Доклад Международного дискуссионного клуба «Валдай»

Валдай | Международный дискуссионный клуб

Realpolitik в «цифре»: суверенитет, союзы и неприсоединение XXI века

Андрей Безруков,
Михаил Мамонов,
Ольга Ребро,
Андрей Сушенцов

ru.valdaiclub.com
#valdaiclub

Сентябрь 2021

ISBN 978-5-907318-47-2

Российская Федерация, 127051, Москва,
улица Цветной бульвар, дом 16/1

Об авторах

Андрей Безруков
профессор МГИМО; президент Ассоциации экспорта технологического суверенитета

Михаил Мамонов
Заместитель министра цифрового развития (2018–2020 гг.)

Ольга Ребро
Эксперт Института международных исследований МГИМО МИД России

Андрей Сушенцов
Программный директор Международного дискуссионного клуба «Валдай», директор Института международных исследований МГИМО МИД России

Авторы доклада выражают благодарность участникам открытых дискуссий, проведенных Международным дискуссионным клубом «Валдай», а именно:

- Дискуссия «Конкуренция технологических платформ в XXI веке» (22.03.2021).
- Онлайн-дискуссия «Цифровое будущее Евразии: приоритеты евразийской интеграции до 2025 года» (25.05.2021).
- Сессия Клуба в рамках ПМЭФ-2021 «Право на частную жизнь в мире Big Data» (03.06.2021).

Содержание

Введение

Мир входит в очередной технологический цикл, наделяющий правительства новыми инструментами для обеспечения их интересов и создающий пространство для межгосударственного взаимодействия, в котором пока не определены правила игры. В условиях, когда ключевое военно-стратегическое изобретение предыдущей эпохи – ядерное оружие – остаётся преимущественно инструментом сдерживания, основным полем наступательных действий между ведущими игроками становится экономическая и технологическая конкуренция. Цифровые технологии постепенно заполняют ту нишу, которую традиционно в эпоху биполярности занимало ядерное оружие – как ключевой стратегический инструмент, одинаково важный для военного лидерства, экономического развития и глобального престижа. С определённой долей метафоричности можно утверждать, что государства, сформировавшие свои суверенные технологические платформы, становятся участниками престижного закрытого клуба, похожего на ядерный.

Цифровизация одномоментно уменьшила разрыв в военно-стратегических потенциалах государств мира, раньше казавшийся непреодолимым: теперь сравнительно низкозатратными кибернетическими средствами стало возможно нанести государству-сопернику пусть и не критический, но существенный ущерб. Рост использования цифровых технологий в военном деле, таким образом, сместил акценты в военно-технологической конкуренции держав. Другим важным свойством цифровых технологий является их гораздо более широкий спектр гражданского применения, что ещё больше стирает грань между экономической конкуренцией и гонкой вооружений.

Происходящие трансформации становятся фактором стратегического планирования государств. Не случайно в военной доктрине Российской Федерации на втором месте в перечне угроз стоит враждебное нарушение критической инфраструктуры России иностранным государством. Во многих странах мира приняты стратегические документы в области кибербезопасности, но в России такого отдельного документа нет. По мере того как ведущие страны вплотную занялись наращиванием своего потенциала в данной области, они начинают апробировать новые возможности на практике, в связи с чем учащается количество киберинцидентов, происходящих в фактически неконтролируемой среде.

Как будет выглядеть мировое устройство в новом технологическом цикле? Какие факторы будут иметь решающее значение для определения мощи страны и как адаптируются под новые условия традиционные характеристики государства? Кто и каким образом будет устанавливать правила поведения в новую цифровую эпоху? Сегодня миру необходимо найти ответы на эти вопросы, поскольку от них будет зависеть стабильность мировой системы в следующие десятилетия.

Повестка дня международного регулирования в новом технологическом цикле

Одним из важнейших результатов цифровизации является создание цифровых реплик объектов и процессов реального мира. Оцифрованные характеристики объектов позволяют ускорить процесс обмена данными, выстраивать взаимосвязи, невозможные в реальном мире, применять новые методы анализа, выявления закономерностей и в целом превращают весь мир в единую измеримую систему. Совершенствование глобальной цифровой реплики сопровождается постоянным развитием технологий хранения, передачи и обработки данной информации, а также обеспечения каналов взаимодействия между реальным и виртуальным миром (сенсоры, телефоны, биометрия). По мере проникновения в жизнь цифровых технологий объектом критической информационной инфраструктуры становится практически всё. Это ставит перед государствами новые вызовы при реализации функций по обеспечению безопасности.

Во-первых, *существенно выросла уязвимость инфраструктуры*. Так, причинить значимый ущерб сейчас можно с помощью обычного смартфона и некоторых познаний в области информационных технологий. Цифровые технологии не только обогатили арсенал традиционных источников угрозы безопасности (армии, террористических и преступных групп), но и расширили их число – теперь таким источником может быть практически любой человек, обладающий достаточными техническими навыками.

Во-вторых, большое количество субъектов пространства цифровой безопасности подразумевает *многообразие мотивов их поведения*, что затрудняет профилактику и предсказание таких угроз. Киберинциденты и кибератаки в XXI веке – это не столько эпизоды межгосударственного взаимодействия, сколько в первую очередь инструмент массы негосударственных игроков. Как показал целый ряд инцидентов в самых разных сферах (хакинг банковских систем, атака на нефтепровод в США, а до этого – атака вируса *NotPetya*), блокировка системы с целью вымогательства превратилась в отдельное направление транснациональной преступности.

В-третьих, переход социальных и коммерческих взаимоотношений в цифровое пространство оставляет открытым вопрос, *что считать кибератакой или киберинцидентом*. Во время избирательной кампании в США 2016 года американские органы безопасности указали на распространяемые в социальных сетях сообщения, задевающие наиболее острые социальные вопросы жизни страны. Установив, что источник сообщений

находится в России, они обвинили российское правительство в дестабилизации американской демократии и попытках повлиять на исход выборов. Появившиеся впоследствии исследования, впрочем, предложили альтернативное объяснение, назвав такое эксплуатирование наиболее «горячих» социальных тем, гарантирующих интерес пользователей, кампанией социального маркетинга и попыткой заработать на количестве переходов *(clickbate capitalism)*[1]. С этим тесно связан вопрос так называемых «инфлюенсеров», способных влиять на настроения больших социальных групп посредством распространения сообщений в интернет-пространстве.

В таких условиях для межгосударственных взаимоотношений крайне актуальным становится *вопрос атрибуции*. Технически очень сложно установить источник кибератаки или киберинцидента. Но даже определив источник, исключительно сложно доказать, что за этим стоит другое государство: атака могла быть произведена с его территории (или сделано всё, чтобы это выглядело таким образом), но действовали ли его граждане по собственной инициативе или по указанию государства, да и были ли это его граждане – наверняка сказать невозможно. Таким образом, любые обвинения пострадавшего государства могут быть названы бездоказательными, ответные действия – необоснованными и непропорциональными, а сам конфликт – быстро перейти в неконтролируемую фазу.

Ответом на такой вызов может стать создание беспристрастного международного органа – *независимого арбитража*. Теоретически оправданная идея на практике сталкивается с проблемами. Как показывает опыт подобных организаций в других сферах (например, Организации по запрещению химического оружия[2]), существует угроза политизации деятельности такого органа, он будет изначально ограниченно легитимен. Технология же «цифровой судебной экспертизы» *(digital forensics)* хоть и развивается, ввиду описанных выше аргументов не позволит беспристрастно рассматривать полученные при её использовании улики.

Помимо роста количества участников, *тотальная цифровизация ведёт к увеличению объёмов имеющихся данных, среди которых следует различать персональные и большие (деперсонифицированные) данные.*

Накопление объёмов персональных данных является неизбежным следствием цифровизации жизни человека. Но несмотря на то, что данный процесс обостряет потребность правового регулирования цифрового

[1] См., например, исследование Оксфордского университета The IRA, Social Media and Political Polarization in the United States, 2012–2018. University of Oxford, 2018. URL: https://int.nyt.com/data/documenthelper/534-oxford-russia-internet-research-agency/c6588b4a7b940c551c38/optimized/full.pdf#page=1

[2] Mate A. Ex-OPCW chief Jose Bustani reads Syria testimony that US, UK blocked at UN // The Grayzone. 5.10.2020. URL: https://thegrayzone.com/2020/10/05/ex-opcw-chief-jose-bustani-reads-syria-testimony-that-us-uk-blocked-at-un/

пространства, такие понятия, как «электронное лицо», «электронное государство», «цифровая экономика», «цифровое право», «цифровой суверенитет», до сих пор являются не до конца проработанными и устоявшимися[3]. Традиционные подходы к определениям, так или иначе связывающие понятия с физической реальностью (граждане, государственные границы, материальные объекты собственности), применительно к цифровой среде теряют смысл, учитывая нематериальную, а следовательно, внепространственную природу его ключевого компонента – цифрового кода. В связи с этим государства пошли по пути насильственной привязки генерируемой информации к физическому миру. Например, в США, России и Европе уже приняты законы, определяющие потребность хранения персональных данных граждан внутри национальных юрисдикций на национальных серверах и в национальных облачных хранилищах.

Одним из ярких примеров данного противоречия является текущая острая дискуссия внутри США относительно необходимости обновления Закона о добропорядочности в сфере коммуникаций *(Communication Decency Act)*. Принятый ещё в 1996 году, он преднамеренно оставляет амбивалентным вопрос принадлежности публикуемой в интернете информации и ответственности за её содержание. В отличие от издательств (например, СМИ), которые могут редактировать публикации, получают на них права и несут ответственность за их содержание, и от площадок (например, операторов сотовой связи), которые не имеют права отказывать в предоставлении услуг, не получают прав на передаваемую информацию, но и не несут ответственности за её содержание, интернет-компании одновременно и могут модерировать контент, и не имеют обязательств относительно его содержания, сохранности и прочего. В результате американские IT-гиганты получили полную свободу рук в определении правил функционирования интернет-пространства, что сделало их самостоятельным и весьма влиятельным игроком внутриполитической жизни страны. Это подтвердил эпизод в январе 2021 года с отключением аккаунтов президента США Дональда Трампа в популярных социальных сетях.

С другой стороны, показателен опыт ЕС, где с 2018 года действует Общий регламент защиты персональных данных. Согласно этому регулированию, связанные с генерируемой информацией права (право на забвение, безопасность, конфиденциальность данных) принадлежат пользователям – гражданам ЕС, а обязанности по реализации несут обрабатывающие такую информацию компании. При этом, однако, такой подход носит крайне рестриктивный характер и максимально ограничивает возможности по сбору и хранению данных в ущерб совершенствованию механизмов работы с большими данными.

[3] См., например: Саркисян Т. Интеграционный «план ГОЭЛРО» для XXI века // Россия в глобальной политике. 9.03.2021. URL: https://globalaffairs.ru/articles/czifrovoj-suverenitet-eaes/; или Трансформация права в цифровую эпоху. Издательство Алтайского государственного университета, 2020. С. 103–110. URL: https://www.asu.ru/files/documents/00023452.pdf

В свою очередь, вопрос обмена большими данными проработан ещё меньше, в то время как для разведсообществ и экономических агентов они гораздо важнее, чем персональные данные. Хорошая работа с массивами больших данных может позволить составить картину об эпидемиологической ситуации в регионе, экономическом развитии, демографической ситуации, социальной стабильности и спрогнозировать развитие идентифицированных трендов. А с использованием исключительных вычислительных мощностей существующих компьютеров можно смоделировать на цифровом двойнике множественные сценарии развития ситуации, а также вероятность и обусловленность их наступления. Это, в свою очередь, даёт возможность не только наблюдать за интересующей ситуацией или процессом, но и оказывать на них влияние в своих интересах. Доступ к такой информации позволяет узнать о государстве практически всё и является колоссальным ресурсом и вызовом для национальной безопасности. Правила обмена массивами такого рода пока не проработаны, и государствам ещё предстоит создать соответствующие механизмы.

Отдельным аспектом, требующим уточнения, является соотнесение персональных и больших данных. Собирая предоставленные, сознательно или нет (так называемый «цифровой след»), данные пользователей, компании или государство используют их как единый массив больших данных в целях, не всегда известных пользователю, что является нарушением его прав. Эффективным решением в этой ситуации является обезличивание больших данных, но в таком случае перед регуляторами встаёт вопрос разработки механизмов по проверке факта обезличивания. Интересным в этом плане может быть пример Эстонии, где вместо обезличивания данных используется принцип обязательности деанонимизации факта использования персональных данных. Доступ к цифровым данным граждан открыт для компетентных служб и компаний, однако каждый факт извлечения таких данных фиксируется и в случае необходимости можно установить, кто именно и для каких целей использовал персональную информацию гражданина[4]. Такая система гарантирует прозрачность и саморегулирование цифровой среды страны: граждане, осознавая, что в любой момент могут проверить, каким образом использовались их данные, более склонны их предоставлять, а компании и государственные учреждения – более осмотрительны в их использовании. В результате повышается уровень доверия между тремя носителями суверенитета в цифровом пространстве, а вся система способствует не ограничению собираемых данных (на что направлено регулирование ЕС, лимитирующее, например, сроки хранения персональных данных), а увеличению накапливаемой информации.

[4] Priisalu J., Ottis R. Personal control of privacy and data: Estonian experience // Health and Technology. 2017. V. 7. P. 441–451.

Наряду с аспектами, связанными с безопасностью, всё большую актуальность приобретает **проблема экономического регулирования цифровой деятельности**. Так, например, многие цифровые транснациональные гиганты не имеют юридического присутствия в России, используют экономические ресурсы наших граждан, национальную инфраструктуру и при этом не платят налогов с извлекаемой на территории Российской Федерации прибыли. Ведущие социальные сети, почтовые сервисы и поисковые системы используют доступ к данным пользователей вне зависимости от их географического местоположения для привлечения рекламодателей. Разработка единых принципов налогообложения цифровых гигантов ведётся с 2013 года в рамках ОЭСР и *G20*, общие принципы регулирования этой сферы стремятся выработать в ЕС.

Схожая природа возникающих цифровых проблем и вызовов подталкивает государства к диалогу. В этом плане цифровая проблематика скорее сближает, чем разделяет, государства мира.

Мир идёт к зарегулированности свободы, обретённой человеком благодаря цифровизации. Если раньше при выборе цифровых платформ определяющим фактором был комфорт в использовании, то сейчас это скорее соображения национальной безопасности, из-за чего многие сервисы могут быть запрещены. Это оправданно с точки зрения государства, однако у граждан возникают понятные опасения по поводу потери контроля над личными данными и сокращения выбора технологических устройств и решений. Отчасти это является неотвратимым процессом, и со временем общество будет вынуждено принять новую реальность: появившиеся в начале XXI века в аэропортах металлоискатели сегодня никого не возмущают. Однако потоки цифровых данных, в отличие от пассажиров в аэропорте, сложно направить через один коридор, и чрезмерное ограничение будет провоцировать создание путей обхода регулирования и развития виртуальных частных сетей *(VPN)*, доступных гражданскому населению средств шифрования (*PGP*, системы сквозного шифрования в мессенджерах и так далее), *darknet*. Перед государствами возникает дилемма поиска баланса между *защитой суверенитета и обеспечением безопасности,* с одной стороны, и *защитой прав граждан и обеспечением доступности информации* **–** с другой. При этом за неимением более действенного ответа на задачу повышения контроля за интернет-пространством государства прибегают к уже описанному проверенному методу – созданию физических ограничений на доступ к национальному сегменту сети. При этом сам интернет сохраняет своё первостепенное значение для технического, экономического, социального развития человечества, оставаясь глобальным.

Пытаясь разрешить это диалектическое противоречие, мир будущего может оказаться в ситуации, когда *цифровое пространство станет разговором суверенных национальных «интернетов»* друг с другом на условиях их принципиальной совместимости. Такой формат позволит государствам решить проблему обеспечения безопасности в цифровом пространстве

с наименьшим ущербом для удобства пользователей, для которых в практическом плане ощутимо ничего не изменится. Альтернативный путь – дезинтеграция коммуникационного единства планеты – ведёт к спирали кризиса без возможности выхода.

Другой особенностью нового этапа развития становится «борьба стандартов» – государства или отдельные (в чём-то уже равновеликие государствам) корпорации пытаются закрепить за отдельными решениями и стандартами статус универсальных, что в дальнейшем предопределит и контуры технологического образа мира будущего: владельцы таких стандартов на старте получат существенное конкурентное преимущество.

В настоящий момент в России *недооценивается значимость этой борьбы***.** А она уже ведётся, например, за использование исчерпаемого радиочастотного ресурса. Если не унифицировать правила работы с ним, то у приграничных стран могут возникать серьёзные проблемы, поскольку использование частей радиочастотного спектра военным ведомством одного государства делает невозможным использование этих же частей спектра для гражданских нужд другими государствами. Без обеспечения координации и совместимости национальных систем эти расхождения в будущем могут стать проблемой, в частности для развития трансграничного движения беспилотного транспорта из России в ЕС.

Неспособность выработать единый стандарт приводит к появлению технологических барьеров, замедляющих экономическое развитие внутри интеграционных объединений. Так, в ЕАЭС не все государства используют стандарты шифрования, которые приемлемы для Российской Федерации с точки зрения обеспечения безопасности национального сегмента интегрированной информационной системы. Отсутствие такого универсального стандарта препятствует юридически значимому электронному документообороту между нашими странами, способному кратно ускорить бизнес-процессы на территории ЕАЭС.

Блоковое противостояние цифровых держав

Как мы писали ранее, соперничество между великими державами приводит к разделению мира на *конкурирующие технико-экономические блоки*, которые функционируют на базе разных технологических платформ[5]. Эти блоки представляют собой государства или межстрановые

[5] Безруков А., Мамонов М., Сучков М., Сушенцов А. Суверенитет и «цифра» // *Россия в глобальной политике*. 1.03.2021. URL: https://globalaffairs.ru/articles/suverenitet-i-czifra/

формальные или неформальные объединения с набором природных и человеческих ресурсов, собственной экономической моделью, финансовой системой, философией развития и технологиями, позволяющими обеспечить суверенитет и безопасность критической инфраструктуры. *Технологическая платформа* – это массив технологических средств, используемый в качестве основы, на которой создаются другие устройства, процессы и технологии.

Сегодня технологические экосистемы становятся орудием противостояния крупных мировых игроков. Те страны, которые не обладают необходимым набором компетенций и национальных технологий в области ИКТ, вынуждены примыкать к существующим технико-экономическим блокам. Крайней формой технологической зависимости государства можно считать его так называемую «цифровую колонизацию».

Если раньше метрополии рассматривали колонии в качестве источника природных ресурсов, то современные «цифровые колонии» станут источником больших данных, превращающихся в новую нефть. Ценность больших данных возникает только тогда, когда имеются возможности для их надлежащей обработки. Государства, не обладающие такими возможностями, не рассматривают большие данные в качестве ценного ресурса и поэтому готовы обменять его на привлекательные предложения передовых стран, позволяющие перепрыгнуть из условного феодализма в цифровую эпоху, минуя этап индустриализации (*5G* без *2G*, использование дронов в местностях, где даже нет дорог, переход от ручного труда к компьютеризированному в обход конвейеров). После того, как государства переходят на стандарты передовых компаний, они превращаются в объекты цифрового и экономического освоения.

Соединённые Штаты Америки

Отдельный технологический блок уже сформировался в США. В американской внутренней политике цифровая повестка становится всё более важной темой. Выборы американского президента 2020 года отчётливо показали роль интернет-платформ в формировании информационного пространства, а следовательно, влияния на предпочтения избирателей. При этом платформы остаются частными компаниями и подчиняются логике максимизации прибыли. Так, например, обвинения в адрес *Facebook* летом 2020 года в нежелании модерировать высказывания правых групп привели к бойкоту социальной сети рекламодателями, что стоило компании 7,2 миллиарда долларов упущенной прибыли и 8,3-процентного падения стоимости акций[6]. Вскоре после этого глава компании Марк

[6] Datoo S. Mark Zuckerberg Loses $7 Billion as Companies Drop Facebook Ads // *Bloomberg*. 27.06.2020. URL: https://www.bloomberg.com/news/articles/2020-06-27/mark-zuckerberg-loses-7-billion-as-companies-drop-facebook-ads

Цукерберг объявил о «пересмотре политики компании в преддверии выборов 2020 года», поскольку в такой напряжённый период жизни страны «*Facebook* должен быть крайне осторожным в поддержании безопасности и информированности» общества[7]. Говорить о прямой координации между Демократической партией и интернет-гигантами сложно, однако разделяемые ими общие либеральные ценности создают атмосферу, в которой публикация отличной от консенсусной точки зрения воспринимается как разжигание социальной ненависти, а значит, подлежит модерации, поскольку угрожает безопасности страны.

Хотя в борьбе с популизмом интернет-платформы оказались по одну сторону баррикад с политическим истеблишментом, необходимость ограничения их всесилия в Вашингтоне осознаётся. 11 июня 2021 года на рассмотрение Палаты представителей было внесено пять законопроектов, содержащих меры по предотвращению монополизации цифрового пространства. Это результат шестнадцатимесячного расследования Конгресса.

Несмотря на декларируемый принцип свободного и открытого цифрового пространства, во внешней политике США переходят к концепции *цифрового Realpolitik*. Вашингтон будет учитывать прежде всего собственные интересы и поддерживать союзнические отношения со странами, рассматривающими возвышение Китая и действия России как вызов. Демонизация Пекина и Москвы, будь то по идеологическому признаку (демократии/автократии) или по экономическому принципу (подрыв «справедливой» рыночной конкуренции), станет важным инструментом сплочения стран вокруг США. Эти союзнические отношения будут выстраиваться на основе двух тенденций: *политизация* (необходимо разделять установки США и признавать их лидерство) и *прагматизм*.

Китай

Однако постепенно США теряют потенциал для поддержания гегемонистской стабильности. На формирование своего блока претендует и Китай. Пекин создаёт собственные платформы и активно инвестирует в искусственный интеллект, квантовые вычисления, полупроводники. Всё чаще он заявляет о своём лидерстве в таких сферах, как кластер наук о мозге, геномика, биотехнологии, глубокий космос.

В киберпространстве Китай стремится одновременно «открыться» и «закрыться». Продвигая идею *суверенного интернета*, Пекин параллельно декларирует концепцию сообщества единой судьбы в киберпространстве и выступает с инициативами международного сотрудничества

[7] Zuckerberg M. *Facebook*. 27.06.2020. URL: https://www.facebook.com/zuck/posts/10112048980882521

(учреждение Ассоциации по цифровой экономике, создание «Цифровой двадцатки», запуск двусторонних цифровых диалогов)[8].

Первенство США и Китая сегодня бесспорно. Как отмечается в докладе Конференции ООН по торговле и развитию (ЮНКТАД) 2019 года, на эти две страны совокупно приходится 75 процентов всех патентов в области блокчейна, 50 процентов мировых расходов на проекты в сфере интернета вещей, более 75 процентов мирового рынка облачных услуг и 90 процентов рыночной капитализации семидесяти крупнейших цифровых платформ, а также 40 процентов информационно-коммуникационного сектора мировой экономики. При этом темпы роста цифровых секторов экономики значительно превышают темпы роста ВВП[9].

Помимо прочего, в последние четыре года происходит разъединение некогда симбиотических экономик США и КНР, ещё в середине 2000-х сращенных в понятие «Кимерика» *(Chimerica)*. Особенно это заметно в области технологий, где зависимость поставок материалов, обмен интеллектуальной собственностью и даже уязвимость логистических цепочек при поставках компонентов электроники воспринимается как угроза национальной безопасности. В таких условиях взаимного недоверия снижается вероятность достижения компромиссов в вопросах регулирования цифровой сферы, что может привести к формированию *биполярности конкурентных платформ* и к началу *холодной информационной войны*. Выступая в роли «цифровых колониалистов», Вашингтон и Пекин будут соперничать за привлечение к своим платформам наибольшего числа государств.

Место России в новом технологическом цикле

В условиях формирования двух крупных экономико-технологических центров все третьи страны оказываются перед выбором между сохранением суверенитета и перспективой отставания в технологическом и экономическом развитии, с одной стороны, или отказом от части суверенитета в обмен на экономические перспективы – с другой. Сама по себе передача части суверенитета не является вопросом выживаемости государства. Отказ от самостоятельности в военной сфере не помешал Японии и Германии

[8] Белова А. Президент Центра Китая и глобализации Ван Хуэйяо рассказал о развитии цифровой экономики Китая // Российская газета. 25.12.2020. URL: https://rg.ru/2020/12/25/sovetnik-gossoveta-knr-van-huejiao-rasskazal-o-razvitii-cifrovoj-ekonomiki-kitaia.html

[9] Digital Economy Report 2019. United Nations, 2019. P. xvi. URL: https://unctad.org/system/files/official-document/der2019_en.pdf

стать влиятельными игроками на международной арене. Аналогичным образом – в цифровой сфере Сингапур, Южная Корея или Израиль не сформировали суверенной технологической платформы, но и не потеряли лидерских позиций в сфере развития высоких технологий.

Готовность к отказу от элементов суверенитета тесно связана со стратегической культурой государства. В России, с её историческим опытом противостояния с другими государствами, сложилось устойчивое и небезосновательное убеждение, что передача даже элементов суверенитета может подорвать выживаемость страны. Поэтому она не может позволить себе не иметь национальной платформы, и обеспечение технологической безопасности – одна из важнейших целей российской внутренней и внешней политики.

На сегодняшний день Россия обладает всеми признаками суверенной технологической платформы, которая опирается на математическую школу, доставшуюся в наследство от СССР. У неё есть собственный поисковик, который лидирует в отдельных регионах мира, собственная соцсеть и целый ряд конкурентоспособных решений (искусственный интеллект, умный город, электронное правительство, кибербезопасность – многие российские компании всемирно известны, например *Kaspersky*, чья деятельность в Северной Америке уже становилась в прошлом объектом политической борьбы[10]).

Стремление нашей страны к созданию независимых национальных решений для обеспечения устойчивости инфраструктуры представляется более чем оправданным. Все помнят о том, как в условиях введённых санкций компания *Siemens* не выразила готовности привезти турбины в Крым, что поставило жизнь и безопасность жителей Крыма под угрозу. Работа российского оборудования целиком на заимствованных решениях, созданных зарубежными государствами, представляет большой риск. Ситуация, аналогичная вышеупомянутой, но в сфере кибербезопасности или функционирования электронного правительства, не позволит государству эффективно выполнять суверенные функции по обеспечению безопасности и прав своих граждан.

Существование таких рисков подталкивает к поиску национальных аналогов глобальным цифровым решениям. Уже сейчас под эгидой Минцифры и Минпромторга России созданы два реестра – национального программного обеспечения и национального радиоэлектронного оборудования. В случае наличия в них отечественных аналогов российские органы власти и госкомпании обязаны выбирать решения из представленных в реестрах списков.

---

[10] Сухаревская А. Власти США ввели постоянный запрет на госзакупки продукции «Лаборатории Касперского» // Ведомости. 16.09.2019. URL: https://www.vedomosti.ru/technology/articles/2019/09/16/811360-zapret

В процессе создания собственных конкурентоспособных решений, для планомерного технологического развития России необходимо найти баланс между обеспечением конкуренции на этом чувствительном рынке и защитой своих интересов. Для начала нужно создать новый механизм инновационной деятельности в рамках *государственного оборонного заказа*, чтобы обеспечить планомерное развитие отечественных технологий. В цифровой сфере можно избежать противоречий между нуждами общества и государства. Как показывает зарубежная практика, сначала технологии развиваются в сфере ВПК, а потом переходят в гражданскую собственность.

В условиях цифрового мира связь между правительствами стран и технологическими компаниями-лидерами будет лишь укрепляться. В США руководители таких компаний посещают различные органы власти до двухсот раз в год. С одной стороны, государство не может обеспечить технологический суверенитет в ограниченных объёмах без опоры на технико-экономических агентов (частный или государственно-частный бизнес). С другой стороны, эти компании обладают не меньшей властью в цифровой сфере, чем государство, и разговаривают с ним на равных, поэтому здесь возможен только диалог, поскольку попытки государства навязать свою линию поведения будут иметь ограниченный успех. К тому же они способствуют развитию критических элементов в интересах технологического прогресса (решения в области искусственного интеллекта, платформенные решения, в области телемедицины и дистанционного образования), позволяют решать большое количество социально-экономических проблем сравнительно недорого, что представляется весьма привлекательным для государства.

В сфере технологической дипломатии главная задача России – защитить свой суверенитет и не впасть в зависимость от китайской или американской технологических платформ. Этого можно добиться посредством более ресурсоёмкого формирования собственной технологической платформы в рамках ЕАЭС, реализации совместных технологических проектов с Европейским союзом (что, впрочем, затруднительно в условиях политической поляризации Запада), а также предложения альтернативного американскому и китайскому пути мирового сотрудничества.

Создание собственной технологической платформы в рамках ЕАЭС имеет прочный задел. И сегодня сформировалась довольно обширная нормативная и финансовая среда для реализации цифровой повестки. Если изначально эта повестка воспринималась через призму информационно-коммуникационных технологий как отдельное направление интеграции, то теперь есть осознание необходимости развития цифровых инструментов продвижения интеграции во всех областях деятельности объединения: транспорт, образование, медицина, повышение мобильности трудовых ресурсов.

Существенным стимулом для развития совместных цифровых проектов стало создание новых инструментов финансирования в рамках Фонда цифровых инициатив Евразийского банка развития. Благодаря этому появились, например, сервисы поиска работы для граждан стран-участниц на всей территории интегрированного объединения. В условиях пандемии *COVID-19* была налажена бесшовная передача данных о результатах тестов и вакцинации, развиваются проекты по навигационным пломбам для отслеживания грузов.

Но для создания единой технико-экономической платформы на базе ЕАЭС предстоит устранить ряд барьеров. Относительно позднее понимание тотального значения глобализации привело к выбору каждой из стран обособленного пути развития информационных технологий и внедрению своих стандартов и нормативов, в том числе правовых, по работе с объёмами данных. В частности, Армения и Киргизия используют нормативы шифрования, которые в Российской Федерации называют недостаточно защищёнными. Казахстан не готов передавать информацию о своих субъектах экономической деятельности в общую систему, так как, считая эту систему чувствительной, предпочитает хранить данные в национальном контуре. Препятствиями к созданию единой платформы являются также различное понимание странами – участницами ЕАЭС уровня угрозы от использования заимствованных технологий и отсутствие политической воли.

Россия может пойти по другому пути и стать лидером движения *цифрового неприсоединения*, которое объединит нежелающих примыкать ни к одной из двух существующих цифровых платформ – ни к американской, ни к китайской. Многие страны, как и Россия, высоко ценят свой суверенитет, но не имеют достаточно ресурсов, чтобы обеспечить себе цифровую независимость. Лидерство России в данной группе может быть обеспечено посредством предлагаемых решений с открытым кодом, использование которого последовательно продвигает Москва. В рамках этого подхода государства вместе с приобретаемой технологией получают её исходный код и, соответственно, возможность его менять. Поставщик не имеет доступа к аккумулируемым в результате изменения кода данным, что устраняет риски «цифрового колониализма» и неинвазивного внешнего контроля.

Приверженность открытому коду может иметь фундаментальное значение для параметров будущего цифрового мира. В отличие от предложений отдельных компаний решения на открытом коде позволяют конечному пользователю вносить изменения в исходный код программы, модифицировать её или менять параметры кибербезопасности. Это позволяет избежать рисков использования оборудования и решений с так называемыми недокументированными возможностями, позволяющими их владельцам вести скрытое наблюдение за пользователем или собирать его данные. Другой риск, который купируется в случае использования

открытого кода, – это дистанционное влияние владельцев проприетарных решений на быстродействие, корректное функционирование принадлежащих им аппаратно-программных средств или отказ владельцев поставлять такие средства государству под предлогом санкций или изменений экспортной политики.

Россия уверенно заявляет свои притязания на позиции лидера в области открытого кода. В этом и следующем году Минцифры России планирует инициировать целую программу мероприятий, посвящённых открытому коду, а сама тематика *open source* является одним из ключевых пунктов предвыборной кампании российского кандидата на пост генерального секретаря Международного союза электросвязи – ведущей международной площадки по глобальной гармонизации подходов и стандартов в сфере цифрового развития и управления.

Заманчивость формирования движения цифрового неприсоединения весьма высока. Склонность к национализации ключевых цифровых инструментов проявляют не только глобальные игроки, но и региональные державы, и просто сильные государства. Предпочтительность открытых решений проприетарным признаётся и лидерами сообщества разработчиков и программистов, что повышает моральный авторитет государства, которое выдвинет такую инициативу на международной арене. Возможно, именно идея цифрового неприсоединения и её продвижение в мировом сообществе станет значимым фактором мобилизации лидерского потенциала России в мире XXI века.

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