно связать IP-адреса, которые однозначно определяют узлы в Интернете, с буквенными обозначениями, которые может легко запомнить человек.

Система доменных имен иерархична, и работает следующим образом. После того как пользователь ввел адрес сайта в строке браузера или отправил письмо на какой-либо адрес, его провайдер пытается найти нужный путь, по которому этот запрос следует отправить. DNS-сервер провайдера, известный также как «рекурсивный резолвер», отправляет запрос вначале на так называемые корневые сервера DNS.

Корневые сервера DNS – начальная точка всего того большого дерева системы идентификаторов, которое позволяет найти любой адрес в Интернете. Корневые сервера содержат информацию об адресах серверов всех доменов верхнего уровня, как страновых, так и общих. Файл, который содержит всю эту информацию, редактируется и обновляется IANA, после чего рассылается по физическим узлам, расположенным в различных точках по всему миру.

Изначально корневых серверов было 13, и названы они были буквами латинского алфавита от A до M. Ими управляют 12 различных независимых организаций, называемых операторами корневых серверов (один из них управляет двумя серверами). По мере того, как Интернет рос и развивался, каждый из операторов увеличивал количество физических узлов, расположенных в сети, чтобы справляться с постоянно возрастающей нагрузкой. Поэтому сегодня мы можем говорить уже не о 13 серверах, а о 13 «облаках», каждое из которых имеет множество физических зеркал, разбросанных по всему миру. Общее количество таких зеркал, управляемых всеми операторами, на апрель 2023 года превышает 1600[94].

При выборе места физического размещения корневого сервера принимаются во внимание географические и топологические факторы. Сервер необходимо установить так, чтобы к нему имело доступ наибольшее количество людей по самому короткому пути и с минимальным временем ответа. Потому часто зеркала устанавливают в точках обмена трафиком, в сетях самых крупных провайдеров, в местах, где соединяются крупнейшие подводные линии связи и т. д. Это позволяет иметь связность с наибольшим количеством автономных систем и сокращает количество хопов, которое сигнал должен пройти от сети абонента до корневого сервера.

Размещение корневых серверов – важная составляющая любых усилий по повышению безопасности и устойчивости сети. Известны

[94] https://root-servers.org/

случаи, когда островные государства в результате техногенных катастроф и стихийных бедствий лишались линии связи с внешним миром, и в том случае если на этом острове отсутствовало зеркало одного из 13 серверов, или связь с ним имели не все местные провайдеры, абоненты не могли воспользоваться Интернетом и открыть даже те сайты, которые были расположены на той же территории.

В 2022 году в Найроби корпорация ICANN запустила свой пятый кластер корневых серверов IMRS (ICANN Managed Root Servers), ставший также первым, работающим в Африке. Результатом этой работы стало снижение DNS-трафика, который выходил за пределы региона, на 25% за счет большей локализации запросов. Это позволило увеличить устойчивость сети, снизило зависимость от внешних каналов связи, и улучшило пользовательский опыт, сократив время ответа. Кластер IMRS обрабатывает запросы с большой скоростью и связан с местными сетями мощными каналами связи, что позволяет снизить чувствительность к распределенным атакам на отказ в обслуживании[95].

Все корневые сервера, которые обслуживаются ICANN, собирают обобщенную статистику их использования, что позволяет в долгосрочной перспективе выявлять закономерности и аномалии в использовании DNS, лучше понимать, что необходимо улучшить в ее работе, как повысить устойчивость и защищенность. Вместе с данными, которые ICANN получает от провайдеров Интернета и от регистратур доменов верхнего уровня это позволяет составить более полную картину «здоровья» системы уникальных Интернет-идентификаторов. В ICANN для этого был создан отдельный проект ITHI (Identifier Technical Health Indicators), который собирает и анализирует эту информацию[96].

Восточная Европа и Центральная Азия имеют крайне неравномерный доступ к корневой инфраструктуре DNS. Например, на территории некоторых центральноазиатских государств в настоящее время нет ни одного корневого сервера, что ставит их в зависимость от связности с операторами других стран. Ближайшие усилия ICANN в партнерстве с другими операторами будут направлены на то, чтобы обеспечить приемлемый уровень сервиса во всем регионе, и таким образом сделать работу системы уникальных идентификаторов более устойчивой.

Развитие системы корневых серверов в регионе открывает множество возможностей для развития Интернета в целом. Помимо надежности и устойчивости к атакам, появляются новые варианты для развития связности. Установка корневых серверов требует подключения по двум протоколам, IPv4 и новому IPv6, что также становится локомотивом для его внедрения.

Стратегия развития системы корневых серверов и усилия по повышению устойчивости и надежности системы уникальных идентификаторов Интернета – это пример концепции технического управления Интернетом, в котором корпорация ICANN принимает активное участие. Техническое управление Интернетом – это координация усилий различных заинтересованных сторон по выработке лучших практик, в основе которых лежит глубокое понимание того, как глобальная сеть устроена с технической точки зрения. К техническому управлению Интернетом можно отнести также разработку технических стандартов и протоколов, практики повышения устойчивости и надежности работы Интернета.

[95] https://www.icann.org/en/blogs/details/icann-imrs-cluster-brings-a-more-resilient-and-stable-internet-to-africa-06-12-2022-en
[96] https://ithi.research.icann.org/

УГРОЗЫ ОБЕСПЕЧЕНИЯ ФИНАНСОВОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ В КИБЕРПРОСТРАНСТВЕ И СПОСОБЫ ИХ МИНИМИЗАЦИИ

Курманова Л.Р., д.э.н., профессор, профессор кафедры финансов и налогообложения Института экономики, финансов и бизнеса Уфимского университета науки и технологий, г. Уфа.
Садыкова А.И., к.э.н., доцент кафедры экономического и финансового образования Государственного университета просвещения, г. Мытищи.

Ключевые слова: финансовая безопасность, киберпространство, кибератака, информационные технологии, Единая биометрическая система.

В статье рассмотрены угрозы обеспечения финансовой безопасности в сети «Интернет». В последние два года наблюдался рост кибератак, направленных на хищение средств со счетов граждан и сведений о клиентах. Активная деятельность мошенников в Интернете объяснялась периодом самоизоляции, в течение которого большая часть населения работала и училась из дома, а также совершала покупки преимущественно через Интернет. Решение данной проблемы требует комплексного подхода, включая участие государственных органов.

На современном этапе развития общества информационные технологии стали неотъемлемой частью жизни. Современный мир невозможно представить без сети «Интернет», банковских карт и платежей в режиме онлайн.

Особую популярность они приобрели в период пандемии новой коронавирусной инфекции, когда на фоне введенных ограничений граждане все чаще начали совершать покупки в Интернете, заказывать доставку до дома и т.д. В этот же период наблюдался всплеск в сфере киберпреступлений. Только за 2021 год было зафиксировано около 518 тыс. киберпреступлений, что почти в 2 раза больше, чем в 2019 году. Большая часть киберпреступлений (70%) была связана с хищением средств с банковских карт клиентов через Интернет или при помощи телефонов (5).

На рисунке 1 представлены основные каналы хищения средств клиентов и получения информации о них. Более 45% приходится на электронную почту и финансовые институты.

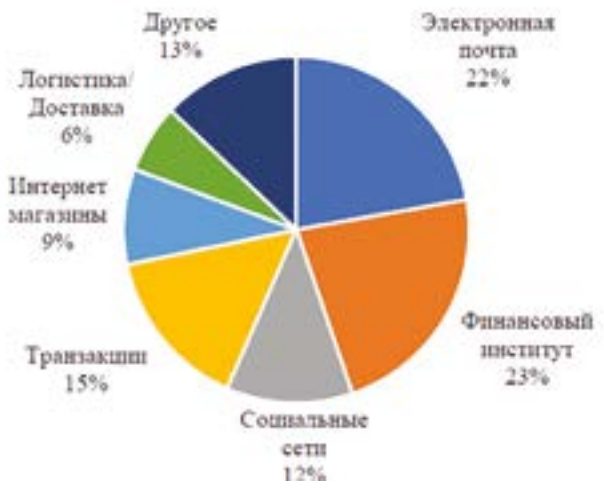

Рисунок 1 - Основные каналы хищения средств клиентов и информации о них [3, с. 3]

ОСНОВНЫЕ КАТЕГОРИИ ИНТЕРНЕТ-ВМЕШАТЕЛЬСТВ ПРЕДСТАВЛЕНЫ НА РИСУНКЕ 2.

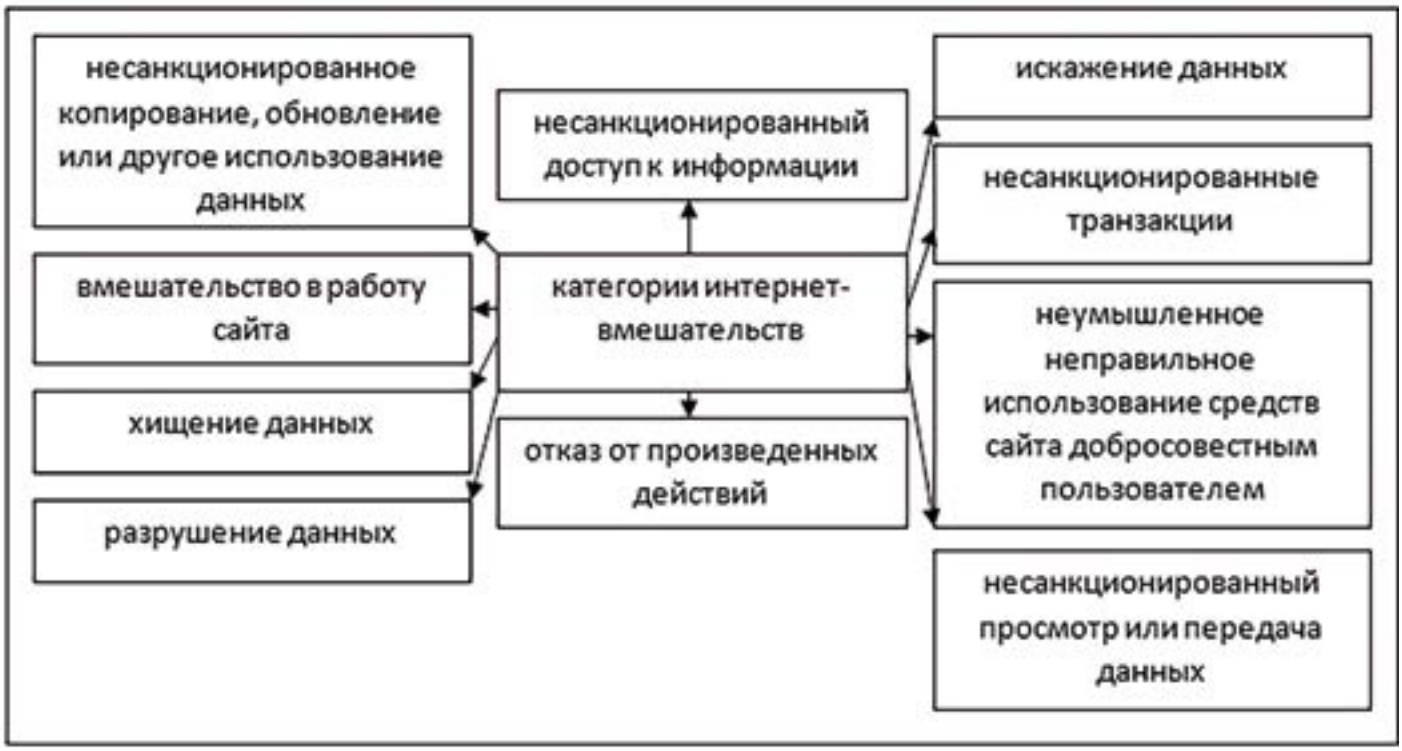

Рисунок 2 - Категории интернет-вмешательств [3, с. 2]

Большая доля мошеннических действий в виртуальной среде направлена против физических лиц. Кроме того, даже если атаки направлены на организации, то в значительной степени они касаются конкретных людей: руководителей или сотрудников. Целью кибератак является получение финансовой выгоды путем распространения вредоносного программного обеспечения. Данные негативные тенденции связаны с цифровизацией общественных отношений, доступностью информации, охватом широкой аудитории, что в результате создает угрозу национальной безопасности страны (2, с. 153).

Защита интересов граждан на сегодняшний день, в том числе, обеспечивается со стороны государства. В 2020 году были внесены изменения в законодательство об использовании Единой биометрической системы (ЕБС), оператором которой является ПАО «Ростелеком». ЕБС позволяет идентифицировать человека по отпечатку пальца, голосу или через распознавание лица. Данная система дает возможность получить клиентам кредит, открыть счет, снять наличные средства через банкомат или в режиме онлайн подписать документы. В будущем планируется создание единой базы данных, содержащей все биометрические данные клиентов. К сожалению, на сегодняшний день, только чуть более 50% граждан знают о существовании ЕБС, только 20% граждан уже предоставили свои биометрические данные.

Еще только около 20% россиян готовы предоставить свои данные. В этой связи по-прежнему эффективным инструментом остается контроль за транзакциями со стороны государственных органов.

Борьбу с мошенниками в сети «Интернет» и защиту интересов граждан осуществляет также Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). Одной из направлений подобной деятельности является выявление фишинговых сайтов, которые создаются кибермошенниками для выманивания средств граждан, кражи реквизитов банковских карт и счетов, а также других сведений о клиентах.

В настоящее время Банком России разрабатывается механизм осуществления расчетов, при котором банки будут списывать средства со счетов клиентов только по истечении 1-2 дней, несмотря на согласие клиента. Такой «период охлаждения» позволит защитить клиентов от несанкционированных списаний со счетов. Кроме того, Банком России планируется предоставление кредитным организациям права временной блокировки расходных операций со счета клиента на срок до 5 дней. В тоже время, введение данного механизма существенно замедлит безналичный оборот по сделкам хозяйствующих субъектов (1, с. 53).

Неотъемлемым элементом защиты граждан от кибермошенничества является повышение финансовой грамотности населения. В последнее время данному вопросу уделяется повышенное внимание. В 2017 г. Правительством РФ была принята «Стратегия повышения финансовой грамотности в Российской Федерации на 2017–2023 годы». Важными целями указанной стратегии являются: формирование знаний граждан о рисках на финансовом рынке, выработка способности распознавать признаки финансового мошенничества, а также умений отстаивать свои законные права как потребителя финансовых услуг (4).

Таким образом, борьба с кибермошенничеством должна быть комплексной и разносторонней. В частности, принятие мер необходимо как со стороны государства, так и со стороны граждан. Рост угрозы со стороны мошенников в сети «Интернет» был обусловлен в последнее время длительным периодом самоизоляции во время пандемии новой коронавирусной инфекции. В этот период граждане активно совершали покупки через Интернет, дистанционно работали и учились.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Дудин М.Н., Шкодинский С.В. Вызовы и угрозы цифровой экономики для устойчивости национальной банковской системы // Финансы: теория и практика. - Т.26. - №6. - 2022. - с. 52-71.

2. Красильников О.Ю. Проблемы обеспечения безопасности экономического следа личности в Интернете // Изв. Сарат. ун-та. Нов. сер. Сер.: Экономика. Управление. Право. - Т. 22. - вып. 2. - 2022. - с. 151-159.

3. Черных Л.В., Горбунова В.Б. Актуальные угрозы обеспечения экономической безопасности в киберпространстве // Вестник молодежной науки. - №3 (35). - 2022. - с. 1-9.

4. Электронный ресурс: Кибербезопасность 2021. Кто виноват и что делать? - https://plusworld.ru/journal/2021/plus-8-2021/kiberbezopasnost-2021-kto-vinovat-i-chto-delat/ (дата обращения: 09.03.2023 г.).

5. Электронный ресурс: Число киберпреступлений в России - https://www.tadviser.ru/index.php.

МАРКЕТИНГОВАЯ ДЕЯТЕЛЬНОСТЬ В СЕГМЕНТЕ B2B

Курманова Д.А.
к.э.н., доцент, Институт международных экономических связей (ИМЭС), заместитель декана

Сфера B2B сегодня расширила свои масштабы во всем мире и представляет собой сферу онлайновых услуг по организации в Интернете информационного и торгового взаимодействия между компаниями-покупателями и компаниями-продавцами. В связи с развитием рынка B2B актуализируется такое направление, как B2B маркетинг.

Под влиянием современных тенденций в мире произошло становление и развитие рынков B2B, под которыми понимается сектор рынка, организующий сотрудничество предприятий в процессе производства и приобретения ими товаров или услуг по определенной специфике. Рынок B2B и тенденции его развития оказывают значительное влияние на конкурентоспособность компаний и отраслей, на возможности их инновационного развития. B2B рынок развивается быстрыми темпами. Так, в 2020 году в мире произошли кардинальные изменения, которые способствовали дальнейшему активном росту B2B коммерции. В первую очередь, развитие B2B рынка ускорила пандемия, которая обеспечила рост электронной коммерции в 2021 году на 265%. Столь быстрое развитие рынка требует изучение основ маркетинга рынка B2B, а также его особенностей.

B2B («бизнес для бизнеса» – Business-to-Business), в узком понимании, включает все средства Интернета (сайты для сделок купли-продажи между компаниями, отраслевые порталы, сайты для закупок, корпоративные сайты и др.). С развитием рынка B2B термин B2B стал использоваться в более широком смысле, предусматривающий сферу онлайновых услуг информационного и торгового взаимодействия между компаниями – продавцами и компаниями – покупателями. Реализация товаров и услуг на B2B рынках совершается оптом на уровне предприятий. Взаимодействие с массовым потребителем исключено.

В научных публикациях отмечается, что B2B рынок: «рынок профессиональных товаров и услуг, на котором в качестве покупателя выступает профессиональный покупатель, представитель компании (бизнеса)» (1).

Характерной тенденцией последнего времени является создание крупными брендами собственных торговых площадок. Так, каждый бренд сегодня имеет свое веб-приложение. Продажи брендов осуществляются на их собственной платформе, в том числе, в сотрудничестве с различными компаниями,

что стимулирует крупные площадки брендов открывать на своей базе платформы для продажи B2B.

B2B секторе особое значение уделяется брендингу, все компании стремятся к глобальному брендингу, что объясняется глобализацией экономики и снижением информационных барьеров между компаниями B2B в разных странах.

Маркетинг B2B – это новое направление маркетинга, которое сформировалось параллельно промышленному, предпринимательскому маркетингу и маркетингу B2B online.
B2B происходит от английского «business-to-business», что в переводе означает «бизнес – бизнесу». Это продажи, в которых заказчиками выступают одни юридические лица, а поставщиками или подрядчиками - другие юридические лица. Помимо B2B рынка существует рынок B2C (business to client), ориентированный на потребителей частных лиц.

Принципиальное различие бизнес-моделей B2B и B2C заключается в следующем:

– главная цель сферы B2B — это постоянная или оптовая продажа товаров и услуг другим компаниям с целью получения прибыли; B2C – розничная продажа товаров физическим лицам;

– метод B2B предполагает реализацию продукции бизнесу, в B2C осуществляются продажи клиентам, то есть физическим лицам, число которых не является ограниченным;

– цели покупки в сфере B2B носят осознанный характер, в B2C - продажа товаров происходит из-за импульсивных решений клиентов;

– B2B предусматривает долгосрочные отношения с целевой аудиторией, в сфере B2C сотрудничество между партнерами носит краткосрочный характер.

Следовательно, B2B рынок представляет собой совокупность потребителей, приобретающих товары для профессионального использования (покупатели здесь – юридические лица и индивидуальные предприниматели). Как правило, товары приобретаются ими для последующей перепродажи, использования в качестве сырья, либо для удовлетворения собственных потребностей. Деятельность в сфере B2B рынка имеет свою специфику, что предопределяет необходимость использования особой методики маркетинга, имеющей название B2B маркетинг, и представляет новое направление маркетинга.

В современной экономике по критериям объема сделок, значимости рынка выигрывает сектор B2B по сравнению с сектором B2C. В целом, два этих рынка в современном мире способствуют опережающему развитию и применению маркетинговых решений. Значительный объем сделок на рынках B2B обеспечивается за счет роста использования товаров и услуг промышленного назначения для экспорта и валового накопления (2).

ТАБЛИЦА 1. ИЗУЧЕНИЕ ТЕОРЕТИЧЕСКИХ ОСНОВ B2B МАРКЕТИНГА ПОЗВОЛИЛО ВЫДЕЛИТЬ ЕГО ПРЕИМУЩЕСТВА И НЕДОСТАТКИ.

Преимущества	Недостатки
Сравнительно невысокий уровень конкуренции в сегменте B2B, по сравнению с розничной торговлей (успех зависит от профессиональных качеств и компетенций продавца)	Субъективизм в управлении B2B маркетингом (субъективный подход менеджера)
Большой охват аудитории (реализации товара B2B сектора не ограничена территориально)	Отсутствие системного подхода (все строится по принципу «переговоров»)
Минимальные затраты при старте деятельности в B2B секторе, что связано с отсутствием большого количества персонала, необходимости аренды офиса и пр.	Небольшая маржинальность (низкая наценка на продукцию, поскольку упор делается на увеличение оборачиваемости и объемов партий товаров)

Составлено автором

Сегодня под B2B маркетингом понимаются коммерческие отношения, которые возникают между двумя бизнес – организациями, одна из которых – продавец товаров и услуг, вторая- покупатель. Продвижение товаров в B2B секторе направлено, прежде всего, на формирование имиджа организации. Здесь ключевую роль играет реклама, которая формирует предпочтительное отношение целевой группы к компании-производителю.

Примеры наиболее часто используемых методов и инструментов продвижения товаров и услуг на рынке B2B отражены в таблице 2.

ТАБЛИЦА 2. МЕТОДЫ И ИНСТРУМЕНТЫ ПРОДВИЖЕНИЯ ТОВАРОВ И УСЛУГ НА РЫНКЕ B2B

Метод продвижения	Инструмент продвижения	Описание
PR в Интернете	Корпоративный блог, публикации о компании, пресс – конференции, онлайн – управление и пр.	Такая деятельность связана с формированием положительного образа компании, с отслеживанием отзывов потребителей и пр.
Социальные сети и email-рассылки	Транзакционные и информационные письма	Email – рассылки способствуют сбору заинтересованной аудитории и «взращиванию» из неё лояльных клиентов. Рассылки – это способ найти точки касания с потенциальными и лояльными клиентами для долгосрочных отношений. Соцсети формируют образ компании и выступают отличным способом коммуникации. Как правило, B2B-товары в соцсетях не продают. Однако соцсети знакомят аудиторию с компанией, привлекают к взаимодействию (например, посредством опросов в Интернете, отзывов и пр.).
Таргет	Таргет Targethunter (подбор целевой аудитории в социальных сетях); Livedune (используют для аналитики социальных сетей) и пр.	Таргет нацелен на формирование узнаваемости компании и повышение охвата. И, конечно, в B2B не обойтись без контекстной рекламы, нацеленной на «горячую» аудиторию. Например, таргетинг присутствует в Facebook Ads и ВКонтакте.
Контекстная реклама	Корпоративный сайт, Яндекс. Директ, рекламная сеть Яндекса, Google Analytics и пр.	Объявления показываются в зависимости от поисковых запросов (реклама на поиске) и характеристик аудитории (реклама в сетях). Чем больше и удобнее к восприятию информация в контекстной рекламе, чем выше потребности в конкретном продукте, тем ближе потенциальный клиент.
Контент - маркетинг	Тематические статьи, обзоры, исследование, фото и видео контент и пр.	Способствует знакомству аудитории с брендом, информирует о продукции, технических характеристиках и преимуществах.

Составлено автором

B2B маркетинг в России развивается медленными темпами. С одной стороны, Россия имеет возможность выстроить маркетинг, используя опыт зарубежных стран, с другой стороны, Россия имеет свою специфику маркетингового поведения.

В последнее время российские компании все более активно начинают использовать различные маркетинговые стратегии, что объяснимо: давлением рынка и его обстоятельств (рост конкуренции, возникновение проблем сбыта и т. д.); инициативой современных топ-менеджеров (работа на опережение проблем).

Сравнение маркетинга B2B разных стран по ключевым показателям проведено с целью выявления особенностей маркетинга по критериям: размер рынка B2B, реклама, отношение к бренду, сетевое общество (таблица 3).

Данные таблицы 3 подчеркивают значительное отставание России от зарубежных стран по развитости рынка. Аналитики Forrester Research оценивают отставание нашей страны от рынка электронной торговли США примерно в 5-7 лет (3).

Можно выделить следующие причины отставания российского рынка B2B от США, Японии: слабое развитие стандартных платформ для оптовых онлайн продаж в России и отставание технологий; низкий уровень ИТ – грамотности, низкая квалификация кадров на рынке B2B; сложные и ненастроенные ERP и прочие причины.

С учетом анализа российского и зарубежного опыта развития B2B маркетинга на современном этапе для России можно определить наиболее существенные факторы, влияющие на развитие B2B: общеэкономические факторы (нестабильность экономики, неблагоприятный инвестиционный климат, экономические санкции); инфраструктурные факторы (невысокий уровень информационных технологий, неразвитость телекоммуникаций и пр.); законодательно - правовой фактор (отсутствие нормативно - правовых актов, регулирующих электронную торговлю).

СПИСОК ЛИТЕРАТУРЫ:

1. Дашков А.А., Судаков К.А. Маркетинговая деятельность компаний сегмента рынка B2B // Экономика. - 2010. - №5. - С. 191-198.

2. Ресурс studmed.ru [Электронный ресурс]: сайт. – Режим доступа: https://www.studmed.ru/view/bek-ma-marketing-v2v-glava-1_ba3b4868f73.html?page=2 (дата обращения: 02.03.2023).

3. E-commerce [Электронный ресурс]: сайт. – Режим доступа: https://www.shopolog.ru/metodichka/analytics/pochemu-optovaya-onlayn-torgovlya-b2b-v-rossii-otstaet-ot-zapada-kitaya-i-roznichnoy/ (дата обращения: 06.03.2023).

4. Божук С.Г. Маркетинговые исследования: учебник для вузов /С. Г. Божук. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2021. – 118 с.

5. VC.RU [Электронный ресурс]: сайт. – Режим доступа: https://vc.ru/marketing/188021-yaponskiy-didzhital-busido-marketologa-v-2020 (дата обращения: 06.12.2021).

ТАБЛИЦА 3. СРАВНЕНИЕ МАРКЕТИНГА СТРАН ПО КЛЮЧЕВЫМ ПОКАЗАТЕЛЯМ [4]

Показатель	Россия	США	Япония
Размеры рынка B2B	В России электронная B2B-торговля пока не очень развита, этот рынок практически не автоматизирован и почти нет B2B-маркетплейсов	В США функционирует значительный рынок B2B	Япония — огромный рынок онлайн-рекламы. В стране 104 000 000 Интернет-пользователей, а это 91% населения [5]. Общие расходы на рекламу в Интернете составляют более 50% от всех расходов на рекламу в стране. В стране особой популярностью пользуются видеореклама и реклама в соцсетях, реклама через лидеров мнений (преимущественно в Instagram)
Реклама	Демонстрация огромных амбиций, культа силы и успеха	Делается по всем канонам рекламной науки. Америка больше, чем другие страны тратит деньги на рекламу	В контекстной рекламе преимущество отдается Google как основной платформе. Корпорация занимает 76% рынка, другие 20% достались Yahoo, Japan.
Отношение к брендам	Положительное, показатель состоятельности	Положительное	Положительное, показатель свободы и финансовой устойчивости
Сетевое общество	Faberlic	США – родина партнерских продаж. Из основных цифр, которые описывают степень влияния сетевого маркетинга на экономику в США, можно выделить то, что: - более 50% товаров реализуется через партнерскую бизнес систему; - в стране функционирует более 1500 многоуровневых компаний	Реакция на информационно-технологическую революцию на уровне отдельных японских компаний проявляется в: B2B (Business to Business – электронные сделки между компаниями), использование межфирменных сетей. Список лучших японских компаний, которые пользуются методами сетевого маркетинга: Mannatech (сайт проекта - mannatech.com) - транснациональная компания, которая занимается реализацией БАДов

Составлено автором

ЦИФРОВОЙ НАЛОГ ДЛЯ ИТ ГИГАНТОВ – ЗА ЧТО ДОЛЖНЫ ПЛАТИТЬ ЦИФРОВЫЕ КОРПОРАЦИИ

Филина Н.А.
Секретарь EURALO (At-Large, ICANN), участник международных экспертных групп по управлению Интернетом

Бизнес должен государству и платит налоги. Доходы от полученных налоговых поступлений финансируют жизненно важные государственные услуги.

Транснациональный бизнес должен государству, в котором ведет свою деятельность и извлекает прибыль, так как этому способствуют граждане, инфраструктура, финансовые, правовые инструменты этого государства.

С 2011 года США, Евросоюз обратили внимание на использование цифровыми корпорациями трюка ухода от налогов: ИТ гиганты не платят налог на доход в странах с высокой налоговой ставкой и перемещаются в страны «налоговых убежищ», где налог на доход низкий или равен нулю (Ирландия и Люксембург), продолжая работать и извлекать гигантские прибыли на рынках в странах неуплаченных налогов.

Эволюция, а точнее революция цифровой экономики, рост количества транснациональных ИТ компаний и появление новых механизмов и практик операционных моделей управления, предусматривающих создание сложных схем дочерних предприятий, не позволило международной системе корпоративного налогообложения своевременно установить строгие правила.

«Согласно расследованию, проведенному американским сенатом, названные фирмы аккумулировали большую часть своей прибыли в Ирландии с помощью дочерних компаний. Налоговая ставка в этой стране одна из самых низких в Европе – 12,5%. Но даже она показалась бизнес-гигантам слишком высокой. Apple еще в 2007 году договорилась с властями Ирландии выплачивать с прибыли всего 1,9%. Сделка была оформлена с помощью сложной схемы, для реализации которой были созданы дочерние фирмы в Ирландии и на Бермудских островах».[97]

Итак, Международная система налогообложения корпораций не была готова предложить решение 12 лет назад, но фокус внимания на проблеме помог странам начать дискуссии и внести на рассмотрение законопроекты, вменяющие унификацию налогообложения ИТ гигантов или позволяющие самостоятельно определить размер налога на прибыль транснациональных ИТ корпораций в отдельных странах.

ПОСЧИТАЕМ УПУЩЕННУЮ ВЫГОДУ

Репутация ИТ гигантов давно подмочена. Доминирование на цифровом рынке, нарушение антимонопольного законодательства, Уклонение ИТ гигантов от уплаты налогов, наравне с

[97] https://sovcombank.ru/blog/biznesu/oblozhili-so-vseh-storon-chto-takoe-globalnii-nalog-dlya-korporatsii?utm_referrer=https%3A%2F%2Fyandex.ru%2F

другими происшествиями, связанными с действиями цифровых платформ по: - извлечению огромной прибыли не совсем законными способами (продажа ПД), - участию в темных политических историях манипулирования общественным мнением, - влиянию на выборы, - финансированию лобби противодействующему принятию GDPR. Список можно продолжить, но мы сейчас считаем только упущенную выгоду и недополученные налоги.

Сколько миллиардов долларов, евро, фунтов стерлингов налоговых поступлений потеряли бюджеты стран, упустив из виду эту хитрую схему транснациональных корпораций, таких как Facebook[98], Amazon, Google, Apple? Сотни миллиардов.

НА ЧЕМ ЗАРАБАТЫВАЮТ IT-ГИГАНТЫ?

На продаже продуктов и услуг (Apple, Microsoft, Airbnb, Uber, Amazon) или на продаже нашего внимания - рекламе (Meta, Alphabet).

Интернет-медиа, потоковые сервисы, такие как Netflix, и другие поставщики цифрового контента, которые не создают контент самостоятельно, без использования контента пользователей, исключаются из сферы сбора цифровых налогов.

ДОХОДЫ КОМПАНИЙ СТРЕМИТЕЛЬНО РАСТУТ.

«Опубликованные финансовые отчеты ИТ-компаний показывают, что пандемия коронавируса подстегнула рост доходов. Совокупная капитализация Amazon, Google, Facebook, Apple и Amazon приближается к $10 триллионам, каждая из них уже перешагнула рубеж в $1 триллион, а Apple и Microsoft достигли $2 триллионов»[99].

В 2021 году технологические гиганты «большой пятерки» — Apple, Amazon, Google (Alphabet), Meta и Microsoft — получили совокупный доход в размере 1,4 триллиона долларов[100].

ЛЕТОПИСЬ DIGITAL TAX

Сложный поиск определения правил налогообложения для союзов и отдельных стран можно проиллюстрировать некоторыми новостями из СМИ 2016 – 2020 гг.:

2016 г., Индия.

«На протяжении нескольких лет с 29 февраля 2016 года в Индии действует аналог цифрового налога — уравнительный сбор. За период с 2017 года по 2018 год данный сбор принес в бюджет Индии около 39 млн долларов США (550 индийских крор).

Уравнительный сбор — прямой налог, взимаемый за B2B сделки в области цифровой рекламы как 6% от дохода, полученного иностранными компаниями в Индии[101]».

Декабрь 2018 г., ЕС

«Министры финансов ЕС так и не смогли договориться о цифровом налоге на доходы технологических компаний, несмотря на то что в последний момент был предложен франко-германский план-компромисс, определивший компании двух субъектов налогообложения - Google и Facebook, исключив из списка другие технологические компании[102]».

[98] Упоминаемая здесь и далее компания Facebook (Meta) запрещена в России
[99] https://devby.io/news/kvartalnye-rekordy-it-gigantov
[100] https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/
[101] https://www.csr.ru/upload/iblock/5ef/5ef5a7831553dc062605b281a53e4350.pdf
[102] https://tribune.com.pk/story/1860703/8-eu-ministers-fail-break-digital-tax-deadlock/

Эта неудача является ударом по президенту Франции Эммануилу Макрону, правительство которого вложило в этот налог значительный политический капитал. «Если страны ЕС не смогут договориться о совместном налоге на цифровые доходы, Франция на национальном локальном уровне начнет налогообложение технологических гигантов в 2019 году[103]».

Декабрь 2018 г.

Франция заявила, что введет свой собственный налог для крупных технологических компаний с 1 января 2019 года, после того как дискуссия в рамках ЕС зашла в тупик. Министр финансов Франции Бруно Ле Маре заявил, что в 2019 году введение налога пополнит бюджет на 500 млн евро[104].

Февраль, 2019 г.

Организация экономического сотрудничества и развития (OECD) предложила общественности представить свои предложения по изменению существующих международных налоговых правил для более целесообразного налогообложения многонациональных цифровых компаний.

Комментарии к консультативному документу ОЭСР запрашиваются до 1 марта; общественные консультации пройдут в Париже 13–14 марта[105].

Февраль 2019 г.

Премьер-министр Джасинда Ардерн заявила, что Новая Зеландия будет работать над изменением налогового законодательства с целью введения налога на доходы компаний с высокой степенью цифровизации (Facebook, Google и Amazon и другие), которые в настоящее время получают значительный доход от потребителей Новой Зеландии[106].

Март 2019 г.

Французское правительство ввело цифровой налог, нацеленный на прибыль Интернет-гигантов, таких как Google, Amazon и Facebook, что стало самостоятельным шагом без ожидания поддержки и единого решения со стороны Европейского Союза. Трехпроцентный (3%) налог будет применяться к доходам, получаемым вследствие деятельности на территории Франции примерно 30 крупных компаний, в основном из США. Офис торгового представителя США в июле начал расследование в отношении нового налога, который он назвал «необоснованным»[107].

[103] https://www.cnet.com/news/france-will-tax-tech-giants-in-2019-regardless-of-eu-agreement/
[104] https://www.bbc.com/news/business-46591576
[105] https://mnetax.com/oecd-seeks-public-input-on-tax-challenges-of-digital-economy-32328
[106] https://www.cnbc.com/2019/02/18/new-zealand-to-target-google-facebook-and-amazon-with-digital-tax-pm.html
[107] https://www.cnbc.com/2019/03/06/france-3-percent-digital-tax-targets-google-amazon-and-facebook.html

Май 2019 г.

Чешское правительство вводит семипроцентный (7%) цифровой налог на крупные Интернет-компании, такие как Facebook и Google, что, по предварительным прогнозам, добавит около 200 млн евро в годовой бюджет. По сообщению министра финансов Чехии, это вынужденная мера и следствие провала переговоров на уровне ЕС и отсутствия прогресса в поиске глобального решения.

Чешская Республика следует примеру Австрии, которая ввела пятипроцентный (5%) цифровой налог, который вступит в силу к 2020 году, а также примеру Франции, национальное собрание которой утвердило трехпроцентный (3%) цифровой налог[108].

Август 2019 г.

Google, Facebook и Amazon входят в число крупных технологических компаний, которые теперь должны платить цифровой налог на доход, полученный во Франции в размере 3%. Представители компаний дадут показания на слушаниях в правительстве США по этому вопросу, заранее имея поддержку правительства США, назвавшего налог неразумным[109].

Декабрь 2019 г., Великобритания

В октябре 2018 года Великобритания объявила о введении налога в размере 2% на доходы поисковых систем, платформ социальных сетей и онлайн-рынков, которые являются прибыльными и приносят доход более 500 млн фунтов стерлингов в год.

Но уже в августе 2020 года правительство Великобритании рассматривало возможность отказа от такого решения, так как это уже привело к разногласиям с представителями США во время торговых переговоров (США пригрозили ввести тарифы для Великобритании и других стран, которые ввели такую политику для американских ИТ корпораций).

Январь 2020 г., Италия.

Италия приняла решение о введении с 1 января 2020 года цифрового налога по ставке 3% с дохода, полученного от определенных B2B и B2C цифровых услуг, оказываемых итальянским пользователям компаниями или МГК15. В отличие от Великобритании (где выражается только неофициальное намерение) итальянским законом формально предусматриваются положения, отменяющие цифровой налог при условии вступления в силу соответствующих международных норм[110].

[108] https://emerging-europe.com/business/czech-republic-introduces-digital-tax-on-internet-giants/
[109] https://www.cnbc.com/2019/08/14/google-facebook-amazon-to-testify-in-us-against-french-digital-tax.html
[110] https://www.csr.ru/upload/iblock/5ef/5ef5a7831553dc062605b281a53e4350.pdf

СОЮЗ НЕРУШИМЫЙ И РЕФОРМА DIGITAL TAX

В 2021 году 130 стран и юрисдикций (в том числе Россия) присоединились к новому двухкомпонентному плану реформирования международных правил налогообложения и обеспечения того, чтобы многонациональные компании платили справедливую долю налогов, где бы они ни работали.

Доходы, которыми страны покроют дефициты бюджетов и смогут инвестировать в развитие экономики и укрепить социальную сферу, будут обеспечены двумя компонентами:

Компонент 1:
Транснациональная корпорация платит налог там, где получает прибыль, вне зависимости от присутствия/отсутствия в этой стране. Налоговое правило коснется крупных бизнес-структур, чистая маржинальность которых составляет не менее 10%, а оборот – более 20 млрд евро в год. Исключения – компании, добывающие природные ресурсы и предоставляющие финансовые услуги (обращаем внимание на то, что новые правила касаются не только ИТ сферы).

Компонент 2:
Налоговая ставка 15% вводится для компаний с выручкой более 750 млн евро. Компания платит налог вне зависимости от места формирования налогооблагаемой прибыли. Налог платится там, где компания зарегистрирована. Компонент 2 исключает вариант переманивания странами налогоплательщиков, играя на понижение налоговых ставок.

В случае успешного внедрения новых правил налогообложения, ожидаемая прибыль составит более 100 млрд долларов США, которая будет ежегодно перераспределяться между рыночными юрисдикциями.

«После многих лет напряженной работы и переговоров этот исторический пакет обеспечит, чтобы крупные транснациональные компании повсюду платили свою справедливую долю налогов», — заявил Генеральный секретарь ОЭСР Матиас Корманн. «Этот пакет не устраняет налоговую конкуренцию, как и должно быть, но устанавливает для нее многосторонне согласованные ограничения. Он также учитывает различные интересы за столом переговоров, в том числе интересы малых экономик и развивающихся юрисдикций. Все заинтересованы в том, чтобы мы достигли

окончательного соглашения между всеми членами Inclusive Framework, как это запланировано позднее в этом году», — сказал г-н Корманн.

Участники переговоров установили амбициозные сроки реализации реформ: в октябре 2021 года завершить оставшиеся технические работы по внедрению двухкомпонентного подхода, а план эффективной реализации в 2023 году[111].

При недостижении консенсуса в ОЭСР любая страна, в том числе и Россия, скорее всего, пойдет по такому пути: «разморозит» собственный односторонний цифровой налог, но важно, чтобы соответствующий законопроект уже был подготовлен и одобрен.

СПОРЫ ПРОДОЛЖАЮТСЯ

Конечно, технологические корпорации «глубоко обеспокоены» налогом на цифровые услуги. И корпорации, и общество будут следить за развитием событий и успехом внедрения реформы.

Бытует мнение, что это не тривиальная задача – расчет налогов для транснациональных ИТ корпораций, вопрос касается и открытости, и доступности информации о финансовых результатах деятельности корпораций во каждой стране и в каждой юрисдикции.

Дискуссии ведутся о базе налогообложения – что удобнее учесть и обложить налогом - доходы или прибыль корпорации?

Также есть опасения, что страны, не согласовавшие унификацию цифрового налога, создадут прецедент двойного налогообложения: будут дважды получать налог с ИТ корпораций – по своей ставке и по ратифицированной.

Так же стоит вопрос: может ли помешать унифицированная ставка цифрового налога предоставлению льгот социально значимым компаниям и отраслям? В России сейчас IT-отрасль – это отрасль особенных льгот и преференций.

Станет ли цифровой налог нарушением мультистейкхолдерной модели, в которой каждая из заинтересованных сторон получает свой бонус от процесса и результата? Будут ли с введением налогового бремени нарушены права конечных пользователей Интернет-платформ и равный доступ к услугам и информации IT-гигантов?

Будем внимательно следить за новостями и успехом внедрения Digital tax на глобальном и локальном уровне.

[111] https://www.oecd.org/newsroom/130-countries-and-jurisdictions-join-bold-new-framework-for-international-tax-reform.htm

ОБ ИЗМЕНЕНИИ ЗАКОНОДАТЕЛЬСТВА В ЦИФРОВОЙ СРЕДЕ В 2022 ГОДУ

Информация подготовлена **Гришиной Ю.С.**, АНО «Цифровая экономика»

Мониторинг изменений законодательства в 2022 году показал активное продвижение к достижению результатов Национальной программы «Цифровая экономика Российской Федерации».

Основными направлениями изменений законодательства в цифровой среде стали:

- регулирование сбора, хранения персональных данных и доступа к ним;
- повышение технологической безопасности предприятий России;
- расширение перечня дистанционно проводимых работ и услуг;
- формирование и объединение баз данных и предоставление доступа к ним;
- поддержка ИТ-компаний.

Законодательство следовало за активно меняющимся рынком. Так, увеличение массива собранных персональных данных и рост объемов мошеннических действий с ними повлекли ужесточение правил их получения и хранения. Теперь госорганы и организации не вправе хранить биометрические персональные данные, а должны передавать их в Единую биометрическую систему (ЕБМ), откуда аккредитованные компании на возмездной основе могут получать их в зашифрованном виде.

С другой стороны, изменился подход к обороту персональных данных в части переосмысления согласия на их обработку. Базой для выработки стали не страхи людей, а экономический анализ ценности данных в обороте и баланс между экономическим развитием и защитой персональных данных. В частности, введены требования к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения законодательства.

Важным нововведением является установление прямого запрета операторам отказывать гражданам в услуге из-за несогласия человека предоставить свои персональные данные (в том числе биометрические), если такое предоставление по закону необязательно. Также операторы должны прекращать дальнейшую обработку персональных данных по требованию их владельца. Одновременно ограничен доступ к персональным

данным, содержащемся в Едином государственном реестре недвижимости: он может быть предоставлен третьим лицам только с согласия их субъекта.

Основные нововведения, направленные на совершенствование правовой защищенности субъектов персональных данных и усиление госконтроля в данной сфере выражались введением новых обязанностей операторов персональных данных: требованием о передаче биометрических персональных данных в ЕБМ; расширен перечень случаев, в которых операторы обязаны уведомлять о планах обработки данных, в т. ч. полученных из других источников; обязанностью информирования об инцидентах с принадлежащими операторам базами данных; обеспечении непрерывного взаимодействия с госсистемой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы России. Введено ограничение на обработку биометрических персональных данных несовершеннолетних. Усовершенствован порядок трансграничной передачи персональных данных. Введена экстерриториальность применения российского законодательства о персональных данных.

Введённые меры по повышению технологической безопасности касались дистанцирования от использования импортных программных продуктов на значимых объектах критической информационной инфраструктуры. Например, введен запрет на закупку иностранного программного обеспечения органам государственной власти и заказчикам, осуществляющим закупки в соответствии с Федеральным законом от 18 июля 2011 года № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц»; утверждены Правила перехода на преимущественное использование российского ПО. Одновременно утвержден перечень федеральных органов исполнительной власти, уполномоченных на согласование возможности осуществления закупок иностранного программного обеспечения.

С 1 марта 2023 года банкам, некредитным финансовым организациям, госкомпаниям, обществам с долей публичного участия в уставном капитале более 50 % и другим организациям запретили применять иностранные мессенджеры для передачи: платежных документов; персональных данных граждан России; сведений о безналичных денежных переводах; информации для проведения платежей; данных о банковских счетах и вкладах россиян. Ограничена возможность владений классифайдами иностранцами.

У зарубежных ИТ-компаний с суточной аудиторией более чем 500 тыс. пользователей появилось обязательство иметь в России свой филиал, уполномоченное юридическое лицо или представительство.

В очередной раз расширен перечень отечественных приложений для обязательной предустановки на отдельные виды технически сложных товаров.

В то же время государство внедряет новые механизмы использования собранных данных для повышения удобства населения и организаций:

- при обеспечении идентификации личности работника допускается дистанционное проведение его медосмотра;
- участники гражданского, арбитражного и административного судопроизводства могут в электронном виде, в том числе через Единый портал госуслуг, подавать исковые заявления, ходатайства и иные документы, дистанционно участвовать в судебных заседаниях;
- начат эксперимент по осуществлению розничной торговли некоторыми видами рецептурных лекарственных препаратов дистанционным способом, в т. ч. на основании рецептов, размещенных в системе Госуслуг.

Кроме того, реализовано около 30 государственных и коммерческих сервисов и услуг с использованием усиленной неквалифицированной электронной подписи в инфраструктуре Госуслуг (сервис «Госключ»), в т. ч. возможность получения ИНН.

Одновременно, формируются реестры в разных сферах: единый реестр Интернет-рекламы; единый регистр застрахованных лиц, имеющих полис обязательного медицинского страхования; с 1 марта 2023 года ведется учет персональных данных лиц, участвующих в осуществлении медицинской деятельности и фармацевтической деятельности, а также лиц, обучающихся по образовательным программам среднего профессионального и высшего медицинского образования, образовательным программам среднего профессионального и высшего фармацевтического образования.

Успешно работает «Витрина данных ГИБДД». С сентября 2023 года создается три региональных информационных ресурса: реестр перевозчиков, реестр такси, реестр служб заказа такси. Все данные из них будут передаваться в федеральную государственную информационную систему.

Деловое сообщество объединяет усилия в защите прав потребителей. Подписана Хартия профессиональной этики сервисов размещения объявлений участниками рынка классифайдов, направленная на создание взаимовыгодной и безопасной среды взаимодействия потребителей и компаний. Кроме того, Wildberries, Ozon и «Яндекс. Маркет» осуществляют совместное ведение единой цифровой информационной системы по борьбе с контрафактной продукцией.

В систему вносятся данные о случаях размещения контрафакта. Остальные площадки могут заблокировать предложение такого продавца у себя.

Также происходит частичное замещение привычного документооборота электронным:

- с 1 апреля 2023 года самоходные машины и другие виды техники, изготовленные или выпущенные в обращение в государствах-членах, регистрируются в Республике Беларусь, Республике Казахстан и Российской Федерации только при наличии электронных паспортов;
- активно внедряется электронный кадровый документооборот;
- действует система электронных перевозочных документов для грузовых автоперевозок;
- увеличивается функционал системы электронного документооборота «Портал Морской порт».

Постоянно расширяется контроль за деятельностью на рынке путем маркировки, в том числе: лекарственных средств, молочной продукции и воды в розничной продаже, изделий из восстановленного табака или расширенной табачной жилки, пива и слабоалкогольных напитков, кресел-колясок и велосипедов.

Одновременно государство расширяет комплекс мер, направленный на ускоренное развитие IT-отрасли:

- до 31 декабря 2024 года применяется пониженная ставка по налогу на прибыль для организаций, осуществляющих деятельность в сфере радиоэлектронной промышленности;
- с 1 января 2023 года установлен повышающий коэффициент к расходам на приобретение некоторых видов российского радиоэлектронного оборудования и российских программ для ЭВМ, а также предоставляется инвестиционный налоговый вычет в отношении затрат на внедрение программ для ЭВМ, радиоэлектронной продукции;
- до 2024 года включительно для IT-компаний установлена нулевая ставка по налогу на прибыль (в части налога, зачисляемого в федеральный бюджет);
- расширен круг IT-компаний, которые могут использовать режим пониженных ставок по налогу на прибыль, а также льготные тарифы по страховым взносам;
- IT-компании могут получить льготный кредит на обеспечение своей деятельности;

- скорректированы правила предоставления субсидий на частичное возмещение затрат на разработку цифровых платформ и программных продуктов для производства высокотехнологичной промышленной продукции;
- утверждены параметры льготной ипотечной программы для специалистов, работающих в сфере информационных технологий;
- с 1 января 2023 года установлены новые основания для ускоренной амортизации отдельных ОС и НМА;
- до 31 марта 2023 года ряд товаров, предназначенных для развития цифровых технологий, освобождаются от уплаты ввозной таможенной пошлины при поставках в страны ЕАЭС;
- упрощена процедура трудоустройства иностранных граждан — IT-специалистов;
- до 31 декабря 2024 года установлен запрет на плановые проверки некоторых аккредитованных IT-компаний, на деятельность которых распространяется Федеральный закон от 26 декабря 2008 года № 294-ФЗ;
- до 3 марта 2025 года в отношении аккредитованных IT-организаций приостановлено проведение выездных (повторных выездных) налоговых проверок.

В конечном счете, все перечисленные меры направлены на защиту прав граждан, повышение доступности государственных услуг и ускоренное развитие IT -сферы.

ЦЕНТР ГЛОБАЛЬНОЙ
ИТ-КООПЕРАЦИИ

www.cgitc.ru

125009, г. Москва, Тверской бульвар, д. 14, стр. 1

Москва, 2023 г.