

Доклад Международного дискуссионного клуба «Валдай»



Валдай | Международный
дискуссионный клуб

Россия и конкуренция технологических платформ: политэкономия рынка ИКТ

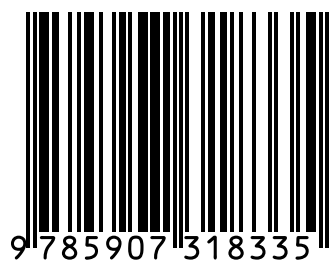
Андрей Терехов,
Станислав Ткаченко

ru.valdaiclub.com
[#valdaiclub](https://twitter.com/valdaiclub)

Май 2021

Данный текст отражает личное мнение автора или группы авторов, которое может не совпадать с позицией Клуба, если явно не указано иное.

ISBN 978-5-907318-33-5



© Фонд развития и поддержки Международного дискуссионного клуба «Валдай», 2021

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

Об авторах

Андрей Николаевич Терехов

Доктор физико-математических наук, профессор,
заведующий кафедрой системного программирования
математико-механического факультета СПбГУ;
президент ИТ-компании «Ланит-Терком»

Станислав Леонидович Ткаченко

Доктор экономических наук, профессор, руководитель
магистерской программы «Дипломатия» СПбГУ;
президент секции «Посткоммунистические системы
в международных отношениях» Ассоциации международных
исследований

Содержание

- 3 Актуальность изучения технологических платформ
- 7 Мировые лидеры в построении технологических платформ и модель догоняющего развития
- 12 Российские ИКТ и национальная технологическая платформа
- 22 Заключение

Актуальность изучения технологических платформ

Термин «технологическая платформа» применительно к информационно-коммуникационным технологиям (ИКТ) стал использоваться относительно недавно и пока не имеет устоявшегося толкования. Обсуждающие проблематику технологических платформ эксперты, политики и бизнесмены в целом понимают, о чём их коллеги ведут речь. Но для научной дискуссии по этому вопросу требуется терминологическая чёткость. По нашему мнению, наиболее ясное и вызывающее меньше всего споров определение, следующее: технологическая платформа – это массив технологических средств, используемых в качестве основы, на которой создаются устройства, процессы и технологии.

Когда предмет дискуссии становится узкоспециальным, в фокусе дискуссии оказываются профессиональные для программистов вопросы: что такое «платформа», какие именно «технологии» она подразумевает и идёт ли речь о явлениях глобальных/универсальных или же разделённых на национальные сегменты.

Период пандемии *COVID-19* привлёк особое внимание к гигантским интернет-платформам: *Amazon, Apple, Facebook, Google* и *Twitter*. В течение 2020 года их могущество, измеряемое как числом пользователей, стоимостью акций и брендов, так и возможностью влиять на политические процессы глобального и национального уровня, достигло максимальных величин. К настоящему моменту уже сформировался консенсус относительно того, что компании категории *Big Tech* представляют угрозу демократии даже в наиболее развитых странах планеты. Но пока отсутствует согласие в вопросе о том, как именно на эту угрозу следует реагировать.

В нашем исследовании технологических платформ и политико-экономических последствий, которые возникают в связи с их развитием, мы ориентируемся на приведённое выше определение. Оно предполагает более узкоспециальный подход к технологическим платформам, определяемый особенностями индустрии, развивающейся на острие современной науки и при этом оказывающей непосредственное влияние на политические и социально-экономические стороны жизни любого человека.

Информационно-коммуникационные технологии многими видятся как явления эфемерные, создающие виртуальный мир и развивающие его путём интеграции процессов, протекающих в реальной жизни. Но для того, чтобы объединённые в единую сеть компьютеры были поставлены на службу интересам государства и частного бизнеса, домашних хозяйств и физических

лиц, необходимо сделать очень многое: создать систему высшего профессионального образования; сформировать научные школы и воспитать профессиональных программистов; создать языки программирования и написать на них управляющие устройства программы; проложить по суше и дну океанов интернет-кабели; запустить в космос спутники связи; согласовать всевозможные технические стандарты. Сегодня и даже в достаточно отдалённом будущем обеспечить необходимые условия для решения этих задач способны лишь суверенные государства, их структуры управления. В распоряжении частного бизнеса имеются ресурсы, сопоставимые в настоящее время с совокупными возможностями, имеющимися в распоряжении органов государственного управления. Но лишь у правительств и парламентов есть право законодательно регламентировать сферу ИКТ, а также сила, использование которой позволяет регулировать применение новейших технологий, даже несмотря на сопротивление.

Объединение планеты в единую информационно-коммуникационную сеть невозможно без политической воли, ясно выраженной ключевыми акторами международных отношений. При этом следует учитывать тот факт, что сообществу суверенных государств характерна иерархическая структура. До относительно недавнего времени у отдельных стран не было права вето на глобальные проекты, к числу которых относятся развивающаяся по единым стандартам индустрия ИКТ и объединяющий все её национальные сегменты интернет. Попытки заблокировать доступ интернета в страну (Северная Корея, Туркмения) или же построить высокотехнологические фajerволы (Китай) вызывали скептическую усмешку. На рубеже десятых – двадцатых годов нынешнего столетия эти идеи, казавшиеся не только трудноисполнимыми технологически, но и нерациональными с экономической точки зрения, приобретают всё больше сторонников. В наступающую эпоху невозможное становится реальным и даже обыденным.

В нашем докладе мы попытаемся найти ответы на следующие вопросы:

- Является ли горячо обсуждаемое многообразие технологических платформ неизбежной альтернативой целостному цифровому миру?
- Применимы ли стратегии догоняющего развития в сфере ИКТ?
- Следует ли суверенным государствам пытаться построить внутри национальных границ «интернет в миниатюре»?
- Способно ли государственно-частное партнёрство ускорить развитие национальной технологической платформы в Российской Федерации?

Вступивший в финальную стадию демонтаж однополярного мира принёс с собой множество политико-экономических последствий, одно из которых – кризис либерального международного порядка. В этом явлении нам наиболее интересен один его аспект – роль гегемонии США в формировании современной глобальной экономики. Сложившаяся в рамках реалистической школы изучения международных отношений теория гегемонистской стабильности утверждает: либеральная экономика возможна только в условиях однополярного мира, который находится под присмотром государства-лидера (гегемона). Признание того, что зарождается новый, многополярный мир, неизбежно приводит нас к мысли о том, что межгосударственные технологические войны не за горами, а технологическая взаимозависимость опасна. Ведь не только футбольные болельщики знают, что лучшая защита – это нападение.

В условиях надвигающейся угрозы граждане обращаются к государству с требованием о защите и обеспечении их безопасности. Цена возможной победы государства над либеральной экономикой будет высока. Речь идёт не только о потере эффективности в реализации хозяйственных решений, традиционно ассоциируемых с государственным вмешательством в экономику. Важен и публично-медийный аспект этого процесса. Способность новостей мгновенно достигать аудитории, обеспеченная благодаря интернету наряду с традиционными телевидением и радио, вынуждает политиков оперативно принимать решения и действовать немедленно, часто в ситуации стресса и отсутствия времени на хладнокровное обдумывание. И если в области традиционной «жёсткой» безопасности органы государственной власти всегда могут оправдаться тем, что они «защищают национальные интересы», то в хозяйственных вопросах, которые сегодня преобладают при анализе развития мировой индустрии ИКТ, такое оправдание является неубедительным.

Именно в этом мы видим ключевую проблему в отношениях по оси «государство – бизнес» при обсуждении проблематики технологических платформ. Каждая из сторон хотела бы сохранить за собой «контрольный пакет», позволяющий доминировать в этом сегменте рынка. Но такое соперничество опасно для стабильности экономики и усложняет решение задачи обеспечения государственной безопасности. Поэтому органы государственной власти и высокотехнологический бизнес должны выработать *modus vivendi*, сотрудничать при решении задачи развития национальными компаниями технологических платформ, не покушаясь при этом на свободу другой стороны действовать в рамках своей основной миссии. Для государства – это обеспечение национальной безопасности; для бизнеса – эффективная хозяйственная деятельность.

Первым сигналом окончания периода триумфального роста индустрии ИКТ стал кризис, известный под названием «пузырь доткомов» (*Dot.com bubble*), разраставшийся с 1995 года на фондовых биржах планеты и взорвавшийся в один день, 10 марта 2000 года, полуторакратным падением индекса крупнейшей для ИКТ-индустрии биржи – американской *NASDAQ*. Взорвавшийся пузырь, однако, вовсе не привёл к краху всей индустрии ИКТ. Скорее он стал первым успешным примером «созидательного разрушения» в этой отрасли экономики. Автор данного термина, австрийский экономист Йозеф Шумпетер, определял созидательное разрушение как «...процесс индустриальной мутации, который непрерывно реконструирует экономическую структуру изнутри, разрушая старую структуру и создавая новую»¹. Но масштабы краха пузыря доткомов заставили правительственные структуры и монетарные власти развитых государств переключиться на ручное управление, подстраховав игроков рынка в ситуациях, когда переживавшая период становления и по-прежнему подверженная внешним шокам индустрия ИКТ могла надолго оказаться в глубоком и затяжном кризисе. В новую эпоху постиндустриального информационного общества за таким кризисом неизбежно следуют другие, не менее трагичные потрясения глобального масштаба.

В начале нынешнего столетия бизнес и политика в рассматриваемой нами сфере двинулись навстречу друг другу. В результате этого сотрудничества возникла современная индустрия ИКТ. В ней уже невозможно провести чёткую границу между двумя главными элементами: частной инициативой и государственным интересом.

По нашей оценке, в 2001–2004 годах завершился период доминирования экономики над политикой в сфере ИКТ, а развитие цифровых технологий перестало быть миссией исключительно бизнеса. Соображения эффективности и приоритет общественных благ² как главные мотивы построения глобальной ИКТ-инфраструктуры отошли на второй план. Актуальность приобрели такие понятия, как «информационная безопасность», «информационное противоборство», «кибероружие»

¹ Шумпетер Й. Капитализм, социализм и демократия. Глава 7: «Процесс созидательного разрушения». М., 1995. С. 73.

² Под общественными благами (*public goods*) мы понимаем блага, которые потребляются коллективно всеми гражданами независимо от того, платят они за них или нет. Отнесение инфраструктуры ИКТ к категории общественных благ – вопрос дискуссионный. Однако некоторым типологическим чертам общественных благ (*неисключение, неконкурентность* в потреблении, *неделимость*, если эти признаки общественных благ обеспечены правовым регулированием и согласованными на межгосударственном уровне институтами) инфраструктура ИКТ, по нашему мнению, соответствует.

и другие³. Возникла новая политико-экономическая реальность, изучение свойств которой сейчас только начинается. Эксперты из самых разных областей науки и практики понимают, что развитие технологических платформ индустрии ИКТ влияет на безопасность государства и общества. Но пока они ещё не знают, как именно это происходит. Около пятнадцати лет назад наступил нынешний период ограниченного *ad hoc* межстранового сотрудничества, прерываемого конфликтами великих держав в киберпространстве.

Мировые лидеры в построении технологических платформ и модель догоняющего развития

В основе теорий догоняющего развития лежит интерес исследователей к изучению явлений и процессов в текущей социально-экономической жизни, а также понимание того, что сменяющие друг друга режимы и экономические модели формируют среду, в которой построение долгосрочных моделей затруднено, а зачастую просто невозможно. Теория догоняющего развития своей целью видит поиск и выявление политико-экономических условий, позволяющих сократить отставание отдельного государства от лидеров в региональной или глобальной системе.

Родоначальником теории догоняющего развития стал немецкий экономист Фридрих Лист. Родившись и начав свою профессиональную карьеру в разделённой на два десятка государств Германии, он значительную часть своей жизни провёл в США. Будучи приверженцем взглядов первого министра финансов США Александра Гамильтона, Лист резко выступал против свободной торговли, считая, что она наносит удар по зарождающейся национальной промышленности и не позволяет государству, в котором отсутствует развитая индустрия, её создать. Лист утверждал: только целевые

³ Накануне саммита президентов США и России в Москве 1–2 сентября 1998 года Кремль предложил обсудить, в частности, проект совместного заявления двух лидеров по проблеме информационной безопасности. В предложенном Российской Федерацией проекте документа было указано, что в современной ситуации в сфере ИКТ создан потенциал развития человечества через глобальную информационно-технологическую революцию, но в то же время усиливаются угрозы использования новых технологий в целях подрыва международной стабильности. Вашингтон предложение обсудить документ и подписать коммюнике проигнорировал. См.: Фёдоров А. В. Информационная безопасность в мировом политическом процессе. М.: МГИМО-Университет, 2006. С. 187.

государственные инвестиции могут дать толчок быстрому росту промышленности, поскольку ни слабые банки, ни лишённые сбережений граждане не способны обеспечить развитие экономики достаточными капиталами. В качестве ключевого элемента программы догоняющего развития Лист видел жёсткую протекционистскую политику, проводимую с самого раннего этапа модернизации. Целью политики догоняющего развития немецко-американский экономист видел полную независимость от импорта высокотехнологической продукции, определяющей уровень развития экономики, а в конечном счёте и гарантирующей военную безопасность государства.

С момента зарождения и вплоть до сего дня политика догоняющего развития – удел школы экономического национализма, противостоящей либерализму. Методологическая трудность, с которой либералы так и не смогли справиться вплоть до настоящего времени, состоит в оценке роли государства в процессе развития. Неолибералы и либертарианцы категорически не желают рассматривать государство (в лице структур его исполнительной и законодательной власти) в качестве основного или просто политически значимого актора в деле достижения целей догоняющего развития. Попытка «рыночников» избежать ответа на вопрос о том, какая структура в системе государственного управления сможет провозгласить курс на ускоренное развитие, разработать сколько-нибудь достоверный и долговременный план движения по указанному пути, свидетельствовала об интеллектуальной слабости их позиции. Опыт успешных модернизационных рывков XIX–XX столетий (объединённая Германия, вышедшая из многовековой изоляции Япония, многонациональная Российская империя) показывает, что государство в лице его политико-экономических институтов играет в решении данной задачи ключевую роль. Помимо государства данную миссию никто выполнить не способен.

Для представителей власти важен диалог с деловыми элитами, научными кругами и структурами гражданского общества. Но данный диалог лишь дополняет действия суверенного государства, его политических лидеров, руководителей правительства, парламента, регионов. Изучая политэкономии ИКТ, мы пришли к выводу о том, что построение отдельными государствами конкурентных в мировом масштабе технологических платформ – частный случай модели догоняющего развития⁴.

Первая научная публикация, в которой использовался термин «информационно-коммуникационные технологии», была опубликована в *Harvard Business Review* в декабре 1958 года⁵. До конца прошлого столетия лидерство США в данной области было бесспорным, и казалось, что бросить вызов

⁴ Tkachenko S. The Political Economy of Russian Information & Communication Technologies // PONARS Eurasia Policy Memo No 533. URL: http://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/Pepm533_Tkachenko_June2018.pdf

⁵ Leavitt H. J., Whisler Th. L. Management in the 1980s // *Harvard Business Review*, 1958. URL: <https://hbr.org/1958/11/management-in-the-1980s>

ему невозможно. Но быстрый рост экономик Китая и Индии, а также развитие сферы высоких технологий в России создали условия для оспаривания доминирования США в области ИКТ. В настоящее время в конкуренции национальных технологических платформ участвуют США, Китай и Россия. При этом Москва разделяет основные принципы политики Китая в области обеспечения кибербезопасности при регулировании интернет-пространства.

С 1980-х годов Китай, встав на путь догоняющего развития, трансформировался в крупнейшую экономику планеты (по показателям ВВП), а также де-факто превратился во второй, равный по большинству показателей США полюс в глобальной политико-экономической системе. Киберпространство и область высоких технологий стали пространством их битвы за глобальное доминирование. При этом соперничество двух крупнейших государств, а также нескольких других полюсов мировой системы, включая Индию, Европейский союз и Россию, идёт не по тем правилам, что действовали в прошлом столетии. Конфликт нарастает в условиях сохранения глобальных цепей поставок и межгосударственного сотрудничества, регулируемого правилами ВТО, а также рядом региональных соглашений. Противостояние США и Китая может привести к тому, что обсуждаемая уже несколько лет угроза «декаплинга»⁶ может стать реальностью, приведя к формированию двух враждебных друг к другу национальных технологических платформ.

Почему излишне энергичное вмешательство государства в развитие индустрии ИКТ не стоит приветствовать, а следует рассматривать в качестве исключительного случая для «трудных времён», от которого нужно отказаться при первой же возможности?

Антропологи Аллен Джонсон и Тимоти Эрл сформулировали на первый взгляд шуточный «принцип наименьшего усилия» как один из главных приводных ремней эволюции и изменений в социальной жизни. Он гласит: всякое общество сопротивляется инновациям и не изменяется настолько долго, насколько хватит терпения⁷. Это противоречащее нашим представлениям о рациональном поведении убеждение основывается на наблюдении о том, что среднеарифметическим элитам не нравятся инновации. Пока они обладают ресурсами и могут относительно безболезненно сдерживать стремление к переменам у основной массы общества, в государстве царствуют застой и консерватизм. Разработка конкурентной на мировом уровне технологической платформы – именно такой инновационный вызов, принять который решаются элиты далеко не каждого государства.

⁶ Под «декаплингом» политэкономы понимают процесс, в результате которого сформировавшаяся в 1980–2010-е гг. экономическая взаимозависимость между Соединёнными Штатами и Китаем постепенно снижается, при этом как технологическое, так и инвестиционно-финансовое разделение США и КНР неизбежно ведёт к ухудшению двухсторонних отношений и увеличению вероятности их полномасштабного конфликта.

⁷ Джонсон А., Эрл Т. Эволюция человеческих обществ. От добывающей общины к аграрному государству. М.: Издательство Института Гайдара, 2017.

У биологической науки исследователи проблем технологических платформ могут позаимствовать активно обсуждаемый сейчас «принцип избыточного разнообразия». Исследование действительно длительных процессов сегодня возможно только в сфере биологии, поскольку история технологий слишком коротка для проведения подобного анализа. В эволюции биологических видов регулярно возникали кризисные ситуации, в которых наиболее полезными для выживания и перехода на новый уровень развития оказывались некие бесполезные ранее, побочные и излишние свойства живых организмов. То есть в ситуации, когда неизвестно, каким именно будет грядущий кризис, наличие разнообразных свойств, выходящих за рамки «минимально необходимых», повышает вероятность успешного преодоления возникающих потрясений. В спокойные периоды разнообразие избыточно, его поддержание требует дополнительных ресурсов. Но и излишняя специализация лишает биологическую или социальную систему необходимой гибкости, ведёт к кризису или даже краху.

Такие же аналогии могут быть проведены в инженерных науках. Экспертам в сфере информационных технологий отлично известно, что абсолютно избыточная система абсолютно ненадёжна, так как выход из строя любого элемента приводит к отказу всей системы. И наоборот – доказана на практике теорема, гласящая, что можно создать сколь угодно надёжную систему из сколь угодно ненадёжных элементов (разумеется, за счёт большой избыточности).

Задача государства сегодня состоит в определении требуемого уровня «разнообразия» в развитии национальной технологической платформы, чтобы российская промышленность и экономика страны в целом были готовы к максимальному числу различных потрясений, которые нам готовит нелинейное развитие окружающего нас мира. Данное разнообразие государство в лице его властных структур создать не может, оно возникает в свободной и конкурентной рыночной среде.

Ещё один принцип, который также активно обсуждается и спор в отношении которого ещё далёк от завершения, получил название «принципа оптимальной фрагментации». Он утверждает, что избыточное соперничество в какой-либо социальной или биологической системе опасно, так как ведёт к хаосу, а недостаток соперничества также неблагоприятен, поскольку стимулирует косность и гасит стремление к переменам. Поэтому ещё одна стоящая перед властью задача, не отличающаяся тривиальностью, потому что от правильности её решения зависят судьбы страны и её граждан, состоит в том, чтобы установить параметры оптимальной зоны, расположенной на оси возможных опций где-то между двумя крайними точками. Эксперты отмечают, что оптимальное число участников конкурентной борьбы, в которой формируются

и соблюдаются правила, но при этом возникают стимулы для соперничества, стимулирующего развитие, – от трёх до шести. При наличии лишь двух сторон возникает фронтальное противостояние, ведущее к подавлению или даже уничтожению одной из сторон. А если число соперников превышает шесть, то, как правило, исчезает возможность учитывать действия других сторон в этой условной «игре», фокус внимания в условиях возникающей анархии теряется⁸.

Авторы этого доклада исходят из убеждения в том, что в долгосрочной перспективе ни одно правительство не способно имитировать конкурентную среду или планировать развитие национальной технологической платформы с учётом множества внутренних и внешних факторов, влияющих на её развитие. Рынок с этими задачами справится успешнее. А у государства появится возможность использовать отдельные достижения национальной индустрии ИКТ для обеспечения государственной безопасности.

Исследования ряда экспертов, в частности Ян Кайфэна и Мелицки Джеймса, показали, что при разработке государственной политики в области развития ИКТ и сопутствующей инфраструктуры органы исполнительной и законодательной власти сталкиваются с комплексом проблем, делающих невозможным стратегическое планирование на сколько-нибудь долгий срок⁹. В реестре приоритетов любого правительства начала нынешнего столетия выше задач развития национальной технологической платформы, как правило, стоят: интересы внутренней и внешней безопасности; электоральные циклы и фактор выборов; противоречия между заявленными целями экономической и социальной политики, требующие постоянного лавирования; конфликты интересов вовлечённых в процесс информатизации структур и отдельных лиц; типичное для большинства людей стремление сопротивляться инновациям; а также правовые коллизии, неизбежно возникающие в процессе перехода на цифровые технологии. Ситуация стала исправляться лишь относительно недавно. Вмешательство органов государственной власти стран, опоздавших в развитии национальных технологических платформ, стало приобретать черты планомерной деятельности лишь после того, как в эту работу включились крупнейшие экономики планеты.

⁸ Данный принцип был сформулирован независимо друг от друга двумя американскими учеными: социологом Рэндаллом Коллинзом и биогеографом Джаредом Даймондом. Самый известный поклонник данного принципа – создатель «Майкрософт» Билл Гейтс, который убеждён в том, что его практическое применение помогает строить сложные системы и наиболее эффективно управлять ими.

⁹ Yang K., Melitski J. Competing and Complementary Values in Information Technology Strategic Planning // Public Performance & Management Review. 2007. Vol. 30. No 3. March. P. 426–427; Holley L. M., Dufnet D. & Reed B. J. Got SISP? Strategic Information systems planning in U.S. state governments // Public Performance & Management Review. 2002. Vol. 27. No 4. June. P. 398–412.

Глобальная экономика, в которой сектор ИКТ является основным на сегодняшний день драйвером роста, наглядно демонстрирует эффективность приватизации. Она требует дерегулирования отдельных сегментов национальной экономики, создаёт условия для партнёрства бизнес-структур, например, посредством создания саморегулируемых организаций или профессиональных ассоциаций (АПКИТ, РУССОФТ).

Отмеченное выше не отменяет того, что в условиях, когда политические угрозы преобладают над экономическими возможностями, органы государственной власти вправе выйти на авансцену и сыграть ключевую роль в минимизации негативного влияния внешних шоков. Именно такой период сегодня переживает Российская Федерация. Оказавшись под ударом спланированных Вашингтоном экономических санкций, направленных на подрыв и последующее уничтожение национальной экономики, правительство России вынуждено предпринимать экстренные меры по отражению агрессии нового типа, по обороне страны в рамках ведущейся против неё экономической войны. Поддержка российских софтверных компаний и иных институтов российской экосистемы ИКТ, а также перенос производства элементной базы и программных продуктов на территорию России являются эффективными ответами на враждебные действия.

В такой непростой для нашего государства период сложно требовать от правительства Российской Федерации поддержания конкурентной среды в экономике. Поэтому со стороны бизнеса к правительству возникает другой, не менее срочный и важный запрос – обеспечить транспарентную и эффективную работу всех институтов национальной экономики, включая независимые суды, борьбу с коррупцией, изгнание из структур власти неквалифицированных руководителей и исполнителей.

Российские ИКТ и национальная технологическая платформа

Российская индустрия ИКТ ещё очень молода – она отмечает тридцатилетний юбилей с момента своего зарождения, поскольку в советские времена такой отдельной отрасли промышленности попросту не существовало. Три десятилетия – это недостаточно долгий период для того, чтобы утверждать, что мы всё знаем об этой отрасли, законах её развития, глобальном влиянии. Тем не менее можно сказать, что российская индустрия ИКТ состоялась. Она не только выжила в бурно меняющейся и временами весьма агрессивной политико-экономической

ТАБЛИЦА 1. ОБЩИЕ ДАННЫЕ, ХАРАКТЕРИЗУЮЩИЕ РОССИЙСКУЮ ИНДУСТРИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ (ПО СОСТОЯНИЮ НА 31.12.2020 Г.)

Количество устойчивых российских софтверных компаний	не менее 4 тыс.
Количество компаний, имеющих экспортные доходы	не менее 2,5 тыс.
Количество программистов	чел.
Разработчики ПО, работающие во всех отраслях (в том числе в ИТ-службах предприятий разных сфер деятельности)	>580 000
Разработчики ПО, работающие в российской индустрии разработки ПО (всего), из них:	>180 000
- в центрах разработки ПО за рубежом	>10 000
- то же в России	≈170 000
Сотрудники сервисных компаний (в том числе работающие на зарубежных заказчиков)	≈90 000 (40 000)
Сотрудники продуктовых компаний	≈70 000
Сотрудники российских центров R&D зарубежных компаний	≈8 000

Источник: данные РУССОФТ. URL: <https://russoft.org/russoft-analytics>

среде, но и превращается сегодня в главную надежду российской экономики, претендуя занять достойное место в системе глобального хозяйства XXI столетия (табл. 1).

Россия всегда была и будет великой державой, имеющей влияние на ход мировой истории, определяющей баланс сил на планете, поддерживающей порядок и противостоящей угрозе анархии в международных отношениях. Экономика нашей страны, переживающая трудности переходного периода, должна войти в пятерку крупнейших экономик планеты. Без успешного развития индустрии ИКТ достичь этой цели будет невозможно.

Исследование практики регулирования индустрии ИКТ в десяти крупнейших рыночных экономиках планеты, проведенное Ян Кайфэнгом и Мелицки Джеймсом, демонстрирует, что, определяя свою стратегию в данной области, органы государственного управления вынуждены делать свой выбор из двух пар политических по своей природе целей¹⁰.

¹⁰Yang K., Melitski J. Competing and Complementary Values in Information Technology Strategic Planning. Observations from Ten States // Public Performance & Management Review. 2007. Vol. 30. No 3. March. P. 426–427.

Первая пара – выбор между приоритетами *внутреннего экономического развития и интеграцией в мировую экономику*. По сути, перед нами пример длящегося почти четырьмя десятилетиями поиска внутренних или внешних драйверов для долгосрочного роста национальной экономики. Зачастую такой выбор оказывался ложным, поскольку для интеграции в мировую экономику требовалось поначалу создать сильную национальную промышленность. Поэтому за этапом «внутреннего сосредоточения» должен следовать этап открытия экономики и дальнейшей экспансии продукции лишь недавно созданной национальной промышленности на внешних рынках.

Вторая пара – это выбор между *построением эффективной экономики*, в которой по возможности учитываются интересы всех стейкхолдеров, и ни один из них не развивается за счёт подавления других, и *формированием приносящей сиюминутные результаты экономической модели*, которая игнорирует или слабо учитывает фактор стратегических последствий текущей деятельности исполнительной и законодательной ветвей власти. В теории такой выбор выглядит искусственным, поскольку эффективная экономика – стратегическая цель для любой страны и её органов государственного управления. Но, поскольку фактор времени в политике зачастую более важен, чем в экономической жизни, государственные деятели очень часто делают далеко не оптимальные, но привлекательные для них шаги, продиктованные краткосрочными электоральными интересами.

Исследование макроэкономической политики государств ОЭСР показывает, что практически всегда их органы управления делают выбор в пользу приоритетов внутреннего развития и построения приносящей сиюминутные бюджетные и операционные результаты экономической модели. Факторы, влияющие на процесс принятия решений структурами государственной власти, многочисленны и не всегда прогнозируемы. К ним следует отнести меняющуюся внутривластную ситуацию, «электоральную политику» (необходимость реализовывать свои идеи в рамках одного электорального цикла и игнорировать более долгую перспективу), трудности выбора приоритетов развития страны в рамках многопартийных правящих коалиций и так далее. В такой среде интересы любого бизнеса, в том числе и высокотехнологического, обычно оказываются на периферии внимания политиков и чиновников.

На практике фундаментальные для глобальной политико-экономической системы процессы развиваются по более благоприятному для индустрии ИКТ сценарию. Частный бизнес уравнивает краткосрочные и тактические по своей сути действия властей своими инвестиционными решениями, которые формируют долгосрочные тренды и реализуют масштабные проекты, игнорирующие «фактор правительства» или же рассматривающие его как неизбежное, но преодолимое препятствие. Изучение глобальной индустрии ИКТ подтверждает актуальность отмеченных выше

тенденций и для Российской Федерации. Неизбежный вывод, к которому следует прийти, состоит в привлекательности всемерного развития государственно-частного партнёрства как институционализованного диалога власти и бизнеса. Они должны выступать равноправными и взаимодополняющими друг друга союзниками в деле развития национального высокотехнологического сектора экономики.

По мнению одного из признанных авторитетов мировой индустрии ИКТ, международного венчурного инвестора Александра Галицкого, государственно-частное партнёрство «следует рассматривать в качестве одной из наиболее эффективных форм стимулирования инновационных процессов в мире»¹¹. Многовековой опыт взаимоотношений государства и рынка показывает, что органы государственной власти – неважные коммерсанты. Сегодня не стоит и думать о том, что чиновникам можно доверить построение национальной технологической платформы и продвижение на рынок отдельных создаваемых в рамках этой деятельности программных продуктов. Учитывая современный уровень развития информационно-коммуникационных технологий, перед государственной властью общество должно поставить другую задачу – развитие рыночной инфраструктуры, включая законодательство, правоприменение, образование и так далее. Для частного инвестора в сфере венчурного капитала главная задача состоит из двух элементов: **во-первых**, нужно выбрать наиболее перспективную инновационную компанию и стартап с высокой степенью «выживаемости»; **во-вторых**, максимально снизить риски провала и потери инвестиций. При соблюдении таких условий у государства появятся и интеллектуальные ресурсы, и финансовые возможности для того, чтобы возглавить процесс построения национальной технологической платформы, оставив инициативу отечественным компаниям индустрии ИКТ.

Именно здесь потенциально пересекаются интересы государства и бизнеса. *Бизнес* должен принимать хозяйственные решения на основе максимально возможных объёмов требуемой для рационального целеполагания информации. Степень «рациональности» (осведомлённости) при принятии управленческих решений повышается, если бизнес твёрдо уверен в стабильности институциональной структуры экономики. *Государство* должно минимизировать угрозу того, что бизнес будет принимать неверные решения, способные привести к финансовым потерям и провалам. Приоритетные направления деятельности органов власти при построении национальной технологической платформы: организационно-консультационное содействие компаниям сектора венчурного финансирования, а также контроль макроэкономических индикаторов на уровнях, при которых обеспечивается наиболее благоприятная среда для развития инноваций.

¹¹ Galitsky A. Public-private partnerships – fostering innovations in Russia // *Baltic Rim Economies*. 2014. Issue 2. April 29. P. 39.

То есть мы можем констатировать, что сделка между бизнесом и властью при создании национальной технологической платформы в сфере ИКТ могла бы состоять в следующем: обмен политической поддержки на начальных этапах реализации инновационных проектов (со стороны правительства) на опыт частного бизнеса в реализации проектов в высокотехнологической сфере, его активную работу на всех этапах реализации проектов, а также готовность вложить масштабные собственные средства, как только станет понятно, что проект выжил и имеет хорошие бизнес-перспективы (табл. 2).

Одна из ключевых проблем состоит в том, что, действуя единолично, правительство может принять ошибочное решение, исходить из неверного понимания сути процессов в сфере ИКТ, у него может отсутствовать вся необходимая для принятия рациональных решений информация. Правительство, по убеждению Маргарет Тэтчер, во многих ситуациях не решает проблемы, а лишь усложняет их. Поэтому определение правильной дистанции между властью и бизнесом, переговорный характер их отношений, переток кадров из правительства в бизнес и обратно – главные внешние условия становления успешной национальной технологической платформы индустрии ИКТ в России.

Сегодня правительство России при реализации проектов поддержки инноваций опирается, прежде всего, на опыт наиболее экономически развитых государств Глобального Севера: США и Западной Европы. Уже принято стимулирующее инновации законодательство, учреждены, начали действовать и даже неоднократно реформированы институты развития (ГК «Внешэкономбанк», ОАО «Роснано», ОАО «Российская венчурная компания»), особые экономические зоны (ОЭЗ «Алабуга» в Республике Татарстан), инкубаторы и технологические парки. При этом, по мнению Александра Галицкого, из-за копирования чужого опыта у российской исполнительной власти сформировались завышенные ожидания в данной сфере, поэтому политики и общественность всякий раз излишне резко реагируют, когда не получают положительных результатов от своих усилий немедленно. Кроме того, оперативность коррекции законодательства и правоприменительной практики в области инноваций пока отстаёт от реальных потребностей, что создаёт простор для коррупции и сохранения ненужных процедур/практик в отношениях между бизнесом и властью¹².

Относительно недавно возникло понимание того, что у развития ИКТ имеются масштабные политические последствия в виде изменения структуры государственной мощи и расширения возможностей госорганов выполнять конституционные задачи по её поддержанию. Сообщество экспертов разделилось в этом вопросе на две большие группы: тех, кто рассматривает ИКТ-технологии, в том числе национальную технологическую платформу, в качестве *экзогенного фактора*,

¹²Galitsky A. Public-private partnerships – fostering innovations in Russia // Baltic Rim Economies. 2014. Issue 2. April 29. P. 39.

ТАБЛИЦА 2. РЕЙТИНГ РЕГИОНОВ РОССИИ ПО УРОВНЮ РАЗВИТИЯ ИНДУСТРИИ ПО (2020)

Две столицы А		Москва и СПб вместе обеспечивают около 50% общего объема разработки ПО			
1 (1)	Москва				
2 (2)	Санкт-Петербург				
Лидеры В		Генезис 1 D		Генезис 2 E	
3 (3)	Новосибирская область	17 (20)	Удмуртская республика	1 (30)	Алтайский край
4 (4)	Нижегородская область	18 (17)	Тульская область	2 (19)	Башкортостан (республика)
5 (5)	Татарстан	19 (15)	Ульяновская область	3 (32)	Белгородская область
Претенденты С		20 (16)	Ярославская область	4 (-)	Брянская область
6 (7)	Ростовская область	21 (24)	Калининградская область	5 (33)	Калужская область
7 (6)	Свердловская область	22 (31)	Республика Марий Эл	6 (38)	Карелия (республика)
8 (13)	Самарская область	23 (23)	Красноярский край	7 (-)	Кемеровская область
9 (9)	Воронежская область	24 (28)	Вологодская область	8 (35)	Приморский край
10 (10)	Томская область	25 (37)	Республика Саха (Якутия)	9 (36)	Рязанская область
11 (12)	Челябинская область	26 (21)	Волгоградская область	10 (29)	Тверская область
12 (11)	Пермский край	27 (27)	Тюменская область	11 (-)	Хабаровский край
13 (14)	Краснодарский край	28 (25)	Иркутская область		
14 (18)	Омская область	29 (26)	Пензенская область		
15 (22)	Саратовская область	30 (34)	Ивановская область		
16 (8)	Московская область				

способного влиять (или не влиять – в зависимости от множества причин) на сравнительную мощь государств в мировой системе. Их оппоненты убеждены в том, что ИКТ и национальная технологическая платформа сегодня и есть *воплощение государственной мощи*, они сами по себе являются факторами, формирующими и изменяющими политико-экономическую природу суверенного государства¹³.

Обе указанные выше позиции (нейтральность ИКТ или же их политико-экономическое всевластие), по нашему мнению, ошибочны в силу своей однозначности. ИКТ, конечно, не являются нейтральными по отношению к государственной мощи; сегодня они не могут быть проигнорированы при сравнении стран между собой. В то же время было бы ошибкой утверждать, что ИКТ – универсальное оружие, которое человечество создавало столетиями и наконец получило в своё распоряжение для того, чтобы заменить им виды оружия и военной техники прежних эпох.

Политологи навязывают нам необходимость выбора между двумя указанными выше позициями. Мы же считаем, что от него следует уклониться, заняв позицию, которую зарубежные коллеги называют *middle ground*. Вопросы, которые должна в приоритетном порядке рассматривать дискуссия о «силе интернета» как факторе государственной мощи, касаются *кибербезопасности, международно-правового режима регулирования интернета* и того, что принято называть *сетевой нейтральностью*. Наличие ИКТ заставляет политиков, военных и разведчиков обращаться к их ресурсам для того, чтобы решать стоящие перед органами государственного управления задачи, как традиционные, так и совершенно новые. Но каким бы ни было отношение органов государственной власти к ИКТ, включая степень свободы интернета, они вынуждены сформулировать свою позицию по указанным выше трём сферам.

Действительно, интернет – это лишь технология, и она не может включать в себя такие нормы и ценности, как демократия, свобода или права человека. Его способность решающим образом влиять на межгосударственные конфликты может оказаться в одном случае реальной, а в другом – фиктивной. Именно поэтому классик современной теории международных отношений Джон Миршаймер в своей монографии «Трагедия великодержавной политики» справедливо отметил: «...хотя нематериальные факторы могут иметь влияние на итоги военного конфликта, иногда даже решающее, тем

¹³ Амбивалентность высоких интернет-технологий как фактора государственной силы ярко выразил бывший президент США Барак Обама, назвавший величайшей иронией цифровой эры то, что государства, наиболее успешно адаптировавшие к интересам своих граждан и наиболее интенсивно эксплуатирующие ресурсы цифровой эры, одновременно оказываются и наиболее подверженными всем тем угрозам, которые данная эра принесла в наш мир. См.: President Barack Obama, 'Remarks by the President on Securing Our Nation's Cyber Infrastructure'. Office of the Press Secretary. Washington, D.C., The White House. May 29, 2009. URL: <https://obamawhitehouse.archives.gov/realitycheck/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>

не менее располагаемые материальные ресурсы государства являются наиболее надёжным и, как следствие, самым важным индикатором того, какое же из государств сможет одержать в конфликте победу»¹⁴. Мы вынуждены с тревогой заметить, что в России вопросы о роли нематериальных факторов в обеспечении национальной безопасности проникают в повестку дня органов государственного управления с большим опозданием. Крайне неохотно отечественные парламентарии и правительственные чиновники привлекают представителей ИКТ-индустрии и экспертного сообщества к их обсуждению.

Российская идея использовать форум БРИКС для того, чтобы построить на специальной технологической платформе «отдельный интернет», где не было бы места регулирующим органам США и других государств – лидеров мировой экономики, нам представляется опасной. Но именно данная идея недавно оказалась в центре дискуссии относительно новой модели управления интернетом и защиты в её рамках суверенитета отдельных государств.

26 сентября 2017 года Совет безопасности России поручил Минкомсвязи совместно с МИД Российской Федерации инициировать в рамках БРИКС обсуждение вопроса о создании для государств – участников данного форума собственной «системы дублирующих корневых серверов доменных имён (DNS)¹⁵. Эта система должна быть независимой от контроля таких международных структур с сильным американским доминированием, как ICANN, IANA¹⁶ и VeriSign¹⁷. Главная цель указанной инициативы состояла в том, чтобы гарантировать обслуживание запросов пользователей из стран БРИКС на случай сбоев глобальной паутины в её нынешней версии или же (и это главное!) на случай попытки полного блокирования доступа пользователей из государств БРИКС к ресурсам интернета. Мотив безопасности в этой российской инициативе является главным. Именно опасениями использования интернета для проведения наступательных киберопераций противниками России, в числе которых прямо названы США и государства НАТО, и руководствовались члены

¹⁴ Mearsheimer J. The Tragedy of Great Power Politics. New York: W. W. Norton & Company, 2001. P. 58.

¹⁵ Совет безопасности поручил создать «независимый интернет» для стран БРИКС // Информационное агентство «РБК», 2017. URL: https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca

¹⁶ IANA (*Internet Assigned Numbers Authority*) – Администрация адресного пространства интернета. Она исполняет функции управления пространствами IP-адресов, доменов верхнего уровня, а также регистрирует типы данных MIME и параметры иных протоколов интернета. Данная деятельность сегодня выполняется компанией *Public Technical Identifiers*, которая находится под контролем ICANN.

¹⁷ Американская компания *VeriSign* – мировой лидер в области доменных имён и обеспечения безопасности в интернете. Компания поддерживает работу многих из самых известных доменных имён и обеспечивает защиту веб-сайтов и предприятий во всём мире. *VeriSign* обеспечивает операционную точность и стабильность работы доменов .com и .net, выполняя функции управления и защиты инфраструктуры DNS для более чем 144,3 миллиона доменных имён. Технологическая платформа компании обрабатывает ежедневно около 135 миллиардов операций, обеспечивая надёжную и безопасную работу интернета во всём мире.

Совета безопасности Российской Федерации при выдвижении указанной инициативы. Однако получить необходимую поддержку этой инициативы на международном уровне пока не удалось.

По нашему мнению, указанные выше опасения выглядят обоснованными, но предложенный механизм противодействия им чрезмерен. В данном случае лекарство может оказаться опаснее, чем болезнь, с которой оно должно бороться. *DNS (Domain Name System)* представляет собой распределённую систему хранения данных, от которой зависит работа всемирной сети, поскольку в ней содержатся все доменные имена и соответствующие им *IP*-адреса. Система *DNS* построена по иерархической модели, в её основе лежат тринадцать корневых серверов, которые обеспечивают доступ к информации обо всех доменах верхнего уровня, в том числе о национальных доменах (*.ru*, *.it*) и доменах общего назначения (*.com*, *.net*). Абсолютное большинство корневых серверов сегодня расположено в США, остальные – в Западной Европе и Японии. В ряде других государств, в том числе и в России, имеются «зеркала», функция которых состоит в том, чтобы запросы пользователей из конкретного государства обслуживались «на месте», в их же собственной стране, а не обращались к *DNS*-серверу, расположенному в другом уголке планеты. Следует лишь помнить, что «зеркала» дублируют информацию корневых серверов и никакой оригинальной информации не содержат.

С точки зрения интересов безопасности России важно помнить, что среди организаций, обеспечивающих работу корневых серверов *DNS*, есть такие структуры исполнительной ветви власти США, как Министерство обороны, а также Национальное управление по аэронавтике и исследованию космического пространства (*NASA*). Никакое «воздействие международного сообщества» на их деятельность невозможно, как невозможна и транспарентность в принятии структурами исполнительной ветви власти США решений относительно других государств.

Является ли в этой ситуации призыв к созданию странами БРИКС собственной системы корневых *DNS*-серверов приемлемым решением, обеспечивающим безопасность государства? Разумеется, всё зависит от того, какова цель этой деятельности и как именно данное решение будет исполнено. В рамках существующей архитектуры глобального интернета нельзя добиться независимости от действий зарубежных партнёров путём создания новых корневых *DNS*-серверов, поскольку любая информация по этим корневым серверам будет расходиться из одной точки – названной выше *IANA*. То есть построение государствами БРИКС системы корневых серверов доменных имён, независимой от международных (американских) администраторов, по сути является призывом к построению параллельного интернет-пространства, альтернативного нынешнему и никак с ним не связанного.

Здесь скрывается сущность затронутой нами проблемы. Предположим, что задача, решаемая Российской Федерацией, – использовать угрозу построения «параллельного интернета» для создания эффективной и конкурентной национальной технологической платформы и, как следствие, для получения сравнительных преимуществ в переговорном процессе с США о благоприятном международно-правовом режиме интернета. Тогда истинной целью, достигаемой при решении данной задачи, должно быть провозглашено построение новой архитектуры международной безопасности, учитывающей реалии эпохи четвёртой промышленной революции.

Если всё обстоит именно так, то нам остаётся только пожелать российской дипломатии успеха. Но считаем нужным предупредить – борьба предстоит очень трудная, а шансы на победу невелики. США, равно как и Россия, никогда не меняли свою политику под давлением со стороны другого государства, особенно если давление осуществляется публично. Не допускать нажима со стороны внешних игроков, оберегать внутриполитическую систему от внешних воздействий – суверенное право любого государства, которым на практике пользуется лишь узкая группа подлинно суверенных держав, которые относятся к категории «великих». Несомненное, что США и Россия к этой категории относятся. Решение отказаться от трудного диалога с США и их союзниками, перейти на язык ультиматумов в вопросах кибербезопасности и обеспечения бесперебойной работы всемирной паутины пока не принято, оно требует широкого экспертного обсуждения. Строить доверительные отношения между великими державами в области киберпространства непросто, но альтернативы в данном случае мы не видим. Эпоха холодной войны оставила Москве и Вашингтону ценное наследие – практику «доверительного диалога» по проблемам безопасности, в ходе которого стороны обменивались информацией и вырабатывали механизмы, помогающие избежать катастрофического конфликта. Мы убеждены – настало время для такого диалога на тему кибербезопасности. Возможно, он уже ведётся, но общественность об этом не информирована.

Также отметим проблематичность обращения России к БРИКС с целью достижения к 2035 году *глобального технологического лидерства*, зафиксированной в Национальной технологической инициативе¹⁸. Перспективы использования БРИКС для построения многополярного мира, ещё недавно присутствовавшие в российской политике по отношению

¹⁸ Идея реализации Национальной технологической инициативы (НТИ) была выдвинута Владимиром Путиным в послании Федеральному Собранию Российской Федерации 4 декабря 2014 года. НТИ является долгосрочной межведомственной программой государственно-частного партнёрства по содействию развитию новых перспективных рынков на базе высокотехнологичных решений, которые будут определять эволюцию мировой и российской экономики через пятнадцать – двадцать лет.

к данному форуму, сегодня выглядят призрачными¹⁹. В то же время БРИКС идеально подходит для формирования пятёркой государств технологических альянсов, способных придать дополнительный импульс развитию наиболее современных отраслей экономики, а также защитить их технологический суверенитет от попыток его маргинализации крупнейшими компаниями стран Глобального Севера при поддержке их правительств. Уровень технологического развития пятёрки стран БРИКС, а также тех государств, которые объективно могут быть отнесены к этой категории (Турция, Аргентина, Саудовская Аравия), в целом близок. Но структура их экономики отличается. Китай специализируется на массовом производстве продукции, Индия – на сфере услуг и ИКТ, Россия является крупнейшим поставщиком сырья и обладает уникальными военными технологиями²⁰. Если три упомянутых лидера БРИКС не начнут выстраивать между собой отношения сотрудничества и взаимозависимости в сфере технологий, это будет упущением с их стороны. Дипломатические усилия по построению многополярного мира могли бы послужить удобным политическим «зонтиком» для такого взаимодействия.

Заключение

В качестве основных выводов нашего доклада отметим следующее.

Во-первых, для создания в России успешной технологической платформы в сфере ИКТ требуется разработка сложного объёмного программного обеспечения, что возможно только при наличии широкого набора созданных отечественными программистами инструментальных средств: графические и текстовые редакторы, трансляторы с алгоритмических языков высокого уровня, отладчики, профиляторы и так далее. Современными компьютерами управляют операционные системы, осуществляющие руководство процессами и памятью, работающие с файловыми системами, обеспечивающие безопасность и тому подобное. Инструментальные средства совместно с операционными системами, а также компьютеры, на которых всё это применяется, называют технологической платформой. Строительство отечественной технологической платформы нужно начинать с фундамента, не пытаясь строить воздушные замки.

¹⁹Ткаченко С. Л., Койл У. БРИКС и новая модель гегемонистской стабильности // Вестник Санкт-Петербургского университета. Международные отношения. 2020. Т. 13. Вып. 3. С. 294–309.

²⁰Dau-Schmidt K. G. Labor Law 2.0; the impact of new information technology on the employment relationship and the relevance of the NLRA // Emory Law Journal. 2015. Vol. 64. P. 1597.

Во-вторых, совершенно очевидно, что в наш век информационных войн все системы, перечисленные выше, уязвимы. Случайно или преднамеренно работа операционной системы или транслятора может быть приостановлена или заблокирована по какому-то сигналу извне, причём обнаружить такой сигнал очень трудно. Это не обязательно какой-то выделенный код – это может быть комбинация безобидных кодов или, наоборот, отсутствие сигналов в течение определённых интервалов времени. К сожалению, история последних десятилетий дала нам множество примеров таких ситуаций. Поэтому стремление создать собственные полностью «национальные» операционные системы и трансляторы – не вызов рациональной логике эффективного рынка, а вынужденный шаг, продиктованный соображениями государственной безопасности. Речь должна идти не о создании Россией, союзными странами ЕАЭС и ОДКБ своего «отдельного интернета» – это затея исключительно дорогая, а её эффективность сомнительна. Но органы федеральной власти России могут уже сейчас поставить задачу разработки узкого сегмента сети, аналогичной интернету, который ни одним проводом не будет связан с мировым интернетом. Такая сеть могла бы использоваться для государственного/военного применения, она может оказаться весьма актуальной в экстренных ситуациях. Российским учёным сегодня по силам оперативно решить эту задачу на основе имеющегося опыта и созданной в стране производственной базы.

В-третьих, попытки разработки национальных технологических платформ в России уже неоднократно предпринимались, но каких-то прорывных решений пока создать не удалось. Противники идеи национальной технологической платформы обычно говорят, что на Западе на создание таких платформ ушли десятилетия и сотни миллиардов долларов, поэтому даже не стоит начинать такую работу в России. Однако не обязательно делать всё сразу. Необходимо в рамках диалога госчиновников и представителей индустрии ИКТ выделить те ниши, где интересы безопасности России могут пострадать в первую очередь, и решить согласованные сторонами задачи в рамках государственно-частного партнёрства. Как говорят в Китае, даже путь в тысячу ли начинается с первого шага.

В-четвёртых, необходимо добиться того, чтобы государственные корпорации как крупнейшие в стране заказчики ПО разрешили пускать заказанные госкорпорациями (причём остро им необходимые) системы, произведённые отечественными софтверными компаниями, в коммерческий оборот.

В-пятых, важно публичное признание работы системных программистов, которые будут создавать национальную платформу. В нашей стране многие используют различные отечественные ИТ-приложения, но практически

никто не знает, кем и с помощью каких средств они были разработаны. Такое «паблисити» особенно важно для молодых программистов.

Итак, создание национальной технологической платформы необходимо для информационной безопасности страны и обеспечения технологической независимости от западных поставщиков платформ. Однако данная задача не имеет простого решения, поскольку в ближайшие годы руководство страны будет сосредоточено на обеспечении безопасности государства, решать проблемы, возникающие в процессе догоняющего развития, пытаясь не уничтожить при этом рыночный характер отечественной экономики.

В завершение подчеркнём: никаких «уникальных российских» ИКТ, оторванных от глобальных технологий, не существует. Национальная стратегия развития рынка ИКТ должна ориентироваться на обеспечение государственной безопасности, а также на ограниченные меры защиты отечественных участников рынка на этапе его формирования. Параллельно следует совершенствовать механизмы продвижения российских компаний на внешних рынках и содействовать повышению их глобальной конкурентоспособности.

Структуры исполнительной власти Российской Федерации имеют подтверждённое законом и традициями право следить за тем, чтобы в сфере ИКТ не возникали угрозы безопасности. А в случае выявления компетентными органами киберугроз российская индустрия ИКТ должна обладать ресурсами для обороны и нанесения ответного удара. Но вся эта деятельность должна быть лишь фоном для главной арены, на которой действует и развивается российская индустрия ИКТ. В этом качестве выступает глобальный конкурентный рынок.

 ValdaiClubRu
 valdaiclub
 ValdaiClub
 valdaiclubcom
 @RuValdaitweets
valdai@valdaiclub.com



СОВЕТ ПО ВНЕШНЕЙ И ОБОРОННОЙ ПОЛИТИКЕ



Российский совет
по международным
делам



МГИМО
УНИВЕРСИТЕТ



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ