Доклад Международного дискуссионного клуба «Валдай»

Валдай | Международный дискуссионный клуб

Международная конкуренция и лидерство в цифровой среде

Андрей Безруков, Михаил Мамонов,
Максим Сучков, Андрей Сушенцов

ru.valdaiclub.com
#valdaiclub

Январь 2021

ISBN 978-5-907318-23-6

Российская Федерация, 115184, Москва,
улица Большая Татарская, дом 42

Об авторах

А.О. Безруков
член Президиума Совета по внешней и оборонной политике;
президент ассоциации экспорта технологического суверенитета;
профессор МГИМО МИД России

М.В. Мамонов
директор блока по поддержке государственных программ
и международной деятельности АО «Почта России»

М.А. Сучков
директор Центра перспективных американских исследований
ИМИ МГИМО МИД России; доцент кафедры прикладного анализа
международных проблем МГИМО МИД России; научный сотрудник
инициативы по диалогу в рамках второго направления дипломатии
в Институте Ближнего Востока в Вашингтоне

А.А. Сушенцов
программный директор Международного дискуссионного клуба «Валдай»;
директор Института международных исследований МГИМО МИД России

Содержание

Вступление

Сфера технологий стала одной из важнейших в борьбе за власть в XXI веке. К началу третьего десятилетия нового века очевидно оформление двух основных «технологических экосистем» – американской и китайской. В этой связи для России актуальна дилемма: подключаться к одной из существующих платформ или разрабатывать собственную? Выбор в пользу первого варианта предполагает определение условий, на которых должно осуществиться такое «присоединение». Вторая опция требует более амбициозной стратегии, которая определит ключевые параметры собственно российской «техноэкосистемы».

Американская система является старейшей, наиболее крупной и развитой. Она опирается на безусловное технологическое лидерство США. Ключевая цель американской стратегии в технологической сфере – удерживать инициативу в области инноваций, продлить собственное доминирование и не допустить появления сопоставимых конкурентов на глобальном рынке. Для этого ведётся активная кадровая работа, создаются льготные условия для развития экосистемы стартапов, используются далёкие от экономических методы конкуренции.

Ёмкость рынка и благоприятные внутренние условия позволили США вывести на рынок наиболее крупных технологических и интернет-гигантов, права интеллектуальной собственности которых законодательно защищены. Косвенным, но значимым фактором американской техноэкономической системы является создание многочисленных продуктов общего доступа *(common goods)*. Всё это позволяет американским компаниям предоставлять всему миру пробную версию собственных продуктов, что даёт пользователю возможность без избыточных затрат получить доступ к одним из наиболее совершенных технологий. Предлагаемые США принципы открытости и свободы в цифровой сфере подкупают. Однако не приходится сомневаться, что в момент, когда американцы усомнятся в собственной гегемонии в технологической среде, эти принципы будут незамедлительно пересмотрены. Возникнут непреодолимые границы и барьеры, нацеленные на сдерживание конкурентов и защиту американского лидерства.

Даже внутри самих США решения техногигантов по блокировке и удалению более 70 тысяч аккаунтов, включая страницы президента Дональда Трампа, похожи на открытые попытки изъятия у власти инструментов управления. В этом случае компании сыграли за политический истеблишмент против неугодного «спойлера» системы. Вероятно, в ближайшие годы команда политических, финансовых и технологических глобалистов будет продолжать сообща противодействовать национал-индустриальной повестке дня в Америке и других странах. При этом из стана демократов всё же доносятся опасения, что, какими бы удобными ни были предлагаемые корпорациями технологии, усиление влияния техногигантов опасно как по причине накопления ими «беспрецедентной экономической силы», так и по причине

наращивания «контроля над политическим общением и коммуникациями»[1]. Доминирование техногигантов в распространении информации и их способность к политической мобилизации масс уже сейчас представляют угрозу для демократических правительств.

Китайская техноэкономическая платформа меньше американской, хотя и здесь очевидны притязания на технологическое лидерство. Значительный объём финансовых и людских ресурсов позволяет китайской экосистеме быть замкнутой на себя и административно перераспределять ресурсы на те области технологического развития, которые представляются Политбюро КПК наиболее перспективными. Китайцы первые в мире поэкспериментировали с автономизацией ряда сервисов и услуг, выстроив «Великую Китайскую цифровую стену» *(The Great Firewall of China)*. И если американцы предоставляют всему миру пробную версию своего продукта, то конкурентоспособность китайской модели опирается на дешевизну их предложения и участие в финансировании передовых разработок в других государствах[2]. При этом Китай опирается на тактику выжидания и не реагирует на провокации США. Америку в Китае справедливо рассматривают как более весомого и сильного игрока в этой сфере. Однако темпы роста китайской технологической индустрии позволяют Пекину рассчитывать на то, что достижение сопоставимого с США положения на рынке – вопрос времени. Маловероятно, что американцы смогут остановить этот процесс. В мировой политике есть запрос на прагматизм. Откликаясь на него, всё большее число американских союзников (включая европейцев) благосклонно воспринимают предложения Китая о сотрудничестве в цифровой сфере[3].

Растущее осознание европейскими странами важности цифрового суверенитета может быть потенциально интересно для России. Ключевые страны Европы – Германия, Франция, Италия, Нидерланды – опасаются зависимости от американцев и китайцев. Необходимость развития национальной технологической платформы особенно акцентируют французы. Европейцы боятся потерять субъектность в мировой технологической среде и в конечном счёте оказаться в ситуации, когда их голос не будет учтён[4].

Россию с европейцами объединяют опасения попасть в зависимость от ведущих игроков и утратить собственную автономию. При этом Россия, как и некоторые другие европейские страны, обладает компетенциями к формированию самостоятельного полюса мощи в цифровой сфере. Российские аргументы о разработке стандарта совместимости данных с большей вероятностью могут быть услышаны в Европе, чем в Китае и США.

---

[1] Гоэл А., Ричман Б., Фукуяма Ф. Как спасти демократию от технологий // Журнал «Россия в глобальной политике», 2021. URL: https://globalaffairs.ru/articles/spasti-demokratiyu-ot-tehnologij/

[2] Уже сейчас китайские компании участвуют в развитии сетей 5G в 45 странах, развивают научные коллаборации в 145 странах и внедряют системы городской безопасности в 71 крупном городе по всему миру.

[3] Венгерские власти активно приглашают китайских производителей настраивать сети 5G в Будапеште. В Германии дискуссия об участии Китая в развитии национальных сетей 5G вышла на уровень президента и канцлера.

[4] Именно этот мотив стоит за инициативой французского президента Эммануэля Макрона вывести 25 французских технологических «единорогов» на рынок к 2025 году.

Последние два государства сами обладают значительным массивом данных и не готовы делиться ими с третьими странами. Однако политические разногласия Москвы с европейцами могут стать непреодолимым препятствием к полноценной коллаборации, что является для России дополнительным мотивационным фактором в формировании собственной технологической платформы.

Мировые тренды развития цифровой среды

Глобальная цифровая революция привела к радикальной трансформации не только технологического и экономического укладов, но и общественных отношений, самой философии жизни человека. Эти изменения в полной мере проявились в сфере международных отношений. Сегодняшняя ситуация в мире схожа (хотя и на принципиально новом уровне) со временем изобретения ядерного оружия и начала освоения космоса, когда технологические изменения существенно изменили международное поведение государств. Уже сейчас можно идентифицировать ряд запущенных новыми технологиями тенденций, которые определят направления дальнейшей эволюции системы международных отношений.

Стремительное развитие науки и техники создало на национальном и глобальном уровнях предпосылки для сокращения социально-экономического неравенства. Однако оно же и повысило уязвимость – и мнительность – общества перед лицом новых (или старых, получивших новое обличье) вызовов и угроз. Новые каналы и способы коммуникации кратно повысили информационную связанность мира. Но они же способствовали атомизации государств, которые стремятся защитить такие каналы от зарубежного вмешательства. Взрывной рост технологий и способов их использования продолжает стирать грань между виртуальным и реальным миром, фактом и вымыслом. Это множит неопределённость в международных отношениях и укрепляет их анархичное состояние.

Эта неопределённость усугубляется всё возрастающим разрывом между динамикой развития и внедрения инноваций и скоростью отражения этих изменений в нормативной ткани. Феномены, неурегулированные международным правом, становятся вызовом классической системе международных отношений. Так, отсутствие кодифицированных договорённостей по ограничению использования искусственного интеллекта

или суперкомпьютеров и облачных вычислений в военной области вовлекает обладающие такими технологиями державы в порочный круг постоянной гонки вооружений, что отвлекает ресурсы и внимание от развития их гражданского применения. Притом что в новых условиях именно Интернет становится ключевым источником новых опасностей, у мировых правительств нет единых подходов к определению понятия «суверенитет в киберпространстве», пока ещё не ведётся работа по разработке международных соглашений, аналогичных договору о космосе, об Антарктике или о суверенитете в воздушном пространстве.

Всеохватывающий характер процессов цифровой трансформации приводит к тому, что они попадают в фокус внимания всё возрастающего числа международных организаций – как профильных (МСЭ), так и непрофильных (ЮНЕСКО, ЮНКТАД, ПАСЕ). Это рассеивает международную цифровую повестку дня и множит взаимоисключающие подходы к её вопросам. Отсутствие единого и чёткого понятийно-категориального аппарата в этой сфере усугубляет противоречия и споры[5].

На более технологически-ориентированных международных площадках – правительственных и неправительственных – борьба разворачивается за универсальное признание создаваемых государствами или крупными корпорациями технических стандартов. Наиболее удачливые лоббисты из числа правительств и бизнеса получают в случае кодификации предлагаемого ими стандарта значительное рыночное преимущество: весь мир начинает потреблять именно их продукцию, а они получают возможность существенно влиять на дальнейшее развитие выбранной технологии. Подобная борьба за стандарты имеет и далеко идущие международно-политические последствия. С учётом продолжающегося стремительного проникновения «цифры» в общественную жизнь страны – поставщики цифровых технологий крепко «привязывают» к себе государства-клиентов, «подсаживая» их на определённые стандарты и типы решений, повышая зависимость таких стран от своего экспорта – по аналогии с экспортом оружия или энергетических ресурсов.

Серьёзность данной проблемы ярко иллюстрирует, например, ситуация, с которой столкнулись страны – участницы ЕАЭС при реализации цифровой интеграции. Создание единой системы электронного обмена юридически значимыми документами оказалось сильно затруднено тем

[5] Показательна в этой связи полемика на площадке ООН вокруг терминов «информационная безопасность» и «кибербезопасность».

фактом, что различные государства ЕАЭС используют различные криптографические стандарты, не все из которых признаны безопасными. Отсутствие координации при их внедрении, пусть и по объективным причинам, привело к появлению технического барьера на пути развития интеграционных процессов, имеющего при этом долгосрочные политические и экономические последствия.

Глобальная цифровизация кратно повысила международную правосубъектность негосударственных участников международных отношений. Изначально техническая НКО «Корпорация по управлению доменными именами и *IP*-адресами», созданная при участии правительства США для регулирования вопросов, связанных с доменными именами, *IP*-адресами и вопросами функционирования глобальной сети, превратилась в ведущий институт «управления Интернетом», где государства не имеют главенствующей роли[6].

Транснациональные гиганты – *Google*, *Facebook*, *Microsoft*, *Huawei*, *TikTok*, *Alibaba*, *YouTube* – уже сегодня на равных разговаривают с национальными и иностранными правительствами. Игнорировать их в качестве фактора национальной безопасности невозможно. С одной стороны, накапливаемая такими экосистемами информация и внедряемые ими передовые решения представляют колоссальный интерес для компетентных ведомств. С другой – их способность как информационных ресурсов транслировать на гигантскую аудиторию те или иные информационные сообщения, напрямую или косвенно – через контролируемую выдачу по поисковым запросам, – становится фактором национальной политической жизни. Указанные свойства таких корпораций наделяют их «правом голоса» на международной арене и одновременно делают их объектами строгого национального регулирования. Объяснимое стремление государств контролировать их информационную деятельность и получать доступ к располагаемым ими данным приводит к эрозии либеральных ценностей – свободы слова, тайны переписки, тайны частной жизни – и поднимает вопрос об их применимости в изменившуюся цифровую эпоху.

Отдельным пунктом в противостоянии корпораций и государств остаётся вопрос их справедливого налогообложения, особенно если их сервисы

[6] В 2016 году организация вышла из контракта с правительством США, но у многих стран сохраняются подозрения относительно политической нейтральности этого некоммерческого института, который определяет «правила игры» в кибермире. Безотносительно справедливости таких подозрений важен сам прецедент регулирования негосударственным игроком критически значимой для национальной безопасности сферы.

действуют в иностранной юрисдикции[7]. Важно не допустить двойного налогообложения таких платформ, дабы избежать ухудшения положения потребителей и получаемых ими продуктов и услуг.

Возможно, впервые обычные граждане получили способность напрямую влиять на международные отношения в таком масштабе, как сегодня. Социальные сети, мессенджеры и интернет-телевидение практически выиграли конкуренцию с традиционными СМИ, сделали из каждого обладателя смартфона потенциального журналиста и наделили его способностью моментально делать свои «новости» для миллионов человек. Столь отрадное, казалось бы, проявление свободы говорить и быть услышанным омрачается тем, что в эпоху «постправды» верификация факта больше не является требованием для нашего доверия к нему. В лучшем случае неумышленный субъективизм или жажда внимания «репортера-любителя», не связанного профессиональной журналистской этикой или политикой издания, а в худшем – распространение заведомо ложной информации могут иметь разрушительные последствия для общества и государства.

Вместе с тем пример с удалением аккаунта Трампа в *Twitter* демонстрирует и другой тренд. На протяжении четырёх лет президентства Трампа *Twitter* был важным ресурсом его власти и главным инструментом борьбы с политическими противниками. С его помощью Трамп задавал информационную повестку дня, диктовал политическую волю, назначал на должности и с позором увольнял вчерашних единомышленников. Для миллионов сторонников президента *Twitter* стал рупором недовольства Вашингтоном. С его помощью можно было, оставаясь непонятым, быть хотя бы услышанным элитами. Поэтому одних твиты президента забавляли, других – пугали, третьих – раздражали.

На уровне символа удаление аккаунта Трампа – даже уже после того, как он сдал назад и призвал своих сторонников к мирному протесту, – гораздо более демонстративная и внезапная его «ликвидация» как президента за две недели до срока окончания полномочий, чем через суд или импичмент. Но что ещё важнее – эту миссию по «ликвидации» осуществили не Конгресс, не военные и не Верховный суд, а глава технологической компании *Twitter*.

Этот случай, вероятнее всего, с одной стороны, поднимет запрос третьих стран на «цифровой суверенитет» от американских техногигантов,

[7] Как исчислить и собрать налоги, например, с такой платформы как Booking.com, которая лишь сводит спрос и предложение и обеспечивает гарантии поступления платежа, но не владеет никаким имуществом, кроме своей цифровой инфраструктуры? Притом что субъекты «физического мира» – владельцы отельной недвижимости и граждане – платят налоги в этой транзакции.

с другой – усилит намерение этих государств защититься от доминирования своих и иностранных технологических компаний путём более жёсткого законодательного регулирования их деятельности на своих территориях. В долгосрочной перспективе это может укрепить политическую фрагментацию мира.

Дальнейшее развитие когнитивных технологий, в первую очередь *deepfake*[8], наделяет злоумышленников неограниченными возможностями по созданию токсичного контента, который по силе воздействия уже может причисляться к оружию массового поражения[9].

Таким образом, рост свободы общества и укрепление инструментов её реализации парадоксальным образом развивается параллельно с укреплением полицейской мощи государства, и это становится новой нормой повседневной жизни. Усиление второй тенденции происходит и по объективным причинам: стремление государств обеспечить безопасность граждан, в том числе ограничив их доступ к «даркнету» и неконтролируемым элементам сети, едва ли можно назвать диктаторской прихотью правительств. Степень деанонимизации пользователей в сети будет и дальше возрастать.

Отсутствие признаваемых всеми игроками институтов арбитража или расследования киберпроисшествий и киберпреступлений, пока ещё слабая развитость инструментов цифровой криминалистики делает практически невозможным достоверное определение виновной в инциденте стороны. Что, в свою очередь, повышает уровень недоверия и конфликтности между странами. При этом в условиях развития новых технологий – в первую очередь Интернета вещей и автономных интеллектуальных систем – злоумышленникам достаточно иметь достаточно мощный бытовой компьютер или даже смартфон, чтобы взломать систему безопасности объекта критической инфраструктуры и вызвать катастрофу или завладеть чувствительной информацией, а хакером совершенно необязательно окажется диверсант или террорист, это может быть и технически одарённый «тинейджер».

Попытка стран оградить себя от такого проникновения имеет ряд последствий. Прежде всего, государства стремятся ограничить уязвимость сети за счёт стимулирования импортозамещения и глубокой локализации – доверять «своему» контролируемому производителю оборудования или решений проще. Это приводит к распаду международных

[8] Методика синтеза изображения, основанная на искусственном интеллекте.

[9] Для создания достоверной подделки уже даже не нужен человек: нейросеть может сама создавать симулякры, наделять их достоверной биографией – а в недалёком будущем, вероятно, и снимать с ними видеоролики любого желаемого содержания.

производственных цепочек и определённой эрозии принципов международного разделения труда. В условиях, когда все, кто может, начинают производить свои собственные критическое оборудование и «софт» (сервера, операционные системы, антивирусы и системы безопасности), экономическая специализация теряет свою привлекательность. Кроме этого, определение уполномоченных операторов, ограничение конкуренции на рынке неизбежно приводит к замедлению развития технологий, заставляя государства жить в дилемме: прогресс или безопасность. Здесь, как и во многих других аспектах глобальной цифровой экономики, проявляется противоречие между информационным обменом как явлением глобальным и физической инфраструктурой, имеющей территориальную привязку, а значит – находящейся под определённым суверенитетом.

Это противоречие выступает со всей очевидностью в вопросе хранения, обработки и перемещения информации по интернет-каналам. Исторически сложился серьёзный дисбаланс в географическом распределении базовой инфраструктуры и национальной принадлежности основных интернет-игроков. Свыше 60 процентов от общего числа доменов управляются американскими игроками *(Verisign, Afilias)*, более чем 50 процентов сетей доставки контента принадлежат американским компаниям *(Amazon, Akamai, CloudFlaire)*, все основные провайдеры первого уровня – резиденты США, в США же находятся и десять из тринадцати *DNS*-серверов. Неудивительно, что при такой «интернет-географии» и осознании готовности США идти в односторонних санкциях на весьма крайние меры[10] государства, не являющиеся непосредственными союзниками Вашингтона, стремятся создать альтернативный защищённый контур «национального, суверенного интернета» – и число таких государств возрастает. С другой стороны, по оценкам экспертов спутниковый Интернет не позднее середины этого века может вытеснить Интернет кабельный – и на новом витке борьба переместится в космос или верхние слои атмосферы[11], но её природа, состоящая в нежелании государств оставлять ключевую инфраструктуру вне зоны своего суверенного контроля, сохранится.

Стремление к суверенному контролю всё большего числа государств находит отражение и в их отношении к вопросу хранения персональных данных граждан. И европейский *GDPR*, и российский так называемый

[10] Например, периодически возникающие разговоры о возможности отключения России от системы быстрых платежей SWIFT, притом что Россия входит в двадцатку самых активных пользователей этой системы, подобный риск нельзя назвать высоким – но он и далеко не нулевой.

[11] Hurst N. Why Satellite Internet Is the New Space Race // PC, 2018. URL: https://www.pcmag.com/news/why-satellite-internet-is-the-new-space-race

«пакет Яровой» при всех нюансах каждого из подходов, постулируют необходимость хранения персональных данных всеми операторами интернет-рынка на серверах, расположенных в национальной юрисдикции. Этому подходу агрессивно оппонируют в первую очередь англо-саксонские государства – участники «системы пяти глаз» (США, Великобритания, Канада, Новая Зеландия, Австралия), указывая на данную меру как избыточную и подавляющую права и свободы. С учётом описанных выше дисбалансов в интернет-пространстве позиция США и их союзников объяснима. Тем не менее, по мере повышения оцифровки личности человека, возможности его цифровой идентификации, перемещения в облачное хранение всех его личных данных цена ошибки при защите такой информации кратно повышается. В случае нарушения контура безопасности информационного хранилища идентичностью гражданина не просто могут завладеть злоумышленники – она может быть полностью стёрта, и такая цифровая смерть отрежет жертв атаки от возможности реализации базовых социальных прав. Именно поэтому возрастающая строгость требований к национальному хранению данных становится доминирующим требованием эпохи.

Для национальных государств в ближайшие годы возникают два важнейших вопроса.

Первый вопрос – насколько они способны гарантировать жизнеспособность своей информационной критической инфраструктуры в условиях кибервойны и роста сетевого пиратства. Кибератаки или системные сбои в сетях способны надолго выключать целые отрасли и города с непредсказуемыми последствиями для страны и её населения, однако актуальность и величина таких угроз ещё далеко не осознаны.

Второй вопрос – насколько хорошо правительства понимают принципы и способы обеспечения безопасности персональных данных и как будет регулироваться порядок оборота деперсонифицированных больших данных. Овладение такими данными другим государством позволит построить ему достоверную картину развития экономики и промышленности, уязвимостей сельского хозяйства, эпидемиологической обстановки, профилей потребления и скорректировать свою политическую, военную или экономическую стратегию соответствующим образом. Очевидно, ускоренное развитие национального законодательства, регулирующего принципы обращения национальных больших данных и выход на межгосударственные переговоры по этому вопросу, – дело недалёкого будущего.

Государства и будущий цифровой мир: дуополия или олигополия?

Уже сегодня присутствие государств в высшей лиге мировой политики невообразимо без стратегии развития в глобальной цифровой среде, наличия ресурсов, собственных идей и продуктов в этой сфере. *Сама категория «великодержавности» в XXI веке подразумевает создание собственных технологических платформ, а в идеале – формирование технико-экономического блока.* Обязательными атрибутами такого блока являются контролируемый им значительный кусок мирового рынка, собственная валютная зона с эмиссионным центром, собственная модель развития, набор ресурсов, технологий и научных компетенций, позволяющие блоку быть независимым от других, по крайней мере в таких ключевых областях, как оборона и критическая инфраструктура.

Попытка каждого из блоков исключить влияние конкурентов на свою критическую инфраструктуру неизбежно приводит к политизации технологий и технологическим войнам. Цифровые технологии, являясь сквозными для всего современного экономического и социально-политического пространства, становятся главным полем новой войны[12]. Кибератаки на цифровую критическую инфраструктуру могут быть не менее деструктивными, чем ядерное или биологическое оружие[13].

На фоне доминирования ряда развитых стран в цифровых технологиях и возникновения глобальных монополий, контролирующих сетевую инфраструктуру и потоки данных, возникает угроза цифрового неравенства и цифрового колониализма. *Цифровой технологический суверенитет становится необходимым условием суверенитета политической и национальной независимости.*

Перестройка принципов функционирования международных экономических отношений и всей модели мировой геоэкономики предоставляет ведущим техноэкономическим блокам, своеобразным «цифровым неоколониалистам» современности, новые возможности. Продолжает

[12] Сучков М., Тэк С. Будущее войны. Доклад Международного дискуссионного клуба «Валдай», 2019. URL: https://ru.valdaiclub.com/files/28848/

[13] Фаттер Э. Необходимость запрета кибератак в ядерной сфере и превентивные меры США и России в сфере контроля над вооружениями. Валдайская записка №95, 2018. URL: https://ru.valdaiclub.com/files/23636/

увеличиваться разрыв – теперь уже цифровой – между глобальными провайдерами цифровых технологий и странами-реципиентами, постепенно подпадающими под всё большую зависимость от технологически развитых государств.

На текущем этапе страны – «цифровые неоколониалисты» предлагают объектам экономического освоения исключительно льготные условия создания необходимой для перехода в цифровое будущее инфраструктуры. Тем самым они сразу же обеспечивают их привязку к собственным решениям – от платёжных систем до систем хранения данных и обеспечения электронного документооборота. Но главное, они обеспечивают себе неограниченный и практически бесплатный доступ к большим данным, получая от этого не только непосредственный экономический эффект и дополнительное преимущество при развитии собственных инструментов искусственного интеллекта и нейросетей[14], но и эффективные инструменты контроля над своими цифровыми колониями.

Цифровой колониализм продолжит укрепляться, и нельзя исключить возрождения Совета при ООН по опеке – уже с новыми, цифровыми функциями и полномочиями. При этом канонические границы стран первого, второго и третьего мира уже претерпели колоссальные изменения и продолжат меняться. Бывшие страны третьего мира получают возможность условного прыжка «из феодализма в социализм, минуя стадию капитализма», – создания передовой инфраструктуры нового поколения без необходимости поддержания функционирования старой инфраструктуры (за её отсутствием).

В этом смысле можно предвидеть цифровой рывок более богатых государств Ближнего Востока и Африки и их выход на значимые на цифровой арене роли. Наконец, изменяются и международные финансовые и трудовые отношения – цифровые активы перемещаются в более комфортные юрисдикции ещё легче, чем финансовые, и практически не оставляют следов такого перемещения. Появление криптовалют лишает государства-монополии на ещё одно суверенное право – право эмиссии. Меняются и понятия «утечка мозгов» и «трудовая эмиграция»: теперь национальные «цифровые пролетарии» не должны переезжать за рубеж – им достаточно, оставаясь в домашних границах, работать на иностранную корпорацию, отчуждая той всю свою интеллектуальную собственность, и наоборот – талантливые хипстеры могут перебраться в более комфортные климатические условия, продолжая при этом развивать национальную экономику.

[14] Уже к 2025 году глобальный рынок больших данных достигнет 230 млрд долл.

В то же время цифровые технологии, формирующие и ежедневный быт, и информационное пространство каждого человека, начинают оказывать всё более заметное влияние на его психику и практики принятия решений. Индивидуум не только становится рабом цифровых платформ глобальных монополий, но и реально поставлен в рамки, где всё его существование привязано к девайсам – мобильному телефону, планшету, «умным часам». Под видом предоставления удобств они ограничивают выбор человека в принятии решений и манипулируют его поведением, в том числе через подталкивание его к следованию «определённым маршрутом». В этих неравноправных отношениях цифровые монополии под страхом исключения из социальной среды экспроприируют и бесконтрольно эксплуатируют персональные данные и даже креативный контент.

Повсеместное внедрение цифровых технологий, в том числе цифровизация промышленности и государственных органов, внедрение сетей *5G*, формирует императив обеспечения безопасности и устойчивости всей цифровой критической инфраструктуры. Без решения этой задачи цифровизация может оказаться строительством «дома на песке».

Чтобы ликвидировать «баррикады» и «минные поля» на пути цифровой экономики, государство должно гарантировать как безопасность граждан и бизнеса, так и понятные правовые отношения в цифровой среде. Особенно это касается собственности и использования персональных и «деперсонализированных» данных и созданного контента.

Принадлежность и стоимость данных – лишь одна из накопившихся в цифровой среде проблем, срочно требующих решения. Не менее актуальна необходимость разрешить противоречие между требованиями национального или локального хранения данных и глобальной транспарентностью технологических и корпоративных процессов, где данные о работе двигателя на самолёте, принадлежащем авиакомпании одной страны и пролетающем над другой страной, обрабатываются в реальном времени в третьей.

По мере того как формируются техноэкономические блоки, конкурентная борьба в цифровом пространстве принимает форму войны платформ и стандартов[15]. В то же время ряд стран и региональных объединений, не обладающих ни контролем над большой частью глобального

[15] Её примеры на текущем этапе – это противостояние американских и китайских техногигантов: Huawei и CISCO, Alibaba и Amazon, Facebook и *WeChat*.

цифрового рынка, ни доминирующими платформами (например, Индия, Бразилия, Япония, Россия или Евросоюз), будут вынуждены искать общие пути сохранения независимости и конкурентоспособности, в том числе путём создания общих платформ на основе открытой архитектуры и открытого кода.

Россия в цифровой повестке дня: возможности и ограничения

Россия является одной из немногих стран, обладающих технологическими заделами и человеческими компетенциями для выстраивания собственной технологической экосистемы. Доставшаяся России в наследство от Советского Союза мощная инженерно-математическая школа остаётся источником ключевого для цифрового развития ресурса – квалифицированных кадров. Россия обладает большинством признаков суверенной технологической платформы. Разработан и продолжает развиваться национальный поисковик. Российские социальные сети «ВКонтакте» и «Одноклассники» по-прежнему популярнее *Facebook* и *Instagram* не только в России, но и в большинстве государств СНГ. Развиваются собственные облачные технологии, создаются отечественные процессоры. Цифровые решения российских компаний обладают существенным экспортным потенциалом – в первую очередь когнитивные и самообучающиеся системы, решения в области кибербезопасности, защищённого электронного документооборота и платформы для оказания услуг населению. Запущенная два года назад национальная программа «Цифровая экономика» обеспечит к 2024 году 97 процентов всех национальных домохозяйств и все объекты социальной инфраструктуры (школы, больницы, полицейские участки) доступом к скоростному широкополосному Интернету. Это радикально изменит возможности для развития предпринимательства, телемедицины и дистанционного образования, позволит России преодолеть «цифровой разрыв». Уже сейчас Россия входит в топ-10 стран по количеству интернет-пользователей, а сайт «Госуслуги» с его двумя триллионами ежегодных транзакций является самым популярным сайтом государственных услуг в мире.

Растёт доля цифровой экономики в ВВП страны. При всей расплывчатости самого термина уже сейчас она составляет порядка 4–5 процентов ВВП, но продолжает стремительно нарастать темпами, сопоставимыми с государствами – цифровыми лидерами. Кроме того, Россия располагает внушительным спутниковым и радиочастотным ресурсом, что является залогом успешного развития сетей нового поколения.

Нельзя преуменьшать и вызовы, с которыми сталкивается Россия в области цифрового развития. Некоторые из них являются лишь «цифровым» следствием «аналоговых» проблем и угроз. Другие же имеют принципиально новую, самобытную природу. В частности, западные санкции не только ограничивают, помимо прочего, доступ к зарубежным технологиям, но и повышают риски сохранения зависимости от таких технологий до неприемлемого уровня. Случай, связанный с отказом компании *Siemens* от поставок турбин в Крым, поставил под угрозу планы по обеспечению полуострова теплом. Если экстраполировать этот инцидент на цифровую сферу, аналогичный отказ *SAP*, *Oracle*, *CISCO* или *Microsoft* обеспечить своевременное обновление своих работающих в России решений может вызвать сбои – даже коллапс – в работе критически важных систем, в том числе государственного управления и банковского сектора.

Эти и другие тенденции развития мировой политики в последние несколько лет актуализировали для России задачу по формированию надёжной защиты собственной цифровой критической инфраструктуры. Выполнение этой задачи зависит как от эффективности поэтапного и постепенного перехода от импортных программных и аппаратных комплексов, так и от создания эффективной командной вертикали от регулятора до исполнителя в масштабах всей страны.

Решение правительства России о создании реестров отечественного ПО и радиоэлектронного оборудования призвано снизить подобные риски. Без попадания в эти реестры компании не могут рассчитывать на поставку своих решений российским госкорпорациям и органам государственной власти. Подобные меры имеют долгосрочный положительный эффект на развитие России как суверенной технологической державы.

Выстраивание противодействия в сфере информационной безопасности осложняется концептуальной неопределённостью – нечётким разделением двух близких, но разных сфер, связанных с информационными

потоками. И безопасность сигналов в физической сети, переносящей информацию, и вредоносный идеологический контент в российской практике определяются одним и тем же понятием «информационная безопасность». В практике же российских конкурентов по цифровому лидерству безопасность сигналов и сети определяется как кибербезопасность *(cybersecurity)*[16]. Противодействие угрозам в этих двух областях требует разных компетенций. В то время как в России существует достаточное понимание того, как бороться с киберугрозами, в сфере информационного контента российская стратегия требует отдельного осмысления и развития.

Обвинения Москвы в кибервмешательстве во внутренние дела ряда государств было использовано в качестве предлога для усиления санкционного давления и, несомненно, повредило международному имиджу России. Однако эта кампания имела последствия и для ряда крупных российских предприятий и фирм. Они столкнулись с проблемами и дискриминацией на рынках некоторых западных стран. Возможно, ещё более значительны, чем репутационные и даже экономические последствия, риски того, что указанные обвинения будут использоваться Соединёнными Штатами и их союзниками как аргументы для проведения «кибердударов возмездия» или даже «превентивных кибердударов» против России.

В информационном пространстве очевидны уязвимости России из-за доминирования в отечественном сегменте американских монополий – *Google* и *Facebook*. Эти монополии бесплатно эксплуатируют российские данные и всё более активно пытаются влиять на информационное поле и политическую ситуацию в российской внутренней политике. В том числе через манипуляции с контентом и ограничениями доступа российских пользователей к информации и средствам общения. С аналогичными вызовами сталкиваются и другие незападные страны. Есть смысл налаживать с ними более активный диалог о принципах законодательства цифровой эпохи, особенно в части прав собственности на данные, правил их хранения и использования, совместной борьбы с сетевым пиратством, общих правил поведения для государств и бизнеса в Интернете. Принципиальный же вызов для российского законодательства в цифровой сфере – максимально динамично шагать в ногу с развитием самих

[16] США официально провозгласили доктрину наступательной кибервойны (“Defend Forward” Cyber Strategy), выделили кибервойска в отдельный род вооружённых сил и создали отдельное агентство по защите своей цифровой критической инфраструктуры.

технологий и практик, особенно в таких важных для общества областях, как киберпреступность и цифровые финансы.

Ещё одна проблема на сегодняшний день – низкая способность российских компаний и правительства конкурировать с глобальными корпорациями за лучшие кадры. При этом формально «утечки мозгов» может и не происходить – российские таланты продолжают оставаться в России, но давать всю интеллектуальную добавленную стоимость для зарубежных компаний. С учётом несопоставимости экономических потенциалов российского и транснационального бизнеса решение этой проблемы возможно только в рамках административной или понятийной (но в любом случае государственной) плоскости отношений.

Также Россия и российские компании практически не ведут на международных площадках работу по внедрению технологических стандартов и регламентов, благоприятных для функционирования российских разработок. Отчасти это объясняется отсутствием у России доктринального документа, излагающего собственные международные приоритеты в этой сфере по аналогии со Стратегией национальной безопасности или Концепцией внешней политики. В перспективе это упущение может стать причиной технологической изоляции или фактического принуждения Москвы работать с признанными в мире стандартами и протоколами, в выработке которых Россия фактически не принимала деятельного участия.

«Дорожная карта» российского лидерства в цифровой среде

Российская цифровая повестка дня должна отражать позицию нашей страны как одной из основных сил в глобальной системе, как экспортёра безопасности и стабильности. Глобальная роль России в цифровом мире – это роль лидера «цифрового движения неприсоединения» для тех стран, которые бы хотели избежать технологического диктата «цифровых неоколониалистов».

Важно, чтобы развитие цифрового сектора российской экономики, включая электронику и информационные технологии, сопровождалось экспансией на глобальные рынки. Только в этом случае Россия сможет окупить инвестиции в прорывные технологии, завоевать ключевые технологические платформы экономики следующего поколения и выстроить крупные, конкурентоспособные бизнесы.

Раскинувшись на одиннадцать часовых поясов, Россия (даже в мире, где дистанции драматически сокращаются) продолжает играть роль безопасного связующего звена между Европой и Азией. Это в одинаковой мере относится и к глобальной энергетической инфраструктуре, необходимой для поддержки весьма энергоёмкой цифровой экономики будущего, и к сети квантовых коммуникаций, необходимых для безопасной передачи данных. Холодный климат северных регионов России вкупе с дешёвой электроэнергией даёт нашей стране конкурентные преимущества в расположении крупных центров хранения и обработки данных.

Одним из важнейших вызовов для России на сегодняшний день является реализация цифровой интеграционной программы ЕАЭС. Необходимо в сжатые сроки обеспечить возможность государственным органам и бизнесу стран – участниц Союза обмениваться юридически значимыми документами через интегрированную информационную систему ЕАЭС (ИИС ЕАЭС). Это позволит повысить скорость прохождения транзитных грузов через территорию ЕАЭС, увеличить экономические эффекты от этого процесса и поднять качество интеграции в Союзе.

Кроме этого, России как главному «акционеру» этого процесса следует содействовать обеспечению интероперабильности ИИС ЕАЭС с информационными системами государств – членов СНГ, тяготеющих к интеграционному объединению, а также государств, с которыми у ЕАЭС существует или планируется соглашение о зоне свободной торговли[17]. Цифровая интеграция здесь может и должна опережать интеграцию физическую. Другим важным инструментом может стать специальная (например, с Евразийским банком развития) программа внедрения национальных стандартов электронного правительства в заинтересованных странах-партнёрах.

Задача расширения российского экономического и цифрового пространства остро ставит вопрос о поиске стратегических союзников

[17] Вьетнам, Иран, Египет, Сингапур, Сербия.

в цифровом мире и использовании существующих политических механизмов для этой цели. В связи с этим стоит использовать позитивный потенциал наших отношений с ведущими экономиками будущего – Индией, Индонезией, Бразилией и другими.

Не менее важна работа по цифровому диалогу с Евросоюзом. **Во-первых**, цифровые транспортные коридоры с опытом бесшовного транзита для бизнеса станут возможны только в случае интероперабельности ИИС ЕАЭС с информационными системами Европы и КНР. **Во-вторых**, на европейском направлении необходима более тесная координация в части использования радиочастотного спектра – пока в этом вопросе много противоречий с приграничными государствами ЕС. Решение этой проблемы особенно важно, если в обозримом будущем грузы между странами будет перемещать беспилотный транспорт. В таком случае и России, и ЕС потребуется единый стандарт сетей нового поколения и выделенный им единый частотный диапазон. **В-третьих**, в России и Евросоюзе приняты сопоставимые (как минимум в плане принципов) нормативные требования к порядку хранения и передачи персональных данных. Важно гармонизировать эти требования для удобства бизнеса.

Помимо этого, Россию и ЕС сближает стремление облагать зарубежные цифровые гиганты, в первую очередь американские компании, справедливыми налогами. Формирование консенсуса о принципах такого налогообложения поможет России и ЕС эффективнее выступать на многосторонних площадках, занимающихся этим вопросом. В среднесрочной перспективе значимость обретает и вопрос создания единого трансграничного «бассейна» больших данных, размеченных унифицированным образом и доступных (в том числе за определённую плату) третьим сторонам, прежде всего американским и китайским компаниям[18].

Коллаборация с ЕС важна хотя бы потому, что российский и европейский интеграционные блоки оказываются зажатыми между двумя весьма самодостаточными информационными платформами – американской и китайской, каждая из которых уже “*bigdata*-монстр”. Чтобы стать дополнительным центром гравитации, России и Евросоюзу, сравнительно малочисленным в плане населения и дата-генерации, просто необходимо объединить усилия.

[18] Единые стандарты разметки таких данных позволят рассматривать их как единый массив. Это увеличит их стоимость и позволит использовать эту «новую нефть» для развития национальных программ поддержки искусственного интеллекта и самообучающихся программ. Что, в свою очередь, повысит конкурентоспособность этих продуктов.

При этом единые правила и принципы функционирования национальных систем управления данными, чётко устанавливающие, кому и при каких условиях эти данные могут или не могут быть доступны, обеспечат национальную безопасность России и ЕС. Очевидно, что весь объём накопленных больших данных государства или группы государств представляет собой исключительную разведывательную, политическую, экономическую и военную ценность, а обеспечение их сохранности – одну из ключевых задач национальной безопасности. Но есть и более сиюминутный политический аргумент в пользу начала взаимодействия между Россией и ЕС в цифровой сфере. Поступательная деградация российско-европейских отношений истощила двустороннюю повестку дня на предмет содержательных тем. По-настоящему сближающие нас вопросы развития цифровой экономики и совместного противостояния общим угрозам в цифровой среде могут предоставить принципиально новые области для неконфронтационного взаимодействия.

Отдельным пунктом для России стоят отношения с ведущими цифровыми державами – Китаем и США. В отличие от европейского и евразийского треков, совместные экономические проекты с Москвой в обоих случаях крайне маловероятны. Тем не менее, политическая ситуация диктует разные логики в отношениях с Вашингтоном и Пекином в этой сфере.

С КНР необходимо продолжать координировать свои позиции на международных площадках в отношении вопросов регулирования Интернета и обеспечения безопасности данных. Наши подходы схожи, хотя российский представляется более либеральным и не предполагает создания у нас аналога «Великой Китайской цифровой стены». Но есть два других деликатных вопроса, которые необходимо, отбросив неловкость, начать обсуждать с Пекином.

Первый – это технологическое проникновение Китая в государства ЕАЭС в рамках доктрины «цифрового Шёлкового пути». Как и в случае с евразийской интеграцией в целом, здесь важно сопряжение, координация действий китайского бизнеса и государства с мероприятиями, реализуемыми в рамках Цифровой повестки ЕАЭС – 2025.

Второй – это выработка правил поведения китайских компаний на российском рынке высококвалифицированной силы и стартапов. В настоящее время *Huawei* ведёт широкомасштабную работу по покупке российских технологических компаний и по привлечению российских специалистов в свои подразделения НИОКР. При этом зарплаты в компании

существенно выше рынка, что ведёт к перетоку специалистов из отечественных компаний. Очевидно, что в условиях рыночных правил и свободы выбора это – естественный процесс, но обсуждать с китайской стороной компенсационные действия для национальной экономики тоже необходимо. Китайская сторона никогда бы не позволила аналогичное поведение компаний третьих стран на своём рынке. Расширение работы с вузами, локализация не только *R&D*-подразделений, но и производства, переход к созданию совместных продуктов, а не «каннибализация» решений стартапов должны стать требованиями к цифровым компаниям, работающим в нашей стране.

Ещё более актуально взаимодействие по политической тематике с США, несмотря на конфронтационный характер двусторонних отношений. В первую очередь – это выработка мер доверия в киберпространстве, обсуждение ограничений на военное использование цифровых технологий, сближение подходов в вопросах регулирования Интернета. Россия и США могли бы выступить инициаторами переговоров о создании новых инструментов контроля за новыми типами военных технологий. Также необходимо совместно разобраться в терминологии: говоря о «русских хакерах», американцы чаще всего приводят примеры «социальной инженерии»[19]. Необходимо приложить максимум усилий, чтобы вернуть прагматизм в российско-американские отношения, даже если со стороны Вашингтона заинтересованность в этом сейчас не просматривается. Речь не идёт о выдаче США нового кредита доверия. Скорее о том, чтобы рассматривать каждый ход Вашингтона взвешенно и оценивать его возможные последствия, не рассматривая его как априори враждебный российским интересам.

России необходима скоординированная, чётко артикулированная и структурированная повестка для работы в многосторонних объединениях – МСЭ, «цифровой двадцатке», ОЭСР. Едва ли разумно тратить всё время на продавливание исключительно российских подходов и вступать в ожесточённые дипломатические баталии с партнёрами. Вместо этого следует хотя бы внутренне признать две группы «цифровых истин».

[19] В отличие от хакеров, осуществляющих незаконный доступ к хранящейся в системе информации или выводящих такую систему из строя, интернет-пользователи, размещающие посты и ролики в социальных сетях, не нарушают информационную безопасность. Задавание легитимных, пусть и тяжёлых вопросов, по которым американское общество до сих пор разделено, совершенно необязательно является «стремлением посеять раздор» и уж точно не подпадает под определение «распространение дезинформации».

Первая. Расположение *DNS*-серверов и основных интернет-магистралей действительно сложилось не в пользу России. Россия не является провайдером первого уровня. В вопросах формирования цифровой повестки дня Россия – крупная региональная держава, а не второй полюс этой системы. Отдельные цифровые корпорации стали настолько мощны, что разговаривают с государствами на равных.

Вторая. Мир гораздо меньше тяготеет к «цифровой биполярности», чем это может казаться. Это особенно показательно на уровне регулирования киберпространства. Несмотря на провозглашаемую свободу движения информации, большинство стран стремится к локализации хранения данных в том или ином виде. В вопросах цифрового регулирования все страны оказываются авторитарны. Есть сферы, которые требуют жёсткого регулирования, даже в более демократических странах. С другой стороны, нерационально полностью отрицать концепцию «мультистейкхолдеризма» – множественности ответственных – в выработке любых решений, касающихся регулирования и дальнейших путей развития новых технологий. Регулятор неизбежно должен вести диалог с владельцами технологий, а это чаще всего бизнес. Осознав эти реалии, Россия сможет выступать в многосторонних объединениях государством-примирителем, настроенным на поиск компромисса.

Также у России есть шансы стать выразителем интересов государств, желающих сохранять свой цифровой суверенитет и не настроенных быть частью китайской или американской цифровой империи, но не имеющих для этого достаточной «субъектности». Обе линии поведения будут расширять наши возможности для реализации лидерского потенциала, наше «гравитационное ядро». Это позволит продвигать российских кандидатов на руководящие позиции таких многосторонних объединений, как, например, МСЭ.

Ещё одним важным шагом по перестройке российской работы в международных организациях должны стать более тщательный подбор членов наших делегаций, обеспечение их многопрофильности. На сегодняшний день реалии таковы, что российские дипломаты не всегда достаточно осведомлены о технических аспектах рассматриваемых вопросов, тогда как профильные технические специалисты недостаточно владеют искусством переговоров. Отдельная роль должна отводиться лоббистам – представителям бизнеса, которые и выступают, по сути, конечным бенефициаром большинства принимаемых решений. Такого рода «цифровой

реализм» вместо отвлечений на провокации и внешнеполитические «шумы» сориентирует Россию на исключительно насущные вопросы обеспечения цифровых интересов страны в мире.

Признание того, что в плане создания сетей *5G* мы полностью утратили инициативу или возможность активно влиять на повестку, должно подтолкнуть Москву к необходимости сосредоточиться на подготовке наших предложений по стандарту сетей *7G* (или всё-таки *6G*?), активизировать работу по нейтрализации угрозы изоляции России в вопросах выделяемого под нужды связи нового поколения диапазона радиочастотного спектра. По этому вопросу российские взгляды с подавляющим большинством стран мира не совпадают. Особенность нормативного регулирования цифровой сферы в том, что новые законы напишут те, кто пишет коды, то есть техническое содержание нововведения во многом определит его регуляторную рамку. Поэтому важно активизировать участие российских специалистов относительно выработки стандартов и протоколов для технологий завтрашнего дня.

Среди технологических рынков будущего особо выделяется рынок платформ для суверенной критической инфраструктуры – систем кибербезопасности, связи, управления энергетикой, транспортом, финансовыми потоками и системами городского хозяйства, биобезопасности и контроля продуктов питания. В свете нарастания напряжённости и неопределённости в мире государства вынуждены уделять всё большее внимание своей безопасности и укреплению национального контроля над своей критической инфраструктурой.

Рынок суверенной критической инфраструктуры, представляющий многие триллионы долларов заказов на десятилетия вперёд, во многом подобен глобальному рынку вооружений. Решения о технологическом партнёрстве принимаются на суверенном уровне по принципу «свой – чужой», продажи производятся системами, а не компонентами, имплементация предполагает высокий уровень доверия с локализацией части технологий и формирует долгосрочное политическое влияние.

Как и на рынке вооружений, на рынке суверенной критической инфраструктуры у России есть своя «ниша», оцениваемая в 20–30 процентов всего глобального рынка[20]. Важным фактором является и то, что Россия позиционирует себя одним из лидеров на рынке систем

[20] Она состоит из стран, с которыми у России сложились привилегированные политические отношения и которые намерены сохранить контроль над своим цифровым суверенитетом.

безопасности и имеет инжиниринговые школы с большим опытом создания сложных систем.

Для России рынок критической суверенной инфраструктуры может стать наиболее перспективным экспортным направлением. Признанные уникальные компетенции в создании сложных систем делают Россию одним из ведущих – наряду с США и частично Китаем – потенциальных поставщиков таких систем. Создаваемая в России независимая программно-аппаратная среда также является очевидным конкурентным преимуществом. Ситуация «холодной войны» между США и Китаем гипотетически открывает для России рынки стран Большой Евразии, Ближнего Востока, Латинской Америки и Африки, которые попытаются сократить технологическую и политическую зависимость от воюющих сторон.

Утвердившись в статусе «экспортёра безопасности» в Евразии, Россия может стать для своих партнёров гарантом их технологического суверенитета. Наличие триллионного рынка потенциальных партнёров и уникальных компетенций может способствовать выстраиванию стратегии высокотехнологичного экспорта на годы вперед[21]. Таким образом страна получит возможность обеспечивать собственную безопасность, наращивать международное влияние и попробовать свои силы в опережающем технологическом развитии.

Однако завоевание рынков суверенной критической инфраструктуры невозможно без создания прорывных интегрированных платформенных решений. Аналогичным образом реализация подобной стратегии невозможна без создания прочных связей с технологическими партнёрами, без создания российских образовательных и технологических плацдармов за рубежом[22].

[21] Перспективными экспортными нишами могут стать:
1) системы и технологии защиты критической инфраструктуры (КИИ);
2) программно-аппаратные решения для обеспечения кибербезопасности;
3) системы «Умный город», включая управление энергетикой;
4) решения для управления логистикой и транспортными потоками;
5) информационные системы для финансового сектора и цифровых валют;
6) технологии, оборудование для экологического мониторинга и кризисных ситуаций.

[22] В целом стратегия экспорта платформ критической инфраструктуры предполагает (1) создание консорциумов, способных предлагать интегрированные платформенные решения, (2) поддержку компаний, способных выступить в роли технологических, финансовых и проектных интеграторов, и (3) создание точек постоянного присутствия ведущих российских высокотехнологичных компаний и университетов. Такая стратегия также потребует создания проектного «штаба» по координации работы компаний и государственных органов по выходу на зарубежные цифровые рынки и глобальной системы «технологической информации и пропаганды», задачей которой будет донести до потенциальных клиентов правду о преимуществах российских технологий в условиях жёсткой и часто недобросовестной конкуренции.

Выводы

На фоне виртуализации всех аспектов социальной жизни происходит милитаризация информационного пространства. Пользуясь отсутствием границ в цифровом пространстве и общепризнанных правил поведения в нём, государства и подконтрольные им организации распространяют предвзятый и дезинформационный контент с целью продвижения собственных интересов и ценностных ориентиров. Новые технологии формирования виртуальной реальности, такие как *deepfake*, практически не оставляют обыкновенному человеку шанса отделить ложь от реальности и способны безнаказанно провоцировать религиозные и этнические конфликты, разрушать семьи, уничтожать репутации политиков и невинных людей.

В ближайшие годы неизбежно встанет вопрос о структуре регулирования всей глобальной сети Интернет. Под давлением блокового технологического противостояния – преимущественно между США и Китаем – и идейно-политической борьбы она уже делится на цифровые «анклавы». Базовую ценность Интернета как общемировой равноправной и демократичной среды (*web neutrality*) подрывают и попытки, продвигаемые, в частности, США, поставить качество и скорость сетевого трафика в зависимость от кошелька клиента. Инклюзивность Интернета становится залогом сокращения цифрового неравенства, а с ним и гарантом мирового экономического роста и социального развития.

Большие данные как «новая нефть» цифрового века должны иметь понятного владельца и понятную стоимость для индивидуума, бизнеса и государства. Только в случае, если в цифровой среде центром сервисов и услуг станет человек и гражданин, будет обеспечен баланс прав человека, национальных приоритетов и интересов бизнеса, появится возможность регулировать ныне бесконтрольные глобальные цифровые монополии на благо всего общества. Удаление страниц президента Трампа и его сторонников, а также «деплатформинг» популярной у республиканцев социальной сети *Parler* ясно обрисовывают перспективу действий техногигантов по устранению экономических и политических конкурентов, если эти техногиганты решат действовать за пределами США. Раз так жёстко и относительно легко можно

расправляться с идеологическими противниками на территории США, почему нельзя сделать эту практику экстерриториальной? Тем более что прецеденты уже есть.

Для России задача минимум – сохранить суверенность при принятии решений, затрагивающих основные сферы национальной безопасности. Задача максимум – создать собственную конкурентоспособную технологическую экосистему, стать лидером техноэкономического блока и ключевым участником процесса выработки новых правил игры в этой сфере. В этом смысле обретение экономического суверенитета – задача более простая, чем обретение суверенитета информационного. Но, похоже, именно от её решения зависит выживаемость государств в будущем.

Экспорт технологий и компетенций защиты суверенной критической инфраструктуры в страны, желающие обеспечить свою независимость и обороноспособность, может и должен стать одним из важнейших политических и внешнеэкономических приоритетов России. Это обеспечит стране значительный финансовый приток и международное влияние. Именно по этому пути уже идут державы, претендующие на лидерские позиции в этой сфере.

В настоящее время реализация стратегии экспорта технологий критической инфраструктуры сдерживается отсутствием у российских высокотехнологичных компаний опыта создания интегрированных платформенных решений, их слабым присутствием на рынках потенциальных партнёров, а также недостаточными финансовыми возможностями для работы над крупными долгосрочными проектами.

По мере того как обостряется цивилизационное и идеологическое противостояние, учащаются примеры подрывной информационной активности, всё больше стран обращают внимание на необходимость более внимательного контроля за вредоносным и подрывным контентом в Интернете. В Соединённых Штатах, где информационная война разворачивается между враждебными политическими силами – как показала президентская кампания 2020 года, – цифровые монополии прибегают к откровенной цензуре и манипуляциям в пользу их идеологических сторонников.

России стоит подумать о механизмах активного формирования информационного пространства, которые позволяли бы лидировать в плане актуальности и качества контента и тем самым ограничивать иностранное влияние в своём информационном пространстве.

Вызов нового времени – это «нетерпение духа»: короткий клип или пост в соцсети «побеждает» полноценный новостной репортаж или аналитическую статью, многообразие мультимедийного опыта рассеивает внимание человека, а скорость происходящих изменений превращает жизнь в гонку со временем. Консервативная, традиционно неспешная сфера межгосударственного общения вынуждена меняться, «бежать очень быстро, чтобы хотя бы остаться на месте». Государства, которые смогут оперативно перестроить неповоротливые внешнеполитические механизмы быстрее других, имеют все шансы выйти на лидирующие позиции в этом стремительном «новом дивном мире».

ValdaiClubRu
valdaiclub
ValdaiClub
valdaiclubcom
@RuValdaitweets
valdai@valdaiclub.com

СОВЕТ ПО ВНЕШНЕЙ И ОБОРОННОЙ ПОЛИТИКЕ

РСМД
Российский совет
по международным
делам

МГИМО
УНИВЕРСИТЕТ

ВЫСШАЯ ШКОЛА ЭКОНОМИКИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ