Международное управление Интернетом

Под редакцией
Е. С. Зиновьевой

УДК 327
ББК 66.4
М43

Рецензенты:

Сергей Владимирович Шитьков,
к.юрид.н., и.о. Ректора Дипломатической академии МИД России

Наталья Александровна Цветкова,
д.полит.н., профессор, и.о. Директора ИСКРАН

Международное управление Интернетом / Е.С. Зиновьева, А.А. Игнатов, А.А. Уланов, Э.Л. Сидоренко, А.В. Сытник, М.М. Базлуцкая, Н.Ю. Силаев, В.Е. Таран, И.О. Яникеева; под редакцией Е.С. Зиновьевой – М.: 2025. – 186 с.

Аннотация:

Книга «Международное управление Интернетом» включает в себя анализ ключевых тенденций развития Интернета и системы управления сетью на современном этапе. Подробно изучена история развития Интернета, рассмотрено, как появлялись институты и механизмы управления сетью, проанализированы современные проблемы и вызовы в области управления Интернетом. Показано, как новые технологии, в том числе технологии искусственного интеллекта влияют на развитие Интернета и цифровой сферы в целом, а также институтов управления процессами глобальной цифровой трансформации.

Подписано в печать 20.03.2025
Формат 70x100/16
Усл. печ. л. 15,12
Тираж 300 экз.
Издатель Серпантин Про (ИП Гончаров А.В.)
ISBN 978-5-6053935-0-4

Международное управление Интернетом

Под редакцией
Е. С. Зиновьевой

2025

Уважаемые читатели!

Интернет уже давно стал неотъемлемой частью нашей повседневной жизни, но он продолжает изменяться, отражая новые вызовы и тенденции в глобальной политике и научно-техническом развитии. Формирование многополярной системы международных отношений, подъем незападных центров силы, а также развитие прорывных технологий, ведущей из которых является искусственный интеллект – все это оказывает влияние на характеристики Интернета и системы управления Всемирной сетью.

Мы стоим на пороге эпохи, когда глобальная сеть становится важнейшей составляющей международной политики и мировой экономики, и изучение ключевых тенденций ее развития необходимо для лучшего понимания природы современной мировой системы и национальных интересов Российской Федерации.

В предлагаемой вашему вниманию книге нашли отражение ключевые тенденции развития Интернета на современном этапе, подробно изучена история развития Всемирной сети, рассмотрено, как складывались институты и механизмы управления ею, проанализирована современная динамика турбулентной международной политики в области управления Интернетом. Соотношение процессов глобализации и фрагментации Интернета, развитие новых технологий связи, в том числе социальных сетей, и изменение моделей распространения и потребления контента, вызовы, связанные с развитием Интернета, в том числе, в сфере безопасности и экологии, были подробно и глубоко изучены. Мы наблюдаем укрепление цифровых границ на уровне стран и регионов, увеличение числа «национальных» и региональных сегментов Интернета. Также в книге рассматривается влияние цифрового суверенитета на обеспечение

информационной безопасности и защиты национальных интересов в цифровом пространстве, как на уровне отдельных стран, так и регионов. Одной из интереснейших тем, которую затрагивают авторы, является рост влияния незападных центров силы в интернет-пространстве. Западные страны, долгое время определявшие правила игры в Интернете, теперь сталкиваются с растущей конкуренцией со стороны таких стран как Китай, Россия и Индия, а также регионов, в числе которых Африка и Латинская Америка, которые активно встраиваются в глобальное цифровое пространство.

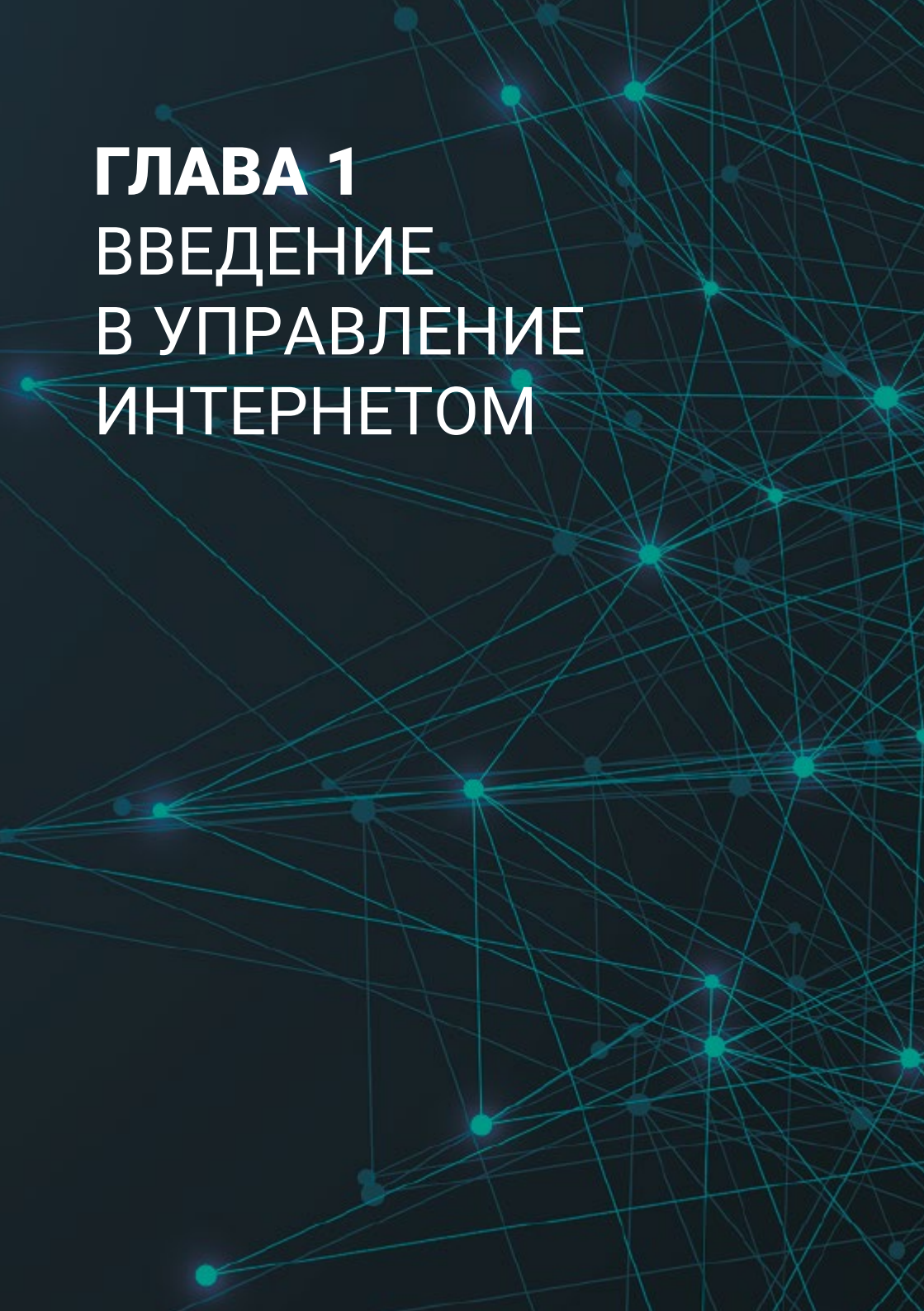
В книге рассмотрены актуальные проблемы развития Интернета, в том числе неоколониализм данных, политическое и экономическое измерение технической стандартизации, выработка этических стандартов развития и регулирования технологий искусственного интеллекта, регламентация криптовалют и технологий распределенных реестров. Искусственный интеллект уже играет ключевую роль в управлении трафиком, безопасности и защите данных, а также в формировании новых методов регулирования. Важно понимать, как данная технология может изменить баланс сил в международном управлении Интернетом и какие вызовы он может принести.

Особый акцент сделан на национальных интересах России в области управления Интернетом, роли и месте нашей страны в глобальном информационном пространстве, внешнеполитических инициативах в области управления Интернетом, обеспечения информационной безопасности, этики искусственного интеллекта.

Книга «Международное управление Интернетом» актуальна не только для специалистов в области цифровых технологий и международной политики, но и имеет огромное значение для всех пользователей Всемирной сети. Книга предоставляет ценную информацию о том, как изменения в цифровом пространстве могут повлиять на будущее Интернета и нашего взаимодействия с ним.

С уважением,
Директор Координационного центра доменов .RU/ .РФ
Андрей Воробьев

СОДЕРЖАНИЕ:



ГЛАВА 1
ВВЕДЕНИЕ В УПРАВЛЕНИЕ ИНТЕРНЕТОМ

1.1. Интернет: определение и тенденции развития

1.1.1. Интернет

Прежде чем определять, что же именно представляет собой «управление Интернетом», необходимо чётко обозначить объём понятия «Интернет» и, соответственно, спектр вопросов, которые должны входить в сферу «управления» им. Интернет – это не просто стандарт технического обеспечения или физическая инфраструктура. Он основан на наборе программных инструкций, широко известных как протоколы, используемые для передачи данных между сетями[1]. В наши дни Интернет представляет собой сложную и неоднородную макросистему, объединяющую очень большое число различных информационных сетей.

Современный Интернет состоит из двух главных компонентов: технической инфраструктуры – аппаратных сетей, включающих в себя серверы, хранилища данных, компьютеры конечных пользователей, маршрутизаторы, кабели и другие устройства, и сервисов – передающейся по этим сетям информации, т.е. собственно содержания Интернета. Самым популярным сервисом является «всемирная паутина» (World Wide Web, WWW), представляющая собой связанные гиперссылками тексты, изображения, видео и другие данные в сочетании с необходимым программным обеспечением для их распространения и воспроизведения. Другими видами интернет-сервисов являются электронная почта, файлообменные сети, IP-телефония, электронные платёжные системы и др. Важным компонентом также является система доменных имён и корневых серверов[2]. Интернет крайне децентрализован, что является, кроме всего прочего, залогом его устойчивости и надёжного функционирования.

В западной литературе часто используется понятие киберпространства, под которым понимается уникальный носитель, не находящийся на определённой территории, но доступный каждому в любой точке мира через Интернет[3]. Несмотря на то, что интернет-информация хранится в компьютерных системах, которые практически всегда находятся в границах той или иной национальной юрисдикции, киберпространство как бы «расположено» вне территории отдельных национальных государств. Такой точки зрения придерживается, в частности, авторитетный американский исследователь Милтон Мюллер[4].

В российской академической литературе большее распространение получил термин «информационное пространство», однако исследователи также отмечают, что Интернет является его ключевой инфраструктурой. При этом российские авторы делают больший акцент на то, что информационное пространство не сводимо к цифровой инфраструктуре, кроме того, делается акцент на значимости цифрового суверенитета и цифровых границ в глобальном информационном пространстве[5].

Аналитиками ЮНКТАД был предложен термин «цифровое общество» (наряду с термином «цифровая экономика»)[6], в рамках которого делается акцент на растущие объёмы данных и развитие технологий, основанных на данных, прежде всего, искусственного интеллекта, но также машинного обучения, технологий распределённых реестров, виртуальной и дополненной реальности, Интернета вещей и др. Данные технологии оказывают растущее влияние в условиях 4-й Промышленной революции и смещают внимание с вопросов управления Интернетом на вопросы регулирования технологий искусственного интеллекта, в том числе в области этики. При этом именно Интернет остаётся ядром и ключевой инфраструктурой и информационного, и цифрового общества.

Интернет – сложный феномен, не сводимый к одному определению, обладающий множеством граней, включающих в себя технические, социальные и политические аспекты. Д.Н. Песков определяет Интернет как «совокупность сетевых отношений, социальных институтов, технологий и технических средств, связанных внутри себя и друг с другом с помощью компьютерно-опосредованных линий, а также характеризуемых единым временем и пространством с особыми характеристиками»[7]. Таким образом, в своём расширенном понимании Интернет включает в себя социальную действительность, претендуя не только на виртуальность, но и на часть традиционно понимаемой реальности, в том числе совокупность сетей социальных, гуманитарных, технологических[8].

Исследователи, работающие в рамках «Проекта управления Интернетом» при Сиракузском университете (Internet governance project)[9], выделяют следующие особенности Интернета, которые следует принимать во внимание в ходе анализа управления:

1. Открытость стандартов – Интернет основывается на открытых технических стандартах, которые может бесплатно использовать каждый. В ряде случаев в стандартах интернет-протоколов используются запатентованные технологии, но они, как правило, доступны по разумной цене.

2. Рыночные механизмы – сети, составляющие Интернет, соединяемые протоколами, принадлежат различным организациям, в большинстве случаев – представителям частного бизнеса. Большая часть инвестиций исходит от частного сектора. Услуги и соединение координируются в основном на рыночной, контрактной основе.
3. Интеллектуальные средства и контрольные функции сосредоточены на периферии сети. Функция сети – передача информации, сами протоколы технологически нейтральны.
4. Трансграничный характер – Интернет не локализован ни в одном национальном государстве, соединение возможно и внутри, и поверх национальных границ[10].

1.1.2. Статистика использования и тенденции развития

Интернет является самой быстро развивающейся информационно-коммуникационной технологией (ИКТ) за всю историю человечества. Масштабы использования Интернета неуклонно возрастают – если в начале 2005 года насчитывалось порядка одного миллиарда пользователей Интернета, то к концу 2023 года число пользователей достигло 5,4 миллиарда[11]. Более 66% всех жителей нашей планеты пользуются Интернетом, и, по последним данным, общее число интернет-пользователей в мире составляет 5,5 миллиарда[12]. За 2023 год аудитория Интернета прибавила 1,8% (97 миллионов новых пользователей с начала 2023 года). Наибольшее число пользователей приходится на Китай (1,1 миллиарда), затем Индия (806 миллионов), США (322 миллиона), Индонезия (212 миллионов), Бразилия (183 миллиона), Россия (133 миллиона)[13]. Страны с самым высоким уровнем проникновения Интернета – Нидерланды, Норвегия, Саудовская Аравия, Швейцария, Объединенные Арабские Эмираты, Дания – в них 99% населения пользуются Интернетом. На сегодняшний день охват Интернета стал действительно глобальным, при этом наибольшее число пользователей проживает в Южной Азии (1,426 миллиарда), на втором месте Восточная Азия (1,3 миллиарда), затем Юго-Восточная Азия (565 миллионов) и Северная Америка (450 миллионов). Важной характеристикой является отношение числа активных пользователей к общему населению страны (проникновение Интернета); самый высокий уровень проникновения – в Северной Европе (97,6%), Северной Америке (97,1%) и Западной Европе (94,5%)[14].

Однако порядка 2,7 миллиарда людей в мире не пользуются Интернетом. Так, например, в Индии живут более 680 миллионов человек, «не подключённых» к сети[15], что составляет порядка 47% населения страны. Таким образом, цифровой разрыв – неравенство в доступе к цифровым технологиям как внутри отдельных стран, так и между странами и регионами мира – сохраняет своё значение и является важным фактором современных международных отношений.

Современный этап развития Интернета называют этапом социальных медиа или социальных сетей. На апрель 2024 года количество профилей пользователей соцсетей превысило отметку в пять миллиардов, что эквивалентно 62,3% населения мира (но профили пользователей соцсетей не обязательно являются уникальными пользователями). За год этот показатель увеличился на 266 миллионов, в результате чего рост за год составил 5,6%[16]. Средний пользователь социальных сетей теперь проводит в них 2 часа 23 минуты в день. Бахрейн, Кувейт, Катар и Саудовская Аравия также демонстрируют особенно высокий уровень проникновения социальных сетей. При этом среди лидеров в этом году появилась и Южная Корея. На другом конце спектра Северная Корея. Здесь по-прежнему самый низкий уровень распространения социальных сетей в мире[17]. Правительства Эритреи и Туркменистана также ввели жёсткие ограничения на использование соцсетей, что объясняет заметно низкий уровень распространения социальных сетей в этих странах[18].

Отдельно следует отметить характер используемых для подключения к Интернету устройств. Сегодня 96,5% подключений к Интернету осуществляется при помощи мобильных телефонов, что способствует изменениям в характере использования технологии, в том числе делает более доступными и повсеместными социальные сети. Более того, это позволяет производителям собирать более детальный «цифровой след» пользователей мобильного Интернета, формируя таким образом «большие данные».

Среднестатистический интернет-пользователь проводит онлайн 6 часов и 40 минут каждый день уже в течение нескольких последних лет (это относительное снижение, во время пандемии люди проводили онлайн порядка 8 часов в день). При этом данный показатель существенно разнится для стран и регионов мира. На первом месте по количеству времени, проводимому в сети, ЮАР – 9 часов 24 минуты в день, на втором Бразилия – 9 часов и 13 минут – и Филиппины – 8 часов и 52 минуты. Меньше всего времени онлайн проводят жители Японии – менее 4 часов в день, Дании – 5 часов 8 минут – и Южной Кореи – 5 часов 19 минут.

Россия – один из лидеров глобального цифрового пространства, наша страна демонстрирует высокие показатели по количеству пользователей Интернета и социальных сетей. По числу регистраций в национальном домене российский сегмент Интернета опережает многие европейские и азиатские страны. На апрель 2024 в России насчитывалось 130,4 миллиона пользователей Интернета, что составляет 90% населения страны. При этом 106 миллионов были активными пользователями социальных сетей, то есть 73,5% населения страны. В среднем россияне проводят онлайн 8 часов 1 минуту в день. В России широкий доступ к Интернету, высокий уровень цифровой грамотности, хорошо развитая цифровая инфраструктура.

Определение Интернета, как и любой другой технологии, будет неполным без характеристики последних тенденций в развитии сети. Очевидно, эти тенденции неизбежно будут иметь значение при формировании механизмов управления.

1. Основное количество вновь подключающихся пользователей проживает в странах Азии и Ближнего Востока, по экспертным оценкам эти регионы сохранят свой потенциал для интернет-технологий и в обозримом будущем. Как следствие, второй по распространённости язык в Интернете – китайский, и у него есть все шансы обойти английский, особенно после внедрения многоязычных доменных имён[19].
2. Идёт формирование т.н. повсеместной сети, или Web 3.0. Большая часть подключений осуществляется не с помощью стационарных компьютеров (как это было предусмотрено создателями сети), а с помощью мобильных телефонов и иных типов устройств, использующих, как правило, динамические IP-адреса[20]. Кроме того, в рамках Web 3.0 широкое распространение получают блоги, социальные и peer-to-peer сети, вследствие чего пользователи являются уже не пассивными получателями информации, а её активными создателями, зачастую создавая серьёзную конкуренцию ведущим медиакомпаниям.
3. Развитие прорывных цифровых технологий, в том числе искусственного интеллекта, Интернета вещей, технологий распределённых реестров, виртуальной и дополненной реальности, изменяют природу Интернета и создают новые проблемы международной повестки дня в области управления Интернетом на глобальном уровне. Так, например, с развитием технологий искусственного интеллекта на международной повестке дня появляется экологическое измерение. Центры обработки данных,

где размещены серверы ИИ, производят электронные отходы. Они являются крупными потребителями водных ресурсов, истощённых на многих территориях. Они работают на важнейших минералах и редких элементах, добыча которых часто нерациональна. Кроме того, они потребляют огромное количество электроэнергии, что приводит к выбросу парниковых газов, вызывающих потепление на планете[21]. Отчасти благодаря стремительному распространению искусственного интеллекта число центров обработки данных выросло с 500 тысяч в 2012 году до восьми миллионов, и эксперты ожидают, что спрос на эти технологии на планете будет увеличиваться[22].

4. В исследовательской литературе отмечается тенденция к «балканизации» Интернета, его локализации[23] вследствие выделения суверенных сегментов глобальной Сети государствами, как правило, по соображениям обеспечения информационной безопасности. Данная тенденция является следствием наметившегося в последние годы усиления влияния государств в информационной сфере и укрепления «цифрового суверенитета»[24]. Вместе с тем, тенденция к локализации является частью более широкой тенденции к регионализации глобального информационного пространства.

Можно сказать, что Интернет как ключевая технология современного цифрового общества тесно вписан в международно-политический контекст. В современной международной политике можно выделить несколько ключевых мегатрендов, в числе которых нарастающая значимость экологической, «зеленой» проблематики и формирование многополярного мироустройства, сопровождающееся нарастающей международной конфликтностью.

На уровне развития Интернета эти тенденции находят отражение в усиливающейся фрагментации и регионализации управления Интернетом, а также в росте значения «зелёных» цифровых технологий. При этом можно также говорить о возрастающей значимости новых технологий, прежде всего, искусственного интеллекта, на повестке дня международных организаций, занимающихся вопросами управления глобальным цифровым пространством.

1.1.3. Управление Интернетом: основное содержание и подходы к определению

Впервые управление Интернетом стало предметом наиболее жарких дипломатических дискуссий в ходе Всемирной встречи на высшем уровне по вопросам информационного общества в 2003 году. Изначально не было даже единого понимания того, что же представляет собой «управление» применительно к Интернету. В самом общем смысле концепция управления содержит идею о руководстве и направлении деятельности[25]. Рядом участников встречи «управление» рассматривалось как синоним «правительства». Однако в ходе дальнейшего обсуждения стороны пришли к согласию, что «управление Интернетом» не тождественно межгосударственному регулированию, а включает в себя множество различных участников и механизмов (подробно они рассмотрены во второй главе настоящего издания).

Таким образом, понятие «управление» в данном контексте близко к тому, что Дж. Розенау понимал под «глобальным управлением». В соответствии с определением, данным Дж. Розенау, «управление представляет собой процесс, посредством которого организация или общество руководит собственной деятельностью, а также включает в себя динамику коммуникаций и контроля, которые являются центральными для этого процесса»[26]. Можно также определить управление как «установление и функционирование набора правил поведения, которые определяют образцы поведения, приписывают роли и направляют взаимодействия, таким образом, чтобы разрешить общие проблемы»[27]. Управление в данном контексте осуществляют не только официальные институты и организации, которыми создаются и поддерживаются правила и нормы, управляющие мировым порядком: государственные институты, межправительственное сотрудничество, – но в том числе и все те организации и группы влияния – от многонациональных корпораций, транснациональных социальных движений до множества неправительственных организаций, – которые преследуют цели и задачи, достижение и решение которых зависит от транснациональных правящих и властных институтов [28]. Однако, ввиду значимости проблематики управления Интернетом и её тесной связи с вопросами обеспечения национальной и международной информационной безопасности, именно государства обладают исключительными полномочиями в области регулирования Интернета и на национальном, и на международном уровнях.

Дискуссии о регулировании всемирной Сети идут на фоне дискуссий о том, каким образом должно осуществляться управление в международной системе. Интернет, по мнению ряда исследователей, является той средой, где проявления взаимозависимости на международном уровне наиболее очевидны. В 2000-е годы высказывались предположения, что именно в ходе развития механизмов управления Интернетом будут выработаны новые формы международного сотрудничества, которые затем можно будет применить к другим областям международных отношений[29] [30]. Достоинством подобного подхода (в теоретической литературе получившего название многоуровневой дипломатии) является то, что по сравнению с более традиционными подходами, в рамках которых государства являлись ключевыми и зачастую единственными акторами, этот допускает участие более широкого спектра заинтересованных групп, обеспечивая таким образом большую эффективность, дополнительную гибкость и более высокий уровень демократической подотчётности (с последним аспектом, однако, соглашаются далеко не все исследователи). Применительно к Интернету подобное понимание делает возможным достаточную гибкость, необходимую для беспрепятственного развития этой относительно новой и многообещающей технологии.

Согласно трактовке российской дипломатии, многоуровневые форматы международного сотрудничества возможны лишь при ведущей и координирующей роли государств, в то время как негосударственные участники переговорного процесса наделены совещательными компетенциями. Такой формат многоуровневого взаимодействия реализован в рамках инициированной российской дипломатией РГОС ООН по международной информационной безопасности.

Предметом дискуссий стало также и то, насколько широкий спектр вопросов следует включать в понятие «управление Интернетом». Сторонниками так называемого «узкого» подхода управление Интернетом сводится к технической стандартизации и координации системы доменных имён и корневых серверов (эти функции на сегодняшний день выполняются ICANN и рядом некоммерческих организаций, большая часть из которых базируется в США). Действительно, Интернет, как и любая информационная система, функционирующая в глобальном масштабе, требует координации. Во-первых, необходима координация присвоения доменных имён или приписывания конкретного адреса каждому компьютеру или серверу. Это подразумевает управление базой данных с адресами и регистрацию новых доменных имён – без этого универсальный характер

передачи информации в Интернете просто невозможен. Во-вторых, должен существовать стандарт, при помощи которого передаётся информация. Этот стандарт обычно трактуется как интернет-протокол передачи данных TCP/IP. Кроме того, технические стандарты передачи информации включают в себя множество дополнительных параметров, например, таких как передача видеосигнала через Интернет. Соответственно, эти стандарты должны быть выработаны, приняты и внедрены, необходимо их координированное хранение и отслеживание соответствия используемых программ необходимым стандартам. И, наконец, в-третьих, необходимо поддержание деятельности так называемых корневых серверов, которые содержат базы данных с интернет-адресами. Существует всего 13 корневых серверов, жизненно необходимых для деятельности всей сети Интернет. Исторически сложилось так, что корневые серверы находятся в собственности правительственных и неправительственных организаций. С географической точки зрения на сегодняшний день наблюдается серьёзная диспропорция в их нахождении: десять корневых серверов располагаются в США, по одному — в Амстердаме, Стокгольме и Токио. Вышеперечисленные «точки координации» Интернета получили название критических ресурсов.

Вместе с тем, управление Интернетом не исчерпывается указанной выше технологической проблематикой, а подразумевает гораздо более широкий круг вопросов. В последние годы среди исследователей и политических деятелей возобладал «широкий» подход, согласно которому управление Интернетом включает в себя не только технические моменты, но и ряд политических, экономических и социальных аспектов, традиционно относимых к государственной политике и имеющих связанное с Интернетом измерение; это, например, проблема «цифрового разрыва», информационной безопасности и др.

«Широкое» понимание управления Интернетом отражено в рабочем определении, данном рабочей группой по управлению Интернетом, созданной по решению Генерального секретаря ООН по итогам женевского раунда ВВУИО, согласно которому:

«Управление Интернетом представляет собой разработку и применение … общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета»[31].

Таким образом, управление Интернетом включает в себя не только техническую стандартизацию, но и ряд других вопросов, в частности, экономическое регулирование, обеспечение «безопасности Интернета, аспекты развития и вопросы применения Интернета»[32].

Ключевой целью управления в данном контексте является обеспечение «стабильности, безопасности и непрерывности»[33], что особо оговаривается в «Тунисской программе для информационного общества».

Что касается представителей академического сообщества, занимающихся данной проблематикой, то в их среде также во всё большей степени наблюдается консенсус относительно того, что управление Интернетом – это нечто большее, чем техническая стандартизация и управление корневыми серверами и системой доменных имён. Практически всеми авторами признаётся, что процесс управления Интернетом – сложный, многоуровневый, с участием множества заинтересованных сторон, принимающих участие в регулировании: национальных государств, бизнес-структур, международных правительственных и неправительственных организаций, при решающей и координирующей роли государств[34].

Нельзя не обратить внимание на то, что определение управления Интернетом 2005 года разрабатывалось с опорой на классическое определение международного режима, предложенное Ст. Краснером в 1983 году. Ст. Краснер определяет международные режимы как набор принципов, норм, правил и процедур принятия решений, вокруг которых сходятся ожидания акторов в данной области международных отношений[35]. Действительно, теория международных режимов, наряду с теорией глобального управления, является наиболее широко распространённым инструментом анализа процессов в области управления Интернетом на международном уровне.

Теория режимов направлена на изучение международного сотрудничества и сохраняет своё влияние в академической среде уже в течение трех десятилетий. Представители теории режимов концентрируют внимание на изучении правил, которыми руководствуются государства и другие акторы международных отношений в своём поведении, а также представлений об этих правилах. Понятие международного режима позволяет интерпретировать особенности сложившихся на определённый момент времени связей между участниками международных взаимодействий и выявлять необходимые условия и причины для международного сотрудничества в той или иной области международных отношений.

Международные режимы – очень распространённое явление в современном международном сообществе. Они охватывают широкий спектр проблем: глобальные и региональные режимы безопасности (в частности, режим контроля над ядерными вооружениями), режимы в

области трансграничных благ совместного пользования (глобальные режимы международной транспортной системы, рыболовство в международных водах, распределение орбит искусственных спутников и т.д.). Режимы могут включать различные географические области и разное количество участников. В настоящее время значительное число исследователей полагает, что происходит формирование глобального режима управления Интернетом, во многом аналогичного режимам, существующим в других областях: экология, морское право и др., – но имеющего свои характерные особенности, обусловленные как спецификой объекта регулирования, так и историей участия различных акторов в создании, развитии и регулировании Интернета.

Международный режим управления Интернетом выступает как глобальное основание для «согласия между правительствами государств, представителями гражданского общества и международными организациями относительно того, каким образом должно осуществляться управление критически важными элементами Интернета, чтобы обеспечить его эффективное и стабильное функционирование»[36]. Формирование международного режима управления Интернетом ещё не завершено, данный режим не является чем-то однородным, но состоит из ряда относительно независимых, но взаимопересекающихся режимов, таких как режим управления доменными именами и адресным пространством сети (эти функции на сегодняшний день выполняет ICANN), режимы защиты интеллектуальной собственности в рамках Всемирной организации защиты интеллектуальной собственности (ВОИС) и Всемирной торговой организации (ВТО) и ряд других режимов как глобального, так и регионального масштаба[37]. Таким образом, можно говорить о режимном комплексе в данной области.

Создание международного режима предполагает достижение согласия относительно его базовых элементов – принципов и норм, а затем правил и процедур принятия решений. «Принципы отражают понимание причинности, фактов и обязательности (честности). Нормы являются стандартами поведения, выраженными в понятиях прав и обязанностей. Правила являются конкретными указаниями к действию. Процедуры принятия решений отражают преобладающую практику совершения и исполнения коллективного выбора»[38]. Причём, если принципы и нормы представляют собой собственно характеристики режима, то договоры и процедуры принятия решений относительно самостоятельны и могут меняться в рамках одного и того же режима.

Очень большое значение на первых двух стадиях имела работа ВВУИО (Всемирная встреча на высшем уровне по вопросам информационного общества – англ. WSIS, World Summit on the Information Society) и РГУИ (Рабочая группа по управлению интернетом – англ. WGIG, Working group on Internet governance), особенно определение, данное в итоговом отчёте данной группы. Именно это определение обозначило консенсус в отношении норм управления Интернетом, тем не менее, пути реализации достигнутых соглашений остаются неопределёнными, как и перспективы интернационализации управления Интернетом. Подобное развитие событий поддерживают представители РФ, Индии, Китая и большинства развивающихся стран, но их позиция наталкивается на активное и последовательное нежелание США уступать контроль в данной области в пользу международного сообщества.

1.1.4. Интернет – регионализация или фрагментация?

В 1990-х годах, на начальном этапе развития Интернета, в научной литературе преобладал подход, согласно которому Интернет считался так называемой ничьей землёй (лат. terra nullius – пространство, в котором социальные отношения и нормы не опираются на исторический опыт и должны быть выработаны заново). При таком подходе нормы международной политики не действовали в киберпространстве, в нём не было государственных границ и к нему не применялась категория государственного суверенитета. Информационное пространство рассматривалось как один из двигателей глобализации, в академической литературе того периода широко использовался также термин «информационная глобализация», призванный подчеркнуть растущий объём трансграничных потоков информации в Интернете.

В настоящее время подобный подход оспаривается представителями различных областей знания – политической науки, международных исследований и др. В научной литературе, российской и зарубежной, публикуется значительное число работ, посвящённых фрагментации Интернета и усиливающейся роли государств в информационной сфере (Drezner 2004; Кучерявый 2015), а также её нарастающей конфликтности (Diebert, Rohozinski 2010). При этом научных материалов, посвящённых глобализации Интернета, становится существенно меньше.

Фрагментация Интернета, пришедшая на смену информационной глобализации, становится новой реальностью. Протекционизм,

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

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

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

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

Однако, несмотря на набирающую силу фрагментацию Интернета, масштабы охвата цифровых технологий на сегодняшний день беспрецедентны. Наиболее популярными социальными сетями остаются компании, базирующиеся в США и КНР. Вообще же, согласно комплексным экспертным рейтингам, в число великих держав в глобальном цифровом пространстве входят Россия, Китай и США[39].

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

В настоящее время укрепляется роль регионального измерения использования информации в Интернете. Особую роль в регионализации информационного пространства играют сложившиеся устойчивые схемы взаимодействия пользователей в ходе поиска информации в сети (то есть работы с информационным содержимым Интернета – контентом). Речь идёт о паттернах использования веб-сайтов в качестве источников информации в разных странах (сегодня наиболее популярными сайтами среди пользователей Интернета являются поисковые системы, социальные сетевые и почтовые сервисы). Главным фактором, определяющим предпочтения пользователей Интернета в отношении контента, является культурная и языковая близость. На постсоветском пространстве активно используются такие сети, как «ВКонтакте» и «Одноклассники», а жители Китая в основном предпочитают национальную социальную сеть WeChat. Также можно выделить информационную подсистему внутри глобального Интернета, в которую входят пользователи из арабских стран, среди которых Саудовская Аравия, Египет, Алжир, Кувейт, Катар, Объединённые Арабские Эмираты[40].

Таким образом, информационные кластеры в Интернете в силу своей культурной и религиозной идентичности несколько обособлены от глобального информационного пространства. «Население стран в рамках одного кластера использует одни и те же сайты для получения информации, общения и пр., что отражается на мировоззрении и самоиден-

тификации населения данных стран. В определённой степени данная тенденция к регионализации обусловлена политическими причинами, а именно, стремлением обособиться от глобального информационного пространства, сохранив национальную и культурную идентичность.

Кроме того, определённое влияние оказывают языковые различия и ограничения на использование американских социальных медиа в отдельных государствах, которые рассматриваются как каналы распространения мягкой силы и влияния США[41]. После событий Арабской весны, которые экспертами рассматривались как сформированные под влиянием цифровой дипломатии США, существенно усилилась тенденция к суверенизации информационной сферы, которая получила своё окончательное оформление в 2020-е годы, с ростом санкционных ограничений и иных запретительных мер со стороны США. После начала Специальной военной операции России на Украине в 2022 году наметилась общемировая тенденция к укреплению цифровых границ. Прежде всего, необходимо отметить, что на территории России были признаны экстремистскими и запрещены социальные сети, принадлежащие компании Meta, а деятельность Twitter (ныне X) была ограничена. Впоследствии данная тенденция получила своё развитие в других государствах. Так, в 2024 году на территории США был принят законопроект о блокировке социальной сети TikTok, принадлежащей китайской компании ByteDance. Китай в свою очередь уже в течение длительного времени блокирует на своей территории доступ к западным социальным сетям и платформенным решениям.

Таким образом, тенденция к регионализации, характерная для современной международной политики и мировой экономики[42], значима для информационного пространства. Регионализация сопутствует и усиливает тенденцию к «балканизации» Интернета, вычленению обособленных национальных сегментов сети с целью защиты «информационного суверенитета», что обусловлено стремлением обеспечить информационную безопасность и извлечь коммерческую выгоду из развития интернет-технологий за счёт закрытия рынков, поддержки национальных компаний[43].

На начальных этапах развития Интернета многие исследователи отмечали, что присущие Интернету открытость и сетевая организация, по мнению ряда исследователей, способствуют глобализации, становлению глобального гражданского общества, а сам Интернет представляет собой глобальное общественное благо[44]. Т. Фридман в книге «Лексус и оливковое дерево», написанной в 1999 году, подчёркивал взаимосвязь между развитием Интернета и процессами гло-

бализации[45]. Позднее в 2005 году в книге «Плоский мир» он утверждал, что Интернет и другие ИКТ сделали нас «соседями» и убивают географию, расстояние и язык – таким образом, подчёркивается трансформирующий потенциал Интернета[46]. Тем не менее, всё, что сегодня понимают под глобализацией – свободный обмен товарами, капиталами, рабочей силой, невзирая на расстояния и государственные границы, – не было бы возможным без преимущественного обмена информацией, знаниями, идеями. В этом смысле природа глобализации лежит в сфере человеческого общения, социальной коммуникации.

Под глобальным информационным пространством в настоящей работе понимается «электронная среда, посредством которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается»[47], а также собственно информация и знания, которые обращаются в рамках этой среды. Таким образом, глобальное информационное пространство не исчерпывается сетью Интернет, в него входят как другие информационные сети, так и информация и знания, создаваемые, хранимые, обрабатываемые и передаваемые посредством этих сетей. Однако именно Интернет представляет собой основную инфраструктуру информационного общества и характеристики, присущие Интернету, оказывают влияние на природу глобального информационного пространства и обеспечение информационной безопасности.

И хотя с ростом коммерческой значимости сети политические и экономические интересы во всё большей степени определяют направления эволюции Интернета, базовые характеристики, изначально присущие технологии, а именно открытость, доступность информации, глобальность охвата, и на сегодняшний день являются определяющими в рамках информационного общества[48].

1.2. История управления Интернетом

1.2.1. Первый этап: технический режим

Можно выделить три стадии в ходе развития режима управления Интернетом, каждую из которых характеризует определённый набор участников управления, механизмы и инструменты регулирования, а также проблемные сферы, на которые собственно распространялось регулирование[49].

Первая стадия получила название «технический режим», поскольку управление Интернетом в этот период фактически означало выработку технических стандартов, она длилась до середины 1990-х гг. Изначально Интернет был создан в рамках одного из проектов Агентства перспективных разработок Министерства обороны США (ARPA), его предшественницей была сеть APRANet. Любопытно, что стартовой точкой для создания стал запуск первого искусственного спутника Земли Советским Союзом в 1957 году – в американской прессе и академической литературе это событие получило название «Спутниковый кризис» (Sputnik Shock), так как ознаменовало отставание США в высокотехнологической космической гонке. Для преодоления отставания в США были выделены дополнительные средства на развитие технических и инженерных наук, созданы новые институты, в их числе APRA, при Минобороны США.

Именно ARPA на первом этапе существования Интернета регулировала вопросы, связанные с его использованием. В то время степень этого контроля была не очень велика, разработчики и первые пользователи сетей обладали достаточно широкой свободой в определении направлений развития и использования Интернета.

Таким образом, влияние военных на параметры развития Интернета продлилось относительно недолго, вскоре значительное влияние перешло на уровень академического сообщества США, в среде которого преобладали анархистские взгляды, вызванные несогласием с внешней политикой США, в том числе ведением войны во Вьетнаме. Именно такие настроения академического сообщества США оказали влияние на архитектуру Интернета, в рамках которой не предусмотрен контроль над информацией, и её передача носит распределённый и децентрализованный характер.

Таким образом, режим управления Интернетом является режимом «смешанного происхождения», в создании и поддержании ко-

торого участвовали как представители сообщества инженеров и разработчиков Интернета (которые впоследствии сформировали специализированные неправительственные организации, «интернет-сообщества»), так и органы государственной власти, прежде всего, Министерство обороны США.

1.2.2. Второй этап: академический режим

Технический режим продлился относительно недолго. Возрастание количества пользователей Интернета и его коммерческой ценности поставило на повестку дня новые задачи и привело к появлению новых структур, участвующих в управлении Интернетом. Вторая фаза эволюции управления Интернетом характеризовалась попытками институционализировать механизмы самоуправления в этой сфере.

К этому периоду относится становление новой области регулирования, системы доменных имён, которая «практически полностью определяла институционализацию структур управления Интернетом»[50]. С момента изобретения и внедрения этой системы в середине 1980-х гг. управлением ею занимался сотрудник Стэнфордского исследовательского института Джон Постел.

По мере того, как количество пользователей Интернета и масштаб охвата технологии возрастали, правовой статус этой деятельности менялся – в 1991 году функции управления системой доменных имён, в первую очередь, технические аспекты, были переданы частной компании Network Solution Inc. (NSI), которая получила разрешение взимать плату за регистрацию доменных имён. Это вызвало широкое возмущение как со стороны интернет-сообщества, негативно относившегося к коммерциализации Интернета, так и представителей различных государств, которые начали понимать значимость контроля над национальной доменной зоной.

В результате в 1997 году правительство США вынужденно выдвинуло сначала план создания некоммерческой неправительственной организации для управления системой доменных имён и выполнения других ключевых для Интернета функций[51]. Предложения правительства США вызвали волну критики по всему миру и были восприняты как свидетельство попыток американского правительства закрепить за собой контроль над ключевыми ресурсами Интернета. Руководство Европейского союза, подчеркнув, что «предложение США может под лозунгом глобализации и приватизации Интерне-

та привести к закреплению постоянной юрисдикции США над всем Интернетом»[52], предложило создать для регулирования Интернета международную организацию, аналогичную МСЭ.

Несмотря на протесты, в ноябре 1998 года создание ICANN было закреплено меморандумом о взаимопонимании между ICANN и Министерством торговли США. Изначально ICANN была создана как неправительственная организация, зарегистрированная в США и подчиняющаяся американским законам. Соглашение между ICANN и Министерством торговли США продлевалось несколько раз, но в 2016 году оно продлено не было, и 1 октября 2016 года корпорация ICANN заявила, что Администрация адресного пространства интернета (IANA) будет под полным контролем международного сообщества, а Соединенные Штаты потеряют даже теоретическую способность контролировать Глобальную сеть. При этом ICANN зарегистрирована в Соединенных Штатах и регулируется законодательством штата Калифорния. В настоящий момент корпорация сделала немало шагов для того, чтобы сделать модель управления ICANN более прозрачной. Например, в Правительственный консультативный комитет (GAC) входят правительства 182 стран и 38 организаций-наблюдателей. Кроме того, ICANN открыла региональные офисы за пределами США, а именно – в Сингапуре, Стамбуле, Брюсселе и Монтевидео [53].

С момента своего создания ICANN подвергалась критике со стороны правительств и организаций гражданского общества, которые видели в ней инструмент закрепления монополии США в интернет-пространстве. По мере того, как экономическая и политическая значимость Интернета возрастала, государства начали искать другие пути участия в управлении Интернетом. Вопросы распределения доменных имён и регулирования Интернета не потеряли своей актуальности и до сих пор остаются в центре международных дискуссий по управлению Интернетом, однако ICANN не сумела стать тем форумом, где бы обсуждались эти вопросы. По словам высокопоставленного представителя МСЭ, у государств «есть свои механизмы и процессы для заключения взаимоприемлемых соглашений – это межгосударственный контекст, а не территория ICANN»[54].

1.2.3. Третий этап: смена форумов и развитие социальных сетей

Начало XXI века стало переходом к третьей фазе управления Интернетом, находящейся сейчас в стадии формирования. Она харак-

теризуется частой «сменой форумов», перестановками в коалициях акторов, попытками найти модель взаимодействия между разнообразными заинтересованными сторонами, в том числе государствами, претендующими на гораздо более активную роль в регулировании Интернета.

Ключевым событием, обозначившим начало третьего этапа, стал Всемирный саммит по вопросам информационного общества (ВВУИО), который прошёл в два этапа: в Женеве в 2003 и в Тунисе в 2005 годах. Инициатором проведения саммита выступил МСЭ, традиционно занимавшийся всем спектром вопросов, связанных с телекоммуникациями, в первую очередь, вопросами стандартизации и распределения ограниченных ресурсов (таких, как радиочастотный спектр).

Согласно официальному пресс-релизу МСЭ, целью первой фазы саммита было «развить и поддержать ясное объявление политической воли и принять конкретные шаги для создания основ информационного общества для всех, отражающего различные интересы»[55]. Однако центральной и наиболее спорной темой дискуссий в ходе саммита стало управление Интернетом. Вопрос о реформировании ICANN вызвал ожесточённые споры. Многие страны, в первую очередь развивающиеся, открыто заявили о том, что контроль США над Интернетом является нарушением их суверенитета. США и представители деловых кругов, в свою очередь, выступили резко против предложений по интернационализации управления Интернетом, мотивировав это недопустимым повышением уровня бюрократизации этой ключевой для Интернета функции.

В результате по этому пункту повестки дня в Женеве не было достигнуто единого понимания. Участники женевского этапа перенесли обсуждение двух оставшихся на повестке дня вопросов – создание «Фонда цифровой солидарности» и реорганизацию механизмов управления Интернетом – на второй этап саммита.

Среди положительных результатов женевского этапа ВВУИО, несомненно, нужно назвать решение создать при Генеральном секретаре ООН рабочую группу на основе участия различных заинтересованных сторон для обсуждения вопросов, связанных с управлением Интернетом. По итогам работы рабочей группы по управлению Интернетом (РГУИ) был подготовлен доклад, в котором, в частности, было сформулировано определение управления Интернетом, которое уже было приведено ранее.

В ходе подготовки второго этапа саммита вновь проявился кон-

фликт нескольких позиций по вопросу управления Интернетом. США, ЕС и ряд других стран настаивали, что регулирование Интернета должно сводиться к техническим вопросам и осуществляться в рамках существующих структур (в первую очередь, ICANN). С другой стороны, значительная группа стран под руководством Китая и членов так называемой Группы 20 (Бразилия, Южная Африка, Индия и другие) заняла существенно отличную позицию, заявив, что управление Интернетом должно включать гораздо более широкий круг вопросов, в том числе борьбу со спамом, незаконным контентом и т.д., а контрольные и управляющие функции должны быть переданы одной из межправительственных организаций в рамках ООН, возможно, МСЭ.

В результате этих разногласий уже накануне открытия саммита его участники (в том числе под давлением США) приняли решение вообще исключить из повестки дня конкретные вопросы, связанные с реформированием структуры управления Интернетом, и передать этот вопрос на рассмотрение специального Форума по управлению Интернетом (ФУИ) с привлечением представителей всех заинтересованных сторон.

По итогам тунисского этапа было достигнуто согласие по нескольким общим вопросам: так, в итоговых документах саммита указывалось, что все правительства будут играть равную роль и нести равную ответственность за управление Интернетом, что одна страна не должна участвовать в решениях, связанных со страновым доменом (ccTLD) другой страны, что необходимо расширять сотрудничество между различными заинтересованными сторонами по вопросам, связанным с доменами верхнего уровня (gTLD). Как и настаивала Россия, в итоговых документах была подчёркнута ведущая роль профильных организаций системы ООН, прежде всего МСЭ, ЮНЕСКО и ПРООН, в координации деятельности по осуществлению решений саммита, одобрено создание на принципах добровольного участия Фонда цифровой солидарности и определены пути совершенствования финансовых механизмов развития ИКТ. Была также подтверждена необходимость обеспечения международной информационной безопасности и предотвращения использования ИКТ в террористических и преступных целях[56].

Однако ключевым решением Тунисского саммита следует считать согласие продолжать обсуждение вопросов управления Интернетом в расширенном формате, включая представителей бизнеса и гражданского общества, и создание соответствующего института –

совещательного Форума по управлению Интернетом. Главными задачами форума являются «обсуждение вопросов государственной политики, касающихся ключевых элементов управления использованием Интернета, в целях содействия обеспечению жизнеспособности, эксплуатационной надёжности, безопасности, стабильности и развития Интернета и содействие диалогу между органами, занимающимися различными перекрёстными вопросами международной государственной политики в отношении Интернета».

Согласно Тунисской программе, ФУИ «опирается на существующие структуры управления использованием Интернета, уделяя при этом особое внимание взаимодополняемости между всеми заинтересованными сторонами, принимающими участие в этом процессе: правительствами, торгово-промышленными объединениями, гражданским обществом и межправительственными организациями»[57]. Основными темами для обсуждения в рамках обеих встреч были выбраны открытость, безопасность, культурное и языковое разнообразие, вопросы доступа к Интернету, а также управление критическими ресурсами Интернета (системой корневых серверов и доменных имён).

1.2.4. Четвертый этап: управление Интернетом в эпоху многополярности

В условиях, когда цифровое пространство милитаризируется и использование цифровых инструментов является неотъемлемой частью войн и конфликтов, для дипломатов и дипломатических ведомств становится важным не столько использовать социальные сети для донесения информации до широкой международной аудитории, сколько формировать правила, управляющие цифровым пространством как таковым. При этом важнейшей задачей выработки подобных правил является предотвращение эскалации межгосударственных противоречий в цифровом пространстве. Россия исходит из необходимости мирного развития глобальной ИКТ-среды, уважения государственного суверенитета, невмешательства во внутренние дела государств и предотвращения конфликтов в ИКТ-среде[58]. Россия выступает за передачу функций управления Интернетом на уровень международной организации, в рамках которой решения принимаются по принципу «одна страна – один голос».

При этом проблематика управления Интернетом тесно вписана в более широкие тенденции развития международной политики, среди которых ведущей является становление многополярной системы международных отношений.

В России концепция многополярности ассоциируется с фигурой Евгения Максимовича Примакова. Будучи министром иностранных дел, он ещё в 1996 году обозначил переход к многополярности как одну из тенденций международной жизни. При этом учёный и дипломат отмечал значимость развития партнёрских отношений в рамках многополярного мира[59].

Особенно изучение многополярности востребовано на современном этапе активной перестройки международной системы. Начало СВО в России ускорило формирование многополярной системы международных отношений. Согласно оценкам директора департамента внешнеполитического планирования МИД России Алексея Дробинина, формирование многополярного мироустройства носит судьбоносный характер и составляет существо современных изменений международной системы[60]. Движущими силами для формирования новой мировой системы, новыми центрами роста стали страны мирового большинства.

Как отмечает министр иностранных дел Российской Федерации С.В. Лавров, «мировому большинству очевидно, что конфронтация и гегемонизм не решат ни одной глобальной проблемы. Они лишь искусственно сдерживают объективный процесс формирования многополярного мироустройства, которое будет опираться на равенство прав больших и малых наций»[61]. По мере перестройки международной системы и формирования многополярности необходима перестройка и международного управления Интернетом, с тем чтобы оно в большей степени отражало сложившийся баланс сил на международной арене.

При этом со стороны США, которые выступают против многополярности, стремясь сохранить своё лидерство, актуализируется запрос на формирование закрытых форматов международного сотрудничества. В частности, в 2022 году США выступили с инициативой Декларации за будущее Интернета[62], к которой присоединились более 60 стран, прежде всего, союзников США. Показательно, что Россию и КНР не пригласили к участию в данной инициативе. Руководитель недавно созданного в рамках Государственного департамента США Бюро по цифровой политике и кибердипломатии заявил, что нормы более эффективны для сплочения союзников, чем для сдерживания противников. Показательно, что в Стратегии кибербезопасности США от 2023 года именно Россия и Китай названы в числе основных вызовов лидерству США в цифровом пространстве[63].

В этих условиях актуализируется вопрос выработки правил в области управления Интернетом на международном уровне. Россия давно

выступает в поддержку интернационализации международного управления Интернетом и передачи соответствующих функций на уровень международной организации. Важно отметить, что на современном этапе эти правила будут включать в себя не только вопросы международной информационной безопасности, но и регулирования новых перспективных технологий, в том числе больших данных, возможно, искусственного интеллекта, машинного обучения и ряда других.

На сегодняшний день возрастает число международных инициатив, направленных на регламентацию перспективных направлений технологического развития, в том числе регулирования потоков больших данных. Показательно, что и в этой области управления Интернетом мы наблюдаем скорее конкуренцию различных подходов. Так, в 2020 году МИД КНР выступил с глобальной инициативой в области безопасности данных, в которой отмечается важность защиты персональных данных, уважения государственного суверенитета в области данных, а также центральной роли ООН в международном сотрудничестве на данном направлении[64]. Россия поддержала видение КНР. Показательно, что в настоящее время страны Запада выступают с альтернативными инициативами, стремясь оспорить регуляторную инициативу Китая на данном направлении, в числе которых Рекомендации ОЭСР в области регулирования технологий искусственного интеллекта[65] и инициатива на уровне Группы семи в области регулирования трансграничных потоков данных[66]. Схожая конкуренция проектов в области управления передовыми технологиями наблюдается и в области технологий искусственного интеллекта, регулирования 5G-сетей связи нового поколения, а также регламентации технологий Интернета вещей и других.

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

Современный режим управления Интернетом не отражает изменяющийся международно-политический ландшафт глобального информационного пространства, что в свою очередь порождает

угрозы конфликтов и нестабильности. Когда политические решения классифицируются как техническое регулирование, становится возможным их принятие за закрытыми дверями, вне общественного контроля, как это показали разоблачения Э. Сноудена, в результате нарушаются не только демократические процедуры, но и разрушается атмосфера доверия, без которой невозможно сотрудничество. Представляется важным, чтобы политические, экономические и технические вопросы, имеющие отношение к управлению Интернетом, решались при участии всех заинтересованных сторон, так как обеспечить информационную безопасность и сохранить связность Интернета как глобальной системы без многостороннего сотрудничества ни одно государство не в состоянии.

Интернет и вопросы управления Интернетом играют ключевую роль с позиции международной информационной безопасности, так как глобальная сеть становится важным инструментом «проекции» власти государств на международной арене: мягкой силы при помощи культурного и лингвистического влияния, жёсткой силы посредством кибератак, кибершпионажа и сбора разведывательных данных, получения коммерческой выгоды благодаря созданию интернет-бизнеса, – а также создаёт возможности наиболее влиятельным акторам задавать «правила Сети»[67] и параметры, на основании которых использование и управление Интернетом будут осуществляться.

В научном и политическом дискурсе стран Запада мультистейкхолдеризм, структурно и институционально воплощённый в работе ICANN и PTI, поддерживается в качестве неотъемлемой нормы, ценностной основы управления Интернетом[68]. Вместе с тем, подобный дискурс может быть рассмотрен в качестве риторического инструмента, направленного на нейтрализацию критики в отношении сложившихся моделей управления Интернетом, а не как действительное подтверждение эффективности и инклюзивной природы подобных механизмов управления на глобальном уровне. Как показывает проведённый анализ, сложившийся режим управления Интернетом непропорционально усиливает политические позиции США в данной области и таким образом не является политически нейтральным. Мультистейкхолдеризм как модель управления Интернетом в большей степени служит задаче усиления сложившихся на сегодняшний день властных отношений в глобальном информационном пространстве, а не росту влияния негосударственных акторов мировой политики в сфере управления Интернетом. В этой связи предлагаемая Россией и её партнёрами модель интернацио-

нализации управления Интернетом, то есть передачи функций технической координации сети межправительственной организации, в большей степени будет способствовать демократизации международного управления Интернетом и ценностным принципам свободы и доступности информации, лежащим в основе инфраструктурного дизайна глобальной сети.

Проблема управления Интернетом в ходе переговорного процесса всё чаще увязывается с вопросами международной информационной безопасности. Формирование системы управления Интернетом, основанной на равной ответственности государств за обеспечение безопасности суверенных сегментов глобальной сети, позволит решить целый ряд проблем международной информационной безопасности, обозначенных во второй главе настоящего исследования. Подобная модель возможна только в рамках интернационализации международного управления Интернетом, то есть передачи функций управления Интернетом к межправительственной организации.

В сложившемся государственно-частном режиме управления Интернетом функции технической координации пространства имён и адресов Интернета возложены на некоммерческую организацию PTI, зарегистрированную в США и формально подчиняющуюся законам США, а также косвенно связанную контрактными отношениями с правительством этой страны. В настоящее время всё большее количество государств оспаривают роль ICANN и PTI в управлении Интернетом, видя в ней инструмент влияния США. Сложившаяся система фактически предполагает монополию одного субъекта в данной сфере, что порождает дополнительные угрозы информационной безопасности в силу нарушения баланса сил, что в свою очередь порождает дисбаланс в международной системе и повышает вероятность межгосударственных столкновений.

Согласно заявлениям руководства ICANN и PTI, PTI представляет собой независимую структуру, построенную по принципам многоуровневого формата управления (мультистейкхолдеризм), который является оптимальным для такой распределенной сети как Интернет. Однако PTI является дочерней структурой по отношению к ICANN и зарегистрирована в США, что позволяет сохранить ключевые технические структуры управления Интернетом под юрисдикцией США и избежать передачи этих функций межправительственной организации[69].

Создание PTI не смогло придать легитимности сложившейся системе управления Интернетом, в том числе, в глазах официальных лиц Российской Федерации, ответственных за стабильное и беспере-

бойное функционирование российского сегмента Интернета[70]. Предоставив ICANN формальную независимость, США, тем не менее, сохранили контроль над инфраструктурой Интернета благодаря рыночному влиянию (большая часть крупных компаний, работающих в интернет-пространстве, имеет американскую принадлежность), экономическому потенциалу (американские корпорации управляют доменными именами общего уровня, на которых зарегистрирована значительная часть доменов), а также управлению корневыми серверами, 10 из 13 из которых остаётся на территории США.

Дубайская конференция МСЭ 2012 года ознаменовала начало нового этапа в данном процессе, так как 89 государств проголосовали за новую редакцию регламента международной электросвязи, в поддержку трансформации режима управления Интернетом на основании уважения принципа государственного суверенитета в информационной сфере. Остановимся более подробно на прогнозах развития режима управления Интернетом, предлагаемых различными исследователями и аналитиками.

США не могут игнорировать обеспокоенность мирового сообщества в отношении их односторонней политики в сфере регулирования Интернета. Складываются благоприятные условия, чтобы передать контроль управления Интернетом МСЭ. Высока вероятность того, что в ходе саммита по вопросам развития информационного общества под эгидой ООН, запланированного на 2025 год, США уступят лидирующие позиции в сфере управления Интернетом. Этому способствует не только растущая уязвимость в сфере информационной безопасности, но и более широкий контекст сложившейся международной ситуации в данной области.

Проблематика управления Интернетом тесно связана с вопросами обеспечения международной информационной и кибербезопасности. От того, на каких принципах будет организован глобальный Интернет, будет зависеть облик глобального информационного пространства, в том числе, в контексте его безопасного функционирования[71]. Россия увязывает управление Интернетом с обеспечением международной информационной безопасности, так как, согласно официальной позиции, монопольное положение США создаёт дополнительные угрозы международной информационной безопасности; схожей позиции придерживается Китай. В июле 2017 года министром связи и массовых коммуникаций России в ходе третьей встречи министров БРИКС был представлен проект Конвенции ООН по безопасному функционированию и развитию сети Интернет. В

числе основных целей концепции конвенции обозначено установление режима равноправного международного сотрудничества в управлении сетью Интернет, при этом отмечено, что государства имеют равные права и обязанности в отношении вопросов государственной политики, связанных с управлением Интернетом на международном уровне[72]. Ключевой угрозой международной информационной безопасности, таким образом, является следующая: в силу того, что инфраструктура управления Интернетом является глобальной критической информационной инфраструктурой, обеспечение её стабильного функционирования необходимо осуществлять на глобальном уровне, в рамках международной организации.

США, будучи государством, финансировавшим работы по созданию Всемирной сети и внесшим наибольший вклад в её формирование и развитие, сформировали систему технической координации, отвечающую национальным интересам, а также выработали дискурс, обосновывающий на ценностном и нормативном уровнях приемлемость, эффективность и этичность сложившегося режима. В официальных заявлениях чиновников и документах США, а также в большинстве исследовательских трудов, написанных западными авторами, сложился дискурс, в соответствии с которым мультистейкхолдеризм в сфере управления Интернетом рассматривается как необходимое условие обеспечения «демократичности», «свободы», «равенства», «доступности» информации в Интернете[73]. Таким образом, критика мультистейкхолдеризма становится критикой подобных ценностей, и данный дискурс служит обоснованием для закрепления уже сложившихся властных отношений в рамках международного режима управления Интернетом. Как отмечается в последней редакции Стратегии национальной безопасности США, Интернет был изобретён в США и, следовательно, его инфраструктура должна отражать ценности США[74]. «Балканизация» Интернета является прямым следствием политика США и располагающихся в их юрисдикции ИТ-гигантов.

Управление Интернетом неизбежно становится предметом политических противоречий ввиду значимости данной технологии. В настоящее время конфигурация геополитических отношений в глобальном информационном пространстве претерпевает изменения, и соответствующие изменения становятся необходимым условием дальнейшего развития глобальной сети. Противоречия между расстановкой сил в информационной сфере и властными отношениями, институционально закреплёнными в организациях, осуществляю-

щих управление Интернетом на глобальном уровне, чреваты новыми угрозами информационной безопасности, в том числе, сегментацией глобального информационного пространства. В этой связи в той или иной форме интернационализация международного управления Интернетом видится неизбежной и соответствующей национальным интересам России.

Более того, поскольку субъектами информационной безопасности являются не только государства, но и негосударственные акторы, интернационализация управления Интернетом позволит разрешить целый ряд проблем информационной безопасности, связанных, в частности, с киберпреступностью и кибертерроризмом. Таким образом, подход России, согласно которому интернационализация управления Интернетом представляется необходимым условием обеспечения информационной безопасности на глобальном уровне, представляется более обоснованным. Возможным компромиссом видится институционализация многоуровневого формата управления Интернетом (при участии бизнеса, гражданского общества и эпистемического сообщества) на площадке ООН.

1.3. Управление Интернетом как международный режим

Регулирование Интернета может осуществляться на различных уровнях: от локального до глобального, в зависимости от особенностей того или иного аспекта регулирования. Но транснациональная природа сети обуславливает необходимость глобального регулирования. Международные меры необходимы в таких областях как защита авторских прав в сети, защита потребителей, спам и ряд других. В «Тунисской программе для информационного общества» было прописано «целевое» состояние режима управления Интернетом на глобальном уровне. Схематично оно может быть представлено в виде следующей таблицы:

Регулирование Интернета – понимание ВВУИО		
Институциональная основа регулирования	**Политическая основа регулирования**	**Сферы регулирования**
Международное управление Интернетом должно быть: • многосторонним; • прозрачным; • демократичным. С участием всех заинтересованных сторон: правител[75]ьств, частного сектора, институтов гражданского общества и международных организаций.	**Цели:** • справедливое распределение ресурсов; • обеспечение всеобщего доступа; • обеспечение стабильного и бесперебойного функционирования Интернета с учётом многоязычия. **Участники:** • государства: государственное регулирование; • частный сектор: техническое и экономическое развитие; • гражданское общество: общественное развитие; • межправительственные организации: координация регулирования; • МНПО: техническая стандартизация и связанное с ней регулирование.	Сферы: • сотрудничество между всеми заинтересованными сторонами; • всеобщий доступ к инфраструктуре и услугам Интернета; • доступ к информации и знаниям; • безопасное и стабильное функционирование сети; • социальные и экономические аспекты использования Интернета; • культурное и языковое разнообразие; • свобода СМИ; • этнический аспект; • международное и региональное сотрудничество.

1.3.1. Сферы управления

Развитие Интернета затрагивает все сферы жизни общества и государства, трансформируя их и при этом ставя новые препятствия с точки зрения юридического, политического и экономического регулирования. В ходе анализа современной ситуации «управления Интернетом», различные исследователи предлагают различные классификации существующих проблемных сфер. Подобные классификации не являются чисто теоретическим упражнением, так как различные группы проблем предполагают использование различных инструментов и механизмов управления, а также различную эффективность в результате участия тех или иных акторов. Таким образом, вновь появляющиеся проблемы, в зависимости от отнесения их к той или иной категории, могут разрешаться с использованием механизмов, уже доказавших свою эффективность по отношению ко всей категории.

А.Н. Михеев полагает, что можно выделять две условные группы проблем с точки зрения «новизны» или «самостоятельности». К первой относятся проблемы более общего плана, не специфические для области Интернета, но применительно к которым развитие Интернета является катализатором, придаёт новое, до того не существовавшее измерение, обостряет их и выводит на новый уровень либо, напротив, даёт новые способы решения. В каком-то смысле можно сказать, что это «старые проблемы в новой оболочке». Примерами могут быть международная безопасность и разоружение, защита свободы слова (и вопросы цензуры в Интернете), «цифровой разрыв» (который, по мнению большинства исследователей, самым тесным образом связан с более широкой проблематикой неравномерности развития на внутригосударственном и межгосударственном уровне) и вся проблематика «ИКТ для развития». Во вторую группу включаются проблемы, специфические для сферы ИКТ, не имеющие аналогов в «офлайновом» мире. Одним из примеров может служить проблема спама[76].

Интересную модель предлагают британские исследователи В. Даттон и М. Пелту, которые выделяют три измерения деятельности, имеющей отношение к управлению Интернетом: «интернет-центричное», включающее в себя проблемы, имеющие отношение непосредственно к функционированию Интернета; «пользователь-центричное», затрагивающее в основном интересы пользователей сети; и «не-интернет-центричное», в которое они включают проблемы, напрямую не связанные с Интернетом, но в отношении которых развитие Интернета и других новых ИКТ оказало трансформирующее

воздействие и придало им новые измерения[77]. Каждое из измерений характеризуется различными механизмами управления, используемыми инструментами, а также акторами и заинтересованными лицами, участвующими в процессе управления. Схематично модель, предложенная В. Даттоном и М. Пелту, представлена ниже:

Проблемы	Описание
Имеющие отношение непосредственно к Интернету (интернет-центричные)	Защита и развитие ключевой инфраструктуры Интернета. Своевременная адаптация к постоянно ускоряющимся технологическим и иным изменениям технологии. **Примеры:** управление системой доменных имён и IP-адресами, управление системой корневых серверов, технические стандарты и т.д.
Затрагивающие в основном интересы пользователей сети (пользователь-центричные)	Использование Интернета на национальном, локальном, региональном и международном уровнях и в рамках различных юрисдикций таким образом, чтобы защитить интересы пользователей, в то же время не препятствуя инновационному развитию сети. **Примеры:** спам, безопасность сетей, киберпреступность; преодоление «цифрового разрыва» в узком понимании – предоставление пользователям доступа к Интернету и др.
Имеющие отношение к Интернету, но влекущие за собой более широкие последствия (не-интернет-центричные).	Политические и иные проблемы, которые в первую очередь затрагивают более широкий политический контекст, чем просто управление Интернетом. Включают в себя широкий спектр экономических, политических, общественных вопросов. **Примеры:** преодоление причин «цифрового разрыва» – экономических, социальных (связанных с полом, возрастом) и др.; электронная коммерция; защита интеллектуальной собственности; свобода слова и самовыражения; поддержка культурного и языкового разнообразия.

Можно привести и другие классификации. А. Курбалийя полагает, что у вопросов, связанных с Интернетом, есть по меньшей мере пять измерений: инфраструктурное, правовое, экономическое, связанное с развитием и социокультурное. В каждом из этих измерений участвует множество лиц – как в частном, так и в государственном секторе. Большинство из них (операторы «корневых» серверов, интернет-провайдеры, специалисты по вопросам защиты торговых марок и проблемам развития, активисты гражданского общества и т.д.) принадлежат к очень специфическим и развитым профессиональным культурам. Различные сочетания вопросов и участников имеют свои цели, задачи, терминологию и сферы сотрудничества и влияния. Вместе с тем, исследователь отмечает, что в настоящий момент многие сферы регулирования существуют в относительной изоляции от остальных.

Подводя итог, следует отметить, что управление Интернетом включает в себя множество проблемных областей, многие из которых взаимосвязаны. Более того, по большей части проблемы междисциплинарны, могут быть отнесены к различным областям управления, а также трансграничны, вследствие чего не поддаются простой классификации и ими невозможно управлять, опираясь на уже существующие международные инструменты и механизмы, т.е. необходима их адаптация к потребностям интернет-пространства.

1.3.2. Субъекты

В уже упоминавшемся итоговом отчете РГУИ отмечается, что «управление использованием Интернета охватывает как технические вопросы, так и вопросы государственной политики, и в нём должны участвовать все заинтересованные стороны и соответствующие межправительственные и международные организации. В связи с этим признаётся, что:

a) политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств. Государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня;
b) частный сектор играет и должен продолжать играть важную роль в развитии Интернета как в технической, так и в экономической сфере;

c) гражданское общество также играет важную роль в обсуждении относящихся к Интернету вопросов, в особенности на уровне общин, и должно продолжать играть такую роль;
d) межправительственные организации играют роль, способствующую координации связанных с Интернетом вопросов государственной политики;
e) международные организации инженерного сообщества и организации стандартизации также играют и должны продолжать играть важную роль в разработке относящихся к Интернету технических стандартов и соответствующей политики»[78].

Комбинации акторов различаются в зависимости от рассматриваемой проблемы, причём зачастую интересы бывают диаметрально противоположными. По мнению М. Мюллера, большое количество заинтересованных сторон с несовпадающими интересами является одним из основных препятствий на пути к разрешению проблемы управления системой доменных имён[79]. В данном случае заинтересованные стороны включают в себя представителей технического интернет-сообщества, регистратур доменных имён, владельцев торговых марок и держателей прав интеллектуальной собственности, провайдеров интернет-услуг, организации гражданского общества (в том числе и международные), межправительственные организации и наиболее влиятельные правительства государств.

Следует отметить, что различные авторы дают зачастую диаметрально противоположные оценки роли и влиянию тех или иных акторов в процессах управления Интернетом. Так, Голдсмит и Ву, работающие в рамках неореалистской парадигмы, указывают, что государства в ходе управления Интернетом могут формировать собственное государственное пространство, создавая национальную информационную систему в соответствии с интересами правящего режима. Это подтверждается политикой цифрового суверенитета в целях создания более безопасного и контролируемого Интернета, осуществляемой такими государствами как Россия, Китай, Бразилия и др.

В России в ноябре 2019 года были принят закон о «суверенном Интернете» (неформальное название федерального закона от 01.05.2019 №90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»), который сформировал правовую базу для централизованного управления Интернетом в государственных границах. В 2021 году был принят «Закон о приземлении Интернет-ресурсов», который обязал владельцев иностранных IT-ресурсов с крупной российской аудиторией открывать официальные представительства в России.

Кроме того, начало Специальной военной операции России на Украине и обострение отношений со странами Запада актуализировали и форсировали политику России в области цифрового суверенитета. В 2022 году на территории России была запрещена деятельность ряда западных IT-платформ, что стало ещё одним шагом на пути к укреплению цифрового суверенитета. При этом, как отмечает А.Ю. Дробинин, обеспечение суверенитета возможно «при открытости к самому широкому взаимообогащающему равноправному международному сотрудничеству, может гарантировать устойчивое развитие России и достойное место нашей страны в многополярном миропорядке» (Дробинин 2022).

Схожих с Россией позиций придерживается КНР. В мае 2015 года Россия и Китай подписали двустороннее соглашение о сотрудничестве в области международной информационной безопасности. В июне 2016 года Владимир Путин и Си Цзиньпин подписали совместное заявление о сотрудничестве в области развития информационного пространства. Оба лидера подчёркивают, что они отстаивают принцип уважения национального суверенитета в информационном пространстве и изучают возможности выработки универсальных правил ответственного поведения в информационном пространстве в рамках ООН.

Китайская модель управления, предполагающая контролируемое информационное пространство, становится всё более распространённой по сравнению с моделью, принятой в США и подразумевающей максимальную открытость и доступность информации. Более того, модель управления Интернетом и в США, и в странах Западной Европы в последние годы во всё большей степени ориентирована на защиту цифрового суверенитета и укрепление цифровых границ.

Российский исследователь А.Н. Михеев отмечает роль таких негосударственных акторов как НКО, технические организации и бизнес-сообщества, так как Интернет был разработан и на протяжении значительной части своей истории использовался в первую очередь академическим и техническим сообществом, а большая часть интернет-инфраструктуры находилась в частной собственности. В то же время, А.Н. Михеев признаёт, что выстраивание эффективных механизмов управления Интернетом, решение возникающих проблем на глобальном уровне невозможно без активного вовлечение государств и межгосударственных органов.

Подводя итог, следует отметить, что состав участников управления Интернетом разнится от проблемы к проблеме, но неизменной остаётся необходимость согласования интересов различных заинтересованных сторон, каждая из которых характеризуется различными ожиданиями, ресурсами влияния, интересами и правилами поведения.

1.3.3. Инструменты

Проблематика управления Интернетом обсуждается уже давно, однако среди исследователей до сих пор нет консенсуса в отношении того, каким образом и с использованием каких инструментов и механизмов должно осуществляться регулирование. По мнению многих авторов, сама природа Интернета как распределённой глобальной сети делает невозможным управление им. Согласно данной точке зрения, трансграничная пространственная структура Интернета вступает в противоречие с границами, в рамках которых привыкли действовать национальные государства[80]. Нельзя не отметить также, что стремительный темп развития технологии практически исключает возможность формирования адекватного современному её состоянию правового инструментария как на национальном, так и, особенно, на международном уровне – можно сказать, что попытки управления с неизбежностью отстают от развития технологии[81].

Тем не менее, после окончания эпохи технооптимизма, преобладавшего на этапе «технического режима» управления Интернетом, больше ничто не предвещает того, что Интернету удастся избежать регулирования в той или иной форме.

Говоря о конкретных инструментах, которые могут быть использованы в ходе управления Интернетом, стоит обратить внимание на их отличие от средств регулирования других сфер деятельности. Еще в 1999 году авторитетный американский исследователь Л. Лессиг отметил тот факт, что политическое и техническое регулирование Интернета неотделимы друг от друга. «Киберпространство требует нового понимания того, каким образом осуществляется регулирование и что регулирует жизнь здесь. ... В реальном мире регулирование осуществляется при помощи законов, а в киберпространстве – при помощи программного кода. В киберпространстве программное обеспечение – это закон»[82]. Как указывает Л. Лессиг, существуют четыре способа управления «киберпространством»: законы, социальные нормы, рынки (механизмы цены и спроса) и архитектура (программный код)[83]. Таким образом, технологические решения также создают регулирующие нормы, которые не обязательно соответствуют законодательным нормам, а зачастую даже являются с ними несовместимыми. Ж. Рейденберг, автор статьи «Лекс информатика», в которой подробно описывается концепция так называемого киберправа, утверждает, что архитектура Интернета ограничивает действия пользователей сети, иллюстрируя это на примере регулирования проблемы авторских прав в киберпространстве[84].

Что касается управления Интернетом на международном уровне, то, по мнению Д. Маклина, оно осуществляется с помощью следующих инструментов: сотрудничество, согласование, стандартизация, юридические инструменты[85]. Нельзя не заметить, что они практически полностью соответствуют стадиям развития сотрудничества, описанным известным российским исследователем М.А. Хрусталёвым: консультативной, координационной, коалиционной и интеграционной[86].

В целях данного исследования инструменты управления можно укрупнить таким образом, чтобы стандартизация являлась частным случаем сотрудничества. Эти инструменты можно градуировать в соответствии со степенью их влияния на поведение государств и иных акторов – от самых «мягких», декларативных инструментов сотрудничества, подразумевающих лишь выработку общей позиции, до самых «жёстких», подразумевающих создание обязывающих норм международного права. При этом инструменты не являются заданными, а представляют собой так называемый континуум, варьируя по шкале от самых жёстких до самых мягких.

****

Трансграничная природа Интернета делает необходимым глобальное регулирование. И если на ранних этапах развития Интернета преобладали негосударственные формы управления, контролируемые доминирующим актором в мировой системе – США, то по мере возрастания значимости технологии государства начали принимать всё большее участие в данном процессе. Это обуславливает необходимость координации их политики с помощью традиционных механизмов – межгосударственных организаций. Однако и неправительственным акторам удалось сохранить своё влияние, вследствие чего потребовалось формирование новых моделей взаимодействия между межправительственными и неправительственными акторами. Это особенно ярко проявилось в ходе работы ВВУИО, РГУИ, а затем и ФУИ, наиболее значимых международных событий в исследуемой области.

Роли и участию международных организаций и институтов, как правительственных, так и неправительственных, в процессах управления Интернетом и будут посвящены следующие две главы.

ГЛАВА 2
ИНСТИТУТЫ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Система управления Интернетом на современном этапе опирается на обширную сеть взаимосвязанных специализированных институтов, курирующих различные аспекты управления всемирной сетью. В данном подразделе мы анализируем особенности выработки решений по вопросам управления Интернетом в рамках ключевых международных институтов и даём оценку их реальному влиянию на данные процессы.

В первую очередь влиянием на принятие решений в области управления Интернетом, значимых в глобальном масштабе, обладают такие институты как организации и специализированные форматы в составе системы ООН, специализированные негосударственные объединения и межправительственные организации.

2.1. Государства в системе управления Интернетом

2.1.1. Защита цифрового суверенитета и формирование цифровых границ государств

В последние годы заметно усилилось внимание учёных к фрагментации Интернета, появились специализированные термины «балканизация Интернета» и «разделённый Интернет», описывающие новое состояние информационного пространства. Как правило, этот процесс связывают с появлением цифровых границ в Интернете и усилением роли государств в управлении сетью. При этом, согласно статистике, объём данных, пересекающих границы государств, продолжает возрастать. Таким образом, информационная глобализация на уровне данных сосуществует с усилением цифровых границ и практикой укрепления цифрового суверенитета. Государства заинтересованы в выгодах, предоставляемых глобальным Интернетом. Его связность обеспечивает бизнес, который содействует глобализации рынка в целях увеличения прибыли.

И хотя проблематика фрагментации Интернета находит своё отражение не только в значительном количестве научных публикаций, но и в докладах международных организаций (например, в докладе ВЭФ «Фрагментация Интернета: обзор»[87]), она вступает в противоречие со статистическими данными, согласно которым на протяжении последних лет объём трансгранично передаваемых данных возрастает[88].

Цифровые границы, разделяющие глобальное информационное пространство, представляют собой социальные конструкты, в которых можно выделить дискурсивный (являющийся отражением властных отношений и дискурса на международной арене) и онтологический уровни (под онтологическим уровнем понимается инфраструктура, программное обеспечение и цифровой контент). На дискурсивном уровне субъектами формирования цифровых границ выступают государства, заинтересованные в укреплении своего суверенитета и защите от угроз информационной безопасности. В силу секьюритизации информационного пространства дискурс о цифровых границах прежде всего ориентирован на обеспечение безопасности, поэтому в нём доминируют государства.

На начальных этапах развития Интернета в 1990-х – начале 2000-х годов российские и зарубежные учёные публиковали работы, посвя-

щённые особенностям его влияния на мировую политику (Mueller 2010), причём Интернет рассматривался как основной двигатель глобализации (Nye, Keohane 2000), способствовал возрастающей роли неправительственных акторов, усилению взаимозависимости и размыванию государственного суверенитета (Михеев 2009). Большинство исследователей противопоставляли сетевую природу Интернета и территориальную природу политической географии (Mueller 2010).

Подобный подход получил название «цифровая исключительность» – пространство Интернета рассматривалось как самостоятельная область, на которую не распространяются законы реальной политики и географии, но которая оказывает существенное влияние на международную политику, усиливая глобализацию (Rosenau, Singh 2002).

Начиная с середины 2000-х годов акценты начали смещаться: подобная точка зрения рассматривается как утопичная трактовка не только самой природы Интернета, но и характера его взаимоотношений с мировой политикой (Herrera 2008). Исследователи полагают, что международная политика, в том числе «откат глобализации», сильно влияет на природу информационного пространства (Drezner 2004), его нарастающую конфликтность, укрепление государственных границ и цифрового суверенитета в условиях растущего количества цифровых угроз безопасности, набирающей силу тенденции фрагментации Интернета (Mueller 2020)[89].

Государства стремятся обозначить границы своей юрисдикции в информационном пространстве, что является двигателем информационной фрагментации мира. Подобная политика обусловлена секьюритизацией данной сферы, так как по мере увеличения количества цифровых угроз правительства рассматривают IT через призму безопасности.

Российский политолог М.М. Кучерявый пишет о необходимости укрепления государственного суверенитета в информационной сфере в условиях нарастающего количества угроз международной информационной безопасности (Кучерявый 2015). А.А. Стрельцов исследует проблематику определения суверенитета и юрисдикции государства в информационной сфере, отмечая, что по мере роста угроз информационной безопасности разрешение соответствующих правовых коллизий становится все более насущной задачей (Стрельцов 2017). О популярности подобной концептуализации в российской научной литературе говорит появление термина «информационная геополитика» (Быков 2008), который показывает растущее влияние государств в глобальном информационном пространстве (Buchanan 2020).

Смену исследовательской парадигмы подтверждает и растущее количество статей в публицистических изданиях. В 2016 году журнал The Economist предложил термин «балканизация Интернета», в 2019 году появился термин «сплинтернет», оба они отражают снижающуюся связность национальных сегментов Интернета. Специальный представитель президента РФ по вопросам цифрового и технологического развития Д.Н. Песков также отмечает тенденцию к «островизации» Интернета как следствие укрепления суверенитета государств и возведения границ в цифровом пространстве[90].

Оксфордский институт исследований Интернета составляет «карты Интернета», отражающие популярность социальных сетей в мире, маршруты трансгранично и трансконтинентально передаваемых данных, общее число доменов или количество пользователей по странам. Однако сама схема построения подобных «карт Интернета» была призвана подчеркнуть различия между физическим и киберпространством и неприменимость к нему простых географических аналогий.

Глобальное информационное пространство Интернета состоит из инфраструктуры, программного обеспечения и контента, информации и данных. Исходя из этого, контроль цифровых границ включает в себя:

- контроль доступа (контроль над инфраструктурой, посредством которой осуществляется доступ в Интернет);
- контроль функциональности (контроль над программным обеспечением, при помощи которого и реализуется основной функционал информационных ресурсов сети);
- контроль данных (также предполагает контроль поведения пользователей Интернета, создающих данные и информацию, в том числе в контексте информационной безопасности, предотвращение незаконной деятельности на уровне отдельного государства и международного сообщества).

Интернет тесно вписан в политику, в том числе международную, так как характеристики технологии являются предметом политических противоречий, а институты, управляющие использованием и развитием технологии, отражают баланс сил в обществе и международной политике. Чем более развита технология, тем большее влияние на неё оказывают международно-политические процессы, что мы и наблюдаем в отношении интернет-пространства.

В 1990-е годы, когда Интернет только набирал популярность в глобальном масштабе, политические деятели США, стран ЕС и представители международных организаций заявляли о нём как о пространстве вне суверенитета[91]. Кроме того, было популярно представление

об Интернете как о всеобщем благе (Introna, Nissenbaum 1999), к которому все люди имеют доступ вне зависимости от национальной или территориальной принадлежности.

С момента создания сети в силу исторических причин США обладали уникальными возможностями трансграничного контроля инфраструктуры и функциональных систем Интернета, которые обеспечивали его связность в глобальном масштабе – а именно пространства имён и адресов Интернета. В силу того, что распределением доменов и IP-адресов[92] в Интернете изначально занималась ICANN, действовавшая по контракту с правительством США (сейчас этим занимается её дочерняя структура – PTI), государства (за исключением США) не имели возможности осуществлять контроль в данной области в полной мере. Подобная ситуация в области международного управления техническими ресурсами Интернета сохраняется до сих пор.

Даже на ранних этапах развития сети контроль США над Интернетом всё же не был абсолютным. Аппаратное обеспечение и серверы, на которых хранится информация, линии передачи данных, посредством которых она передаётся, всегда находились в границах юрисдикции отдельных государств и имели географическую принадлежность, это было характерно для всех этапов его исторического развития. В рамках этой же логики программное обеспечение, установленное на этих устройствах, также подпадает под юрисдикцию той страны, на чьей территории они размещены. Таким образом, на ранних этапах развития Интернета государства имели возможность осуществлять ограниченный контроль на уровне инфраструктуры и программного обеспечения (однако не абсолютный в силу того, что США сохраняли контроль над пространством имён и адресов). Кроме того, на тот период программные средства не всегда позволяли определить территориальную принадлежность данных и пользователей и контролировать данные и информацию, пересекающие границы.

Иными словами, глобализация и дискурс о «конце географии» легитимировали стремление стран Запада и крупных компаний контролировать процессы, выходящие за пределы их юрисдикции. Схожие выводы настоящее направление позволяет сделать и относительно информационной глобализации.

В 2000 году в США почти половина граждан имела доступ к Интернету, но в Азии, Африке и Тихоокеанском регионе у более чем 90% населения доступа не было. Уже к 2005 году число пользователей Интернета в других частях света возросло, в основном за счет Азии и особенно Китая[93]. Рост числа пользователей, ставший следствием

информационной глобализации, оказался важным фактором, обусловившим растущий интерес к укреплению государственного влияния в информационном пространстве и формированию цифровых границ.

На этот период пришлись первые шаги в области формирования международно-политического дискурса о границах в Интернете. В 2003 и 2005 гг. по инициативе России в документы Всемирной встречи на высшем уровне по вопросам информационного общества, которая прошла под эгидой ООН, был внесён пункт о том, что на национальный сегмент Интернета распространяется суверенитет государств[94]. Позднее под влиянием протестов Арабской весны в 2011 году, в ходе которых информационные технологии сыграли роль катализаторов (Зиновьева 2013; Farrell 2012), вопрос о цифровом суверенитете стал активнее обсуждаться на международном уровне, в частности, в рамках ШОС и ОДКБ (Зиновьева 2013)[95]. В докладах Группы правительственных экспертов ООН от 2013 и 2015 гг. по международной информационной безопасности было зафиксировано признание суверенитета государств над национальным сегментом Интернета[96]. С позиций критической географии это можно рассматривать как дискурсивное закрепление границ государств в Интернете. Одновременно с этим принимались инициативы по контролю границ, которые не только имели политическое измерение, но и воплощались в технологические решения, влияющие на онтологию сети.

КНР первой предложила новую практику определения государственного суверенитета не только на уровне инфраструктуры и программного обеспечения, но и на уровне контента – информационного содержимого всемирной сети: «Великий китайский файрвол» был запущен в 2003 году при участии компании IBM (Бухарин 2016: 78). Подобная практика получила широкое распространение. Россия со второй половины 2010-х годов укрепляет собственный информационный суверенитет, причём наибольший прогресс достигнут в таких областях как российские поисковые системы, социальные сети, а также навигационная система (там же: 76). Как отмечают исследователи, в настоящее время во всех государствах мира принимаются инициативы, направленные на укрепление суверенитета и цифровых границ[97], хотя трактовки и используемая терминология и различаются, смысловое ядро дискурса сводится к обозначению легитимных властных притязаний государств на контроль цифровых границ.

Во второй половине 2010-х годов по мере развития технологий сложился целый ряд решений и политических практик, направлен-

ных на контроль цифровых границ (инфраструктуры, программного обеспечения и данных).

1. Отключение / ограничение доступа к Интернету внутри государственных границ. Хотя это, как правило, крайнее средство, оно весьма эффективно демонстрирует полноту власти государства, как показал опыт Египта в ходе Арабской весны в 2011[98] и Ирана в 2019 году, Казахстана в 2022[99].
2. Геолокационное программное обеспечение, которое устанавливает связи информационного пространства и реального мира, разделённого государственными границами, для пользователей и устройств, подключённых к Интернету.
3. Законодательно закреплённое регулирование трансграничной передачи данных за счёт программных средств (только в наименее развитых странах отсутствует регулирование данной области (Casalini, Gonzales 2019)).
4. Локализация персональных данных граждан (определённые виды данных граждан собираются, хранятся и обрабатываются только на территории страны, причём зачастую список компаний, управляющих данными, также формируется на основании того, подпадают ли они под юрисдикцию государства). Согласно данным ОЭСР за 2020 год, в 40% государствах-членах ОЭСР действует соответствующее регулирование[100].

Эти технологические решения дают возможность государствам контролировать цифровые границы даже в условиях сохранения монополии американской некоммерческой организации PTI на управление пространством имён и адресов в Интернете, существенно укрепляя цифровой суверенитет. При этом преследуется цель обеспечения безопасности и государственного суверенитета, поэтому, как правило, это не препятствует трансграничным потокам информации.

Таким образом, национальные сегменты информационного пространства аналогичны территориальным юрисдикциям в киберпространстве, которые удобны и понятны для лиц, принимающих решения в области государственной политики. Основной причиной возведения цифровых границ является секьюритизация информационного пространства, когда по мере роста угроз информационной безопасности актуализируются вопросы обеспечения безопасности, в принятии решений относительно которых государства играют главную роль. При этом государства заинтересованы в экономических выгодах, которые предоставляет глобальный связный Интернет[101].

Укрепление цифровых границ представляет собой перестройку пространственной организации информационной сферы на основании цифрового суверенитета в условиях изменившихся властных отношений – снижения влияния США в международной политике и информационной сфере, формирования многополярности, растущего количества угроз международной информационной безопасности.

2.1.2. США в системе управления Интернетом

США являются лидером в области цифровой экономики, обладают наиболее развитой ИКТ-инфраструктурой, как в экономическом, так и в военно-политическом измерениях. В США сосредоточены 50% центров обработки данных, 94% всего финансирования стартапов в области искусственного интеллекта[102].

США, финансируя работы по созданию Интернета, участвовали и в определении характеристик управляющих структур, что является причиной политических принципов современного режима управления всемирной сетью. Так, Интернет был создан в рамках работ Агентства перспективных разработок (Advanced Research Project Agency, ARPA) Министерства обороны США. Изначально управление техническими инфраструктурами, обеспечивающими связную работу Интернета, выполнялось отдельными учёными и исследовательскими структурами, работающими по контракту с Минобороны США.

Поскольку США и их союзники не были уверены в том, каким образом следует осуществлять управление Интернетом в тот период, когда он только приобретал популярность, они предоставили свободу действий экспертам (разработчикам и инженерам, сформировавшим устойчивое сообщество)[103]. При этом сообщества инженеров и разработчиков глобальной сети, несмотря на относительную свободу действий, никогда не обладали полной автономией, их ключевые решения направлялись правительством США, на гранты которого они осуществляли свою деятельность[104].

С конца 1980-х годов, по мере роста количества пользователей и коммерческого потенциала новой технологии, государства, как развитые, так и развивающиеся, стали стремиться усилить своё влияние в данной области, в том числе совершая внешнеполитические усилия, направленные на интернационализацию управления Интернетом – то есть передачу функций управления технической инфраструктурой международной правительственной организации,

в качестве наиболее вероятного преемника ICANN называли Международный союз электросвязи (МСЭ).

Ответной реакцией со стороны правительства США стала попытка передать управление технической инфраструктурой Интернета от исследовательского сообщества частному сектору. Эта инициатива спровоцировала протест со стороны широкой общественности (прежде всего, пользователей Интернета) и представителей государств, которые видели угрозу в коммерциализации Интернета. В целях сохранения контроля над ключевыми элементами инфраструктуры Интернета правительство США приняло решение передать функции управления системой доменных имён (Domain Name System, DNS – ключевая техническая система, обеспечивающая связную работу сети в глобальном масштабе)[105] некоммерческой организации. В ноябре 1998 года был подписан меморандум о взаимопонимании между ICANN и Министерством торговли США, который стал правовой основой существования ICANN. ICANN была зарегистрирована в США – и её работа регулируется соответствующими нормами законодательства США[106].

ICANN была создана для выполнения следующих функций (IANA-функций (Internet Assigned Numbers Authority)):

- координация работ по выработке технических параметров интернет-протоколов;
- административные функции по управлению базами данных корневого сервера системы доменных имён;
- распределение блоков IP-адресов.

В 2016 году под давлением международного сообщества была предпринята реформа ICANN. Функции управления адресным пространством сети были переданы дочерней организации ICANN – Public Technical Identifiers (PTI). Данная организация формально независима от Министерства торговли США (то есть для внесения изменений в базу данных корневой зоны и в целом для выполнения административных функций ей не требуется формального одобрения со стороны Министерства торговли США), но при этом зарегистрирована в США и не имеет права выводить критические инфраструктуры адресного пространства Интернета за пределы штата[107]. Большая часть Совета директоров организации была назначена представителями ICANN, все они – граждане развитых государств. Решения в рамках PTI принимаются на основании многоуровневой модели, в которой право голоса имеют государства, организации гражданского общества, бизнес, эксперты. PTI по отношению

к ICANN выполняет функции субподрядчика; работа PTI будет прекращена в том случае, если Министерство торговли США расторгнет контрактные отношения с ICANN[108]. Таким образом, вышеназванная реформа не решает проблем с легитимностью существующей модели управления Интернетом, оставляя правительству США весьма существенные рычаги влияния.

Более того, как отмечает И. Щёголев, помощник президента Российской Федерации, создание PTI потенциально порождает новые проблемы: в случае возникновения технических неполадок в работе Интернета в том или ином государстве необходимо взаимодействовать напрямую с данной НПО, которая не является субъектом международного права и подчиняется законам США[109]. Таким образом, Россия не признает эффективность и легитимность текущего институционального дизайна управления ключевыми техническими ресурсами Интернета и намерена в рамках международных переговоров добиваться интернационализации этих функций и передачи их Международному союзу электросвязи, где одна страна имеет один голос и решения принимаются на основании межправительственной модели.

Как показывает М. Карр, сотрудник департамента международной политики Университета в Аберсвитте, распространение многосторонних моделей управления Интернетом в основном служит задаче усиления существующих властных отношений на международной арене, а не их разрушению. Более того, многоуровневая модель управления Интернетом ставит в привилегированное положение тех акторов, которые стояли у истоков сети – а именно, США и те государства, чьи интересы находятся в одном ключе с внешнеполитической повесткой дня, продвигаемой Штатами[110].

Следует подчеркнуть политическое измерение IANA-функций. Техническая координация обеспечивает возможность принятия решений, традиционно относимых к сфере государственной политики, таких как управление интеллектуальной собственностью, рыночной структурой индустрии распределения доменных имён, защита прав отдельных пользователей сети, в частности, обеспечение неприкосновенности частной жизни.

Таким образом, ICANN контролировала и продолжает косвенно контролировать посредством отношений с PTI экономически и политически значимые технические ресурсы, что объясняет взаимосвязь выполняемых ею функций с целым набором очень важных задач из области внутренней и международной политики.

ICANN и PTI стремятся к деполитизации своей роли в управлении Интернетом и обеспечении информационной безопасности с тем, чтобы избежать обсуждения политических аспектов данной проблемы на международном уровне. Однако несмотря на все усилия США и вышеупомянутых организаций, избежать подобных обсуждений не удалось. Не раз высказывались опасения, что правительство США может использовать ICANN и PTI для реализации своих внешнеполитических целей. Функции IANA предполагают возможность удаления записи о доменах враждебных США государств из базы данных корневого сервера. Несмотря на то, что формально PTI независима от правительства США в процессе принятия решений, она является дочерней структурой ICANN, которую связывают с правительством США так называемые особые отношения, описанные выше.

Подводя итог, можно сказать, что при всей политической значимости принимаемых решений PTI, как ранее ICANN, не нашла поддержки у международного сообщества. Дебаты в отношении легитимности ICANN шли с момента её создания и продолжаются до сих пор, теперь уже в отношении PTI. Критика ведётся по следующим основным направлениям:

- критика односторонней политики США в отношении контроля над системой корневых серверов;
- недовольство институциональной структурой PTI, в рамках которой правительства обладают лишь консультативными полномочиями;
- общее восприятие PTI как организации, в недостаточной степени учитывающей интересы незападных стран[111].

Управление Интернетом – это политическая проблема, причём её значимость возрастает по мере увеличения количества и потенциальной опасности угроз информационной безопасности. Учащающиеся кибератаки, в частности, атаки вируса Wannacry в 2017 году, наглядно демонстрируют, что информационные войны и информационное оружие — это реальная международная практика, в этом контексте передача управления Интернетом на межгосударственный уровень видится как важное условие более безопасного и стабильного Интернета.

США заинтересованы в укреплении своего лидерства и однополярном информационном порядке, однако сталкиваются с растущей конкуренцией со стороны КНР. Эксперты говорят о новом технологическом противостоянии, которое наиболее ярко проявляется в глобальном информационном пространстве. В этой ситуации США прини-

мают официальные документы, которые характеризуют агрессивные устремления США, – меры для укрепления и защиты своего лидерства и обеспечения цифрового и технологического суверенитета.

В сентябре 2018 года Д. Трамп подписал Национальную киберстратегию США[112]. Структурно она подразделяется на четыре направления: защита американского народа, Соединенных Штатов и американского образа жизни; положение о сохранении мира посредством силы в качестве главной цели США: «выявление, противодействие, пресечение, ослабление интенсивности, а также сдерживание действий в киберпространстве, которые противоречат национальным интересам США, с сохранением превосходства США в киберпространстве и посредством киберпространства», обеспечение процветания США; сохранение мира методом принуждения; продвижение американского влияния.

Важнейшей задачей киберстратегии провозглашается защита национальной инфраструктуры Интернета на федеральном уровне. По мере роста значимости технологий искусственного интеллекта возрастает внимание США к данной области.

При этом обеспечение информационной безопасности на международном уровне напрямую связано с форматом управления глобальной сетью Интернет. Однако США стремятся сохранить свой особый статус и с этой целью выступают с внешнеполитическими инициативами, ориентированными на формирование международного порядка, основанного на правилах, но в цифровом пространстве. Одной из таких инициатив стал Альянс за будущее Интернета, который США планировали представить в ходе Саммита демократий в декабре 2021 года. Сам документ был опубликован журналом Politico (non-paper), и в нем в качестве ключевой задачи было обозначено формирование позитивной повестки дня в области развития Интернета – который был бы «открытым, устойчивым и безопасным и способствовал продвижению основных демократических ценностей и защиты прав человека». В качестве угроз данному видению развития Интернета были обозначены действия КНР и России, продвигающих альтернативную точку зрения, основанную на государственном контроле и «эпидемии дезинформации», концентрации власти в руках ограниченного числа высокотехнологичных компаний, а также растущем количестве кибератак и иных угроз кибербезопасности. Даная инициатива столкнулась с масштабной критикой и в итоге так и не была реализована. Однако её основные тезисы нашли продолжение в представленном Вашингтоном в апреле 2022 года документе «Декларация о будущем

Интернета»[113], к которому на сегодняшний день присоединились порядка 60 государств, включая страны ЕС, а также Австралию, Японию, Южную Корею и Украину. Его цель – поддержание Интернета открытым, свободным, взаимозависимым, безопасным и надёжным. При этом в числе угроз безопасности Интернета обозначена информационная политика так называемых авторитарных государств, которые запрещают доступ к глобальным онлайн-платформам и цифровым инструментам. Очевидно, что речь вновь идёт о России и Китае, уже обозначенных в предыдущей редакции. При этом политика крупных цифровых платформ, ограничивающих доступ к российским СМИ, в данном документе и в позиции США не принимается во внимание несмотря на то, что важный акцент сделан на защите прав человека в цифровой среде и свободе доступа к информации. Ещё одной особенностью подхода является его экстратерриториальный характер – то есть ориентация на распространение принципов и ценностных ориентиров законодательства США на международный уровень, что ограничивает цифровой суверенитет государств, присоединившихся к данному документу. Нельзя не принять во внимание и незначительное число сторонников данного документа вне влияния США, их менее трети всех государств-членов ООН. Следует отметить, что это лишь одна из последних, но не единственная инициатива, ориентированная на распространение западных ценностей на глобальное цифровое пространство: в числе подобных – Парижский призыв к доверию и безопасности в киберпространстве от 2018 года, Программа действий по продвижению ответственного поведения государств в киберпространстве ЕС от 2020 года, Инициатива по борьбе с вымогателями США от 2021 года. Все вышеперечисленные инициативы так или иначе затрагивают проблематику управления Интернетом, но при этом характеризуются ограниченным членством.

2.1.3. Растущая роль КНР

Китайская Народная Республика является технологическим и цифровым лидером и основным соперником США в сфере цифровой экономики. Масштабы цифровой экономики КНР в 2020 году достигли 5,4 триллиона долларов. Экономическая и военная мощь КНР в киберпространстве подкрепляется политическими и дипломатическими инициативами в области регулирования глобального киберпространства, а также развитой нормативно-правовой базой.

Седьмого ноября 2016 года был принят закон о кибербезопасности КНР. В документе закреплена обязанность государства обеспечивать «суверенность, безопасность и удовлетворение национальных интересов в киберпространстве». Закон о кибербезопасности стал логичным продолжением проведения политики обеспечения контроля национального информационного пространства «Золотой щит», благодаря которой вероятность иностранного влияния на информационное поле внутри государства невысока.

Закон о кибербезопасности определил ключевые направления деятельности КНР в области обеспечения безопасности в сфере использования ИКТ: противодействие угрозам и рискам в информационном пространстве, в том числе борьба с незаконным вторжением в национальный сегмент сети Интернет, атаками на критическую инфраструктуру; важность противодействия террористической и экстремистской деятельности с использованием ИКТ на территории Китая; важность реализации превентивных и защитных мер в области неправомерного использования интеллектуальной собственности и противоправного использования персональных данных.

В 2017 году китайским правительством была утверждена Стратегия международного сотрудничества в киберпространстве. В документе закреплены следующие цели КНР:

- защита интернет-суверенитета и невмешательство во внутренние дела суверенных государств;
- формирование системы международных правил в глобальном информационном пространстве;
- содействие установлению равноправного и справедливого участия государств в управлении Интернетом;
- защита законных прав и интересов граждан в киберпространстве;
- содействие международному сотрудничеству в цифровой экономике;
- создание платформ для обмена киберкультурой.

В стратегии определен план реализации политики КНР на международной арене по достижению стратегической стабильности, установлению мира, выработке международных правил ответственного поведения государств в глобальном информационном пространстве, а также закреплены направления деятельности в области противодействия кибертерроризму и киберпреступности путём обмена опытом и технологиями с другими государствами.

Одним из ключевых приоритетов внешней политики КНР в области цифровых технологий в настоящее время является регулирование технологий искусственного интеллекта. 1 июля 2024 года на 78-й сессии Генеральной Ассамблеи ООН консенсусом была принята резолюция «Укрепление международного сотрудничества в области создания потенциала искусственного интеллекта», автором которой выступил Китай, а соавторами — более 140 стран. Принятие резолюции и широкий круг соавторов отражает консенсус между всеми странами по вопросу укрепления потенциала в области ИИ и демонстрирует политическую волю международного сообщества к укреплению потенциала и преодолению разрыва в области ИИ на основе солидарности и сотрудничества[114].

В документе зафиксированы принципы человекоцентричного ИИ, использования ИИ во благо и на благо человечества, резолюция посвящена теме наращивания потенциала, подчёркивает необходимость повышения роли развивающихся стран в глобальном управлении ИИ, выступает за создание справедливой и недискриминационной деловой среды, поддерживает центральную роль ООН и призывает оказывать эффективную помощь развивающимся странам в наращивании потенциала посредством международного сотрудничества и практических действий с тем, чтобы обеспечить устойчивое развитие ИИ[115].

Важнейшим приоритетом в области цифрового развития КНР является политика в области больших данных. Именно в Китае появилось первое в мире правительственное ведомство, которое будет определять национальную политику в области данных. В 2022 году объём производства данных в Китае достиг 8,1 зеттабайт, увеличившись по сравнению с предыдущим годом на 22,7%. Доля Китая в мировом производстве данных составила 10,5% (второе место в мире после США). По состоянию на конец 2022 года суммарная вычислительная мощность в центрах обработки данных превысила 180 экзафлопс (второе место в мире)[116].

Двадцатого июля 2017 года Государственный совет Китая опубликовал «Программу развития искусственного интеллекта нового поколения», которая, хотя и базируется на накопленной к этому моменту нормативной базе, помещает вопрос о технологиях ИИ в иной контекст: в центре находятся не просто сюжеты экономической конкуренции или ускоренного развития инноваций, но в первую очередь вопросы геополитической конкуренции и обеспечения национальной безопасности. ИИ становится стратегической возможностью,

которую нельзя упустить, чтобы обеспечить прочные позиции страны на мировой арене[117].

Как отмечает И.Е. Денисов, «для Китая ситуация в области национальной безопасности и международной конкуренции становится более сложной, и это является ключевым стимулом для того, чтобы придать развитию Big Data и ИИ общегосударственный, системный и стратегический характер. Вопросы развития новых технологий неизменно находились в центре внимания Си Цзиньпина, который, еще работая в начале 2000-х гг. губернатором провинции Фуцзянь, запустил программу «Цифровая Фуцзянь». Фактически этот опыт, уже на более высоком уровне технологического развития и на новом витке глобальной конкуренции, был масштабирован на весь Китай»[118].

Глобальная инициатива в области безопасности данных была выдвинута МИД КНР 8 сентября 2020 года и представляет собой взгляд на управление данными, ориентированный на уважение государственного суверенитета, внимание к угрозам международной информационной безопасности и признание ведущей и координирующей роли ООН в управлении современными цифровыми технологиями.

Таким образом, в настоящее время политические подходы России и КНР к управлению Интернетом, а также к обеспечению международной информационной безопасности и защите цифрового суверенитета во многом совпадают, что обусловливает тесное взаимодействие государств по всем направлениям российских внешнеполитических инициатив в цифровой сфере, рассмотренным ниже.

2.1.4. Позиция и интересы России в области управления Интернетом

В соответствии со спецификой объекта регулирования можно выделить следующие составляющие национальных интересов РФ в интернет-пространстве: национальная безопасность, экономические и социально-политические интересы, защита прав человека. Как правило, национальные интересы в вышеперечисленных сферах по-новому преломляются в «киберпространстве». Следует также отметить, что вследствие трансграничной природы исследуемой технологии интересы РФ в данной области имеют не только национальную, но и международную составляющую.

Значимость российских национальных интересов в данной области объясняется продолжающимся ростом масштабов использования Интернета, его экономической значимости, а также его ис-

пользования органами государственной власти. История развития Интернета в России насчитывает более 30 лет. 7 апреля 1994 года международный сетевой информационный центр InterNIC делегировал для Российской Федерации национальный домен верхнего уровня .RU. Этот день принято считать отправной точкой развития российского Интернета.

Однако свои первые шаги российский Интернет сделал значительно раньше – ещё во времена СССР. В Советском Союзе идею связать ЭВМ единой сетью – аналогом Интернета – впервые озвучил Анатолий Китов в 1959 году, предложив создать единую автоматизированную систему управления для Вооруженных сил. Первые наработки в этой области появились в 1962 году, когда Виктор Глушков представил проект Общегосударственной автоматизированной системы учета и обработки информации, которая предназначалась для автоматизированного управления всей экономикой СССР. Эта система была нацелена на то, чтобы стать общенациональной компьютерной сетью удалённого доступа в реальном времени, призванной вести постоянный учёт и контроль за любой точкой в гигантской экономике страны. Однако проект Глушкова не встретил понимания у советского руководства и был закрыт, но его идеи всё же были частично реализованы. Так, на ряде крупных промышленных предприятий и в оборонно-промышленном комплексе стали внедряться автоматизированные системы управления и автоматизированные системы управления технологическим процессом[119].

1 августа 1990 года была запущена советская сеть, которая функционировала на программном обеспечении, разработанном группой ученых из Института атомной энергии имени И.В. Курчатова (сейчас Национальный исследовательский центр «Курчатовский институт»). К ней подключили в основном компьютеры в научных институтах Москвы, Ленинграда (сейчас Санкт-Петербург), Новосибирска и Киева. 28 августа 1990 года прошёл первый сеанс модемной связи советского компьютера, находившегося в ИАЭ имени И.В. Курчатова, с зарубежным терминалом Хельсинкского университета, который положил начало регулярному каналу передачи почты по международному Интернету[120].

В сентябре 1990 года был официально зарегистрирован домен .SU (от Soviet Union – Советский Союз), администрированием которого занималась некоммерческая организация «Российский научно-исследовательский институт развития общественных сетей» (РосНИИРОС). С распадом СССР право представлять Россию в Интернете получила доменная зона .RU[121].

Доменная зона .РФ запустилась в 2010 году в качестве первой в мире кириллической зоны. А зона .SU использовалась с 1990 года как национальная доменная зона для Советского Союза и постсоветского пространства и до сих пор продолжает функционировать[122].

На 2024 год в доменной зоне .RU было зарегистрировано более 5,5 миллиона активных доменов. В национальной доменной зоне .РФ зарегистрировано 778 тысяч адресов. В старейшей доменной зоне .SU – 109 тысяч зарегистрированных адресов. Всего же, если сложить данные по всем трём доменным зонам, в российском сегменте Интернета зарегистрировано 6,4 миллиона доменов[123]. Число пользователей Интернета в России достигает 130 миллионов человек, что превышает 90% населения[124]. При этом число пользователей за последние 20 лет увеличилось более чем в 100 раз. Высок и уровень использования социальных сетей – среди взрослых пользователей интернета 74,5% общаются в социальных сетях[125].

Россия занимает четвёртое место в мировом рейтинге по количеству совершаемых звонков или видеоразговоров онлайн (88%). При этом Интернет играет важнейшую роль в экономике, социокультурной сфере и национальной безопасности страны.

Высок уровень цифровизации государственного управления, значительная доля государственных услуг также оказывается в цифровом формате: 86,6% населения, обращавшегося за государственными и муниципальными услугами в 2022 году, получили их в электронной форме, и подавляющее большинство оценили их качество положительно[126]. В 2018 году Москва заняла первое место в рейтинге умных городов ООН[127].

Цифровые технологии играют важную роль в экономическом развитии страны. В 2023 году была начата работа над национальным проектом «Экономика данных»[128]. Нацпроект направлен на цифровизацию отраслей экономики и социальной сферы и достижение технологического суверенитета и лидерства[129].

Инициативы в рамках проекта включают в себя:

- разработку и внедрение решений на базе искусственного интеллекта;
- развитие инфраструктуры доступа в Интернет;
- цифровые платформы в областях социальной сферы, в том числе в целях упрощения взаимодействия государства с гражданами;
- цифровизацию государственного управления;
- поддержку отечественных IT-решений;

- развитие квантовых технологий и технологий 5G и 6G;
- инфраструктуру кибербезопасности;
- развитие экосистемы подготовки IT-кадров.

Россия также обладает развитой цифровой экономикой. Капитализация 30 крупнейших интернет-компаний выросла за год с 55 миллиардов долларов до 59 миллиардов, то есть на 7% в долларовом выражении. Для сравнения, капитализация технологических компаний мира составляет 34 триллиона долларов, а 30 крупнейших из них стоят 25 триллионов долларов. Если 2023 был для интернет-бизнеса годом разделения «Яндекса» и переездов IT-компаний из-за рубежа в Россию, то 2024 стал годом импортозамещения. Российские интернет-компании, в частности, разработчики ПО активно осваивали опустевшие ниши после ухода иностранных компаний[130].

В конце декабря 2024 года MTS Web Services в своем исследовании прогнозировала, что по итогам года объём выручки IT-рынка вырастет на 22% и достигнет 3,3 триллиона рублей, или около 33 миллиардов долларов, а его доля в ВВП России составит 1,8%. В числе лидеров цифровой экономики России в 2025 году можно назвать «Яндекс» (IT-холдинг), Ozon (маркетплейс), РВБ (Wildberries; маркетплейс), Avito (интернет-сервис), Cloud.ru (разработчик ПО), «Лабораторию Касперского» (кибербезопасность), HeadHunter (интернет-сервис), «СКБ Контур» (разработчик ПО), «1С» (разработчик ПО), «Леста Игры» (разработчик ПО)[131].

Всё это свидетельствует о значимости интернет-технологий для всех отраслей экономики и всех сфер жизни Российской Федерации. Официальные представители государства неоднократно заявляли, что полностью поддерживают принцип, в соответствии с которым «ни одно правительство не должно обладать преимущественными полномочиями в вопросах международного управления Интернетом»[132]. РФ активно отстаивала свою позицию в ходе ВВУИО, выступая за передачу функций ICANN под международный контроль.

Российские участники ФУИ с 2006 года активно заявляют о позиции российского государства. Традиционно в ходе ФУИ РФ выносит на обсуждение следующие вопросы: обеспечение информационной безопасности, сокращение «цифрового разрыва», многоязычие, обеспечение стабильности, безопасности и непрерывности Интернета, доступности, надёжности и качества сервиса, которые являются отражением национальных интересов РФ в данной сфере. Россия выступает «за переход к международному управлению Интернетом», что подразумевает обсуждение практических шагов по посте-

пенному переходу системы управления использованием Интернета под контроль международного сообщества и вовлечение заинтересованных сторон, особенно из развивающихся стран, для участия в принятии решений по вопросам политики, связанным с управлением использованием Интернета.

При этом интернационализация управления Интернетом в рамках внешней политики России рассматривается как составляющая более широкой проблемы обеспечения международной информационной безопасности. Позицию Российской Федерации по проблематике международной информационной безопасности можно обобщить следующим образом: необходимость строгого соблюдения принципов неприменения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека и недопущения использования информации и телекоммуникаций в противоречащих Уставу ООН целях. Современный режим управления Интернетом не предусматривает обеспечения безопасности интернет-пространства. Одностороннее влияние США на процессы управления Интернетом лишь усугубляет опасения РФ.

Помимо участия в ФУИ, российская дипломатия активно использует возможности межправительственных организаций. Обсуждение проблематики управления Интернетом с участием РФ проходит в рамках таких форумов как ООН, МСЭ, БРИКС, ШОС, СНГ. РФ часто является инициатором внесения в повестку дня этих форумов вопросов по инфо- и кибербезопасности, правового регулирования информационных технологий, управления Интернетом.

В рамках СНГ было заключено Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации, проведён Международный семинар «Управление использованием Интернета»[133]. В итоговом документе страны-участники заявили, что необходимо «повышение роли межправительственных организаций (в том числе Международного союза электросвязи) в координации связанных с Интернетом вопросов государственной политики. Также идёт работа по гармонизации правового пространства СНГ и разрабатываются модельные законы, направленные на регулирование Интернета и иных ИКТ.

Значимой также представляется инициатива Шанхайской организации сотрудничества (ШОС) по обеспечению международной информационной безопасности, в том числе и в интернет-пространстве. На саммите в Душанбе, прошедшем в августе 2008 года, было принято решение разработать межправительственное соглашение в рамках ШОС в области

международной информационной безопасности. Соответствующее соглашение было заключено в 2009 году, вступило в силу в 2011 и стало первым межправительственным соглашением в исследуемой области. В рамках ШОС проблематике управления Интернетом традиционно уделяется существенное внимание. В частности, в Нью-Делийской декларации ШОС от 2023 года отмечается, что государства ШОС «считают важным обеспечивать равные для всех стран права на регулирование сети Интернет и суверенное право государств на управление ею в своем национальном сегменте»[134]. Эта же формулировка сохранилась и в Астанинской декларации ШОС от 2024 года[135]. При этом особый акцент был сделан на обеспечение международной информационной безопасности, в частности, подчеркивается ключевая роль ООН в сфере противодействия угрозам в информационном пространстве, создания безопасного, справедливого и открытого информационного пространства, построенного на принципах уважения государственного суверенитета и невмешательства во внутренние дела других стран, постулируется приверженность недопустимости милитаризации сферы информационно-коммуникационных технологий (ИКТ)[136].

Российская Федерация является одним из активных участников программы ЮНЕСКО «Информация для всех» (ПИДВ) с момента её учреждения. Наша страна была первым государством-членом ЮНЕСКО, создавшим в 2001 году национальный комитет ПИДВ (Роском). За последние несколько лет в рамках реализации ПИДВ Роскомом при участии экспертов ЮНЕСКО организован целый ряд международных конференций и форумов по вопросам регулирования Интернета, в частности, формирования национальной и международной информационной политики, проблемам доступа к информации, этическим и правовым аспектам использования Интернета и т.д.[137].

Россия поддерживает активную позицию МСЭ и желание этой организации играть ключевую роль в сфере управления Интернетом. Конечная цель РФ и наиболее желательный для нашей страны исход событий – передача функции ICANN к МСЭ, у которого уже есть расширения своей сферы ответственности и принятие на себя новых функций в сфере регулирования телекоммуникаций. При этом Россия выступает за сохранение принципов многостороннего партнёрства и участия в управлении Интернетом не только государств, но и представителей гражданского общества, бизнес-сообщества и академического сообщества инженеров и разработчиков интернет-технологий, что позволит в перспективе сохранить инновационную природу Интернета, его открытость и доступность.

Важную роль играет платформа БРИКС как одна из наиболее подходящих для выработки странами-партнёрами коллективных решений в пяти основных областях управления Интернетом: инфраструктурное развитие; правовые вопросы; экономическая проблематика; содействие достижению целей развития; вопросы социально-культурной политики[138]. При этом именно участие развивающихся стран позволяет обеспечить легитимность принимаемых в рамках БРИКС решений в рассматриваемой области.

Россия апеллирует к следующим принципам: равные права и обязанности в сфере управления Интернетом, недопущение использования доступа к сети Интернет государствами в качестве инструмента влияния на другие государства, воздержание государств от действий, направленных на ограничение функционирования и (или) доступа к сети Интернет на территории других государств, суверенные права государств на управление национальным сегментом сети Интернет.

Согласно предложенному Россией в 2017 году документу «Концепция Конвенции ООН – Концепция безопасного функционирования и развития сети Интернет», «… ни у одного государства или группы стран не должно быть права создавать помехи для функционирования сети Интернет, единолично устанавливать нормы и правила для него, заниматься слежкой за гражданами, пытаться манипулировать зарубежным общественным мнением или дестабилизировать обстановку в суверенных государствах».

Однако, несмотря на активные действия российской дипломатии, данный принцип не нашёл отражения в принятом на уровне ООН в 2024 году Глобальном цифровом договоре. Данный документ завышает роль негосударственных акторов в управлении Интернетом, способствуя размыванию межправительственной природы ООН, акцентирует значимость прав человека в западной трактовке и не учитывает принцип государственного суверенитета. ГЦД, который уравнивает роль государств, гражданского общества и бизнеса, а также акцентирует правочеловеческий и гендерный нарратив в западной трактовке, прежде всего, усиливает глобальный Север, который лидирует в указанных областях. Для глобального Юга приоритетным представляется акцент на цифровом суверенитете и преодолении цифрового разрыва, борьбе с цифровым неоколониализмом и неоколониализмом данных, что позволит сделать цифровое пространство подлинно инклюзивным. Однако, не желая политизировать диалог, многие страны Юга всё же присоединились к Пакту и ГЦД как его приложению, выражая таким образом солидарность с Генераль-

ным секретарём в стремлении преодолеть системный кризис ООН, особенно, учитывая, что текст не имеет обязательной силы.

Россия не поддержала ГЦД, дистанцировавшись от консенсуса, а сам текст получил в российском обществе преимущественно негативные оценки, как на уровне официальных лиц, так и среди экспертного сообщества. Для нашей страны, которая является первопроходцем в обсуждении вопросов информационной безопасности и цифрового суверенитета, справедливая и инклюзивная система глобального управления в цифровом пространстве имеет приоритетное значение. Однако, несмотря на очевидные недостатки ГЦД, затронутые в нём вопросы нуждаются во внимательном анализе. В условиях повсеместной и стремительной цифровизации данная проблематика является одной из приоритетных в повестке ООН. Углубление и развитие цифрового сотрудничества – необходимое условие трансформации всемирной организации в соответствии с требованиями сегодняшнего дня, её выхода из длительного политического кризиса.

Российская делегация предложила поправку к Пакту, согласно которой данный документ представляет собой вмешательство ООН в вопросы, которые относятся к внутренней юрисдикции государства. Нашу страну поддержали Беларусь, КНДР, Иран, Никарагуа, Судан и Сирия, а 15 стран воздержались от голосования[139].

Россия последовательно исходит из необходимости адаптировать ООН к современным реалиям многополярного мира, в том числе в цифровом пространстве. Это предполагает среди прочего интернационализацию управления Интернетом. Российская дипломатия неоднократно подчёркивала центральную роль ООН в обеспечении международной информационной безопасности, борьбе с преступным использованием ИКТ, выработке этических норм для регулирования технологий искусственного интеллекта, преодолении цифрового разрыва и юридического закрепления принципа цифрового суверенитета. С точки зрения регулирования цифровых платформ Россия также исходит из необходимости уважения государственного суверенитета и выработки соответствующих правил на межправительственной основе.

Однако непрозрачность и забюрократизированность переговорного процесса привели к тому, что несколько значимых предложений России не вошли в текст ГЦД. Как отметил министр иностранных дел России С. Лавров, «надо договариваться по-честному, с участием всех членов ООН, а не так, как готовился Пакт во имя будущего

— без единого пленарного раунда переговоров, на котором присутствовали бы все страны. Вместо этого велась работа под контролем западных манипуляторов».

Россия стала первой страной, заявка которой на получение интернационализированного доменного имени на кириллице была утверждена. В 2010 году в Москве прошел первый Российский форум по вопросам управления Интернетом. По замыслу организаторов, форум должен был стать отправной точкой для активизации участия российских представителей в работе международных организаций, занимающихся вопросами интернет-управления. Форум с 2010 года проходит ежегодно и вызывает большой интерес среди бизнес-сообщества, академических структур и организаций гражданского общества.

Россия выступает за интернационализацию системы управления Интернетом, что подразумевает обсуждение практических шагов по постепенному переходу системы управления использованием Интернета под контроль международного сообщества. От того, на каких принципах будет организовано управление сетью Интернет, которая выступает в качестве системообразующей инфраструктуры глобального информационного общества, будут зависеть политические и экономические характеристики глобального информационного пространства, что не может не влиять на международную информационную безопасность.

Сложившийся в рамках ICANN и PTI государственно-частный режим управления Интернетом не только не соответствует интересам большинства государственных акторов (в том числе и РФ), которые видят в нём институционализацию доминирования США в информационном пространстве, но не устраивает также организации гражданского общества, которые выступают за большую подотчетность и демократическую легитимность организации. ICANN на протяжении всей своей истории с момента создания подвергалась существенной критике, причём главным объектом являются её «особые отношения» с Министерством торговли США, который сохраняет за собой контрольные функции по отношению к данной организации. Создание PTI не смогло придать легитимности сложившейся системе управления Интернетом, в том числе, в глазах официальных лиц Российской Федерации, ответственных за стабильное и бесперебойное функционирование российского сегмента Интернета[140].

Таким образом, ни ICANN, ни PTI не удалось стать той организацией, в рамках которой обсуждались бы проблемы управления Интернетом на межгосударственном уровне. Однако остальным организациям «интернет-сообщества» пока удаётся сохранять свои позиции

в процессах управления. Стремление правительств принимать участие в процессах управления Интернетом как по символическим, так и по практическим причинам сохраняет свою актуальность.

Очевидно, что США не могут игнорировать обеспокоенность мирового сообщества в отношении их односторонней политики в сфере регулирования Интернета. Со стороны Вашингтона была сделана следующая уступка – предоставление ICANN независимости от Министерства торговли США, что позволило избежать наиболее нежелательно варианта – интернационализации управления Интернетом и перехода функций ICANN к международной организации. Однако, предоставив ICANN формальную независимость, США, тем не менее, сохранили контроль над инфраструктурой Интернета благодаря рыночному влиянию (большая часть крупных компаний, работающих в интернет-пространстве, имеет американскую принадлежность), экономическому потенциалу (американские корпорации управляют доменными именами общего уровня, на которых зарегистрирована значительная часть доменов), а также управлению корневыми серверами, большая часть из которых так и останется на территории США.

Россия последовательно выступает за передачу прерогатив по техническому управлению Интернетом Международному союзу электросвязи, который обладает необходимой экспертизой, опытом и универсальной легитимностью. МСЭ является специализированной организацией «семьи ООН», и он в настоящее время не участвует в управлении Интернетом, более того, расширению его полномочий в данной области противодействуют США и их союзники, которые не желают отказываться от своего «особого» статуса в режиме управления Интернетом. Россия поддерживает необходимость усиления роли государств в управлении Интернетом, а также сохранение их суверенного контроля над национальным сегментом Интернета. Позицию России поддерживают многие государства, в том числе наши партнёры по ШОС, БРИКС, СНГ и другим региональным и макрорегиональным организациям.

В настоящее время проблематика управления Интернетом на международном уровне политизируется и секьюритизируется, всё чаще рассматриваясь в контексте международной информационной безопасности, количество угроз которой лишь возрастает. Россия после начала специальной военной операции на Украине сталкивается с беспрецедентным количеством кибератак. Однако трансграничная природа глобального информационного пространства способствует тому, что угрозам от растущей кибернестабильности подвергается вся международная система.

2.2. Международные организации в системе управления Интернетом

2.2.1. ООН и специализированные учреждения ООН

Включение ООН в процессы управления Интернетом неразрывно связано с политизацией проблемы управления Интернетом, однако, на практике спектр рассматриваемых Всемирной организацией вопросов весьма широк.

Интерес представляют следующие механизмы, созданные и функционирующие на базе ООН: Форум Всемирной встречи на высшем уровне по вопросам информационного общества (World Summit on the Information Society Forum; WSIS Forum); Форум управления Интернетом (Internet Governance Forum; IGF) и Многосторонняя консультативная группа (Multistakeholder Advisory Group; MAG); и Рабочая группа открытого состава (Open Ended Working Group; OEWG). В этом ряду следует также упомянуть также Международный союз электросвязи (МСЭ) (Рис. 1).

Рис. 1. Механизмы принятия решений по вопросам управления Интернетом в ООН.

Генеральная Ассамблея ООН выступает в качестве механизма легитимации решений, формируемых в рамках других форматов, поэтому не рассматривается как самодостаточный механизм в системе управления Интернетом[141].

Форум Всемирной встречи на высшем уровне по вопросам информационного общества (Форум ВВУИО)

Форум Всемирной встречи на высшем уровне по вопросам информационного общества (Форум ВВУИО) – это ежегодное собрание на высшем уровне с участием многих заинтересованных сторон по вопросам использования ИКТ в целях развития. В соответствии с Резолюцией Генеральной Ассамблеи A/RES/70/125 определен ежегодный порядок проведения Форума ВВУИО «для обсуждения всеми заинтересованными сторонами хода выполнения решений Всемирной встречи на высшем уровне и обмена соответствующей передовой практикой»[142].

С 2009 г. Форум ВВУИО служит в качестве основной платформы для представления результатов и обсуждения дальнейших действий по выполнению задач в рамках Женевского плана действий Всемирной встречи на высшем уровне по вопросам информационного общества.

На сегодняшний день ВВУИО остается одним из важнейших событий в процессе становления международного режима управления Интернетом. Инициатива о проведении ВВУИО принадлежит Международному союзу электросвязи – такое решение было озвучено по итогам Полномочной конференции МСЭ, прошедшей в Миннеаполисе в 1998 г.[143] В 2001 г. Генеральная Ассамблея ООН приняла решение о проведении Встречи в два этапа – в Женеве с 10 по 12 декабря 2003 г. и в Тунисе в 2005 г. Задачи по подготовке Встречи были делегированы межправительственному комитету открытого состава при ведущей роли МСЭ[144].

Мероприятие, сравнимое по масштабу и амбициозности с «Саммитом Земли» 1992 г. и Четвертой Всемирной конференцией по положению женщин 1995 г.[145], сфокусировалось на широком перечне вопросов, связанных с развитием цифровой среды и, в частности, на управлении Интернетом.

Первый «женевский» этап ВВУИО отметился широкой критикой в адрес ICANN со стороны МСЭ, правительств ЮАР, Китая, Бразилии и ряда других развивающихся государств. Сам факт создания Корпорации рассматривался как одностороннее действие Правительства США, которое обеспечило себе монопольное право контролировать

управление системой доменных имен. Критики сомневались в том, что в таких условиях Корпорация будет способна обеспечить принятие политических решений, отвечающих глобальным потребностям, а не только интересам американского руководства. Фактически, через критику ICANN недовольные стороны выступали против диктата США в системе управления ключевыми элементами системы глобального Интернета. Прямо противоположную позицию заняли США, Общество Интернета и представители частного сектора, для которых сложившаяся на тот момент система соглашений по вопросам управления Интернетом, включающая технологические стандарты МСЭ, решения IETF, ВОИС и ICANN, являлась достаточно совершенной и полностью удовлетворяющей текущей повестке управления всемирной сетью.

Ключевым результатом «женевского этапа» в отношении развития системы управления Интернетом стало решение о созыве Рабочей группы по вопросам управления Интернетом (WGIG)[146]. Рабочая группа должна была реализовать весьма амбициозную повестку: 1) разработать само определение понятия «управление Интернетом»; 2) выделить ключевые политические проблемы, связанные с управлением Интернетом; 3) согласовать общее виденье роли и пределов ответственности национальных правительств, международных и межправительственных организаций, иных международных форматов, частного сектора и организаций гражданского общества развитых и развивающихся государств в управлении Интернетом. Рабочая группа из 40 человек начала свою работу в ноябре 2004 г. и представила первый отчет о результатах проведенных консультаций и обсуждений в июле 2005 г.[147] В отчете было представлено рабочее определение понятия «управление Интернетом» - «разработка и применение правительствами, частным сектором и гражданским обществом, согласно их соответствующим ролям, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и использование Интернета»[148], а также рекомендация учредить специальный многосторонний форум для решения проблем управления Интернетом. Несмотря на то, что рекомендации Рабочей группы относительно мандата и операционной модели форума носили весьма расплывчатый характер, ключевым моментом стало утверждение касательно роли государств в управлении Интернетом – соблюдение «национальных интересов», тогда как частному сектору и неправительственным организациям были переданы задачи «технического управления» и поддержание «непрерывной работы» сети.

Выработанные Рабочей группой по вопросам управления Интернетом в 2005 году предложения были подвергнуты критике[149]. Указывается на то, что предложение о создании Форума по управлению Интернета не сопровождалось пояснением относительно методов его работы и внутренних процедур за исключением утверждения о его открытом и многостороннем характере. Проблему представляет и избранный экспертами подход, разделяющий роль и функции государств и негосударственных акторов в управлении Интернетом – принимая во внимание природу всемирной сети, на практике невозможно провести четкое разделение между «национальными приоритетами» и «техническим управлением» Интернетом. Кроме того, как считают авторы указанной работы, Рабочая группа не смогла отразить в докладе глобальную природу Интернета и то, каким образом это свойство может повлиять на легитимность ее системы управления и возможности национальных государств в этом отношении.

Второй этап ВВУИО прошел в Тунисе с 16 по 18 ноября 2005 г. Ключевым документом, зафиксировавшим решения, принятые на встрече, стала Тунисская программа для информационного общества[150]. Один из ключевых на тот момент вопросов, связанных с управлением Интернетом – статус ICANN и проблема государственного влияния на ее работу – не был разрешен. В тексте документа было зафиксирована «необходимость упрочения сотрудничества в будущем, – с тем, чтобы правительства могли на равной основе играть свою роль и выполнять свои обязательства», под чем можно рассмотреть попытку «растворить» единоличный статус США как ключевой инстанции в работе Корпорации. Международное сотрудничество, по мнению авторов документа, должно ориентироваться на «разработку применимых на глобальном уровне принципов государственной политики, касающейся координации и управления использованием имеющих важнейшее значение ресурсов Интернета». Поскольку механизм выработки принципов не был описан достаточно конкретно, фактически, эта задача была делегирована Форуму по управлению Интернетом. Непосредственно по вопросам управления DNS-пространством были приняты решения о содействии развитию многоязычия в доменных именах и укреплению сотрудничества в области доменов высшего уровня[151].

Результаты процесса достижения целей Женевского плана действий ВВУИО с 2006 по 2008 гг. представлялись на ежегодных собраниях высокого уровня, проводимых под эгидой МСЭ. Работа Форума ВВУИО была начата в 2009 г. Ежегодные встречи проходят с марта

по май в Женеве; в редких случаях, как это произошло в 2020 году, некоторые мероприятия переносятся на лето или осень.

Форум ВВУИО не принимает обязательных, юридически обязывающих решений. Его основную функцию в качестве многосторонней переговорной платформы можно рассматривать как способ обеспечения подотчетности и легитимности международной дискуссии по вопросам развития глобальной цифровой экономики. Так, в ходе Форума согласовываются и затем публично представляются итоговые отчеты, рекомендации высокого уровня и аналитические документы[152].

Международный союз электросвязи

Международный союз электросвязи является специализированным учреждением в системе ООН. Отличительными характеристиками МСЭ является широкий охват членства и многовекторность деятельности, а также оценочно наиболее высокий сравнительный уровень легитимности среди межправительственных организаций в сфере международного регулирования развития ИКТ и управления Интернетом, в частности[153].

Текущая организационная структура МСЭ была определена в декабре 1992 г. и включает следующие подразделения:

- ITU-T (МСЭ-Т) — Сектор стандартизации электросвязи,
- ITU-R (МСЭ-Р) — Сектор радиосвязи,
- ITU-D (МСЭ-Д) — Сектор развития электросвязи.

В соответствии с целью и задачами настоящего исследования наибольший интерес представляет деятельность Сектора стандартизации электросвязи.

Как и в случае с ООН в целом, следует отметить работу МСЭ в части формирования репрезентативной выборки данных об уровне развития ИКТ в отдельных странах. С 2009 по 2017 гг. МСЭ публиковал международный рейтинг цифровой развитости стран мира, основанный на собираемой статистике; компиляция была приостановлена в связи с проблемой доступности и достоверности собираемых данных[154]. Статистика цифрового роста продолжает публиковаться МСЭ в формате сборников Measuring digital development: Facts and Figures[155].

К настоящему моменту МСЭ согласованы более 4000 рекомендаций по широкому перечню вопросов, включая общие принципы тарификации электросвязи; аудиовизуальные и мультимедийные

системы; техническое обслуживание международных каналов передачи звуковых и телевизионных программ; глобальная информационная инфраструктура, аспекты протокола Интернета и сети будущих поколений; языки и общие аспекты программного обеспечения для систем электросвязи и т.д.[156]

МСЭ не принимает юридически обязательных документов[157]. Основным продуктом его деятельности являются типовые Рекомендации, которые определяют особенности функционирования и взаимодействия сетей электросвязи. Несмотря на их изначально неформальный характер, многие Рекомендации МСЭ интегрируются в национальное законодательство, обретая таким образом юридический статус. МСЭ высоко оценивает соответствие национального законодательства 193 стран-членов формулируемым рекомендациям.

Таким образом, за пределами вопросов стандартизации технологий связи роль МСЭ в текущей структуре и вероятной будущей конфигурации системы управления Интернетом представляется достаточно ограниченной в силу наличия выраженных противоречий между ведущими акторами. Наряду с Обществом Интернета МСЭ можно считать важным механизмом обеспечения технологического единообразия на всем пространстве Интернета, влияние которого поддерживается высокой оценочной легитимностью и широким страновым представительством.

Форум управления Интернетом и Многосторонняя консультативная группа

Идея о созыве специализированного постоянного форума, объединяющего представителей различных групп интересов для обсуждения вопросов управления Интернетом, прозвучала в ходе тунисского этапа ВВУИО в 2005 году. Решением рабочей группы по управлению Интернетом форум должен был заниматься одной из важнейших проблем – согласованием общих принципов функционирования системы управления глобальной сетью. Предложение о создании форума было внесено Аргентиной, представители которой подчеркнули в своём выступлении поддержку эволюционного развития системы управления Интернетом на принципах прозрачности, демократичности и многосторонности[158]. В пункте 72 «Тунисской программы для информационного общества», принятой 15 ноября 2005 года, договаривающиеся стороны обратились к Генерально-

му секретарю ООН с просьбой провести ко второму кварталу 2006 года «собрание нового органа для ведения политического диалога с участием многих заинтересованных сторон» в рамках «открытого и всестороннего процесса»[159].

Наряду с обсуждением общих принципов управления Интернетом, Форуму были переданы следующие функции:

- содействие диалогу между органами, занимающимися различными перекрёстными вопросами международной государственной политики в отношении Интернета, и обсуждение вопросов, не относящихся к компетенции какого-либо из существующих органов;
- взаимодействие с соответствующими межправительственными организациями и другими учреждениями по вопросам, относящимся к их компетенции;
- содействие обмену информацией и передовым опытом и с этой целью использование в полной мере опыта академических, научных и технических сообществ;
- предоставление консультаций всем заинтересованным сторонам с предложением путей и средств ускорения доступности и приемлемости в ценовом отношении Интернета в странах развивающегося мира;
- обеспечение и оценка на постоянной основе практического осуществления принципов ВВУИО в процессе управления использованием Интернета – и ряд других.

Решение о созыве форума было закреплено резолюцией 60/252 ГА ООН от 27 апреля 2006 года в соответствии с решениями Тунисского саммита 2005 года[160]. Инаугурационные мероприятия прошли в Афинах, Греция, с 30 октября по 2 ноября 2006 года после двух раундов консультаций в Женеве в феврале и мае 2006. В ходе консультаций был определён перечень наиболее важных вопросов, требующих принятия многосторонних решений: спам; поддержка языкового разнообразия; киберпреступность; кибербезопасность; защита неприкосновенности частной жизни и защита данных; свобода выражения и права человека; стоимость международных цифровых коммуникаций; преодоление цифрового разрыва через расширение доступа и принятие качественных политических решений; преодоление цифрового разрыва через меры финансирования; регулирование электронной коммерции, цифровых бизнесов и защита потребителей[161]. В докладе секретариата форума также подчёркивалось, что одним из приоритетов многосторонней работы должно стать «создание потен-

циала» и «расширение способности всех стран участвовать в управлении Интернетом». Наряду с этим подчёркивалось, что имеющимся на момент проведения первой встречи форума механизмам управления Интернетом «успешно удавалось ограждать базовую технологическую инфраструктуру от манипуляций в политических и коммерческих целях»; сохранение данного статус-кво было признано одним из принципов дальнейшей многосторонней работы[162].

Один из ключевых органов форума – Многосторонняя консультативная группа (МКГ) – была учреждена решением организационного комитета 17 мая 2006 года. Генеральный секретарь ООН ежегодно назначает 40 членов группы из представителей национальных правительств, частных компаний, гражданского общества и профессиональных объединений. Каждый член МКГ может быть повторно назначен на должность, однако в этом отношении действует ограничение – не более трёх сроков по одному году. Отмечается, что по своему статусу лица, формально представляющие правительства, не имеют никаких преимуществ перед коллегами из других сообществ, действуя, фактически, в качестве частных лиц. МКГ обсуждает и утверждает программу предстоящего форума, однако за её составление на деле отвечает отдел государственных институтов и цифрового правительства департамента ООН по экономическим и социальным вопросам. Страна, принимающая ежегодный форум, таким образом, обладает достаточно ограниченным влиянием на формирование повестки дня[163].

ФУИ служит, прежде всего, площадкой для обмена мнениями между представителями различных заинтересованных сообществ. Форум на ежегодной основе публикует результаты многосторонних дискуссий по широкому кругу вопросов в форме итоговой декларации и не принимает решения, обладающие признаком «обязательности» в той или иной форме. Повестка работы форума за более чем 15 лет не претерпела фундаментальных изменений, по-прежнему фокусируясь на вопросах защиты прав человека, защиты данных, развития инфраструктуры Интернета, преодоления цифровых вызовов, включая борьбу с киберпреступностью, и т.д.[164] Количество делегатов может достигать шести тысяч человек, при этом формат «национальной делегации» не предусмотрен как таковой, что, по мнению экспертов Национальной ассоциации международной информационной безопасности (НАМИБ), делает работу форума «непредсказуемой»[165]. С другой стороны, несомненной положительной характеристикой форума является его открытость и многосторонность,

допускающая участие всех заинтересованных сторон в обсуждении в соответствии с решениями ВВУОИ[166].

Группы правительственных экспертов (ГПЭ) и рабочая группа открытого состава (РГОС) по безопасности использования ИКТ при первом комитете ГА ООН

Многосторонняя международная дискуссия по вопросам информационной безопасности была инициирована Россией в 1998 году, когда была принята первая резолюция ГА ООН «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Изначально в 1998 году целью РФ было достижение двусторонней договорённости с США о совместном призыве к международному сообществу приступить к согласованию взглядов на военное применение ИКТ, использованию терминов «информационное оружие» и «информационная война», а также изучить возможности цифровых технологий для разработки новых видов вооружений. Инициативой России было положено формирование режима обеспечения безопасности мировой информационной среды на глобальном и впоследствии на региональном (СНГ, ШОС, ОДКБ) и макрорегиональном (БРИКС) уровнях, однако данный процесс по сей день нельзя считать завершённым[167].

Инициированная Россией дискуссия достаточно долгое время не приводила к практическим результатам. В 2004 году с целью разрешения выявленных проблем была создана группа правительственных экспертов ООН, куда были включены представители 15 стран, отобранные по принципу наилучшего географического представительства[168]; в дальнейшем состав участников расширился сначала до 20 государств, а затем – до 25. Мандат первой ГПЭ, как и всех последующих, был определён сроком на один год. ГПЭ созывались шесть раз: в 2004–2005 гг., 2009-2010 гг., 2012-2013 гг.; 2014-2015 гг.; 2016-2017 гг.; 2019-2021 гг. Четыре состава ГПЭ смогли представить по итогам обсуждения субстантивные доклады: в 2010, 2013, 2015 и 2021 году. Функции секретариата ГПЭ выполняло управление ООН по вопросам разоружения.

Как уже было сказано выше, ГПЭ созывались для разрешения вопросов, связанных с кибербезопасностью. Несмотря на то, что в целом деятельность ГПЭ принесла достаточно ограниченные практические результаты, за ГПЭ следует признать выполнение двух важных задач. Во-первых, вопреки противоречиям, возникшим в

процессе обсуждения вопросов об ответственности государств за любую деятельность в цифровом пространстве в пределах их юрисдикции, участники переговоров признали необходимость выработки специализированных международных норм и механизмов контроля над цифровыми технологиями[169]. Во-вторых, в 2013 году третий состав ГПЭ закрепил предложенный еще на начальном этапе переговоров российской делегацией принцип ответственности государств за деятельность в киберпространстве в пределах их территориальной юрисдикции. Эксперты выступили с призывом к национальным государствам принимать в добровольном порядке меры доверия и транспарентности. Анализируя итоги деятельности ГПЭ, Ромашкина Н.П. указывает на то, что на данном этапе ГПЭ работала в парадигме увязки существующих норм международного права и избегала выдвигать рекомендации относительно создания принципиально новых регуляторных норм[170]. Эта проблема остаётся неразрешённой до сих пор. В-третьих, следует отметить принятый ГПЭ четвёртого состава добровольный кодекс правил поведения государств в целях обеспечения международной информационной безопасности, предложенный странами-членами ШОС в 2011 году[171].

Кризис в работе ГПЭ наступил в 2017 году, когда по итогам прошедших заседаний не был согласован итоговый доклад. Невозможность согласования заключительного документа связывают с обострением межгосударственных противоречий и различием в подходах относительно применимости права на самооборону в ИКТ-среде. Следует также отметить ограниченный состав участников, который за весь период работы группы (2004-2021 гг.) хоть и расширился с 15 до 25 государств, не позволил многим государствам, особенно из числа развивающихся стран, поучаствовать в многосторонней дискуссии.

На фоне кризиса ГПЭ Россия вновь выступила с инициативой, призванной снять часть накопившихся противоречий. В конце 2018 года параллельно с шестым составом ГПЭ была запущена рабочая группа открытого состава, коренным отличием которой стал принцип открытого членства – участие в работе РГОС может принять любое государство-член ООН[172]. После завершения мандата шестого состава ГПЭ в 2021 году полномочия РГОС были продлены до 2025 года[173], несмотря на то, что итоговый доклад РГОС первого созыва в своей рекомендательной части воспроизводил ранее согласованные в рамках ГПЭ призывы к наращиванию потенциала государств в противодействии киберугрозам, расширению обмена наилучшими практиками, укреплению дове-

рия и т.д. и мало чем дополнял дискуссию по основным вопросам международной информационной безопасности[174].

Ключевой задачей РГОС на 2021-2025 гг. в настоящий момент является выработка консенсуса по ключевым вопросам информационной безопасности в преддверии учреждения ООН постоянно действующего институционального механизма в области ИКТ безопасности[175]. Перспективы достижения консенсуса в рамках РГОС представляются достаточно туманными. Во-первых, какими бы конкретными ни были вероятные заключения, принятые РГОС, они остаются «добровольными, не имеющими обязательной силы нормами» и в целом могут рассматриваться только как декларация о намерениях, не подкреплённая соответствующими уровню проблемы механизмами принуждения. Широкий состав участников, с одной стороны, позволяет избежать патовых ситуаций, сложившихся в рамках ГПЭ и приведших к свёртыванию формата, но, с другой стороны, вызывает обоснованные опасения относительно реальной перспективы выработки прорывных и при этом универсально приемлемых решений.

С 2019 по 2024 год при третьем комитете ГА ООН также функционировал специальный комитет по выработке конвенции по противодействию ИКТ-преступности, создание которого также было инициировано российской дипломатией. По результатам работы комитета, председателем которого выступила представитель Алжира, в 2024 году была принята конвенция о противодействии ИКТ-преступности на уровне ГА ООН. Она стала первой за последние 15 лет международной конвенцией, принятой ООН.

Целями согласованного текста конвенции названы содействие принятию и укрепление мер, направленных на повышение эффективности и результативности предупреждения и пресечения киберпреступности; поощрение, облегчение и укрепление международного сотрудничества в предупреждении и пресечении киберпреступности; поощрение, облегчение и поддержка технической помощи и создания потенциала в области предупреждения и пресечения киберпреступности, особенно в интересах развивающихся стран[176]. Документ подразумевает следование ключевым принципам устава ООН – суверенное равенство государств и невмешательство во внутренние дела через наращивание международного сотрудничества компетентных ведомств в информационном пространстве, совершенствование механизмов и расширение охвата такого взаимодействия[177].

В 2021 году Генеральный секретарь ООН А. Гуттериш представил доклад «Наша общая повестка», в рамках которого была озвучена идея принятия Глобального цифрового договора (англ. Global Digital

Compact). Генеральный секретарь ООН внес следующее предложение: «Организация Объединенных Наций, правительства, частный сектор и гражданское общество могли бы … совместно наладить работу на многостороннем треке «Цифровые технологии», чтобы согласовать Глобальный цифровой договор». Глобальный цифровой договор продолжает практику глобальных договоров ООН, которые не являются договорами в юридическом смысле данного термина, а представляют собой набор общих принципов, призванных регулировать деятельность различных акторов мировой политики.

В 2024 году Глобальный цифровой договор был принят на уровне ООН, подробнее о ГЦД рассказывается в разделе «Позиция и интересы России в области управления Интернетом» (стр. 61).

Анализируя роль и место ООН и подотчетных организации механизмов в системе управления Интернетом, следует отметить следующее. Во-первых, ООН, вне всякого сомнения, является наиболее представительной и легитимной универсальной площадкой в рамках рассматриваемой структуры. Несмотря на трудности, связанные с выработкой решений в ключевых областях управления Интернетом в рамках ООН, особенно в тех вопросах, которые так или иначе связаны с политическими мотивами и национальными интересами, каждый достигнутый результат, например, Кодекс ответственного поведения государств в киберпространстве или сам факт признания существования киберугроз как реальной проблемы, требующей многостороннего решения, имеет огромную значимость. Во-вторых, нельзя не отметить то, что ни один из рассмотренных форматов, посредством которых ООН участвует в управлении Интернетом, не принимает юридически обязательных решений. Наибольшим потенциалом в этом отношении обладает Международный союз электросвязи, вырабатывающий универсально применимые технические регламенты, однако за пределами технической стороны управления Интернетом МСЭ сталкивается с проблемами несовместимости позиций ведущих акторов, вследствие чего принятие конкретных решений крайне затруднено. В целом, роль ООН в системе управления Интернетом представляется как площадка для согласования общих позиций и подходов, выработки единой методологии и терминологии, а также легитимизации решений, формирующихся на других площадках. С учётом выявленных особенностей текущего этапа формирования международного режима управления Интернетом, согласование принципов и позиций представляется важной и необходимой работой, закладывающей основы для прогресса в будущем.

2.2.2. Региональные организации интеграции в системе управления Интернетом

Европейский союз

Чтобы снизить геополитические риски раскалывающегося мира, в котором рушатся устоявшиеся производственные и логистические цепочки, Евросоюз решил овладеть ключевыми передовыми технологиями в области микроэлектроники, квантовых вычислений, искусственного интеллекта (ИИ) и блокчейна, а также озаботился поиском надёжных цепочек поставок[178].

В феврале 2020 года принята Стратегия ЕС в области данных, направленная на укрепление лидерства в цифровом обществе. Стратегия ставит перед собой преимущественно экономические цели, однако проблема обеспечения цифрового суверенитета в контексте информационной безопасности также занимает важное место.

Согласно стратегии, цифровое развитие рассматривается Брюсселем как сравнительное конкурентное преимущество и фактор укрепления позиций на международной арене. При этом, помимо экономического потенциала цифровых технологий, в стратегии также отмечается значимость новых угроз безопасности, обусловленных развитием ИКТ.

Основополагающий документ, регламентирующий ключевые направления цифрового развития ЕС, – Европейская цифровая стратегия (Shaping Europe's digital future) от февраля 2020 года. В стратегии представлены три сферы приоритетов деятельности Еврокомиссии на период 2019–2024 по поддержке процессов цифровизации:

1. Разработка и внедрение технологий, которые функционируют в интересах людей (искусственный интеллект, облачная обработка данных и блокчейн-технологии, высокопроизводительные вычисления и квантовые технологии; связь; 5G и Интернет вещей; цифровые технологии; фотонные и электронные средства).
2. Развитие справедливой и конкурентоспособной цифровой экономики (базы данных, онлайн-платформы и электронная торговля; авторские права).
3. Формирование открытого, демократического и устойчивого цифрового общества (культура СМИ и цифровая культура; доверие и безопасность личного электронного пространства; цифровая система здравоохранения и цифровое правительство; умные города; безопасный Интернет; женщины в цифровом пространстве) (Еврокомиссия, 2020).

Стратегическая цель ЕС, согласно данному документу, – повышение своей роли как глобального игрока. Развитие европейских IT-технологий и платформ должно укрепить автономию ЕС, снизив его зависимость от технологических поставок из-за рубежа (прежде всего, из США и КНР).

Европейская стратегия в области данных от 2020 года вписывается в общую концепцию построения демократического и открытого общества, что в свою очередь преследует укрепление «нормативной силы ЕС», основанной на привлекательности европейской модели для других стран и регионов. («Нормативная сила ЕС» подразумевает создание гарантий личной, национальной и общественной безопасности, а конечная цель заключается в повышении статуса ЕС на международной арене (Diez, 2013).)

В декабре 2020 года также была принята Стратегия кибербезопасности ЕС в цифровую декаду. Данный документ ставит задачей обеспечение стратегической автономии ЕС в информационной сфере, сохраняя открытость экономики[179]. Возможность принимать независимые решения в области кибербезопасности рассматривается как важное условие укрепления цифрового лидерства Евросоюза и его стратегических возможностей.

Государства-члены ЕС имеют серьёзный технологический задел. Например, у всех на слуху финская Nokia, немецкие Siemens и Bosch, французская Orange и так далее. Если рассматривать сферу микроэлектроники, то в странах ЕС умеют делать широко востребованное в мире оборудование для производства полупроводников (нидерландская компания ASML), криптографические чипы (немецкая Infineon), полупроводниковые компоненты (нидерландская NXP) и прочее. Помимо этого, стоит обратить внимание и на имеющиеся вычислительные мощности. Например, французская компания Atos занимается производством суперкомпьютеров, а также ведёт разработки в области квантовых вычислений[180].

Однако, несмотря на серьёзный технологический потенциал, в современных нестабильных геополитических условиях этого оказывается недостаточно. По численности населения ЕС отстаёт от США и Китая (эти две страны являются лидерами в области информационных технологий): по данным на 1 января 2020 года этот показатель в ЕС составил 447,7 миллиона человек. Это ограничивает возможности со стороны европейских компаний, прежде всего, из области платформенной экономики, на равных конкурировать с американскими и китайскими гигантами (такими, как группа GAFAM – Google,

Apple, Facebook, Microsoft – и китайские BATX – Baidu, Alibaba, Tascent) как в области контроля над данными, так и в отношении развития технологий искусственного интеллекта (развитие которого опять же опирается на доступ к большим массивам данных, необходимых для машинного обучения). Всё вышеперечисленное создаёт вызовы для положения ЕС как одного из лидеров мировой экономики и мировой политики, что актуализирует пересмотр стратегии в данной области.

В Евросоюзе много внимания уделяется выработке технологических стандартов и норм в цифровом пространстве, которые должны помочь в установлении контроля над технологиями. Например, там уже действует закон о защите персональных данных (GDPR), а также закон о цифровых рынках (DMA) и закон о цифровых услугах (DSA), призванные ограничить доминирующее положение американских техногигантов в Европе и защитить пользователей в цифровом пространстве.

Важной инициативой стало принятие закона ЕС об искусственном интеллекте. EU AI Act – это первый в мире закон, регламентирующий системы ИИ. Закон регламентирует разработку и использование ИИ, предусматривает значительные штрафы и широкий набор обязательных требований для организаций, занимающихся разработкой и внедрением ИИ.

Европейский союз продемонстрировал довольно жёсткий подход к регулированию ИИ: фактически это централизованный контроль всех стадий разработки и применения генеративных нейросетей с тщательным их тестированием перед использованием

ЕС этим документом пытается создать глобальный стандарт регулирования ИИ, что может повлиять на общемировой опыт развития регуляторики в данной области. Это заявка на глобальное нормативное лидерство в области цифровой экономики, которая призвана компенсировать отсутствие у Европейского союза собственных платформенных решений и значимых технологий в области генеративного ИИ.

Но жёсткий подход – не единственно возможный, поэтому он вряд ли получит глобальное распространение. Так, многие страны ориентированы на более гибкое регулирование ИИ. В Китае, например, в большей степени используется не жёсткое, запретительное, а нейтральное регулирование, когда законодатель находит баланс между развитием и безопасностью с точечным характером ограничений. Подобный подход близок и России.

Закон предполагает трансграничное экстерриториальное регули-

рование ИИ – он будет применяться не только к европейским компаниям, разрабатывающим и внедряющим ИИ, но и к компаниям вне ЕС, если их ИИ-системы используются в Европейском союзе. Это заявка ЕС на реализацию «права длинной руки» с тем, чтобы усилить международное влияние в сфере ИИ и при этом защитить европейских потребителей зарубежных ИИ-решений.

Впрочем, в настоящее время в условиях растущей фрагментации цифрового пространства ЕС не может быть единым нормативным лидером в данной области. В БРИКС по предложению Китая, например, запущена инициатива по исследованию ИИ. Обсуждается также возможность создания новой структуры по его управлению.

Таким образом, в системе управления Интернетом ЕС во многом следует в фарватере внешней политики США, поддерживая лидирующую роль США в данной области, самостоятельность проявляется лишь в области нормативной силы.

Африканский союз

Цифровой рынок Африки растёт очень быстро, развивается международное сотрудничество в рамках континента в исследуемой области. Население Африки, оцениваемое в 1,3 миллиарда человек, молодо и всё более активно использует Интернет; в 2025 году число пользователей Интернета превысило 800 миллионов. Цифровизация и связь обеспечивают для Африки платформу, чтобы перепрыгнуть через этапы развития цифровых технологий. Поэтому инвестиции в цифровую инфраструктуру, продвижение цифровых навыков, содействие исследованиям и инновациям, укрепление кибербезопасности и развитие возможностей управления данными – один из приоритетов европейской интеграции в Африке. В частности, была принята Стратегия цифровой трансформации Африканского континента 2020–2030[181]. Стратегия подчёркивает огромные экономические возможности континента и его молодое население как ключевые движущие силы в цифровую эпоху. Эта стратегия направлена на приоритет социально-экономического развития с использованием цифровых технологий для стимулирования создания рабочих мест, решения проблемы бедности, сокращения неравенства и содействия доставке товаров и услуг, что вносит вклад в достижение повестки для Африки 2063 и целей устойчивого развития.

Стратегия, разработанная в сотрудничестве с Экономической комиссией ООН для Африки, Smart Africa, AUDA-NEPAD, региональны-

ми экономическими сообществами, Африканским банком развития, Африканским союзом электросвязи, Фондом наращивания потенциала Африки, Международным союзом электросвязи и Всемирным банком, основывается на существующих инициативах по развитию единого цифрового рынка для Африки. Это стратегическое видение является частью инициативы Smart Africa, отражающей интеграционные приоритеты Африканского союза.

Стратегия по ИИ в Африке («Континентальная стратегия по искусственному интеллекту») обсуждалась в июне 2024 на уровне министров в рамках исполнительного совета Африканского союза и была одобрена. В Стратегии Африканского континента по ИИ делается акцент на «использовании технологии в целях сохранения идентичности, языков и культур африканских народов», «создании общего цифрового рынка» и выработке правил и регуляторики, «наказывающих злонамеренное использование ИИ и цифровых технологий и предотвращающих возможное злоупотребление»[182].

Документ соотнесен со Стратегией цифровой трансформации Африканского союза и Повесткой 2063. Также принят Африканский цифровой договор, который был представлен на «Саммите будущего» ООН в сентябре 2024[183].

Меркосур

Технологическое развитие и сокращение технологического разрыва между членами Меркосур (общий рынок стран Южной Америки) являлось важной задачей развития интеграционного блока с момента образования в 1992 году. Однако работа над общей правовой и технологической базой была включена в его повестку лишь после 1998-2000 гг.

Основные инициативы Меркосур в области цифровой интеграции включают в себя защиту прав потребителей, содействие электронной торговле, внедрение электронной подписи. Однако отсутствуют инициативы, направленные на создание единого цифрового рынка, а такие важные вопросы как повышение уровня доверия к цифровым технологиям в обществе и сотрудничество в области кибербезопасности, цифровые государственные услуги и внедрение лучших практик в области открытого обмена данными лишь частично включены в текущую цифровую повестку дня Меркосур[184]. В настоящее время к взаимодействию с интеграционной структурой и со странами региона в цифровой сфере проявляют интерес многие внерегиональные акто-

ры – среди них лидеры электронной экономики Китай, США и ЕС.

ЕАЭС

Старт цифровой повестке ЕАЭС был дан 26 ноября 2015 года в Минске на первом заседании президиума Делового совета Евразийского экономического союза (ЕАЭС). В 2016 году ЕАЭС были выработаны и представлены Предложения по формированию цифрового пространства[185].

В предложениях было отмечено, что за счёт объединения усилий и ресурсов стран ЕАЭС при создании общего цифрового пространства возможно достижение синергетического эффекта, что расширит возможности и преимущества ЕАЭС в области экономического развития. Кроме того, формирование общего цифрового пространства призвано открыть новые возможности в модернизации традиционных отраслей экономики и рынков союза[186]. Важнейшим документом на данном направлении стали принятые в 2017 году Стратегические направления развития цифровой повестки ЕАЭС до 2025 года[187].

Россия является лидером в области цифровой интеграции ЕАЭС и на уровне государственной политики оказывает поддержку цифровой повестке. Указом президента Российской Федерации от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» правительству РФ поручено обеспечить в 2024 году решение задачи по разработке и внедрению национального механизма осуществления согласованной политики государств-членов ЕАЭС при реализации планов в области развития цифровой экономики[188].

С целью интенсификации цифрового измерения интеграционных процессов 8 июня 2023 года главы правительств приняли доклад о дальнейшем развитии интегрированной информационной системы ЕАЭС и цифровой повестки Союза, а также распоряжение, предусматривающее дальнейшие шаги по цифровой трансформации сфер сотрудничества, определённых Договором о ЕАЭС. Евразийская экономическая комиссия утвердила Целевую программу развития интегрированной системы (ИИС) Союза до 2027 года[189]. Значительное внимание в рамках цифровой повестки ЕАЭС уделено цифровому суверенитету стран-участниц, что предполагает снижение зависимости от западных цифровых технологий и стратегическую автономию в цифровой сфере. В 2022 году началось обсуждение возможности разработки межгосударственной программы развития полупроводниковой про-

мышленности в странах-членах Евразийского экономического союза. В настоящее время обсуждаются также вопросы сотрудничества ЕАЭС и в других высокотехнологичных областях, однако эксперты отмечают слабость технологической базы ЕАЭС и высокую зависимость от иностранных поставщиков в сфере высоких технологий[190].

В числе вызовов цифровой интеграции на пространстве ЕАЭС различие в уровнях развития цифровой инфраструктуры и доступе к Интернету. Недостаточно высокие темпы цифровой интеграции на пространстве ЕАЭС также связаны с межстрановыми различиями в нормативно-правовой базе. Цифровизация интеграционных процессов ЕАЭС позволит повысить экономические преимущества от сотрудничества, получить доступ к новым цифровым рынкам, а также реализовывать программы снижения зависимости от западных онлайн-платформ и технологических решений.

В политическом измерении ставится задача укрепления ЕАЭС как центра силы в современной глобальной цифровой политике, при этом Россия выступает в роли лидера в интеграционных процессах на постсоветском пространстве. Для достижения данной цели необходимо развитие сотрудничества с третьими странами и интеграционными структурами и включение в повестку такого взаимодействия вопросов цифровизации в целях обмена опытом, получения доступа к технологиям и лучшим практикам.

Одной из тенденций международного сотрудничества в цифровой сфере является трансрегионализм – сотрудничество между интеграционными объединениями различных регионов. ЕАЭС стремится играть возрастающую роль в экономическом сотрудничестве на евразийском континенте, для достижения этой цели необходимо трансрегиональное экономическое сотрудничество и расширение сети партнёрского взаимодействия.

АСЕАН

АСЕАН — крупнейшая межгосударственная политико-экономическая организация Юго-Восточной Азии: по данным на 2018 год, численность населения составила 642,4 миллиона человек, совокупный ВВП – 2,7 триллиона долларов, внешнеторговый оборот – 2,5 триллиона долларов. Поставлена цель к 2030 году стать четвёртой экономикой мира[191]. Цифровая трансформация, рассматриваемая как важнейший инструмент достижения целей интеграции АСЕАН, находится в центре внимания уже более двух десятилетий с момента

подписания Рамочного соглашения об электронной АСЕАН в ноябре 2000 года. Цифровизация в рамках АСЕАН направлена на ускорение развития цифровой экономики за счёт формирования единого цифрового рынка, порождающего «эффект масштаба» и «сетевые эффекты», а также обеспечивающего усиление притока инвестиций в цифровую сферу АСЕАН[192]. Показательно, что Ассоциации удалось добиться 100% реализации всех 87 проектов, отмеченных в Генеральном плане АСЕАН по развитию ИКТ до 2015 года[193].

Быстрые темпы проникновения новых технологий обусловили растущий интерес к полноценному доступу и использованию цифровых технологий гражданами стран АСЕАН, среди которых цифровые технологии развиты неравномерно. В числе лидеров – Сингапур и Малайзия, при этом отдельные страны, такие как Камбоджа, Лаос, Мьянма, характеризуются значительно более низкими уровнями проникновения цифровых технологий. Без решения проблемы цифрового разрыва невозможно укрепление цифровой связности региона и решение задач интеграции.

Для развития цифровой интеграции на уровне АСЕАН в 2021 году была принята Повестка цифровой трансформации АСЕАН для восстановления экономики и цифровой интеграции[194]. Она призвана создать институциональную и правовую основу для цифровизации экономики.

2.2.3. БРИКС и «Группа двадцати»

Форум ведущих индустриально развитых государств[195] – «Группа двадцати» – относится к неформальным институтам глобального управления. Следует отметить, что «Группа двадцати» не принимает юридически обязательных решений. Действия, согласуемые в рамках «двадцатки», опираются исключительно на политическую волю стран-участников и их невыполнение не влечет применения санкций[196].

«Группа двадцати» начала работу над решениями в области цифровой экономики и управления Интернетом в 2015 году в ходе председательства Турции, когда были приняты Обновлённые стратегии роста, учитывающие достижения в области цифровых технологий. В ходе китайского председательства 2016 года лидеры «двадцатки» согласовали План действий по инновациям и План действий в связи с новой индустриальной революцией. При поддержке ОЭСР была запущена целевая Рабочая группа «двадцатки» по цифровой экономике. Инициатива «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики утвердила приверженность членов

«двадцатки» положениям Итоговых документов Всемирной встречи на высшем уровне по вопросам информационного общества, в частности, стремление к обеспечению многосторонности в принятии решений в области управления Интернетом. «Двадцатка» поддержала политику по сохранению глобального характера сети Интернет при соблюдении правовых рамок защиты неприкосновенности частной жизни и личных данных.

Качественное развитие повестка управления Интернетом в «двадцатке» получила в 2019 году в ходе председательства Японии – в Осаке лидеры «Группы двадцати» приняли совместное Заявление по предотвращению использования Интернета для осуществления экстремистской и террористической деятельности. Решением лидеров был запущен т.н. «Осакский трек», одной из задач которого является содействие свободной трансграничной передаче данных в атмосфере доверия[197].

В контексте пандемии COVID-19 «Группа двадцати» приняла ряд решений, направленных на использование возможностей цифровых технологий для преодоления новых вызовов. Согласованные в 2020 году на уровне министров «двадцатки» шаги в широком смысле затрагивали обеспечение интероперабельности и выработку общих стандартов работы с данными, обмен которыми стал краеугольным камнем политики сдерживания трансграничного распространения пандемии – это соответствует содержанию одного из треков сотрудничества, заложенных в декларации министров «Группы двадцати» от 22 июля 2020 г.[198] Приверженность «двадцатки» свободной трансграничной передаче данных, основанной на доверии, была подтверждена в Эр-Риядской декларации «Группы двадцати» 2020 года[199] и в принятой годом позже Римской декларации[200].

Вопреки ограничениям в деятельности «двадцатки», связанным с её неформальным статусом и отсутствием компонента юридической обязательности принимаемых решений, данный форум показывает достаточно высокую эффективность в деле согласования подходов и общих позиций. Учитывая текущее состояние режима управления Интернетом, возможность обеспечивать консенсус по наиболее общим и принципиальным вопросам может рассматриваться даже как более важное свойство, нежели формальный статус согласуемых решений. Несмотря на то, что Россия и ее ближайшие страны-партнеры, в первую очередь страны-члены БРИКС, также являются членами «двадцатки», данный формат имеет выраженную прозападную направленность, обусловленную сильным влиянием на процесс выработки итоговых реше-

ний «Группы семи»[201]. Понимание особенностей функционирования системы принятия решений в рамках «Группы двадцати» представляется важным в контексте определения роли и возможностей стран БРИКС и БРИКС как института глобального управления Интернетом.

С точки зрения внешнеполитических приоритетов России, БРИКС является одной из приоритетных международных площадок. С институциональной точки зрения, БРИКС обладает тем же набором преимуществ, что и Группа двадцати – в частности, гибкостью в отношении определения повестки многостороннего сотрудничества и формулирования коллективных политически обязательных решений. В то же время, «пятерка» в значительной степени избавлена от проблем, связанных с внутренним согласованием приоритетов взаимодействия – в «двадцатке» наблюдается четкий разрыв между странами «глобального Севера» и ведущими представителями «глобального Юга», то есть преимущественно развивающихся стран; особенно сильно выделяется позиция стран-членов «Группы семи», пользующихся своим влиянием для продавливания решений в более широком формате «Группы двадцати», обеспечивая видимость глобального консенсуса между развитым и развивающимся миром в приоритетных областях. В данном контексте БРИКС следует рассматривать как идейно отличный институт, фокусирующийся на развитии многополярности и расширении представительства интересов развивающихся стран. Немаловажно и то, что в контексте роста геополитической напряженности последних лет страны-партнеры России по БРИКС выразили поддержку России и воспрепятствовали многочисленным попыткам отстранить ее от участия в решении глобальных вопросов.

Вопросы цифрового развития вошли в повестку БРИКС относительно недавно. В качестве самостоятельного блока указанное направление работы «пятерки» оформилось в 2015 г., в год второго председательства России в БРИКС, в рамках которого прошла первая встреча министров связи БРИКС. До этого момента указанная проблематика рассматривалась в качестве компонента широкой повестки научного сотрудничества[202].

Цифровая повестка востребована на платформе БРИКС – ретроспективный анализ повестки объединения говорит о том, что с точки зрения количества принимаемых решений сфера «ИКТ и цифровая экономика», куда органично входит проблематика управления Интернетом, относится к числу основных сфер сотрудничества, незначительно уступая вопросам борьбы с терроризмом, макроэкономической политики, региональной безопасности, международной торговли и содействия развитию.

Примеры принятых решений и согласованных коллективных инициатив стран БРИКС в ключевых областях управления Интернетом

Сфера	Принятые решения (примеры)
Инфраструктура	Мы обязуемся сосредоточить наши усилия на расширении всеобщего доступа ко всем средствам цифровой связи и на повышении информированности людей в этой области[203] (Уфа, 2015) Мы будем поощрять совместные исследования, разработки и инновации БРИКС в области ИКТ, включая следующие направления: Интернет вещей, облачные вычисления, большие объёмы данных, аналитика данных, нанотехнологии, искусственный интеллект и 5G, – а также их инновационное внедрение в целях совершенствования инфраструктуры ИКТ и повышения её взаимосвязанности в наших странах[204] (Сямэнь, 2017) Инициатива Компетенции Сети E-Port БРИКС (Сямэнь, 2017)[205] Мы продолжим принимать взаимовыгодные инициативы по шести направлениям сотрудничества, которые определены в Плане работы Партнёрства, в соответствии с договорённостями, принятыми на II Встрече Партнерства БРИКС по вопросам новой промышленной революции, состоявшейся в г. Бразилиа в сентябре 2019 года, включая создание промышленных и научных парков, инновационных центров, технологических бизнес-инкубаторов и сети коммерческих предприятий стран БРИКС[206] (Бразилиа, 2019) [Страны БРИКС предпримут следующие действия:] расширение сотрудничества стран БРИКС в области программного обеспечения и ИКТ-оборудования, а также реализация проектов в этой области[207] (Москва, 2020)

Правовые вопросы	Мы будем поддерживать выработку признанных на международном уровне и приемлемых для всех заинтересованных сторон правил в области безопасности инфраструктуры ИКТ, защиты данных и Интернета, совместно строить надёжную и безопасную сеть[208] (Сямэнь, 2017) Мы вновь заявляем о важности расширения сотрудничества в рамках «пятёрки», в том числе посредством рассмотрения соответствующих инициатив и реализации дорожной карты практического сотрудничества стран БРИКС в обеспечении безопасности в сфере использования ИКТ[209] (Москва, 2020)
Экономика	Мы будем действовать на основе таких принципов, как инновации, партнёрство, синергия, гибкость, открытая и благоприятная деловая среда, доверие и безопасность, а также защита прав потребителей в целях обеспечения условий для процветания и динамичного развития цифровой экономики, что будет способствовать глобальному экономическому развитию и приносить пользу каждому[210] (Сямэнь, 2017) + Инициатива сотрудничества в сфере электронной торговли БРИКС[211] (Сямэнь, 2017) [Учитывая ускоренное развитие сектора электронной торговли и рост объёма онлайн-транзакций во всем мире], мы будем углублять наше сотрудничество в рамках рабочей группы БРИКС по электронной торговле[212] (Москва, 2020)
Развитие	Мы заявляем о нашей приверженности сокращению цифрового и технологического разрыва, в частности, между развитыми и развивающимися странами[213] (Гоа, 2016) [Страны БРИКС предпримут следующие действия:] решение проблемы цифрового разрыва путем преодоления неравномерности в доступе населения стран БРИКС к цифровой инфраструктуре, навыкам и услугам, а также повышение цифровой инклюзивности населения, проживающего в сельских районах, а также людей с ограниченными возможностями, посредством совершенствования доступа к Интернету и повышения взаимосвязанности населения[214] (Москва, 2020)

Социокультурная компонента	[Страны БРИКС предпримут следующие действия:] разработка программ цифровой грамотности для гармоничной и инклюзивной адаптации населения стран БРИКС (Москва, 2020)[215] [БРИКС, 2020]

К наиболее востребованным областям сотрудничества БРИКС в вопросах управления Интернетом следует отнести развитие цифровой инфраструктуры и общие экономические вопросы. Превалирование вопросов развития инфраструктуры и экономических аспектов сложилось во многом под влиянием Китая, что обусловлено его экономическим весом. Несмотря на то, что объединение БРИКС уже в существенной степени отошло от исходного посыла как объединения быстрорастущих экономик, и его повестка носит плюралистический характер, вопросы экономического сотрудничества сохраняют свою значимость. Китай стал инициатором ряда инициатив и решений БРИКС по вопросам развития цифровой инфраструктуры, что согласуется с декларируемыми и последовательно реализуемыми приоритетами национального развития этой страны. Предлагаемая Китаем повестка, в свою очередь, встречает поддержку со стороны стран-партнёров по БРИКС.

Другой важной особенностью повестки БРИКС в рассматриваемой области является наблюдаемый рост интереса к вопросам обеспечения сетевой безопасности с особым вниманием к противодействию терроризму и экстремизму. Данная проблематика была введена в повестку усилиями Российской Федерации в год очередного председательства и встретила определённую поддержку со стороны стран-партнёров. Опыт анализа исторической динамики развития повестки БРИКС говорит о востребованности российских инициатив, однако, в отличие от инфраструктурного блока, подходы к обеспечению сетевой безопасности, в том числе к контролю над распространяемой в сети информацией, в странах БРИКС различаются, что может препятствовать выработке новых комплексных решений.

БРИКС может внести существенный вклад в процесс формирования международного режима обеспечения кибербезопасности в ча-

сти формулирования основных принципов сотрудничества, а также, вероятно, в создание механизмов обеспечения доверия в глобальном масштабе. Данное утверждение основывается на положительном опыте в деле институционального развития, примером чего является создание Нового банка развития, а также на результатах ретроспективного анализа повестки БРИКС, который говорит о высокой способности объединения принимать и исполнять коллективные решения в приоритетных областях сотрудничества, в частности, в области развития ИКТ и кибербезопасности.

Включение развивающихся государств в состав членов форума закрепляет образ БРИКС как представителя глобального Юга на мировой арене. При этом углубление взаимодействия в области преодоления цифрового разрыва способно стимулировать сотрудничество и на уровне координации внешней политики, в том числе в области цифрового суверенитета и международной информационной безопасности. Расширение БРИКС создаёт позитивные ожидания в части масштабирования принимаемых решений в области управления Интернетом на страны вне объединения, в основном за счёт привлечения развивающихся государств.

2.3. Неправительственные участники управления Интернетом

2.3.1. Корпорация по присвоению доменных имён (ICANN) и её дочерняя структура PTI

ICANN – это «некоммерческая общественная корпорация, участники которой стремятся обеспечить безопасность, стабильность и функциональную совместимость Интернета. Благодаря своей координирующей роли ICANN оказывает «существенное влияние на расширение и развитие Интернета»[216].

В техническом плане интернет-корпорация по присвоению имён и адресов ICANN является учредителем юридического лица PTI, которая выполняет функции Администрации адресного пространства Интернета (IANA), предоставляющей ключевые услуги для работы системы доменных имён. Функции IANA включают в себя:

- координацию работ по выработке технических параметров интернет-протоколов;

- управление доменными именами (управление корневыми DNS, доменами .INT и .ARPA и ресурсами IDN, создание новых доменов верхнего уровня);
- управление ресурсами нумерации Интернета (координация глобального пула IP-адресов и автономных номеров).

В своей деятельности ICANN опирается на два основных инструмента: рыночный и делиберативный. Этому есть две причины: во-первых, цель создания организации заключается в демонополизации рынка интернет-услуг; во-вторых, общественно-политическая повестка формируется «снизу вверх». Таким образом, политика ICANN основывается на поиске консенсуса с участием многих заинтересованных сторон.

2.3.2. Организации технического сообщества

«Общество Интернета» (ISOC)[217]

В настоящее время «Общество Интернета» (Internet Society, ISOC) можно рассматривать в качестве ключевого института в системе управления Интернетом, ответственного за поддержание единообразия и развитие технологической базы всемирной сети.

«Общество Интернета» было создано в 1992 году группой энтузиастов, входивших в состав членов Инженерного совета Интернета. Исходная задача ISOC была сформулирована как «обеспечение институциональной основы и финансовой поддержки процесса развития стандартов Интернета»[218]. Развитие экосистемы Интернета, потребность в организации региональных представительств для поддержания единообразия в разработке и внедрении новых технологических стандартов и регламентов потребовали расширения финансирования сверх возможностей государственных программ.

Основная декларируемая цель ISOC остаётся практически неизменной на протяжении всей истории общества – «Интернет для всех», под чем подразумевается максимальное расширение географии доступа к всемирной сети, сохранение децентрализованного характера управления Интернетом, поддержка инициатив, связанных с расширением доступа к Интернету, на уровне местных сообществ[219].

ISOC на постоянной основе публикует множество документов, освещающих те или иные аспекты развития Интернета. Формирующиеся на их основе технические руководства не обладают фор-

мальным статусом, а также не предполагают создания формализованных механизмов мониторинга и оценки. К публикуемым ISOC документам относятся RFC (Request For Comments, «запросы на комментарии») – то есть технические стандарты Интернета, планы действий, глобальные отчеты о развитии Интернета, аналитические материалы, а также списки наилучших практик в области сетевой безопасности, составляемые подотчетным обществу Альянсом за доверие в Сети (OTA).

ISOC как спонсор деятельности рабочей группы проектирования Интернета и исследовательской рабочей группы Интернета обладает авторскими правами на все опубликованные RFC и сформированные на их основе стандарты Интернета.

Стандарты Интернета не относятся к юридически обязательным документам, однако высокая важность стандартов Интернета для поддержания его бесперебойной работы позволяет рассматривать их в качестве некой разновидности «мягкого права» – к такому выводу также приходит известный юрист Лоуренс Лессиг[220]. Стандарты Интернета, утверждаемые организациями «Общества Интернета», признаются в качестве универсальных в каждом сегменте мирового Интернета. Учитывая, что роль Интернета в современном производстве, связи и государственном управлении является определяющей, формируемые «Обществом Интернета» стандарты Интернета фактически носят безальтернативный характер.

В силу того, что стандарт подразумевает некую форму контроля над технологией, в некоторых работах[221] решения, связанные с их формулированием и утверждением, расцениваются как политические. Государства, заинтересованные в усилении конкурентоспособности национальных компаний, могут поднять изначально техническую проблему до уровня международной политической дискуссии. Стандартизация приносит неоспоримые выгоды, однако даже неформальное утверждение «де-факто» того или иного стандарта в качестве международного и общепринятого так или иначе будет более выгодно одним сторонам и ограничивать возможности других[222]. Здесь мы вновь можем обратиться к понятию навязанного режима и привести в качестве примера режим регулирования технических вопросов управления Интернетом, сложившийся под влиянием правительства США и преимущественно американского и европейского сообщества инженеров, по сей день составляющих основу руководящих кадров организаций в системе «Общества Интернета».

2.3.3. Бизнес в системе управления Интернетом

В отличие от других пространств, территориализация Интернета предполагает первоначально «овеществление», создание территории, так как кибертерритория не является данностью. В этом процессе ведущую роль играют негосударственные акторы – представители бизнеса и интернет-сообщества. Именно в результате деятельности бизнеса формируются новые форматы использования Интернета, новые площадки для взаимодействия пользователей, причём следует отметить высокий динамизм бизнес-активности на этом направлении.

Наиболее значимым последствием развития Интернета стало формирование новой платформенной экономики. В современных условиях всё большее значение приобретают наукоёмкие отрасли, завязанные на новые ИКТ и Интернет, а вопросы цифрового суверенитета становятся одним из определяющих.

Согласно отчету DinarStandard, 370 крупнейших «цифровых платформ» в мире, представляющих предполагаемый годовой доход в размере 1,87 триллиона долларов США и 371 миллиард среднемесячных пользователей в 2022 году[223].

Цифровые платформы, базирующиеся в США, доминируют в мировом охвате и доходе со значительным отрывом. Китай, второй по величине, представляет только 3% мирового охвата, за ним следуют Россия, Япония и Южная Корея[224].

В самом широком смысле под платформенной экономикой понимается новая парадигма социально-экономического развития, напрямую связанная с распространением цифровых платформ и экосистем. Они становятся драйверами инновационной активности, качественных преобразований социальной сферы, ключевым фактором успеха предпринимательской деятельности и конкуренции между компаниями за потребителей и поставщиков продукции и услуг.

На российском рынке развиваются более десятка цифровых платформ и экосистем. Без крупных отечественных игроков (Wildberries, «Авито», Ozon, «AliExpress Россия», «Сбер», «СберМаркет», ВТБ, Тинькофф, «Яндекс», VK, «Лаборатория Касперского», «1С», ЦФТ, HeadHunter и др.) сегодня уже немыслимо функционирование многих секторов экономики. В 2021 году суммарный торговый оборот крупнейших российских маркетплейсов и агрегаторов – «Яндекса», Wildberries, Ozon, «Ali-

Express Россия» и «СберМаркета» – достиг 2,5 триллиона рублей. Экосистемы вносят весомый вклад в обеспечение устойчивости экономики, в том числе за счет динамичности, адаптивности, разнообразия сервисов, гибкости и вариативности форм взаимоотношений между сторонами[225].

Важно отметить нарастающую роль бизнеса в управлении глобальным цифровым пространством. В 2025 году к власти в США вновь пришел президент Дональд Трамп, который делает ставку на крупный бизнес, прежде всего, в сфере высоких технологий.

В США усиливаются позиции глобальных технологических корпораций Big Tech, которые претендуют на мировое влияние, не ограничиваясь масштабами государства. Государственная поддержка амбиций высокотехнологического сектора в США усиливается на фоне роста технологической конкуренции с КНР. Так, в 2025 году в США запланировано создание компании Stargate для развития инфраструктуры искусственного интеллекта. Будет построена «физическая и виртуальная инфраструктура для поддержки следующего поколения ИИ», включая центры обработки данных по всей территории США. Первый объект по обработке данных уже строится в Техасе. Три компании (OpenAI, SoftBank и Oracle) вложат в проект 100 миллиардов долларов, в ближайшие годы инвестиции увеличатся до 500 миллиардов, будут созданы 100 тысяч новых рабочих мест в США[226].

Вопросы растущего влияния технологических гигантов уже давно стоят на повестке дня. В США большая пятёрка технологических гигантов включает в себя Microsoft, Amazon, Meta (признана в России экстремистской организацией), Alphabet и Apple. Из небольших IT-компаний они достаточно быстро выросли до корпоративных гигантов, совокупная капитализация которых в 2022 году достигла 8 триллионов долларов (больше, чем ВВП большинства стран «Группы двадцати»)[227]. В настоящее время к ним прибавились компании Илона Маска и Open AI Сэма Альтмана.

Трамп неоднократно критиковал чрезмерное регулирование, утверждая, что излишние ограничения на ИИ могут навредить росту бизнеса и технологическому прогрессу. Поэтому можно ожидать снижения регуляторного давления на высокотехнологичный бизнес при попытке закрытия цифровой сферы и нарастающей конкуренции с КНР. США ввели односторонние технологические санкции в отношении КНР, а КНР ввела встречные рестрикции по редкоземельным металлам.

По мере роста влияния правых взглядов в США будет возрастать и «спайка» государства с высокотехнологичными компаниями. Яркий

тому пример – все лидеры BigTech присутствовали на инаугурации Дональда Трампа в 2025 году.

При этом можно ожидать снижения регуляторного давления на эти компании даже со стороны европейских регуляторов и их более агрессивную политику по захвату и контролю внешних рынков. Снижение регулирования контента социальных сетей и отказ от внимания к интересам других стран будет означать, с одной стороны, стремление США к конкуренции с высокотехнологичными компаниями КНР, а с другой – насаждение правил мира «дикого Запада» в социальных сетях и ИИ, контролируемых американскими компаниями.

КНР также делает акцент на развитие цифровых технологий. Для китайских инноваций и IT-индустрии патриархом является Джек Ма, основатель корпорации «Алибаба». Инновационные подходы, колоссальный масштаб китайского рынка, а также государственная политика протекционизма позволили «Алибаба» вытеснить американские компании с внутреннего рынка – сначала был создан «Таобао» (фактически дублирующий eBay), затем Tmall (копия Amazon), а в 2010 появилась торговая площадка AliExpress, которая совмещала различные форматы и была ориентирована на завоевание мирового рынка.

Прошедшее десятилетие часто называют золотой эрой развития китайского технологического сектора. Многие компании за короткий срок из небольших стартапов выросли в международных технологических гигантов. Еще в 2020 году шесть из десяти крупнейших мировых компаний-единорогов (с капитализацией свыше 1 миллиарда долларов) были китайскими. Компания ByteDance по-прежнему сохраняет статус самого дорогого стартапа мира с капитализацией 140 миллиардов долларов. Однако 2021 год стал поворотным моментом для развития китайского Big Tech: на фоне ужесточения регулирования технологический сектор в Китае за год потерял около 2 триллионов долларов капитализации. И хотя в текущих экономических условиях Пекин сделал определённые поблажки для технокомпаний, долгосрочный тренд на жёсткое регулирование сектора, вероятно, сохранится[228].

Другой двигатель «цифровизации с китайской спецификой» – компания «Тенсент». Её главный актив – интернет-мессенджер WeChat («Вэй-синь»), он появился еще в 2010 году, когда в КНР был популярен местный аналог ICQ – QQ. В настоящее время «Вэй-синь» для китайских пользователей предлагает очень

широкий функционал и заменяет телефон, СМИ и социальные сети, мини-программы, интегрированные в WeChat, позволяют совершать покупки, вызывать такси, заказывать еду, арендовать велосипед. Аккаунт в мессенджере привязан к банковскому счёту.

По мнению И. Зуенко, успех частного капитала во введении цифровых платежей привёл к тому, что с 2019 года государство занимается развитием «цифрового юаня», ставшего первой в мире государственной криптовалютой, которая в перспективе позволит совершать платежи, не требующие транзакций через платежные системы типа SWIFT, и даст цифровому юаню возможность составить конкуренцию доллару в качестве мировой валюты, особенно в расчётах между Китаем и теми странами, которые находятся под западными санкциями[229].

В КНР сделана ставка на суверенное развитие IT-отрасли и цифровой суверенитет. Это предполагало государственную поддержку цифровых компаний. Практически все крупнейшие технологические компании Китая – Alibaba, Tencent, Huawei, Inspur и т.д. – пользовались статусом эксклюзивного партнёра в одной, а то и нескольких провинциях Китая и становились практически монопольным поставщиком товаров и услуг, на которых они специализировались. Кроме того, эти же компании получали и значительные субсидии от местных властей, которые иногда покрывали более 30% от их издержек[230].

В КНР заблокирован Google, не работают YouTube, Instagram, Facebook, X и многие другие популярные на Западе интернет-ресурсы. В Китае есть внутренняя версия TikTok (DouYin), а международный заблокирован.

Во внешней политике Китай противопоставляет международным отношениям прошлого идею о «сообществе единой судьбы человечества», и в перспективе политика Пекина в отношении ИИ и больших данных не сводится к технологической конкуренции с США, но ставит задачу перестроить подход к государственному управлению и регулированию цифровой сферы в целом. Китай стремится к созданию новой модели, гораздо более справедливой, построенной не на стремлении к наживе, а на гармоничном распределении прав и обязанностей[231].

Важную роль играют и сами пользователи, которые либо поддерживают существующие цифровые площадки, либо создают новые. Цели, преследуемые сообществами пользователей, как правило, лежат в ценностной плоскости – чаще всего это свобода доступа к информации (в качестве примера можно привести движение «Пиратский интернационал», который ставит задачу свободного доступа ко всей информации, защищённой авторским правом). Ценности носят трансграничный характер, поэтому на онтологическом уровне новые цифровые территории, создаваемые пользователями, необязательно совпадают с государственными границами. Однако сообщества пользователей всё же обладают меньшим влиянием по сравнению с бизнес-структурами в силу того, что у них нет возможности влияния ни на инфраструктурном, ни на функциональном уровнях; их главный ресурс – это данные, которые в результате их деятельности агрегируют цифровые платформы. Пользователи вынуждены выбирать между интернет-площадками, созданными бизнес-структурами.

В свою очередь крупные компании, владеющие цифровыми платформами, имеют возможности создания цифровых границ информационных экосистем на всех уровнях – контроль инфраструктуры, программного обеспечения и контента, а также возможность управлять предпочтениями и поведением пользователей информационных услуг. Тем не менее, в политической области у них нет влияния, сопоставимого с государствами, и поэтому они практически не принимают участия в дискурсе о границах в Интернете. Доминирующее положение государств в дискурсе объясняется растущим количеством угроз информационной безопасности в силу того, что государства обладают монополией на легитимное насилие и таким образом могут гарантировать безопасность цифровых границ.

Бизнес преследует цели получения выгоды, поэтому заинтересован в расширении рынков сбыта, т.е. в информационной глобализации. Именно бизнес-активность играет существенную роль в увеличении объёма трансгранично передаваемых данных – прежде всего, речь идёт о деятельности глобальных цифровых платформ (таких как компании группы BATX – Baidu, Alibaba, Tascent, Xiaomi). Как отмечают авторы доклада ЮНКТАД о цифровой экономике за 2021 год, крупные IT-компании имеют возможность управлять огромными цифровыми экосистемами, зачастую ставя под вопрос возможности суверенного контроля отдельных государств над потоками данных, которые пересекают их границы[232].

В 2019–2020 гг. в связи с ограничительными мерами, принятыми США в отношении китайской компании Huawei, китайских социальных медиа TikTok и WeChat[233], наметился новый виток фрагментации Интернета, обусловленный конкуренцией между двумя наиболее технологически развитыми странами – США и Китаем[234]. Это в очередной раз продемонстрировало сложный и неоднозначный характер отношений крупных государств с IT-компаниями. Французский исследователь Ж. Носетти полагает, что «роль этих частных предпринимателей напоминает роль, которую в Европе XVII и XVIII веков играли ост-индские компании: они то объединялись, то соперничали с европейскими государствами, а иногда и полностью игнорировали законодательство последних»[235].

При этом наиболее крупные компании базируются в США и Китае. Согласно статистике ЮНКТАД, на компании, штаб-квартиры которых находятся в этих двух странах, в 2019 году приходилось 90% рыночной капитализации всех цифровых платформ. Как отмечает Д. Фаррелл, «государства используют крупные IT-компании как «точки контроля» над поведением пользователей или других негосударственных акторов» (Farrell 2012: 361), таким непрямым образом укрепляя своё влияние внутри цифровых границ. Компании соглашаются на это, опасаясь коммерческих издержек, связанных с конфронтацией с правительствами стран. Однако интересы государств и бизнеса всё же лежат в различной плоскости, что во многом объясняет расхождение дискурсивного и онтологического уровней цифровых границ. Важнейшим элементом формирования цифровых границ является легитимация власти государства над определённой «цифровой территорией», при этом важным легитимирующим фактором на дискурсивном уровне выступает секьюритизация глобального информационного пространства и рост угроз информационной безопасности. На уровнях данных и инфраструктуры, а также программного обеспечения главным субъектом глобализации выступает бизнес.

*****

Интернет тесно вписан в международно-политический контекст, и природа международной политики оказывает существенное влияние на характеристики глобальной сети. Современная международная система характеризуется многополярным характером, а также

растущей напряжённостью между ключевыми центрами силы. Формирование универсального и инклюзивного режима управления Интернетом, основанного на учёте интересов всех государств и уважении государственного суверенитета, становится важным фактором международной стабильности и безопасности. Обращаясь к историческим аналогиям, можно вспомнить эволюцию международных режимов в других высокотехнологичных областях мировой политики, таких как космос или режим контроля над ядерными вооружениями, в рамках которых в результате длительных переговоров были сформированы универсальные договорённости, основанные на учёте интересов всех государств и уважении государственного суверенитета. Как представляется, перспективные тенденции развития международного режима управления Интернетом также будут развиваться в данной плоскости.

ГЛАВА 3
ПРОБЛЕМНЫЕ ОБЛАСТИ УПРАВЛЕНИЯ ИНТЕРНЕТОМ

3.1. Международно-политический контекст режима управления Интернетом

3.1.1. Международное право и цифровой суверенитет в Интернете

Международное право уже содержит ряд положений относительно государственного суверенитета, которые если не по букве, то, по сути, вполне применимы к глобальному информационному пространству и к проблематике управления Интернетом.

Статья 2 Устава ООН 1945 года определяет принцип суверенного равенства государств как основополагающий принцип международного права. По смыслу Декларации о принципах международного права и Хельсинского акта 1975 года каждое государство имеет право на обеспечение своей безопасности, не нанося ущерба безопасности других государств. Как представляется, данные права и обязанности, вытекающие из суверенитета, также в полной мере применимы к интернет-пространству. Проявлением суверенного равенства государств является иммунитет каждого из них от юрисдикции другого государства. Однако пространственные пределы государственного суверенитета в сети Интернет в настоящее время не определены. Авторитетный российский юрист А.А. Стрельцов отмечает, что ИКТ-среда как объект международных отношений представляет собой юридическую фикцию, которая заключается в том, что соответствующая совокупность устройств и средств связи, локальных вычислительных сетей, информационных систем, существующих в пространстве цифровых идентификаторов и протоколов их взаимодействия, а также субъектов обеспечения согласованного функционирования выделенных устройств, средств, сетей и систем в составе глобальной ИКТ-среды, рассматривается как составляющая территории государства, что позволяет распространить на ИКТ-среду понятия «суверенитет государства» и «юрисдикция государства» (Стрельцов 2017). Ряд технических возможностей современных цифровых технологий осложняет однозначное соотнесение данных, программного обеспечения и др. с территорией определённого государства и не позволяет дать однозначного определения данной категории. Делимитация цифровых границ государства также затруднена в условиях значительного объёма трансграничных данных (UNCTAD, 2021; Зиновьева, 2022).

Трансгранично передаваемая информация регулируется в рамках ещё одной отрасли международного публичного права – права массовой информации. В частности, распространяемая трансгранично информация не должна представлять собой вмешательство во внутренние дела суверенных государств. При этом независимость средств массовой информации не должна отрицать принцип международной ответственности государств за деятельность своих национальных СМИ на трансграничном уровне. Провозглашенное во Всеобщей декларации прав человека и гражданина 1946 года право искать, получать и распространять информацию и идеи независимо от государственных границ (ст. 19), не является абсолютным и ограничено правом государства в законодательном ограничении свободы информации для охраны национальной безопасности, здоровья и нравственности населения, провозглашенном в ст. 19 Международного пакта о гражданских и политических правах 1966 года. Как представляется, подобный подход в полной мере применим к современным цифровым СМИ и, более того, может быть основой для обсуждения на международном уровне международных норм и правил, регламентирующих деятельность глобальных цифровых платформ и IT-гигантов. Однако данные нормы права не дают ответа на вопрос о проведении границ государства в цифровой среде.

Таким образом, в международном праве уже заложены основы для дальнейшего развития принципа государственного цифрового суверенитета в соотнесении с принципом невмешательства во внутренние дела и предотвращением международных конфликтов.

Однако в последние годы расширяется практика вторжения в информационное пространство различных стран как со стороны других государств, так и со стороны негосударственных акторов, причём мотивы такого вмешательства (сбор информации, воздействие на информационную политику страны, нарушение работы информационных инфраструктур) достаточно сложно определить. В литературе подобная ситуация получила название «цифровой дилеммы безопасности» и широко представлена в трудах российских и зарубежных авторов[236]. В целом подобная ситуация способствует дестабилизации международной безопасности, усиливая взаимное недоверие государств и подталкивая их к односторонним действиям в информационной сфере, что в свою очередь актуализирует необходимость международного сотрудничества в области информационной безопасности, основанного на принципах уважения государственного суверенитета.

Несмотря на отдельные правовые лакуны и терминологические разночтения, цифровой суверенитет уже стал неотъемлемой частью политической и академической риторики, различные трактовки и подходы к данной категории находят отражение в официальных документах государств и международных организаций.

Цифровой суверенитет, под которым в самом широком смысле понимается независимость государства во внутренней и внешней политике в цифровой сфере, становится важнейшим мерилом состоятельности государства, безопасности и экономического потенциала. Особенности цифровых технологий, в том числе трансграничный характер, доступность и анонимность, существенно осложняют проведение аналогий между территориальным и цифровым суверенитетом, но не делают обеспечение суверенитета и защиту юрисдикции государств в цифровой среде невозможной.

При этом подходы к определению и содержанию понятия «цифровой суверенитет», предлагаемые в научной литературе и в официальных документах различных государств и международных организаций, существенно различаются, что отражает различные особенности политической культуры, уровня цифровизации и внешнеполитических приоритетов стран и регионов. Появляются новые подходы и термины, такие как «цифровой суверенитет личности» или «суверенитет данных». В академической литературе КНР широко используется термин «интернет-суверенитет», российские авторы чаще обращаются к термину «информационный суверенитет».

При этом внимание к суверенитету в практике международных отношений, помимо экономической целесообразности, обусловлено необходимостью обеспечить национальную и международную безопасность, также важную роль играет проблема «цифрового невмешательства».

Цифровые технологии трансграничны, но в политической сфере мир разбит на суверенные государства. В этих условиях суверенитет может выступить в роли общего знаменателя, необходимого для дальнейшего развития международного сотрудничества в сфере обеспечения информационной безопасности при уважении интересов всех государств.

В условиях глобальной цифровой трансформации категория государственного суверенитета дополняется новым цифровым измерением. Цифровой суверенитет, под которым в самом широком смысле понимается независимость государства во внутренней и внешней

политике в цифровой сфере, становится важнейшим мерилом состоятельности государства, безопасности и экономического потенциала. Для лучшего понимания природы цифрового суверенитета необходимо обратиться к концептуальным основаниям самого понятия «государственный суверенитет».

Исследования суверенитета восходят к работе Ж. Бодена «Шесть книг о республике» 1575 года, где он определяет суверенитет как «наивысшую, абсолютную власть над гражданами и подданными», которой обладает монарх как представитель Бога на земле (цит. по: Марченко, 2016). Изначально категория государственного суверенитета была тесно связана с контролем над определённой территорией. Важный вклад в становление теории суверенитета в политической и юридической науках внесли труды Гуго Гроция, Т. Гоббса, Дж. Локка.

В политической науке сложился консенсус, согласно которому суверенитет стал играть определяющее значение в мировой политике после 1648 года, когда был подписан Вестфальский мирный договор, заложивший основы Вестфальской политической системы мира, которая сохраняет своё значение до сих пор. Суверенитет, понимаемый как как полнота власти государства внутри границ и независимость на международной арене, стал важнейшим общим знаменателем, определяющим равенство государств в мировой политике и международном праве (Лебедева, 2009). И хотя дискуссии о трансформации и размывании суверенитета были популярны в 1990-е и в 2000-е годы (Krasner, 1999), в настоящее время признаётся, что суверенитет является важнейшим и неотъемлемым свойством государства.

Важно отметить, что суверенитет никогда не был статичной категорией, он эволюционировал и включает в себя не только территориальный суверенитет, но и суверенитет в области территориальных вод, воздушного пространства государства, валютный суверенитет и ряд других компонентов.

На современном этапе технологического развития важнейшее значение приобретает суверенитет в области цифровых технологий. Внимание к цифровому суверенитету обусловлено радикальной трансформацией экономического и технологического укладов, общественных отношений и политической жизни, вызванной глобальной цифровой трансформацией. Эти изменения проявились и в сфере международных отношений – цифровое пространство стало полем геополитических противоречий, а уровень цифровизации становится важным фактором, определяющим положение страны на

международной арене и спектр доступных ей внешнеполитических возможностей.

Возрастает экономическая значимость способности эффективного развития при обеспечении надлежащего уровня безопасности в цифровой сфере.

Исследования в области цифрового суверенитета тесно связаны с анализом технологического суверенитета, под которым понимается обеспечение независимости в научных разработках, определении стандартов, безопасности физической инфраструктуры связи (Crespi, 2021). Кроме того, многие авторы увязывают проблематику цифрового суверенитета с вопросами обеспечения информационной безопасности (Tikk, Kerttunen, 2020). Отдельным вопросом стоит проблема цифрового вмешательства как нарушения суверенитета государств, причём эта проблематика рассматривается как российскими (Зиновьева, Булва, 2021), так и зарубежными учёными. Также необходимо упомянуть взаимосвязь с исследованиями в области технологических укладов, которые проводятся в рамках экономических наук и подчёркивают экономический потенциал цифровых технологий в рамках перехода к Четвёртой промышленной революции (Schwab, 2017; Глазьев, 2010).

Существуют терминологические разночтения. Так, например, в российском академическом дискурсе чаще используется термин «информационный суверенитет», призванный подчеркнуть важность контроля не только над технической инфраструктурой в целях обеспечения суверенитета, но и над трансграничным контентом. Западные авторы преимущественно оперируют терминами «цифровой суверенитет» или «киберсуверенитет», которые рассматриваются через призму государственной юрисдикции над инфраструктурой, программным обеспечением и данными и в меньшей степени затрагивают проблемы контроля над трансграничными потоками информации.

Среди российских авторов проблему информационного суверенитета изучали М.М. Кучерявый (Кучерявый, 2014), А.А. Сергунин (Сергунин, 2010), Н.В. Стариков (Стариков, 2010), В.Н. Супрун (Супрун, 2010), В.В. Бухарин (Бухарин, 2016). Они рассматривали суверенитет через призму угроз в сфере информационной безопасности. Д.В. Винник связывает цифровой суверенитет с политическими и правовыми режимами обработки данных в Интернете (Винник, 2014: 97). М.М. Кучерявый определял информационный суверенитет как верховенство и независимость государственной власти при формировании и реализации информационной политики в национальном

сегменте и глобальном информационном пространстве (Кучерявый, 2014). Российский автор В.В. Бухарин выделяет следующие компоненты информационного суверенитета России, «технически обеспечивающие национальную безопасность: поисковая система, социальные сети, операционная система и программное обеспечение, микроэлектроника, сетевое оборудование, национальный сегмент сети Интернет, платёжная система, собственные средства защиты, криптографические алгоритмы и протоколы, навигационная система» (Бухарин 2016).

Анализируя подходы европейских авторов, А.Н. Толстухина отмечает, что некоторые учёные полагают, что цифровой суверенитет можно интерпретировать как «необходимость для страны развивать или сохранять в отношении ключевых технологий собственную автономию или же иметь как можно более низкий уровень структурной зависимости». Другие считают, что это «способность страны (или группы стран) автономно генерировать технологические и научные знания или использовать технологические возможности, разработанные внешними игроками, за счёт активизации надёжных партнёрских отношений» (Толстухина 2022).

Особенностью европейского академического дискурса также является концепция цифрового суверенитета личности. Под цифровым суверенитетом личности понимается безопасность персональных данных и защита от негативного информационного воздействия и дезинформации, а также защита от практики «надзорного капитализма» со стороны IT-гигантов, под которым понимается сбор персональных данных и их последующее использование в целях воздействия на предпочтения пользователей (UNCTAD 2021).

По инициативе исследователей из КНР в академический дискурс было введено понятие «интернет-суверенитет» – права государства устанавливать собственные правила функционирования интернет-пространства, отвечающие национальным интересам и традициям (Zeng, 2017).

Необходимо отметить, что в научной литературе США долгое время критически относились к самой категории цифрового суверенитета, отмечая её связь с цензурой (Mueller, 2010). Более того, исследователи США долгое время продвигали идею, согласно которой Интернет является общим пространством человечества, по аналогии с открытым морем или космическим пространством, и на него не распространяется категория государственного суверенитета. Во внешнеполитическом дискурсе США такой подход до сих пор сохра-

няется. Однако в последние годы вопросы фрагментации Интернета и проблема вмешательства во внутренние дела США (тема, смежная с проблематикой суверенитета) занимают важное место в академическом дискурсе США (RAND, 2021) и политической риторике официальных лиц.

Таким образом, в научной литературе сложилось несколько различных подходов к определению содержания понятия «цифровой суверенитет», разнятся также и используемые термины. Во многом это обусловлено политическими противоречиями между странами, различиями в политических режимах и культурах государств, в уровнях развития цифровых технологий.

Важно также указать на ряд специфических особенностей цифровых технологий, которые не позволяют просто экстраполировать категорию суверенитета из реального в виртуальное пространство. К числу таких особенностей относится трансграничный характер потоков информации и данных, высокая роль частных компаний и отдельных пользователей в создании контента, сложность определения границ государственной юрисдикции в отношении данных и ряд других особенностей, которые должны быть приняты во внимание при определении сущностных характеристик концепции цифрового суверенитета в международных отношениях и в международном праве.

Цифровые технологии развиваются очень быстро, в частности, актуальной тенденцией последних нескольких лет стало формирование метавселенных, развитие технологий виртуальной и дополненной реальности, а также широкое распространение криптовалют. В 2022 году возросшая напряжённость вокруг независимости Тайваня поставила вопрос об автономном производстве компьютерных чипов на территории страны как важной составляющей технологического и цифрового суверенитета. После начала Специальной военной операции России на Украине в 2022 году западные интернет-платформы отказались предоставлять сбалансированную и объективную информацию о России и были заблокированы на территории страны, что показало важность наличия автономных интернет-платформ и контента как элементов информационного суверенитета.

В этих условиях представляется весьма релевантной концепция, согласно которой цифровой суверенитет по своей природе является нестатичной, динамической категорией. Как отмечает коллектив авторов под руководством В.А. Никонова, цифровой суверенитет явля-

ется эмержентным свойством государства как сложной системы и меняется наряду с развитием государственной политики и технологическим прогрессом (Никонов и др., 2021; Ребро, 2021).

3.1.2. Международная информационная безопасность

Интернет и социальные сети порождают новое пространство для международной конфликтности и конкуренции в силу того, что цифровые технологии – это важный стратегический ресурс и инструмент воздействия на противников и оппонентов в рамках «гибридных войн». США и страны НАТО рассматривают ИКТ-среду как новое поле боя – наряду с сушей, морским и воздушным пространствами и космосом. В 2010 году США объявили о создании кибервойск. В настоящее время активно идёт милитаризация ИКТ-среды, и такого рода инструменты создаются в структурах вооружённых сил многих государств. США также вовлечены в практику «когнитивных войн». В военных целях используются также и технологии искусственного интеллекта, значимой темой на международной повестке дня становится проблема регулирования смертоносных автономных систем и военной робототехники. Главной угрозой в данной области видится возможность эскалации цифровых противоречий между великими державами и их переход в реальную вооруженную конфронтацию. Таким образом, современные цифровые технологии и искусственный интеллект становятся важной составляющей глобального уравнения стратегической стабильности.

С начала проведения СВО число компьютерных атак на информационные ресурсы существенно увеличилось. Так, только за 2023 год совершено более 200 тысяч наиболее опасных компьютерных атак, уровень организации которых говорит о том, что к их планированию и проведению причастны зарубежные спецслужбы[237]. При этом на Украине при поддержке Запада сформировалось международное сообщество специалистов-хакеров для осуществления компьютерных атак на Россию, получившее название «IT-армия Украины». Также имеются сведения об организации там колл-центров для телефонного мошенничества в отношении российских граждан.

Россия ставит своей задачей мирное развитие глобальной ИКТ-среды. В Стратегии национальной безопасности Российской Федерации от 2021 года отмечается, что «информационное про-

странство активно осваивается как новая сфера ведения военных действий»[238]. Наибольшую угрозу для мира представляет военно-политическая составляющая информационной безопасности, однако именно преступное использование ИКТ несёт наибольшую опасность для мировой экономики. Как отмечается в статистических данных ООН, ущерб мировой экономики к 2025 году может составить 9 триллионов долларов[239]. Серьёзную опасность также представляет использование цифровых технологий в террористических целях. Террористические группировки и преступные организации активно пользуются «теневым Интернетом», через который осуществляется доступ к чёрным рынкам наркотиков и оружия. Мошенники воруют личные данные через Интернет, а террористы вербуют новых бойцов в свои ряды и распространяют свою человеконенавистническую идеологию[240].

Рис. 2. Ущерб от киберпреступлений.

Кроме того, существует угроза использования отдельными странами своего технологического доминирования в политических целях, в том числе как инструмент давления на развивающиеся страны.

В Основах государственной политики в области международной информационной безопасности от 2021 года[241] обозначены шесть приоритетных направлений угроз, которые могут быть сгруппированы в три большие группы, представленные на схеме.

Атаки на объекты критической информационной инфраструктуры государства		
Использование ИКТ в военно-политических целях	**Использование ИКТ в преступных целях**	**Использование ИКТ в террористических целях**
Stuxnet 2010	Colonial Pipeline 2021 Мясоперерабатывающая компания JBS 2021 CNA Financial 2021 Harris Federation 2021 Ущерб (ВЭФ): $6 трлн	Крайстчерский террористический акт 2019 Деятельность ИГИЛ в социальных сетях
Использование ИКТ в целях: 1. Ущемления суверенитета 2. Нарушения территориальной целостности 3. Осуществления государством действий в информационном пространстве, препятствующих поддержанию международного мира, безопасности и стабильности.	1. Неправомерная деятельность в отношении цифровой информации (включая персональные данные) и информационно-коммуникационных сетей 2. Создание и распространение вредоносных программ 3. Распространение неправомерной информации (порнографические изображения несовершеннолетних, призывы к самоубийствам, вовлечение несовершеннолетних в совершение противоправных действий) 4. Подстрекательство к вооруженной деятельности 5. Использование ИКТ для незаконного оборота наркотических средств, оружия, фальсифицированных лекарственных средств 6. Реабилитация нацизма, оправдание геноцида и преступлений против мира и человечности 7. Нарушение авторских и смежных прав	1. Пропаганда идеологии терроризма 2. Привлечение новых сторонников 3. Внутренняя коммуникация

Рис. 3. Триада угроз международной информационной безопасности[242].

В Стратегии национальной безопасности Российской Федерации от 2021 года информационная безопасность выделяется в качестве самостоятельной сферы нацбезопасности и стратегического национального приоритета[243].

Россия с 1998 года выступает с инициативами, направленными на выработку правил ответственного поведения государств в глобальном информационном пространстве. Достижением российской дипломатии стало инициирование и поддержание переговорного процесса под эгидой ООН (сначала в рамках группы правительственных экспертов (ГПЭ), включавшей в разное время от 15 до 25 государств, затем в рамках Рабочей группы открытого состава (РГОС), объединившей все 193 государства-члена ООН), укрепление диалога по мерам укрепления доверия в ОБСЕ, а также запуск переговоров по линии ШОС, БРИКС, СНГ, АСЕАН, со странами Африканского Союза, арабского мира и Латинской Америки.

Во многом благодаря усилиям России и Китая норма уважения государственного суверенитета в ИКТ-среде получила закрепление в ряде документов ООН. Важным вкладом в развитие нормативных оснований международной информационной безопасности стало принятие в 2018 году резолюции ГА ООН «Достижения в сфере информатизации и телекоммуникаций», в которой нашёл закрепление набор из 13 норм и принципов ответственного поведения государств, в том числе «суверенное равенство; разрешение международных споров мирными средствами таким образом, чтобы не подвергать угрозе международный мир и безопасность и справедливость; отказ в международных отношениях от угрозы силой или её применения как против территориальной неприкосновенности или политической независимости любого государства, так и каким-либо другим образом, несовместимым с целями Организации Объединённых Наций; уважение прав человека и основных свобод; невмешательство во внутренние дела других государств»[244].

На основании данной резолюции была сформирована рабочая группа открытого состава ООН по безопасному использованию ИКТ и самих ИКТ, которая приняла итоговый доклад в 2021 году и продолжила свою работу в формате второго созыва.

В 2023 году в ходе заседания комитетов ГА ООН были вынесены два проекта резолюции – российский, который предполагает продление работы РГОС на очередной, третий срок, а также французский, который ориентирован на создание нового переговорного механизма – Программы действий в области поощрения ответственного

поведения государств в ИКТ-среде. Фактически французская инициатива ориентирована на «подмену» переговорной площадки РГОС удобным для Запада форматом, который позволит продолжить обсуждать проблематику информационной безопасности в русле прозападных подходов, ориентированных на легитимацию военного использования ИКТ. Россия выступает за мирное развитие глобального информационного пространства путём формирования всеобъемлющего международно-правового режима информационной безопасности и принятия Конвенции ООН по международной информационной безопасности. Как показывают обсуждения в ООН, именно российский подход поддерживает большинство стран.

Под эгидой ООН реализуется российская инициатива о создании Глобального межправительственного реестра контактных пунктов для налаживания практического сотрудничества по вопросам реагирования на компьютерные инциденты[245].

Россия инициировала обсуждение выработки всеобъемлющей конвенции о противодействии преступному использованию ИКТ в рамках ООН в рамках созданного по предложению России профильного Специального комитета ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий (ИКТ) в преступных целях при Генеральной Ассамблее. Проект конвенции был предложен Россией и разрабатывался с участием 46 государств. В переговорах участвовали представители более 160 стран, включая экспертов из политических и правоохранительных структур.

24 декабря 2024 г. Генеральная Ассамблея ООН консенсусом одобрила разработанную по инициативе России Конвенцию против киберпреступности (полное название – «Конвенция против киберпреступности; Укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям»).

Принятый документ – итог пятилетней кропотливой работы государств-членов ООН. Он стал первым в истории универсальным международным договором в области информационной безопасности, подтвердил востребованность новых норм международного права для справедливого регулирования цифровой сферы в интересах всего мирового сообщества.

Конвенция призвана стать прочной основой для налаживания правоохранительного сотрудничества в противодействии использованию

информационно-коммуникационных технологий (ИКТ) в преступных целях. Нацелена на борьбу с несанкционированным доступом к электронным данным и их незаконным перехватом; подлогом, хищением или мошенничеством; отмыванием доходов от противоправных деяний; сексуальной эксплуатацией детей и надругательством над ними. Закрепляется цифровой суверенитет государств над своим информационным пространством, в том числе посредством наращивания международного взаимодействия между компетентными ведомствами.

В перспективе сфера охвата соглашения может быть расширена за счет разработки протокола по дополнительным составам преступлений. В фокусе – борьба с использованием ИКТ в террористических и экстремистских целях, а также торговля наркотиками и оружием.

Церемонию подписания Конвенции планируется провести в Социалистической Республике Вьетнам в 2025 году[246]. Документ нацелен на борьбу не только с хакерами, но и со всеми видами преступлений, совершаемыми при помощи ИКТ, и, в отличие от поддерживаемой странами Запада Будапештской конвенции Совета Европы от 2001 года, основан на принципе уважения государственного суверенитета в цифровом пространстве.

Наряду с ООН, российской дипломатией ведётся активная работа в области информационной безопасности в рамках СНГ, ШОС, ОДКБ; развивается двустороннее взаимодействие со странами-партнёрами, представителями мирового большинства.

3.1.3. Экологическая проблематика и «зелёный» Интернет

В настоящее время человечество настойчиво ищет новые модели экономики, которые бы учитывали устойчивость развития и экологические ограничения. «Зелёная» повестка в современном мире включает целый спектр компонентов: политических, экономических, экологических, климатических.

Невозможность продолжения роста на базе традиционного экономического развития становится всё более очевидной в связи с масштабной деградацией природных ресурсов и окружающей среды, быстро идущих климатических изменений в мире. Ответом стало формирование концепции устойчивого развития как новой парадигмы развития человечества в XXI веке[247].

Важный вклад в осмысление данной проблематики вносит доклад ЮНКТАД 2024 года. В докладе приводится впечатляющая ста-

тистика по различным аспектам влияния цифровых технологий на окружающую среду. Так, потребление электроэнергии 13 крупнейшими операторами центров обработки данных с 2018 года по 2022 год увеличилось более чем в два раза; список потребителей возглавила четвёрка крупнейших американских IT-компаний. По данным Международного энергетического агентства, в 2022 году объём потребления электроэнергии центрами обработки данных составил во всём мире около 460 тВт/ч (для сравнения, это больше, чем энергопотребление всей Франции в том же году).

Другой глобальной проблемой является рост отходов, связанных с цифровой трансформацией. За второе десятилетие XXI века объём отходов от экранов и мониторов, а также телекоммуникационного оборудования увеличился во всём мире на 30% – с 8,1 миллиона до 10,5 миллиона тонн. Причём цифровизация влияет на общий рост отходов не только напрямую, но и опосредованно, стимулируя дополнительное потребление через рекомендательные алгоритмы.

Эксперты ЮНКТАД отмечают, что цифровые технологии традиционно преподносятся как средство перевода реальных процессов в виртуальную среду в «облаках», что должно снизить нагрузку на окружающую среду. Однако эти ожидания не получают подтверждения, поскольку цифровизация в значительной степени опирается на материальный мир. Так, для производства компьютера весом 2 кг требуется 800 кг сырья. И здесь важно отметить ещё один интересный нюанс: необходимые металлы и минералы в значительной степени сконцентрированы в узкой группе стран. К примеру, 68% от мирового производства кобальта приходится на Демократическую Республику Конго, а 59% марганца – на Габон и Южную Африку. Данный фактор следует иметь в виду при анализе геополитических процессов современности.

Экологический след сектора ИКТ ещё больше повышают сложные цифровые технологии – блокчейн, искусственный интеллект, мобильные сети 5G и Интернет вещей. Почему это происходит? Потому что речь идёт не только об обработке уже существующих данных и обслуживании уже зарегистрированных пользователей, а о бесконечном создании новых, более сложных услуг и добавлении новых подключённых устройств, а также дальнейшем росте объёмов обрабатываемых данных в геометрической прогрессии.

В докладе приводится интересный факт. В ходе обучения GPT-3 (большая языковая модель, на которой основан ChatGPT) в центрах обработки данных в США было израсходовано 700 тысяч литров

питьевой воды для охлаждения. И это при отсутствии доступа к питьевой воде у огромного числа людей на планете! Эти цифры позволяют представить, каким масштабным является водный след современных цифровых товаров и услуг.

Всё чаще экологическая и зелёная проблематика рассматриваются как одна из проблем управления Интернетом. На конференции ООН по климату в Баку, КС-29, была принята декларация, в которой страны, компании и некоммерческие организации обязались использовать цифровые технологии для ускорения мер по борьбе с изменением климата. Одновременно с этим они будут сокращать выбросы углерода, бороться с загрязнением от технологического производства и решать проблему электронных отходов[248]. Генеральный секретарь МСЭ подчеркнула неразрывную связь между цифровой трансформацией и устойчивым развитием: «Технологические компании входят в число крупнейших покупателей возобновляемой энергии, а некоторые уже полностью перешли на неё. Устойчивая цифровая трансформация должна стать стратегическим приоритетом для всех стран»[249].

3.1.4. Цифровое неравенство и цифровой неоколониализм

Развитие Интернета отнюдь не влечёт за собой гомогенизацию и универсализацию мира. Ответом на стремительный рост объёма мировой информации и агрессивные глобализационные процессы стала сегментация цифрового пространства и разделение на множество закрытых и изолированных друг от друга сообществ. На смену государственным, географическим разграничениям приходят новые информационные границы.

Развитие Интернета создаёт новые линии неравенства между «инфо-богатыми» и «инфо-бедными», что порождает новые линии противоречий на международной политической арене. Речь идёт о проблеме так называемого цифрового разрыва[250].

Цифровой разрыв — это не только экономическая проблема, но и важный фактор международной безопасности и стабильности. Необходимыми условиями преодоления цифрового разрыва являются помощь в развитии и международное сотрудничество, направленное на выработку правил ответственного поведения государств в глобальной информационной среде.

Как отмечают эксперты Всемирного экономического форума, сегодня проблема неравномерного доступа к ИКТ — это основное препят-

ствие для достижений Целей устойчивого развития ООН. В докладе ЮНКТАД о цифровой экономике за 2021 год подчеркивается, что по мере роста значения данных в цифровой экономике появляются новые измерения проблемы цифрового разрыва, связанные с ростом значения данных в современных глобальных цепочках создания добавленной стоимости. В докладе даже предложен новый термин — «неравенство в области данных», которое авторы определяют как разрыв в доступе к источникам данных и к программным возможностям обработки данных между развитыми и развивающимися странами.

Если в 1990-х и начале 2000-х гг. цифровой разрыв воспринимался как искусственно навязанная международному сообществу крупными западными IT-гигантами проблема с целью расширить свои рынки сбыта, то сегодня ни у кого не вызывает сомнений её высокая значимость, которая находит отражение на различных уровнях мировой политики и мировой экономики. Так, например, в докладе ЮНКТАД 2024 года отмечается, что развивающиеся страны несут основную тяжесть экологических издержек цифровизации, получая при этом меньше выгод. Они экспортируют сырье с низкой добавленной стоимостью и импортируют устройства с высокой добавленной стоимостью, а также увеличивают цифровые отходы. Геополитическая напряжённость из-за критически важных минералов, которыми изобилуют многие из этих стран, усложняет проблемы[251].

3.2. Новые вызовы в сфере управления Интернетом

3.2.1. Развитие искусственного интеллекта

Под ИИ понимают реализацию вычислительным устройством присущих человеческому мозгу мыслительных процессов. Разработка методов ИИ началась в середине прошлого века, однако их прикладное внедрение стало возможным лишь в конце 2010-х гг. В настоящее время подавляющее число разработок в ИИ, помимо генеративных моделей, можно отнести к следующим категориям:

- обработка знаний;
- распознавание и синтез речи;
- эволюционные вычисления;
- компьютерное зрение;
- машинное обучение и ряд других[252].

В 2022 году началась революция генеративного искусственного интеллекта – чат-бот LaMDA от Google, а затем ChatGPT от компании OpenAI смогли заставить человека поверить, что тот переписывается не с компьютерной программой, а с другим человеком, и прошли Тест Тьюринга впервые с момента его изобретения в 1950 году.

Переломным в области ИИ можно считать 2023 год. В ноябре 2022 вышел ChatGPT от разработчиков корпорации OpenAI, всего за пять дней на платформе зарегистрировался один миллион человек. ChatGPT и его аналоги, такие как YaGPT, совместно с ростом пользовательского интереса вынудили законодателей и дипломатов активнее разрабатывать меры по обеспечению безопасности граждан от возможного негативного влияния.

Генеративный ИИ (Generative AI) — это тип системы ИИ, способной генерировать текст, изображения или другие данные в ответ на подсказки (prompts), т.е. запросы через диалоговое окно. Согласно Национальной стратегии развития искусственного интеллекта до 2030 года Российской Федерации от 2024 года, «большие генеративные модели – это модели искусственного интеллекта, способные интерпретировать (предоставлять информацию на основании запросов, например, об объектах на изображении или о проанализированном тексте) и создавать мультимодальные данные (тексты, изображения, видеоматериалы и тому подобное) на уровне, сопоставимом с результатами интеллектуальной деятельности человека или превосходящем их»[253].

Базовая модель генеративного ИИ использует последние достижения в области машинного обучения и нейросетей, которые существуют около 70 лет. Однако вплоть до 2010-х гг. не хватало вычислительных мощностей и объёмов данных. Когда эти возможности появились, началось «десятилетие» глубокого обучения (deep learning — вид машинного обучения с использованием многослойных нейронных сетей, которые самообучаются на большом наборе данных). Благодаря успехам в области глубокого обучения ИИ последовательно обошёл человека в тестах по таким задачам как распознавание изображений, понимание текста, обработка естественного языка, завершение фраз с учётом здравого смысла, решение задач школьной математики и, наконец, программирование.

Большие фундаментальные модели уже сейчас способны писать программные коды по техническим заданиям, сочинять поэмы на заданную тему, давать точные и понятные ответы на тестовые вопросы различных уровней сложности, в том числе из образовательных программ[254].

Глубокое обучение в области машинного перевода привело к появлению модели-трансформера, которая используется, к примеру, в «Яндекс.Переводчике» и в конечном итоге позволило создавать большие языковые модели (LLM, large language models) – глубоко обученные нейронные сети, используемые для обработки естественного языка. Эти модели обучены на миллиардах данных и специально ориентированы на выполнение языковых задач, таких как обобщение, генерация текста, классификация, открытые вопросы и ответы, а также извлечение информации. Именно они лежат в основе генеративных предобученных трансформеров (GPT, Generative Pre-trained Transformer).

Согласно данным «Яндекса», собственные базовые модели генеративного искусственного интеллекта в мире разрабатывают около десяти стран, в том числе Россия, при этом наша страна занимает седьмое место в мире по уровню поддержки государством сферы разработки искусственного интеллекта[255].

Технологии ИИ являются областью острой международной конкуренции и геополитических противоречий. Технологическое лидерство в области ИИ может позволить государствам достичь значимых результатов по основным направлениям социально-экономического развития. Развитие искусственного интеллекта существенно повлияло на международную политику и безопасность. Прежде всего, появились новые угрозы международной информационной безопасности. Речь идёт о новых возможностях манипуляции общественным мнением, создаваемых ИИ. Однако ИИ открывает также и новые возможности для экономического роста и развития. В Москве в ноябре 2023 года прошла Международная конференция по искусственному интеллекту и машинному обучению Artificial Intelligence Journey 2023 на тему «Революция генеративного ИИ: новые возможности». В ходе конференции президент России В.В. Путин отметил, что «искусственный интеллект делает более простыми и удобными многие повседневные процессы, улучшает качество управления, механизмы предоставления государственных услуг, всё шире применяется в организациях, на предприятиях, в работе регионов», а также в науке и образовании, по сути, открывая новую главу в истории человечества[256]. Однако возможности генеративного ИИ также создают угрозу распространения запрещённой информации, нарушения авторских прав и генерации ошибочных сведений[257].

В связи с развитием ИИ в международных отношениях начинается гонка за данными для обучения ИИ. GPT обучают на задаче

«предскажи-следующее-слово» («Next-Word-Prediction»), а чтобы ИИ мог хорошо предсказывать, какое слово идёт следующим, он должен хорошо понимать весь предшествующий контекст. Это требует богатой модели мира: чем больше данных, тем выше шансы создать человекоподобный ИИ. Проблема состоит в том, что доступные ресурсы существуют преимущественно у развитых стран, а также больших компаний. Поэтому в мире развивается неравенство, известное как цифровой колониализм (digital colonialism), колониализм данных (data colonialism) или колониализм ИИ (AI colonialism). Чем больше пользователей компания может привлечь для своих продуктов, тем больше людей будут использовать её алгоритмы и тем больше ресурсов – данных – она может извлечь из их действий. К тому же, глобальный Север часто эксплуатирует глобальный Юг как дешёвую рабочую силу для разметки данных. Таким образом, существует угроза формирования неравноправных, эксплуатационных отношений между развитыми и развивающимися странами в данной области, что отмечается также в Концепции конвенции ООН по международной информационной безопасности, представленной в 2023 году Российской Федерацией на рассмотрение ООН[258].

Более того, конкуренция в области ИИ выражается в создании препятствий в области импорта передовой электроники, привлечения квалифицированных специалистов, а также во введении ограничений на свободное распространение технологий[259].

Помимо нового колониализма, можно говорить и о фрагментации Интернета вследствие развития генеративного ИИ. В создании ИИ-ботов, помимо глубокого обучения, используется обучение на основе обратной связи от людей (RLHF, Reinforcement Learning from Human Feedback). Таким образом, вторая фаза обучения ИИ зависит от мировоззренческих особенностей государства или региона, в котором разрабатывается эта технология. К примеру, китайский ИИ-бот Ernie от Baidu обучен на китайском суверенном Интернете. В России у «Яндекса» есть преимущество в сборе данных на русском языке. С высокой долей вероятности китайский ИИ-бот Ernie от Baidu и американский ChatGPT могут выдавать различные ответы о причинах американо-китайской торговой войны.

Генеративный ИИ способен изменить модель получения информации, поскольку уже сейчас он даёт ёмкие выжимки по интересующим запросам, составляя конкуренцию как глобальным поисковиками, так и открытым онлайн-энциклопедиям, например, «Википедии». Генеративный ИИ может использоваться злонамеренно в манипулировании

общественным сознанием, создавая убедительный текст, изображения или видео с нуля и в любых масштабах, что выводит на новый уровень угрозы международной информационной безопасности. Эти вызовы требуют создания особых правил регулирования использования генеративного ИИ мировым сообществом. Международные организации и дипломаты уже начали заниматься выработкой правил использования и применения этой технологии. На этом пути, однако, они сталкиваются со сложностями, связанными со скоростью развития технологий и размытостью объекта регулирования.

Таким образом, на сегодняшний день остро стоит вопрос о выработке универсальных международных норм в области искусственного интеллекта, основанных на равноправии и учёте интересов всех сторон[260]. Именно в поддержку такого подхода выступает российская дипломатия. Развитие и углубление международной кооперации в исследуемой области диктует необходимость в выработке единого понятийного аппарата; определения сфер, требующих наднационального регулирования; консолидации подходов всех государств на принципах, зафиксированных в Уставе ООН, прежде всего, принципах равноправия и взаимоуважения.

Одним из первых значимых международных документов в области регулирования ИИ стали рекомендации Организации экономического сотрудничества и развития (ОЭСР) по искусственному интеллекту от 22 мая 2019 года, подписанные всеми странами-участницами организации (36-ю странами), а также Аргентиной, Бразилией, Румынией, Колумбией, Коста-Рикой и Перу. Документ был призван «ускорить процесс разработки и внедрения инноваций и продвигать управление надёжным ИИ». Рекомендации включают в себя два больших раздела: ценностно-ориентированные принципы (в их числе содействие инклюзивному росту, устойчивому развитию и благополучию, человекоцентричность и справедливость, прозрачность ИИ и объяснимость алгоритмов, безопасность и устойчивость ИИ-систем, подотчётность акторов) и рекомендации для политических лидеров (содействие инвестициям в ИИ, развитие цифровых экосистем, политическая поддержка доступности инфраструктуры и данных для ИИ, развитие человеческого потенциала, содействие приобретению необходимых квалификаций и знаний, а также поддержка международного сотрудничества)[261]. В 2020 году ОЭСР создала обсерваторию по политике в области ИИ и секретариат Глобального партнерства по ИИ в целях распространения этических

принципов и доверенного использования указанных технологий. Данный документ не является юридически обязывающим, однако ранее рекомендации ОЭСР в других областях оказали влияние на международные стандарты и национальные регуляторные практики[262]. Рекомендации ОЭСР по ИИ также получили поддержку от Европейской комиссии в 2019 году.

В ходе 41-й сессии с 9 по 24 ноября 2021 года страны-члены ЮНЕСКО проголосовали за принятие первого в истории глобального стандарта этических аспектов ИИ. В них были изложены «общие ценности и принципы правовой инфраструктуры для обеспечения здорового развития искусственного интеллекта». Основной акцент сделан на недопущении использования новой технологии во вред человечеству и окружающей среде, а также на применении ИИ в исключительно мирных целях.

Развивается концепция человекоцентричного ИИ, который переводит фокус внимания с алгоритмов на людей, создавая условия не для замещения их машинами, а для улучшения качества жизни и усиления способностей человека[263]. Так, еще в 2019 году на саммите G20 в совместном заявлении министров торговли и цифровой экономики появился пункт «Человекоориентированный ИИ», в котором отмечалось, что «Большая двадцатка» стремится к формированию благоприятной среды для развития человекоцентричного ИИ, способного «принести большую пользу обществу и расширить возможности людей», «создать потенциал для общества будущего, ориентированного на человека»[264]. Необходимо отметить, что вопрос о регулировании ИИ также неоднократно поднимался в ходе встреч «Группы двадцати». В частности, в 2023 году в ходе председательства Индии в Декларации Нью-Дели отмечалась необходимость ответственной разработки, внедрения и использования ИИ, защиты прав человека в данной области, прозрачности, справедливости и подотчётности ИИ, обеспечения информационной безопасности, надлежащего человеческого надзора над системами ИИ. В декларации подчёркнута необходимость международного сотрудничества в сфере регулирования ИИ[265]. Сформулированный на саммите «Большой двадцатки» подход к человекоориентированному искусственному интеллекту нашёл отражение как в проектах ООН[266], так и в программных документах Китая[267], Бразилии[268], Южной Кореи[269], Европейского союза[270], США[271] и других крупных экономик мира. Российская Федерация не осталась в стороне: в Концепции развития регулирования отношений в сфере технологий искусственного

интеллекта и робототехники на период до 2024 года, утверждённой распоряжением правительства РФ от 19 августа 2020 г. № 2129-р, постулируется, что одним из принципов регулирования отношений в сфере технологий искусственного интеллекта и робототехники должен быть «человекоориентированный подход, предусматривающий, что конечной целью (…) является обеспечение защиты (…) прав и свобод человека и повышение благосостояния и качества жизни граждан»[272]. При этом Стратегия научно-технологического развития России от 2024 года в качестве первого приоритета научно-технологического развития на ближайшее десятилетие выделяет переход к передовым технологиям, основанным на применении роботизированных и высокопроизводительных вычислительных систем, технологий машинного обучения и искусственного интеллекта»[273].

Стоит также обратить внимание на то, что искусственный интеллект должен быть не только человеко-, но и социально-ориентированным. Здесь на первый план выходит концепт «доверенного ИИ» (Trustworthy AI), нашедший отражение в документах на уровне международных организаций[274] и отдельных стран, в том числе России[275]. Доверие к искусственному интеллекту, которое подразумевает уверенность людей и организаций в правильной работе систем ИИ, становится крайне важным условием для обеспечения социальной стабильности.

На основе этических принципов доверенного ИИ разрабатываются технические стандарты ИИ в рамках таких организаций как Международный союз электросвязи (МСЭ), Международная организация стандартизации (ISO) и Международная электротехническая комиссия (IEC). В условиях глобальной конкуренции за лидерство в области ИИ международная стандартизация перестала быть политически нейтральной, и международные организации стали площадкой для борьбы за экспортные рынки в области ИИ и технологическое влияние. Насколько технологии ИИ будут доверенными, человекоцентричными и подконтрольными человеку, зависит в том числе от работы международных организаций стандартизации[276]. Сегодня технологии ИИ тесно вписаны в международную политику и являются объектом и инструментом борьбы за власть на международной арене, подтверждением чему является их обсуждение в СБ ООН.

В июле 2023 года по инициативе британского председательства прошло заседание Совета Безопасности ООН, в ходе которого Генеральный секретарь выступил с идеей создать новый орган ООН для поддержки коллективных усилий по управлению ИИ. В разви-

тие озвученного предложения Генсекретарь ООН создал под своей эгидой Консультативный совет высокого уровня по искусственному интеллекту из числа независимых (отобранных Секретариатом без формального участия государств) экспертов. В сентябре 2024 года совет опубликовал доклад с рекомендациями по регулированию технологий искусственного интеллекта[277].

Кроме того, вопросы регулирования ИИ входят в повестку Глобального цифрового договора ООН – еще одной инициативы Генсекретаря ООН. Открытым остаётся вопрос о целесообразности новых инициатив в данной области. Так, Российская Федерация, будучи одним из постоянных членов ООН, придерживается позиции о недопустимости формирования наднациональных надзорных органов в сфере ИИ в отсутствие исчерпывающей убедительной аргументации в пользу их создания. Кроме того, важно чётко очертить сферу функций и полномочий новых органов ООН по ИИ, чтобы не было дублирования усилий, которые уже принимаются на других площадках организации, в том числе в рамках уже упомянутой РГОС ООН по международной информационной безопасности. В силу того, что ИИ относится к ИКТ, вопросы регулирования аспектов, связанных с безопасностью разработки и применения ИИ, целесообразно обсуждать в рамках РГОС. В 2024 году КНР инициировала успешно принятую ГА ООН резолюцию по ИИ и содействию международному развитию, Россия вошла в число соавторов.

21 марта 2024 года по инициативе США в рамках ГА ООН была принята резолюция «Использование возможностей безопасных, защищённых и надёжных систем искусственного интеллекта для устойчивого развития» (Россия присоединилась к консенсусу, но не вошла в число соавторов), а также в марте 2024 года была принята Конвенция Совета Европы по ИИ. В январе 2023 года был опубликован «нулевой» драфт данного документа, в котором делается акцент на защите прав человека, основных свобод и принципов демократии, трактуемых в соответствии с западными подходами и не учитывающих разнообразия политических и культурных систем в области защиты прав человека[278].

В 2024 году президент Российской Федерации внёс уточнения и дополнения в Национальную стратегию развития искусственного интеллекта на период до 2030 года, принятую в 2019 году[279] (в ней впервые появился международный раздел). Согласно документу, вызовом для развития ИИ в России являются ограничение доступа к технологиям искусственного интеллекта в связи с недобросовестной конкуренцией со стороны недружественных иностранных госу-

дарств. При этом с такой проблемой сталкивается не только Россия, но и многие развивающиеся страны. В условиях, когда в сфере ИИ наметилась острая геополитическая конкуренция, особенно важно выработать международно-правовые нормы, обеспечивающие мирное развитие и использование технологий ИИ.

Помимо глобального, можно выделить региональный и макрорегиональный уровни взаимодействия. На уровне ЕС в 2019 году были приняты региональные этические принципы доверенного ИИ, которые включают в себя человеческий контроль над системами ИИ, техническую надёжность и устойчивость ИИ, защиту персональных данных, прозрачность алгоритмов, разнообразие, отсутствие дискриминации и справедливость ИИ-систем, общественное и экологическое благополучие, подотчётность акторов[280].

В 2024 году Европейский Союз принял Закон ЕС об искусственном интеллекте. Основное внимание уделяется управлению рисками ИИ, которые разделены на четыре уровня: неприемлемого, высокого, ограниченного, низкого или минимального. К первой группе относятся технологии, использующие манипулятивные техники для нанесения вреда здоровью населения или контролируемые государственными структурами для социального мониторинга. Согласно новому закону, такое применение ИИ запрещено. Вторая группа регулирует программы, которые касаются человеческой безопасности и основных прав человека. Среди них можно выделить биометрическую идентификацию, образовательные технологии на основе ИИ, программы, отвечающие за безопасность критической инфраструктуры, и т.п.

Дополнительные правила созданы и для генеративного искусственного интеллекта. На территории ЕС подобные системы будут обязаны раскрывать информацию о сгенерированном контенте; разработать модель, предотвращающую создание нелегального контента; публиковать отчёты об использовании данных, защищённых авторским правом, для обучения ИИ. Акт ЕС об ИИ предусматривает запрет систем биометрической категоризации, основанных на чувствительных характеристиках, а также нецелевое извлечение изображений лиц из Интернета или записей камер видеонаблюдения для создания баз данных распознавания лиц (за отдельными исключениями)[281].

Работа по регулированию ИИ ведётся и на уровне Ассоциации государств Юго-Восточной Азии. АСЕАН находится на стадии разработки руководящих этических принципов и принципов управления в сфере искусственного интеллекта.

Подчёркивается важность формирования системы управления ИИ на пространствах ШОС и БРИКС. В ходе саммита БРИКС в Йоханнесбурге в 2023 году председатель КНР Си Цзиньпин выступил с инициативой формирования общей структуры БРИКС в области управления ИИ[282]. Им же в 2023 году была выдвинута инициатива создания системы глобального управления ИИ. При этом Россия исходит из того, что вопросы информационной безопасности, связанной с развитием ИИ, необходимо обсуждать в РГОС ООН. Так, в 2023 году «Лаборатория Касперского» обратилась к РГОС с предложением подготовить принципы развития ИИ для обеспечения кибербезопасности. Регулирование ИИ обсуждалось в ходе Казанского саммита БРИКС в 2024 году.

В целом, можно отметить, что подходы к регулированию ИИ на национальном и региональном уровнях на сегодняшний день разнятся по шкале от «нуля» до «жёсткие предписания». На это влияет целый ряд факторов: от уровня развития отрасли и доступности инфраструктуры и данных до правовой культуры и традиций тех или иных стран и объединений.

В России уже сформирована серьёзная регуляторная база в сфере ИИ. Важнейшим документом стала обновлённая в 2024 году Национальная стратегия развития искусственного интеллекта на период до 2030 года. Благодаря накопленной технологической базе и сильной инженерно-математической школе Россия является одним из лидеров в области развития ИИ, активно участвует в выработке международных правил и стандартов в данной области, а также развивает внутреннее регулирование. Россия является одной из немногих стран, развивающих модели генеративного ИИ, при этом по одному из ключевых факторов развития ИИ – участию государства – Россия на 2023 год занимала седьмое место в мире. Полный экономический потенциал ИИ в России составляет 22–36 триллионов рублей, и он может вырасти до 4% ВВП к 2028 году[283]. На сегодняшний день более 60 стран, в их числе Россия, утвердили принципы и стандарты, регулирующие ИИ. В России речь идёт, прежде всего, о ГОСТ Р-59276-2020 о способах обеспечения доверия к системам искусственного интеллекта, в котором определены понятия ИИ, приведена классификация факторов, влияющих на качество ИИ, приведена классификация основных способов обеспечения доверия к системам ИИ.

В России созданы благоприятные условия для развития ИИ и привлечения инвестиций в данную область. Регулирование развивается и на частном уровне, можно говорить о сложившемся в рамках данной отрасли подходе к саморегулированию с постепенным набором масси-

ва различных технических стандартов в тех аспектах, которые выходят за рамки аспектов безопасности, защиты данных, предупреждения и борьбы с кибератаками. В России крупнейшие российские IT-компании создали национальный Кодекс этики в сфере ИИ, открытый для присоединения иностранным профильным организациям и общественным структурам. По состоянию на декабрь 2024 года 44 федеральных органа исполнительной власти, 20 органов исполнительной власти субъектов РФ, 335 российских организаций и 50 иностранных организаций присоединились к Кодексу этики как к стандарту, признанному на международном уровне[284]. Лидеры российской ИИ отрасли сформировали национальный Альянс по ИИ, который в 2024 году инициировал создание международной сети альянсов (с ядром в БРИКС).

Для участия в международном сотрудничестве в рамках органов стандартизации в 2019 году в России был создан Технический комитет по стандартизации «Искусственный интеллект».

В КНР 11 апреля 2023 года на общественное обсуждение был вынесен черновой вариант Мер по управлению сервисами генеративного искусственного интеллекта. Документ предусматривает международное сотрудничество в области развития ИИ; запрещает использование подобных технологий во вред частной жизни, в нарушение авторских прав, в дискриминационных целях. К системе регулирования ИИ в Китае, действующей с 10 января 2023 года, необходимо также отнести Положения об управлении технологиями глубокого синтеза. В число последних входят дипфейки и другая текстовая, аудио- и визуальная информация, созданная генеративным ИИ. Данный документ призван обеспечить безопасность граждан и системы в целом от манипулирования контентом. Китай рассматривает развитие технологий искусственного интеллекта как возможность укрепления позиций в качестве глобального лидера. Особенностью политики Пекина является чётко выстроенная долгосрочная стратегия в области ИИ, которая предусматривает большой объём инвестиций в исследования и разработки, укрепление регуляторных рамок и контроль внедрения и использования технологии[285].

США, помимо национального регулирования, выдвигают инициативы на мировой арене. Борьбу за лидерство в области технологии ИИ США считают ключевой. Работа ведётся на полях ОЭСР, «Большой семёрки», Совета США и ЕС по торговле и технологиям, а также в рамках инициативы Глобальное партнёрство по ИИ (Global Partnership on AI). Инициативы ОЭСР были рассмотрены в предыду-

щем параграфе. Что касается «Большой семёрки», то здесь необходимо отметить принятые в 2023 году в рамках «Хиросимского процесса искусственного интеллекта» Международные руководящие принципы искусственного интеллекта (International Guiding Principles on Artificial Intelligence) и Кодекс поведения для разрабатывающих системы искусственного интеллекта компаний (Code of Conduct for AI developers)[286]. Принципы носят максимально общий характер и отражают обязательства по снижению рисков и предотвращению злоупотреблений, поощрению обмена информацией о рисках и уязвимостях, уведомлению об инцидентах, укреплению кибербезопасности, а также маркировке для сгенерированного искусственным интеллектом контента[287]. Западные эксперты оценивают данные инициативы как первый шаг на пути к укреплению позиций «Большой семёрки» как института глобального управления в области ИИ[288].

Принятая в рамках ГА ООН резолюция по ИИ (подробнее см. на стр. 129) также была разработана по инициативе США. Данный блок международной кооперации направлен на сохранение лидерства США и их союзников в научно-технической сфере. В частности, США делают акцент на безопасности ИИ в контексте защиты прав человека и демократических ценностей, трактуемых в рамках западных подходов[289]. Важное значение США придают участию в работе международных организаций стандартизации в области ИИ, в том числе на уровне МСЭ, ISO и др. Для скоординированных действий в области стандартизации США создаются коалиции с союзниками и единомышленниками с целью оказания максимального сопротивления продвижению позиций иначе мыслящих государств, а также США стремятся оказывать максимальное влияние на голосование стран, которые не обладают развитыми технологиями ИИ, но имеют возможность влиять на принятие международных стандартов в области ИИ. При этом опережающий темп развития ИИ в Китае и в России расценивается США как угроза национальной безопасности. На национальном уровне США ограничивают внедрение ИИ в областях с высокой степенью риска, таких как здравоохранение, но в то же время стимулируют саморегулирование на уровне отрасли, в рамках которого ведущие компании берут на себя обязательство управлять рисками, выступая связующим звеном между индустрией и законодателями[290]. Долгое время стратегия США в области ИИ носила фрагментарный характер, задачи для бизнеса и государственного сектора были сформулированы в разных документах, ставка на государственно-частное партнерство в области ИИ стала приоритетом относительно недавно[291].

Как подчеркнул министр иностранных дел России С.В. Лавров, Россия продвигает международное сотрудничество в данной сфере на принципах равноправия, взаимного учёта интересов и общей ответственности за будущее человечества[292]. США заинтересованы в кулуарном формировании норм в закрытых форматах, чтобы распространять их на глобальном уровне как универсальные стандарты. В завершение стоит ещё раз подчеркнуть крайнюю озабоченность международного сообщества из-за скорости развития технологий ИИ, которые требуют скорейшего создания регулирующих механизмов, в том числе обеспечивающих его безопасное развитие в интересах всего человечества и с учётом актуальных проблем международной информационной безопасности.

3.2.2. Технологии распределённых реестров и криптовалюты

За последние несколько лет отношение к технологиям распределённых реестров (Distributed Ledger Technology, DLT) совершило полный разворот от сдержанной осторожности до разработки национальных программ их тестирования и внедрения. Среди всех рассмотренных выше передовых технологий распределённые реестры являются наиболее ярким примером подрывных инноваций (disruptive innovation).

По своей сути распределённые реестры являются новым подходом к организации баз данных, который за счёт использования криптографических механизмов обеспечивает неизменяемое распределённое хранение состояний некоторой системы и, в частности, позволяет определить состояние системы в любой момент времени. В условиях отсутствия доверия между субъектами/объектами цифровой среды это создаёт определённые гарантии безопасности. Технология распределённых реестров, в отличие от распределённых баз данных, создаёт возможность организации хранения реестра без единого центра управления, получения синхронизированных копий реестра на всех узлах распределённой сети (их специалисты называют нодами, англ. node).

«Каждый узел составляет и записывает обновления реестра независимо от других узлов. В отличие от распределенных баз данных, каждый участник системы распределённого реестра хранит всю историю изменений и валидирует добавление любых изменений в систему с помощью алгоритма консенсуса, который математически гарантирует невозможность подделки данных при определённой доле достоверных

нод. Однако ни один участник не может изменить данные в системе таким образом, что другие участники не узнают об этом. Благодаря этому данные, которые находятся внутри системы распределённого реестра, становятся доверенными, а все изменения – прозрачными»[293].

Технология цепной записи данных, блокчейн (англ. block – блок, chain – цепочка), является одной из разновидностей DLT. В ней отдельные записи сначала объединяются в блок, который и заносится в реестр. Каждый информационный блок имеет ссылку на предыдущий и временну́ю метку. Криптографические алгоритмы связывают эти блоки между собой в хронологической последовательности, образуя цепочку. Переставить местами блоки или изменить их содержание невозможно. Блоки хранятся децентрализованно, вся информация в системе является доступной и достоверной.

Для общественности первое знакомство с термином «блокчейн» связано с появлением криптовалюты Bitcoin в 2008 году, оборот которой обеспечивает система на этой технологии. Теперь различных наименований нефиатных денег тысячи, а сферы использования технологии постоянно расширяются[294].

В мире наблюдается стремительный рост криптовалют, на 2024 год общий объём их капитализации составил 3% от глобальных финансовых активов. Наибольший объём капитализации приходится на биткоин (60%), следом за ним идет Ethereum (13%)[295]. На рынке стейблкоинов доминирует Tether. Активизируется торговля производными финансовыми инструментами, связанными с криптовалютами, развиваются экосистемы децентрализованных финансов (DeFi). Российские граждане являются активными пользователями интернет-платформ, осуществляющих торговлю криптовалютами, Россия находится в числе лидеров в мире по объёму майнинговых мощностей[296].

Отсутствие единого эмитента, возможность осуществлять микроплатежи, режим работы 24/7, отсутствие посредников в виде кредитных организаций, низкая себестоимость транзакций, отсутствие юрисдикционных границ сделало криптовалюты привлекательным денежным инструментом. У них есть возможность сделать платежи проще, быстрее и дешевле, а также предоставить альтернативные методы для тех, у кого нет доступа к обычным финансовым продуктам. Однако они порождают множество рисков. Помимо высокой волатильности, криптовалюты уязвимы для кибератак и мошенничества. Без надлежащего регулирования виртуальные активы могут стать инструментом для финансовых операций преступников и террористов.

В числе угроз криптовалюты для российских граждан Банк России выделяет:

- угрозу для благосостояния граждан;
- угрозу для финансовой стабильности;
- угрозу для расширения нелегальной деятельности.

Большинство стран ещё не внедрили эффективные правила. Пробелы в глобальной системе регулирования повышают риски совершения преступлений и становятся угрозой безопасности на национальном и международном уровне. Проблема регулирования криптовалют занимает важное место на повестке дня ведущих международных организаций.

ООН. В августе 2022 года ООН впервые заняла принципиальную позицию относительно преимуществ и рисков оборота криптовалюты, когда Конференция ООН по торговле и развитию (ЮНКТАД) публично призвала к сдерживанию оборота криптовалют в развивающихся странах. Агентство предупредило, что частные цифровые валюты нестабильны, они могут нести социальные риски и издержки, если они продолжат развиваться как платёжное средство, «денежный суверенитет» стран может оказаться под угрозой.

В качестве альтернативы криптовалюте ЮНКТАД предложила развивать принципиально новую цифровую платёжную систему на основе цифровой валюты центральных банков и систему быстрых розничных платежей[297].

ОЭСР придерживается утилитарного подхода к обороту криптовалют. Вслед за созданными в 2014 году и успешно внедрёнными в более чем половине стран мира Общими стандартами отчётности (CRS) ОЭСР совместно с G20 создала Систему стандартов отчётности в отношении криптоактивов (CARF). ОЭСР ориентирована на создание приемлемого регуляторного ландшафта, прежде всего, в части расширения платёжной системы и увеличения адаптивных возможностей криптовалюты как альтернативы традиционным средствам расчётов. Рекомендации ОЭСР ориентированы преимущественно на развитые государства и слабо пригодны для развивающихся стран.

Всемирный банк. В феврале 2023 сотрудники Всемирного банка опубликовали доклад, где осветили основные проблемы в сфере криптовалютных банкротств[298].

В числе ключевых проблем крипторынка были обозначены:

- криптовалюта в различных юрисдикциях рассматривается и как собственность, и как ценная бумага, и как валюта;
- отслеживание и возврат криптоактивов. В частности, «холодные» кошельки обеспечивают высокий уровень децентрализованной безопасности и их практически невозможно взломать без закрытого ключа. Вернуть средства с «холодного» кошелька без участия владельца крайне сложно;

- высокая волатильность криптовалют;
- сложности движения криптовалюты между различными юрисдикциями[299].

Международный валютный фонд. В июне 2023 МВФ подготовил доклад о ситуации в Латинской Америке, в котором отметил, что запрет криптовалюты негативно повлияет на экономический рост. В частности, МВФ отметил, что Сальвадор признал биткоин законным платёжным средством в сентябре 2021, а Багамы первыми в мире запустили собственную криптовалюту CBDC (Sand Dollar) в октябре 2020. Бразилия, Аргентина, Колумбия и Эквадор входят в число стран с самым высоким объёмом криптофинансов. Как отмечается в исследовании, запрет криптовалют даёт слабые результаты в долгосрочной перспективе. Для противодействия обороту частных денег нужны системные меры, направленные на снижение спроса в криптовалюте за счёт развития цифровой валюты центральных банков[300].

В феврале 2023 Фонд призвал к «защите денежного суверенитета и стабильности через укрепление денежно-кредитной политики и отказ признавать виртуальные токены законным платёжным средством». В июне 2023 МВФ предложил создать мировую расчётную платформу, участниками которой станут центробанки и кредитные учреждения. Эта инициатива была встречена решительным протестом. Организацию обвинили в попытке централизации власти через интерес стран к криптоактивам. Эксперты опасаются, что глобальный реестр даст государствам возможность контролировать деньги граждан не только в стране присутствия, но и за рубежом[301].

ФАТФ. Группа разработки финансовых мер борьбы с отмыванием денег является, пожалуй, единственной международной организацией, которая подходит системно и последовательно к разработке стратегии регулирования криптоэкономики. Она исходит из того, что виртуальные валюты имеют плюсы и минусы. В октябре 2021 года ФАТФ выпустила обновлённое руководство по применению риск-ориентированного подхода в отношении виртуальных активов и провайдеров услуг в сфере виртуальных активов[302].

Рис. 4. BRICS Pay – единая платёжная система стран БРИКС[303].

Нет единообразия и в подходах к регулированию криптовалют на уровне региональных международных организаций.

БРИКС. Страны БРИКС сегодня разрабатывают BRICS Pay — платёжную систему для операций между странами БРИКС без конвертации местной валюты в доллары.

Ведутся разговоры о криптовалюте БРИКС и о согласовании единой стратегии цифровых валют центральных банков для обеспечения функциональной совместимости валют и экономической интеграции. Поскольку многие страны выразили заинтересованность в присоединении к БРИКС, группа, вероятно, расширит свою программу дедолларизации[304]. На официальном сайте BRICS Pay заявлено, что расчёты между странами БРИКС будут осуществляться с использованием оптовой цифровой валюты. Принципы взаимодействия с национальными валютами, расчёты курсов, эмиссии и клиринга находятся в стадии разработки[305]. Что же касается криптовалют, то страны-участницы БРИКС высказывают настороженность в части расширения их оборота, по большей части, в связи с высокими рисками волатильности, вовлечения в криминальные схемы и возможности внешнего финансового контроля.

ЕАЭС. Евразийский экономический союз ориентирован на развитие цифровых финансов, но в большей степени склоняется к разработке цифровой валюты центральных банков, нежели к стимулированию оборота частной цифровой валюты. Россия готова выступить инициатором создания и внедрения в рамках ЕАЭС общей криптовалюты, а также формирования интегрированного валютного рынка и единых стандартов валютного регулирования[306]. В феврале 2023 Кыргызстан предложил взять курс на развитие регионального стейблкоина, который будет привязан к валютам стран Евразийского экономического союза, однако этот вопрос по-прежнему находится в стадии обсуждения.

В целом, ЕАЭС ориентирован на создание единых стандартов цифровой платёжной инфраструктуры в рамках концепции цифровой валюты центральных банков.

Европейский союз. В июне 2023 законодатели ЕС подписали Закон о рынках криптоактивов (MiCA), вступивший в силу в 2024 году. MiCA устанавливает чёткие требования в отношении поставщиков цифровых услуг и создаёт единый нормативный ландшафт для развития цифровых финансов. Согласно закону, поставщики услуг криптоактивов (криптовалютные обменники) обязаны предоставлять информацию об источнике актива и его бенефициаре компетентным органам. Контроль движения криптовалют осуществляется в отношении всех операций – минимальные пороговые значения не предусмотрены.

Африканский союз. В июле 2023 на сайте Агентства развития Африканского союза был опубликован доклад, описывающий

преимущества использования криптовалют. В частности, обращалось внимание на то, что криптовалютные транзакции безопасны – благодаря реализации криптографических протоколов – и обрабатываются намного быстрее по сравнению с традиционными банковскими переводами. Кроме того, комиссии, связанные с такими транзакциями, в настоящее время ниже. Более того, криптовалюта доступна любому, у кого есть мобильное устройство и доступ в Интернет, независимо от его географического или финансового положения. Агентство отмечает положительный опыт отдельных африканских стран по внедрению криптовалют в платёжную системы.

АСЕАН. Ассоциация государств Юго-Восточной Азии настороженно смотрит на создание единой стратегии оборота криптовалюты, что, однако, не препятствует её странам-участницам активно внедрять собственную финансовую политику. Отсутствие единообразного подхода приводит к очевидной рассогласованности позиций: одни страны АСЕАН (Сингапур и Филиппины) ввели в оборот криптовалюты, другие (Индонезия, Вьетнам), напротив, ограничили их использование. Противоречивый нормативный ландшафт существенно затрудняет расчёты и заметно увеличивает риски совершения финансовых преступлений.

В пользу создания единой криптовалютной экосистемы АСЕАН говорят и экономические тренды. По оценкам экспертов, только в Таиланде в 2027 году число пользователей криптовалюты достигнет 5,12 миллиона человек, а общий прогнозируемый доход составит около 581 миллиона долларов США. В 2022 году оборот криптовалюты во Вьетнаме уже превысил 195 миллионов долларов; по прогнозам, он должен достичь 493 миллионов долларов США к 2027 году[307].

Чем более развитой является традиционная финансовая и платёжная система в стране, тем с меньшим энтузиазмом она готова рассматривать развитие национального криптовалютного рынка. Однако отказ от финансовой криптовалютной инфраструктуры в обозримом будущем может привести к заметному отставанию от других стран. Государства окончательно не определились, какой разновидности отдать предпочтение: оптовой или розничной валюте. Развитие оптовой валюты центральных банков позволит обеспечить стабильность межгосударственных финансовых расчётов и «обкатать» технологию на уровне центробанков, в то время как внедрение розничной валюты придаст динамику расчётам и увеличит объёмы товарообмена. Каждая из моделей предпола-

гает разработку международных рекомендаций по минимизации финансовых рисков, которые, однако, до настоящего времени не выработаны.

Таким образом, цифровые технологии и развитие искусственного интеллекта существенным образом трансформируют природу современной дипломатии, создают новые точки роста, при этом порождают цифровые угрозы национальной и международной безопасности.

3.2.3. Большие данные

Понятие «большие данные» стало популярным около 15 лет назад, когда заголовок Big Data был вынесен на обложку самого влиятельного в мире научного журнала Nature. Понятие «большие данные» («big data») относится к большим и разнообразным наборам информации, растущим в реальном времени с постоянно увеличивающейся скоростью. Данное понятие охватывает три основных характеристики: объём информации (volume); скорость, с которой она создаётся и собирается (velocity); а также разнообразие (variety), или объём охватываемых данных. Перечисленные три характеристики известны в отечественной и международной науке как основополагающие «три 'V' больших данных». Это определение было фактически введено в употребление экспертом американской исследовательской и консалтинговой компании Gartner Дугласом Лэйни в начале 2000-х годов[308], и до сих пор на его основе строятся всё новые и новые трактовки явления «больших данных», включающие уже и четыре, и пять, и даже больше „V" (Veracity, Validity, Volatility, Variability и т.д.). При этом не существует точного определения того, что по размеру является «большими данными», а что ещё обладает недостаточным объёмом, чтобы считаться таковыми. Так, например, президент группы компаний Real World Technologies Дэвид Кантер полагает[309], что большими данными можно назвать только те массивы информации, которые не помещаются в памяти одного сервера и «весят» более 3 терабайт. В то же время, например, исследователи Оксфордского университета полагают, что большие данные определяются как «исключительно большие множества данных, поддающиеся вычислительному анализу для выявления паттернов, трендов и ассоциаций, в особенности применительно к человече-

скому поведению и контактам»[310], то есть фактически их размер никак не регламентируется. В этой связи необходимо упомянуть и о понятии «малые данные» («small data»), традиционно используемом в качестве противопоставления «большим данным». Малые данные, собранные исследователем самостоятельно (т.н. capta), отличаются от больших данных тем, что позволяют проявить исследовательские компетенции при построении инфологической и даталогической моделей. «Малые данные» полностью контролируются исследователем, при этом обычно подробно обосновываются репрезентативность и целостность самостоятельно собранных данных, а для нужд вторичного использования проводится подробное документирование источников таких коллекций данных. Иными словами, отсутствует признанный исследовательским сообществом количественный показатель, который отсекал бы «большие данные» от всех остальных данных. По сути, речь идёт о таких объёмах данных, которые требуют машинной обработки для извлечения знания, а также пригодны для анализа средствами математической статистики.

Большие данные являются объектом интеллектуального анализа данных, поступая при этом «к аналитику» в различных своих формах и типах. Интеллектуальный анализ данных, в свою очередь, – это применение специфических алгоритмов для извлечения так называемых паттернов из данных. В интеллектуальном анализе акцент делается на применении алгоритмов, в ходе которых машинное обучение используется в качестве инструмента для извлечения потенциально ценных паттернов, содержащихся в наборах данных. Все формы данных, обрабатываемых «интеллектуальным анализом», следует условно разделять на структурированные, полуструктурированные и неструктурированные.

- Структурированные данные имеют связанную с ними архитектуру таблиц и отношений (также называемую «онтологией»). В качестве таких данных, например, выступают хранящаяся в системе управления базами данных (СУБД) информация, файлы CSV, Excel и, проще говоря, любые уже структурированные другими исследователями базы данных.
- Полуструктурированные (называемые также слабоструктурированными) данные не соответствуют строгой структуре, однако имеют другие маркеры для отделения семантических элементов и обеспечения иерархической структуры записей и полей. Например, информация в электронных письмах или

сообщениях в Twitter, собранная по определённому поисковому запросу.

- Неструктурированные данные, в свою очередь, не имеют никакой связанной с ними структуры, либо не организованы в установленном исследователем порядке. Обычно это текст на естественном (привычном «обывателю» русском, английском и др.) языке, файлы документов и изображений, аудио, видео и т.д.

Таким образом, в настоящий момент понятием «большие данные» можно обозначить значительный объём информации из любой предметной области: от изучения бизнес-процессов до исследования современных международных отношений. Однако несмотря на то, что большие данные «необъятны», всё же имеются некоторые ограничения их применения в исследованиях, в особенности, если речь заходит об исследованиях международных политических процессов.

Как отмечает И.Е. Денисов, в современную эпоху вопрос о том, что контролирует и чем должно управлять государство, имеет абсолютно новое измерение – это уже не просто население и территория, скрытые в земле и на дне морей минеральные богатства, но и массивы данных, которые сегодня превратились в такой же фактор производства и роста могущества страны, как и традиционные ресурсы. В 2017 году в редакционной статье The Economist отмечалось, что «самым ценным ресурсом в мире уже являются данные, а не нефть».

Данные – «кирпичики», из которых строится цифровая экономика, сферу внешней политики трудно себе представить без цифровой дипломатии. Идеологические конфликты между государствами и блоками государств всё чаще приобретают характер информационных войн с помощью сетевых интернет-платформ. В эпоху новых «интеллектуальных военных конфликтов» от умелого и эффективного использования больших данных безопасность страны зависит не меньше, чем от численности армии или её оснащённости традиционными средствами ведения войны. Искусственный интеллект, который «тренируется» на больших данных, меняет буквально все сферы жизни – от государственного управления до индустрии развлечений, от дизайна до программирования или академических исследований. Важным направлением обеспечения государственного суверенитета становится «национализация» данных и контроль за их трансграничным перемещением.

3.3. Интернационализация управления Интернетом: проблемы, подходы, перспективы

3.3.1. Многоуровневое управление Интернетом

Транснациональная природа Интернета диктует необходимость в международном и даже глобальном регулировании. Более того, в современных условиях государства уже не могут осуществлять управление в одиночку, без привлечения негосударственных акторов. В Тунисской программе особо подчёркивается тот факт, что поскольку Интернет превратился в общедоступный глобальный ресурс, «его управление на международном уровне должно иметь многосторонний, прозрачный и демократический характер, при полном участии правительств, частного сектора, гражданского общества и международных организаций»[311]. Действительно, сохранение традиционно характеризующей Интернет инновационной природы требует организованного на постоянной основе взаимодействия правительств, представителей экспертного и бизнес-сообщества, неправительственных организаций. Выработка новых форм управления Интернетом – только часть более широкого процесса поисков во всём мире новых, международных форм управления, регулирующих процессы миграции, торговли, безопасности, развития и других глобальных проблем.

На фоне глобализации наметились объективные тенденции к глобальному регулированию, возрастанию роли транснациональных акторов в мировой политике. Усиление взаимозависимости, переплетение внутренней и внешней политик, меняющаяся роль государства как политического актора – всё это ведёт к укреплению позиций международных организаций и институтов, осуществляющих координацию политики и выработку решений на глобальном уровне. Как пишет отечественный исследователь Т.П. Лебедева, «глобализация провоцирует потребность в общеобязательных международных регламентациях, в международных конвенциях и институтах для транзакций, перешагивающих границы»[312]. Более того, как отмечает П.А. Цыганков, «отныне ресурсы воспринимаются глобально – как огромные запасы, которые необходимо наилучшим образом распределить между всеми людьми планеты. В распределении этих ресурсов и в формировании системы глобального управления в целом участвуют не только государственные институты, но и организации гражданского общества, и многообразные бизнес-структуры. Их

представители во всех трёх названных секторах заинтересованы в надёжных формах регулирования мировых процессов»[313].

Эта тенденция находит своё отражение и в отношении Интернета, который всё больше рассматривается как общий ресурс всего человечества, в рациональном использовании и разумном регулировании заинтересованы не только государства, но и все иные акторы. В сфере управления Интернетом мы наблюдаем, как складывается многоуровневая модель взаимодействия, в которой участвуют различные типы акторов – государственные, межправительственные, негосударственные. В литературе подобные модели получили название многосторонних партнёрств, некоторые исследователи также используют такие определения как многоуровневая дипломатия, неофициальная дипломатия или track-two diplomacy. Многосторонние партнёрства складываются в различных областях мировой политики и международных отношений – при урегулировании конфликтов, решении экологических проблем (Всемирная встреча на высшем уровне по вопросам устойчивого развития, Йоханнесбург, 2002 год), при заключении соглашений о запрете отдельных видов оружия (противопехотных мин) и др.

Однако именно в сфере управления Интернетом многоуровневое взаимодействие получило наиболее «сильное» институциональное оформление. В работе ВВУИО в беспрецедентном масштабе участвовали не только государства и межправительственные структуры, но и организации гражданского общества, специализированные институты интернет-сообщества, а также представители бизнес-сообщества. ФУИ же, согласно мандату, организован в формате многостороннего партнёрства. Это даёт повод утверждать, что ВВУИО и ФУИ представляют собой институты нового, поствестфальского глобального управления. Таким образом, тенденции, наблюдаемые в отношении Интернета, – ещё один симптом эрозии вестфальской системы мира, перестройки традиционной системы взаимоотношений между различными заинтересованными группами и изменения подходов к регулированию той или иной области международных отношений.

Складывающаяся многоуровневая модель регулирования привлекает закономерное внимание многих исследователей-теоретиков, таких как З. Баирд, С. Верхулст[314], Д. Дрезнер, В. Кляйнвехтер[315], И. Курбалийя, Дж. Малкольм, М. Рабой[316]. Всё более популярной является точка зрения, согласно которой в ходе развития механизмов управления Интернетом будут выработаны новые, наиболее плодотворные формы международного сотрудничества, которые затем бу-

дут распространены на другие области международных отношений.

Анализом многоуровневых моделей управления и их реализации в ходе регулирования Интернета занимается М. Рабой. М. Рабой работает в рамках теории глобального управления и полагает, что для успешного регулирования Интернета необходимо участие не только государственных акторов, но и организаций гражданского общества и представителей бизнес-сообщества. По его мнению, в данной сфере международных отношений особенно очевидны процессы «распыления» власти и появления новых форм управления и сотрудничества[317].

Дж. Малкольм также полагает, что будущее – за новыми моделями управления, которые создают условия для сотрудничества различных партнёров в поисках приемлемого для всех решения, причём каждый раз акторы находят новые пути и схемы объединения своих усилий в зависимости от характера и условий проблемы[318]. Такие модели более гибкие и адаптивные, лучше приспособленные к глобализации с её стремительно меняющимися обстоятельствами, рождающими новые проблемы, требующие быстрого реагирования, на которое не способны традиционные межправительственные организации.

Сходной точки зрения придерживаются и исследователи, работающие в рамках теории международных режимов, в особенности её конструктивистского направления. Согласно их мнению, режим управления Интернетом находится на начальной стадии своего развития, когда происходит выработка основополагающих норм и принципов регулирования. Таким образом, на современном этапе складываются основы международного режима, причём эти основы лежат в сфере идей, общепринятых практик и представлений. И именно на начальном этапе познавательная, обучающая функция сотрудничества является ключевой, то есть ВВУИО и ФУИ – это эксперименты, в ходе которых различные акторы учатся эффективному, продуктивному и конструктивному взаимодействию между собой.

Межправительственные организации, в особенности организации системы ООН, часто критикуют за то, что они не приспособлены к новым условиям возросшей взаимозависимости, глобализации, усилившегося влияния новых транснациональных акторов. Высказываются мнения, что эти организации были созданы с целью постоянного балансирования между великими державами в период биполярности, а их адаптация к новым условиям идёт слишком медленно, а в качестве примера, как правило, приводится затяжной процесс реформирования ООН. Исследователи пишут о необходимости полноценного

включения новых сильных государств и наиболее влиятельных неправительственных акторов в систему глобального управления с целью повышения эффективности работы многосторонних институтов и обеспечения легитимности принимаемых ими решений.

Высказывается мнение, что эффективность и легитимность традиционных межправительственных организаций может повысить их сотрудничество с международными неправительственными институтами. В сфере управления Интернетом это особенно актуально, так как эта область международных отношений особенно явно демонстрирует тот факт, что глобализация стимулирует появление новых смыслов в понятиях легитимности и демократичности. Проблемы, подорвавшие эффективное функционирование ICANN и деятельность ряда других институтов, участвующих в управлении Интернетом, демонстрируют, что любой режим управления Интернетом должен быть в первую очередь легитимным. Таким образом, эффективность управления во многом будет зависеть от легитимности регулирующих институтов, а легитимность предполагает представленность различных групп интересов, что возможно только в том случае, если представители различных регионов и групп акторов могут быть услышанными.

Текущая модель управления Интернетом, опирающаяся в основном на возможности неправительственных акторов (в первую очередь ICANN), также не представляется адекватной текущей международно-политической ситуации. В последние годы число пользователей Интернета наибольшими темпами растёт в развивающихся странах, в особенности, в странах Азии, которые фактически не имеют возможностей участия в традиционных организациях интернет-сообщества. В этих условиях требования развивающихся государств о предоставлении межправительственным механизмам большего веса в режиме управления Интернетом, в особенности на глобальном уровне – в первую очередь имеются в виду ООН и МСЭ, – выглядят всё более легитимными. Конечно, не все проблемы, связанные с Интернетом, должны регулироваться на глобальном уровне. Большая часть вопросов может быть решена на региональном уровне (в рамках соответствующих региональных институтов, которые приобретают всё больший вес в данной области), а также на уровне отдельных государств или даже сообществ пользователей. Однако для успешности этих действий они должны соотноситься с глобальной картиной. В этих условиях формирование многосторонних партнёрств в рамках глобальных и региональных международ-

ных межправительственных организаций (ММПО), т.е. привлечение к их деятельности представителей бизнеса и НПО, представляется оптимальным решением.

Таким образом, многоуровневое глобальное управление Интернетом призвано учесть требования развивающихся стран о необходимости контроля над средством коммуникации, от функционирования которого они во всё большей степени зависят; опираться на опыт и знания специализированных организаций и представителей экспертного сообщества; мобилизовать опыт и легитимность международных неправительственных организаций, а также ресурсы легитимности и правосубъектности государств и межправительственных организаций; и, кроме того, стимулировать инновационное развитие технологии за счёт привлечения частного сектора. При этом роль государств и межправительственных организаций в процессах управления должна быть ведущей, координирующей.

3.3.2. Координирующая роль государств в рамках многоуровневой модели

На протяжении всей истории Интернета важную роль в его регулировании играли государственные акторы. Это верно даже для начальных этапов развития сети, несмотря на преобладавший в то время оптимизм относительно новых, негосударственных моделей управления Интернетом. В данной связи важно отметить, что модель глобального управления, формирующаяся в ходе регулирования Интернета и в ряде других областей мировой политики, призвана дополнить, а не заменить государственное управление. Государству, как ключевому актору в многоуровневой дипломатии, принадлежит ведущая и организующая роль. Вместе с тем, многоуровневый подход отнюдь не исключает интернационализации управления Интернетом и ни в коем случае её не подменяет.

Более того, рождение многоуровневого подхода не означает исчезновения традиционной силовой политики и проведения государствами своих национальных интересов. Так, Дж. Най полагает, что киберпространство не заменит географическое пространство и не уничтожит государственный суверенитет, но будет сосуществовать с ними и значительно усложнит существование суверенных государств и в особенности сильных государств. По мере того, как США формируют свою внешнюю политику в информационную эпоху, им

придётся во всё большей степени осознавать значимость того, каким образом IT создают новые коммуникации, усиливают отдельных граждан и неправительственных акторов и увеличивают роль «мягкой силы»[319]. И действительно, США зачастую используют многоуровневую дипломатию в качестве прикрытия своих интересов в сфере экономики и безопасности. Конечной целью проводимой Вашингтоном политики является сохранение лидерства в информационном пространстве.

Д. Дрезнер в своей статье «Глобальное управление Интернетом: восстановленное влияние государств» на основании анализа регулирования Интернета делает выводы относительно того, что государство отнюдь не утрачивает своих позиций, а наоборот, лишь усиливает своё влияние на процессы глобального управления, в том числе и на процессы глобального управления Интернетом[320].

Ситуация, сложившаяся в сфере управления Интернетом, хорошо описывается с использованием концепции глобального управления, предложенной в 1990 году Дж. Розенау, который отмечал, что современный мир «раздваивается» на два взаимозависимых поля. С одной стороны, это межгосударственные взаимоотношения, определяемые «законами» классической дипломатии и стратегии; с другой – взаимодействие «акторов вне суверенитета», негосударственных участников. Новизну ситуации он характеризовал как «постмеждународную политику». Исследователь подразумевал как новые, так и традиционные (межгосударственные) явления и процессы, подчёркивая растущую роль международных институтов (МВФ, МБ, ВТО), ММПО, предпринимательских структур и иных частных акторов.

Схожую мысль высказывает отечественный политолог А. Коновалов. По его мнению, в настоящее время происходит формирование новой биполярности. Один из её полюсов представлен государствами, которые руководствуются в своём поведении едиными ценностями, правилами и нормами. На другом полюсе группируются как государства, так и негосударственные действующие лица. Проблема для управления Интернетом и глобального управления в более широком контексте заключается в том, что среди государств не наблюдается консолидации. Каждое из государств продолжает действовать, исходя из своих национальных интересов, а не руководствуясь глобальными интересами мирового сообщества в целом. Глобализация только обострила межгосударственное соперничество. Это хорошо видно на примере регулирования столь ценного в экономическом и политическом плане ресурса как Ин-

тернет. Интернационализация регулирования Интернета неизбежно противоречит экономическим и политическим интересам США. Глобальное управление требует частично отказаться от суверенитета, но руководство США продолжает считать, что США должны воздерживаться от обязательств, подрывающих их единоличную роль, дистанцироваться от связывающих их действия международных организаций[321].

3.3.3. Ограничения многоуровневого подхода

Многосторонние партнёрства имеют целый ряд ограничений, которые легко прослеживаются на примере режима управления Интернетом. Одно из них, отчасти являющееся следствием недостаточности накопленного опыта сотрудничества в подобном формате, – это сложности с согласованием большого числа разнородных интересов, необходимым для достижения консенсуса. Как отмечает П.А. Цыганков, сосредоточенный на разных уровнях многослойный конгломерат разнообразных политических субъектов, которые имеют как совпадающие, так и противоположные интересы, потребности и цели, обладают неодинаковым потенциалом, используют разные и зачастую неожиданные средства, очень трудно свести к «единому знаменателю». По мере роста количества акторов, участвующих в управлении, всё сложнее становится обеспечить их устойчивое, эффективное и, главное, результативное взаимодействие[322].

Это усугубляется разрывом в компетенциях и ресурсах, которыми обладают акторы, что в итоге приводит к принятию рядом акторов пассивных стратегий, или еще хуже, прямому противодействию принимаемым решениям. Многие представители развивающихся стран не только не обладают достаточным уровнем развития Интернета и иных ИКТ, но и финансовыми ресурсами, необходимыми для участия в работе различных форумов по этой тематике. В результате, с одной стороны, это приводит к консервации «цифрового разрыва», а с другой, может блокировать переговорный процесс, так как эти государства не заинтересованы в принятии решений и стремятся противодействовать «неоколониализму» развитых государств, блокируя переговорный процесс с целью получения уступок по другим вопросам. Что же касается МНПО и других неправительственных акторов, они, как правило, чувствуют себя исключёнными из межгосударственных механизмов сотрудничества и заявляют, что они

предпочитают процессы принятия решений «снизу-вверх» и консенсусное принятие решений. Всё это ведёт к осложнению взаимодействия в рамках многосторонней модели. Подтверждением тому является медленный прогресс в ходе ФУИ. Возможно, ситуация может быть разрешена в случае перехвата инициативы в сфере управления Интернетом со стороны МСЭ.

Это приводит к резкой критике многосторонних механизмов управления Интернетом и призывам исключить МНПО и бизнес-акторов из процессов принятия решений. Всё более популярной становится точка зрения, согласно которой ничего фактически не изменилось с появлением Интернета, и международный режим – это необходимость согласования различных национальных интересов скоординированным и справедливым способом. Без общего регулирующего института будут неизбежные негативные последствия. В соответствии с этой точкой зрения, МСЭ традиционно справлялся с регулированием телекоммуникаций и должен продолжать этим заниматься. Ряд экспертов, исследующих вопросы, связанные с управлением Интернетом, полагают, что возвращение к традиционным межгосударственным переговорам было бы более эффективным и, возможно, даже более демократичным.

Сходной позиции придерживается ещё один значимый актор, Китай, также выступающий за переход к межгосударственной модели регулирования. Китай, скорее, склонен поддерживать усиление позиций МСЭ в сфере управления Интернетом, в частности, это неоднократно отмечали в своих выступлениях официальные представители государства, в том числе в ходе Всемирной конференции по управлению Интернетом в Учжене[323]. При этом МСЭ в соответствии с позицией Китая отводятся функции технической координации, а культурные, политические и иные аспекты регулирования Интернета должны оставаться в ведении специализированных организаций, таких как ЮНЕСКО, ВОИС и др. Таким образом, позиция Китая состоит в том, чтобы вернутся к межгосударственному согласованию в рамках множества форумов. В этих условиях международные институты будут выполнять взаимодополняющие и в ряде случаев взаимозаменяемые функции, что позволит государствам проводить более гибкую политику.

Ряд авторов делает предложения относительно оптимизации переговорного процесса в рамках многосторонней модели, в том числе ФУИ. Так, ранее Дж. Малкольм предлагал усилить влияние секретариата ФУИ и перестроить переговорный процесс таким

образом, чтобы взаимодействие шло между тремя различными группами акторов: правительствами, организациями гражданского общества, представителями бизнес-сообщества. Итоговые документы, таким образом, должны являться результатом согласования агрегированных позиций этих заинтересованных групп[324].

Мандат Глобального форума по управлению интернетом был продлен в 2015 году на 10 лет, и следующий форум по управлению интернетом, который будет заключительным в рамках текущего 10-летнего мандата, пройдёт в июне 2025 года в Норвегии. А в сентябре 2025 года Генеральная Ассамблея ООН на Всемирной встрече по информационному обществу (WSIS+20) подведёт итоги и обсудит возможное продление мандата IGF.

На наш взгляд, оптимальный вариант – использование предыдущего опыта успешного многостороннего сотрудничества. Речь идет о ВВУИО и, в особенности, РГУИ, которые, очевидно, были более плодотворными, чем ФУИ, а в более широком контексте можно использовать опыт заключения Соглашения о запрете противопехотных мин[325]. Приведённые выше примеры демонстрируют тот факт, что решения (официальные документы, имеющие силу международного права) должны приниматься исключительно государствами, которые ответственны перед гражданами, обладают легитимностью, правосубъектностью и ресурсами, необходимыми для реализации достигнутых соглашений; в то же время, мнение других акторов (в том числе и представителей МНПО) может быть услышано и принято во внимание. Эти модели сотрудничества характеризуются ограничениями, накладываемыми на возможности участия неправительственных акторов. Таким образом, ограниченная многосторонность позволит обойти ограничения современных ММПО и в то же время добиться реальных результатов. На сегодняшний день это возможный вариант организации конструктивного, предметного и результативного диалога, который, в свою очередь, опирается на более ранний опыт традиционного межгосударственного сотрудничества. Подобный формат позволяет обеспечить преемственность в развитии моделей сотрудничества, что и будет являться залогом успеха. В этой связи МСЭ, который давно сотрудничает с крупным бизнесом и уже рассматривает возможности включения в свою работу представителей МНПО, представляется оптимальным институтом, который мог бы осуществлять международное управление Интернетом.

3.3.4. Реформирование системы управления Интернетом: концептуальное осмысление и позиция России

Оставаясь ключевыми носителями суверенитета, национальные государства мирового большинства являются наиболее активными сторонниками реформы системы управления Интернетом в интересах расширения их влияния. Далее представлен обзор нескольких основных концепций реформирования системы управления Интернетом, отличающихся как практической целесообразностью и реализуемостью, так и потенциальными выгодоприобретателями.

Концепции реформирования системы управления Интернетом, их основные бенефициары и противоречия

Краткое изложение концепции	Ключевой (ые) выгодоприобретатель (и)	Противоречия
Максимизация цифрового суверенитета государства	Национальные государства с высоким уровнем цифровой развитости	Техническая сложность установления всеобъемлющего контроля над устройствами с функцией сетевого доступа
Интернет как «новая Антарктида» и глобальное общественное благо	ICANN (после реформирования) и её основные спонсоры	Амбициозный характер предлагаемых реформ, вероятные трудности согласования необходимых изменений, излишне «громоздкая» ICANN
«Совет управления Интернетом» с мандатом «Группы двадцати»	Ведущие индустриально развитые державы в составе «Группы двадцати»	Противоречия внутри «двадцатки», проблематичность обеспечения легитимности принимаемых решений
Реформа негосударственных институтов управления Интернетом	Национальные государства с высоким уровнем цифровой развитости	Не решает большинство выявленных проблем

Максимизация цифрового суверенитета государств

Первым среди рассматриваемых и наиболее радикальным сценарием реформирования системы управления Интернетом является полноценная реализация цифрового суверенитета государства. Концепция была рассмотрена в 2019 году в аналитическом эссе М. Мюллера, который выступил с критикой данного подхода[326].

Идея предполагает формирование множества территориально обусловленных и обособленных друг от друга национальных киберпространств. В текущем виде глобальное киберпространство опирается на единые технические стандарты, в таких условиях формирование настоящих обособленных национальных сегментов невозможно – при этом до определённой степени национальные государства могут устанавливать контроль над передаваемой информацией, однако предпринимаемые меры, как правило, слишком затратны и малоэффективны.

Что означает для глобального Интернета и вовлечённых в управление им акторов полноценная реализация цифрового суверенитета государства? Во-первых, будут практически повсеместно упразднены автономные сети, границы которых фактически выходили бы за рамки конкретной территориальной юрисдикции. Во-вторых, произойдёт полная увязка сетевых идентификаторов с конкретными юрисдикциями, в частности, доменных имён, адресов сетевых устройств и т.д., что в настоящий момент находится в распоряжении негосударственных организаций по типу ICANN. В-третьих, повсеместное внедрение контролируемых государством узлов выхода в «международный» Интернет сделает невозможным предоставление трансграничных цифровых услуг; в каждом отдельном случае поставщик цифровых услуг будет вынужден в индивидуальном порядке определять условия сотрудничества с каждым национальным государством. В-четвертых, будут учреждены специализированные государственные органы сертификации индивидуальных пользовательских устройств сетевого доступа, программных продуктов и базового инфраструктурного оборудования. Наконец, в-пятых, случится институциализация таких мер верификации и отслеживания, которые позволят полностью контролировать передачу и хранение всех данных в рамках одного сегмента сети, обеспечив тем самым полное выполнение требований о локализации данных. Мюллер сравнивает эту ситуацию с режимом работы телефонных, почтовых и телеграфных сетей. Итоговая «география» Интернета будет совершенно отличной от той, которую мы имеем сейчас – произойдёт «балканизация», то есть разделение некогда единого пространства

на более мелкие подпространства, которые могут быть враждебно настроены по отношению друг к другу[327].

В текущем виде «Группа двадцати» является эффективной, но недостаточно репрезентативной площадкой для согласования коллективных решений. Следует принять во внимание существующие противоречия внутри «Группы двадцати». В настоящий момент очевидно наличие трудностей, связанных с формулированием недекларативных решений во взаимодействии России, США и других стран Запада, которые предпринимают попытки отстранить Россию от участия в многосторонней дискуссии. Несмотря на то, что Россия неизменно получает поддержку от других стран-членов «двадцатки» в вопросе о допустимости ограничения её членства в неформальном межгосударственном клубе[328], глубина текущих проблем в отношениях двух стран, в полной мере проявивших себя на площадке ООН в переговорах о кибербезопасности, ставит под вопрос возможность выработки компромисса даже с учётом неформального характера дискуссии в «Группе двадцати».

Другая важная проблема – влияние «Группы семи» на процесс принятия решений в «двадцатке». «Семёрка» может рассматриваться как полноценная и консолидированная группа влияния внутри «двадцатки», способная достаточно эффективно продавливать необходимые ей решения или, по крайней мере, препятствовать принятию невыгодных ей обязательств. В рамках «двадцатки» только БРИКС может рассматриваться как полноценная альтернатива «Группе семи», отстаивающая интересы развивающихся стран или глобального Юга в широком смысле, однако раскол членского состава форума на две противоборствующие группировки приведёт к утрате «двадцаткой» её основных конкурентных преимуществ, а именно гибкости в определении повестки работы и сравнительно более высокой эффективности в процессе принятия решений.

С точки зрения реализуемости данный сценарий представляется возможным, но его реализация сопряжена со множеством трудностей. Создание Совета финансовой стабильности стало своего рода экстренной мерой, призванной обеспечить скорейшую стабилизацию мирового финансового рынка, что позволило избежать стадии продолжительного многостороннего согласования. Даже в текущих условиях взаимного недоверия и усиления конкуренции государств за влияние в киберпространстве создание условного «Совета управления Интернетом» не следует рассматривать как срочную меру, экстренность которой способна снять вопросы о легитимности подобного решения.

Реформа негосударственных институтов управления Интернетом

Наиболее мягкий сценарий дальнейшего развития системы управления Интернетом был представлен в совместной работе Игнатова А.А. и Васильковского С.А.[329]

Анализ системы управления Интернетом на современном этапе выявил наличие таких фундаментальных проблем как децентрализованность и недостаточная легитимность принимаемых решений. Проблема легитимности и подотчётности была атрибутирована авторами к таким институтам управления Интернетом как ICANN и «Общество Интернета». Было отмечено, что «Общество Интернета» в принципе не имеет в своей структуре органов, отвечающих за взаимодействие с органами государственной власти. Корпорация имеет в своем составе комитет государственных представителей, однако эта структура не создаёт механизмов обратной связи с государствами, то есть не даёт им возможность влиять на процесс принятия решений.

Таким образом, прежде всего, авторы предлагают предпринять шаги по решению проблемы подотчётности системы управления Интернетом. Предлагается начать с учреждения в системе «Общества Интернета» органа, аналогичного по своему функционалу комитету государственных представителей ICANN. Далее обе структуры должны получить более широкие полномочия и право голоса в процессе назначения ключевых фигур в руководстве организаций. Авторы концепции считают, что данная мера уравняет государства в правах с остальными участниками процесса, в частности, с медийными корпорациями, что значительно продвинет систему управления Интернетом по пути реализации принципов Декларации 2003 года[330].

Среди описанных сценариев данная схема представляется наименее конфликтогенной и противоречивой, однако и масштаб предлагаемых изменений остаётся достаточно ограниченным. Предложенный сценарий не решает многие из проблем, выявленных в системе управления Интернетом в ходе исследования, в частности, никаких изменений не предполагается в области согласования общих принципов режима управления Интернетом. В соответствии с ранее описанной концепцией оценки влияния различных групп акторов в системе управления Интернетом, данный сценарий фактически ограничивается повышением значимости государств в технологическом аспекте управления сетью. Сценарий также не предлагает пути уравнивания влияния государств с высоким уровнем развития цифровой экономики в целом и сильным цифровым частным сектором и теми

государствами, которые отстают в отношении технологического и рыночного развития; в данном случае, как и в других описанных сценариях, выгодополучателями остаются высокоразвитые в цифровом отношении государства, тем самым ключевые диспропорции современной цифровой экономики воспроизводят сами себя.

В целом, анализ представленных на данный момент концепций реформирования системы управления Интернетом показывает, что основной вектор трансформаций пронизывает аспект вовлечённости государств в управление сетью. Общим для всех сценариев моментом является то, что любые гипотетические изменения в положении национальных государств принесут выгоды, прежде всего, развитым цифровым державам, которые способны максимизировать выгоды, создаваемые новым положением. Например, достаточно очевидным и не требующим дополнительного обоснования следствием реализации цифрового суверенитета государства на пространстве Интернета будет формирование более крупных транснациональных обособленных сегментов глобальной сети во главе с ведущими державами, способными обеспечить «полный цикл» реализации концепции от разработки новых технологических регламентов до формирования соответствующих институтов и практик тотального цифрового контроля. Схожий финал можно ожидать и в случае, если «Группа двадцати» сумеет согласовать решение о создании Совета управления Интернетом и приступит к реализации предлагаемых им решений – желаемая многосторонность системы управления сетью будет подменена безальтернативностью навязываемых ведущими государствами принципов и готовых практических рекомендаций.

Важно отметить, что из всех рассмотренных сценариев только один, предлагающий закрепление за Интернетом статуса глобального общественного блага, работает со всей совокупностью проблем современной системы управления Интернетом, в то время как первый сценарий предполагает упразднение системы управления глобальным Интернетом как таковой, а третий и четвертый воспроизводят существующие системные противоречия и существенным образом не меняют суть системы. Одновременно необходимо признать невозможность длительного поддержания статус-кво в связи с экспоненциальным ростом угроз цифровой безопасности и следующими за этим попытками национальных государств усилить свое цифровое присутствие; ограниченность имеющихся у государств рычагов влияния на принимаемые решения приводит к росту антагонизма и делает сценарий «балканизации» Интернета всё более реальным.

ЗАКЛЮЧЕНИЕ

ЗАКЛЮЧЕНИЕ

Значимость цифровых технологий с точки зрения международной политики объясняется, прежде всего, их значимостью с точки зрения охвата по количеству пользователей, масштабам использования и степени проникновения во все сферы жизни общества и государства. Охват цифровых технологий беспрецедентен. На конец 2023 г. доступ к Интернету имело порядка 70% населения планеты[331], при этом в среднем люди проводили онлайн порядка 6.5 часов в день на различных платформах и сервисах. Использование цифровых технологий и платформенных решений определяет то, как люди общаются, работают и совершают покупки, получают услуги.

Видение глобального Интернета, в котором нет государственных границ, характерное для 1990-х–2000-х гг., не оправдало себя. Государства и региональные организации проводят политику выделения национальных и региональных сегментов сети. На современном этапе цифровой дипломатии важнейшую роль играет обеспечения цифрового суверенитета и стратегической автономии в информационном пространстве.

Интернет был создан как исследовательский проект, поддержанный Министерством обороны США и до сих пор отдельные функции технического управления Интернетом, а именно координация пространства имен и адресов Интернета, находятся под контролем частной некоммерческой организации, расположенной на территории США – PTI, Public Technical Identifiers. Данная организация зарегистрирована на территории США и подчиняется законам данной страны. Россия выступает за передачу этих функций под эгиду ООН или специализированной организации ООН – Международного союза электросвязи (МСЭ).

В 2003 и 2005 гг. в два этапа прошла Всемирная встреча на высшем уровне по вопросам информационного общества, по итогам которой был создан Форум по вопросам управления Интернетом. Форум представляет собой площадку для обсуждения вопросов управления Интернетом, в которой принимают участие представители государств, бизнеса и гражданского общества. Столь широкий формат участия дает возможность для инклюзивного обсуждения, однако, затрудняет принятие

решений. Россия исходит из того, что вопросы безопасности и управления Интернетом необходимо обсуждать прежде всего, на межгосударственном уровне, в силу того что только государства обладают легитимностью и возможностями обеспечения безопасности, в том числе и в сфере управления Интернетом. Последняя сессия Форума прошла в 2024 г. в Саудовской Аравии, и одной из ключевых тем стали вопросы фрагментации Интернета. Также обсуждались внедрение инноваций и управление рисками в цифровом пространстве, усилении роли технологий в поддержании мира, стимулировании устойчивого развития и содействии инклюзии. Особое внимание было уделено защите прав человека в цифровой среде и совершенствованию процессов управления Интернетом.

Россия исходит из необходимости интернационализации управления Интернетом и апеллирует к следующим принципам: равные права и обязанности в сфере управления Интернетом, недопущение доступа к сети Интернет как инструмента влияния на другие государства, воздержание государств от действий, направленных на ограничение функционирования или доступа к сети Интернет на территории других государств, суверенные права государств на управление национальным сегментом сети Интернет.

Россия выступает за формирование международного режима в области информационной безопасности, основанного на уважении государственного суверенитета в цифровой среде, мирном развитии цифровых технологий и предотвращении конфликтов в данной области. Следует отметить, что развитие ИИ, с одной стороны, порождает целый ряд новых вызовов и угроз информационной безопасности, а с другой – создает новые инструменты дипломатической работы. При этом развитие ИИ в контексте международной политики и безопасности диктует необходимость выработки единого понятийного аппарата на международном уровне; определения сфер, требующих наднационального регулирования; консолидации подходов всех государств на принципах равноправия, взаимоуважения и иных принципов, основанных на уважении Устава ООН как фундамента современного международного права.

ПРИМЕЧАНИЯ

1 IP – интернет-протокол разбивает информацию на пакеты, отмечая адреса отправителя и получателя информации, чтобы пакеты могли достичь адресата. TCP – протокол, отвечающий за качество передачи информации.

2 DNS (англ. Domain Name System — система доменных имён) — распределённая система (распределённая база данных), способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить IP-адрес или (в зависимости от запроса) другую информацию.

3 Shapiro A. The control revolution: how the Internet is putting individuals in charge and changing the world we know — N.Y.: Public Affairs, 1999 — 286 p.; Menthe D., Jurisdiction In Cyberspace: A Theory of International Spaces // Michmann Telecommunication Technical Revue - № 69 http://www.law.umich.edu/mttlr/vol-four/menthe.html

4 Mueller M. L. Against sovereignty in cyberspace //International studies review, 2020. Т. 22. №. 4 – с. 779-801.

5 Зиновьева Е.С. Международное управление Интернетом: конфликт и сотрудничество. М.: МГИМО, 2011.

6 UNCTAD Digital Economy Report 2019 https://digital.econ.cam.ac.uk/digital-economics-policy-focus/unctad-2019-digital-economy-report

7 Песков Д.Н. Интернет в мировой политике // Современные международные отношения и мировая политика / Под ред. Торкунова А.В. М.: Просвещение, 2004 – с. 223.

8 Там же.

9 www.igp.org – официальный сайт «Проекта управления Интеретом».

10 Mathiason J. Internet Governance: The State of Play // Internet Governance Project, 2004 http://dcc.syr.edu/miscarticles/MainReport-final.pdf

11 www.statista.com

12 https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2024-v-mire-i-v-rossii/

13 https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/

14 www.statista.com

15 https://www.web-canape.ru/business/statistika-interneta-i-socsetej-na-2024-v-mire-i-v-rossii/

16 Там же.

17 Там же.

18 Там же.

19 Многоязычные доменные имена - имена, представленные символами национальных алфавитов, а не только латинского алфавита.

20 Динамические IP-адреса присваиваются устройству, подключаемому к сети, только на время подключения, в отличие от традиционных, статических IP-адресов, которые присваиваются устройствам (персональным компьютерам) на неограниченный период времени.

21 https://www.unep.org/ru/novosti-i-istorii/istoriya/iskusstvennyy-intellekt-sozdaet-ekologicheskie-problemy-chto-my-mozhem

22 Там же.

23 См. напр.: Cavelty M. The Resurgence of the State: Trends and Processes in Cyberspace Governance / M.Cavelty, M.Dunn, S.Krishna-Hensel, V.Mauer - Asghate: Ashgate Publishing, Ltd., 2007 - 165 p.

24 Benhamou B. Souveraineté et Réseaux Numériques / B. Benhamou, L. Sorbier // Politique Étrangère. 2006. № 3 http://www.netgouvernance.org/politiqueetrangere.pdf

25 Rosenau J. Governance in the 21st century // Global governance: a review of multilateralism and international organization – 1995. № 1 (1) – p. 13.

26 Там же – p. 14.

27 Stokke O. Regimes as governance systems // Global governance: drawing Insights from the environmental experience / Edited by Young O – Cambridge, 1997 - p. 28.

28 Хэлд Д. Глобальные трансформации: политика, экономика, культура / Хэлд Д., Гольдблатт Д., Макгрю Э., Перратон Дж. / Пер. с англ. – М.: Праксис, 2004 - с. 57.

29 Kleinwächter W. Internet Co-Governance. Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation (M3C3) // E–Learning. 2006 - № 3(3) https://www.wgig.org/docs/

Kleinwachter.pdf

30 Raboy M. The World Summit on the Information Society and its legacy for global governance // The international journal for communication studies. 2004 – № 3-4 (66) – p. 225–232.

31 Доклад рабочей группы по управлению Интернетом - Шато де Босси, 2005 http://www.wgig.org/docs/WGIGReport-Russian.doc

32 Там же.

33 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества - 18 ноября 2005 года http://www.itu.int/wsis/docs2/tunis/off/6rev1-ru.pdf

34 Курбалийя Й., Гелбстайн Э. Управление Интернетом: проблемы, субъекты, преграды / Пер. с англ. Михеева А.Н., Лазуткиной А.В. – М.: МГИМО, 2005 – 184 с.; Cukier K. The Next Internet Governance Battles // The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment / Ed. By Kleinwächter, W. – Berlin: Wagner Translations Ltd., 2008 – p. 285-296; Kleinwächter W. Internet Co-Governance. Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation (M3C3) // E–Learning – 2006 — № 3(3)

35 Krasner S. Structural causes and regime consequence: regimes as intervening variables // International Regimes / Ed. by Krasner S - Ithaca, 1983 - p. 2.

36 Mathiason J., Mueller M., Klein H., Holitscher M., McKnight L. Internet governance: The State of Play / Report commissioned by the UN ICT Task Force - 2004

37 Mueller M. Mathiason J. McKnight L. Making sense of "Internet governance": defining principles and norms in a policy context // Internet Governance: a grand collaboration. An edited collection of papers / Ed. by MacLean D. - New York, 2004 - p. 105.

38 Там же.

39 https://www.belfercenter.org/publication/national-cyber-power-index-2022

40 См. статистику Oxford Internet Institute. URL: http://geography.oii.ox.ac.uk/

41 Стратегическое прогнозирование международных отношений. Коллективная монография / Под ред. А.И. Подберёзкина, М.В. Александрова - М.: МГИМО, 2016 - с. 338.

42 См. напр.: UNCTAD World investment report 2014 Investing in the SDGs: an Action Plan. UNCTAD/WIR/2014. Geneva, 2014. URL: https://unctad.org/publication/world-investment-report-2014

43 Стратегическое прогнозирование международных отношений. Коллективная монография / Под ред. А.И. Подберёзкина, М.В. Александрова - М.: МГИМО, 2016 - с. 337.

44 Governance.com: democracy in the information age / Ed. by Kamarck C., Nye J. – Washington, D.C.: Brookings Institution Press, 2002. – 192 p.; Chadwick A., Howard P. Routledge Handbook of Internet Politics – London: Taylor & Francis, 2008 — 496 p.

45 Friedman T. The Lexus and the Olive Tree – N.Y.: Farrar Straus & Giroux, 1999 — 394 p.

46 Friedman T. The world is flat: a brief history of the twenty-first century — N.Y.: Farrar, Straus and Giroux, 2007 — 660 p.

47 Rauscher K. F., Yaschenko V. Russia–US Bilateral on Cyber Security: Critical Terminology Foundations // NY: East West Institute. 2011. URL: https://www.files.ethz.ch/isn/130080/Russia-U%20S%20%20bilateral%20on%20terminology%20v76%20(2)-1.pdf

48 Михеев А.Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности? // Современные глобальные проблемы мировой политики / под ред. Лебедевой М.М. — М.: Аспект Пресс, 2008 – с.139-152.

49 Hofmann J. Internet Governance: A Regulative Idea in Flux // Social Science Research Centre - Berlin, 2005 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327121

50 Там же.

51 Kleinwächter W. De-Mystification of the Internet Root: Do we need Governmental Oversight? //Reforming Internet Governance. Perspectives from the Working Group on Internet Governance / Ed. By Drake W. – United Nations, ICT Task Force Series, 2005. - https://www.wgig.org/docs/book/Wolfgang_Kleinwächter.html

52 Council of the European Union and the European Commission. Reply of the European Community and its Member States to the US Green Paper – 1998. Цит. по Hofmann J. Internet Governance: A Regulative Idea in

Flux // Social Science Research Centre - Berlin, 2005 - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327121

53 Joint Project Agreement between the US Department of Commerce and the Internet Corporation for Assigned Names and Numbers — 2006 — http://www.ntia.doc.gov/ntiahome/domainname/icann.htm

54 Shaw R. Reflection on Governments, Governance and Sovereignty in the Internet Age — August 24, 1999 – http://web.archive.org/web/20010112082400/http://people.itu.int/~shaw/docs/reflections-on-ggs.htm

55 International Telecommunications Union. Basic Information: About WSIS - http://www.itu.int/wsis/basic/about.html

56 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство - 18 ноября 2005 года - https://www.itu.int/net/wsis/docs2/tunis/off/7-ru.pdf

57 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества — 18 ноября 2005 года — https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

58 Крутских, А.В., Зиновьева, Е.С., Булва, В.И., Алборова, М.Б., Юдина, Ю.А. (2022) Международная информационная безопасность: подходы России.

59 Примаков Е.М. Международные отношения накануне XXI века: проблемы, перспективы // Международная жизнь. 1996. № 10. с. 3-13. https://general-history.ucoz.ru/primakov.pdf

60 А. Дробинин. Уроки истории и образ будущего: размышления о внешней политике России // Международная жизнь. 03.08.2022 https://interaffairs.ru/news/show/36410

61 Лавров С.В. ООН: вновь быть центром для согласования действий наций // Россия в глобальной политике. № 6, 2024, ноябрь/декабрь - DOI: 10.31278/1810-6439-2024-22-6-98-110

62 Declaration for the Future of `Internet. USA Department of State, 2022 https://www.state.gov/declaration-for-the-future-of-the-internet

63 https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

64 Глобальная инициатива в области безопасности данных МИД КНР,

2020 (на английском языке) // Global Initiative on Data Security. MFA of PRC, 08 Septemeber, 2020.

65 Recommendation of the Council on Artificial Intelligence, 2019 OECD/LEGAL/0449.

66 Дорожная карта «Группы семи» по сотрудничеству в области свободных потоков данных и доверия. Лондон, 2021 (на английском языке) – извлечение.

67 См.: Castells M. Communication, Power and Counter-power in the Network Society // International Journal of Communication – 2007 - № 1 - p. 238-266.

68 См. напр.: Carr M. Power plays in global internet governance // Millennium - 2015 - T. 43 - №. 2 - p. 640-659.

69 IANA Naming Function Contract. 30 September 2016. https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

70 Щёголев И. Весь наш Интернет уязвим к внешнему воздействию // РБК. 27.03.2017. http://www.rbc.ru/newspaper/2017/03/27/58d3bc559a79471ca8c1fbbd

71 Cukier K. The Next Internet Governance Battles // The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment / Ed. by W. Kleinwächter - Berlin: Wagner Translations Ltd., 2008 - p. 285-296.; Cukier K. The WSIS Wars: an Analysis of the Politicization of the Internet // The World Summit on the Information Society: Moving from the Past into the Future / Ed. by D. Stauffacher, W. Kleinwächter - NY: UN, ICT Task Force Series, 2005.

72 Концепция безопасного функционирования и развития сети «Интернет» от 27.07.2017.

73 Cukier K. Multilateral Control of Internet Infrastructure and its Impact on US Sovereignty // Telecommunications Policy and Research Conference - Alexandria, VA. October 2004; Dutton W. The emerging internet governance mosaic: connecting the pieces: Discussion Paper No 5 / W.Dutton, M. Peltu // Oxford Internet Institute Forum - Oxford, 2005; Dutton W. The New Politics of the Internet. Multistakeholder Policy Making and the Internet Technocracy / W. Dutton, M. Peltu // Routledge Handbook of Internet Politics / Ed. by A.Chadwick, P.Howard - London: Routledge, 2008 - p. 384-401; Hofmann J. Internet Governance: A Regulative Idea in Flux // Social Science Research Centre - Berlin, 2005; Klein H. Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society // The Massachusetts Institute of

Technology Information Technologies and International Development - 2004 - № 3–4 (1) - p. 3-13; Kleinwächter W. Global Governance in the Information Age // Center for Internet Research, University of Aarhus - 2001 - p. 1–46; Kleinwächter W. De-Mystification of the Internet Root: Do we need Governmental Oversight? // Reforming Internet Governance. Perspectives from the Working Group on Internet Governance / Ed. by W. Drake – N.Y.: UN, ICT Task Force Series, 2005; Kleinwächter W. Internet Co-Governance. Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation (M3C3) // E–Learning - 2006 - № 3(3).

74 National Security Strategy of the USA. White House. December, 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

75 Доклад рабочей группы по управлению Интернетом ООН. Шато де Босси, 2005 г. – http://www.wgig.org/docs/WGIGReport-Russian.doc

76 Михеев А.Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности? // Современные глобальные проблемы мировой политики / под ред. Лебедевой М.М. - М. 2008.

77 Dutton W., M. Peltu. The emerging internet governance mosaic: connecting the pieces // Discussion Paper No 5. // Oxford Internet Institute Forum – Oxford, 2005.

78 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии — 12 декабря 2003 года. http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf

79 Mueller M. Ruling the Root: Internet Governance and the Taming of Cyberspace. London: MIT Press, 2002 — p. 68.

80 Barlow J. A Declaration of the Independence of Cyberspace – 1996 — http://homes.eff.org/~barlow/Declaration-Final.html

81 Михеев А.Н. Информационно-коммуникационные технологии: глобальные проблемы и/или глобальные возможности? // Современные глобальные проблемы мировой политики / под ред. Лебедевой М.М. — М.: Аспект Пресс, 2008 – с. 139-152.

82 Lessig, L. Code: And Other Laws of Cyberspace – Basic Books, New York, 1999.

83 Там же.

84 Reidenberg J. Lex Informatica: The Formulation of Information Policy Rules Through Technology // Texas Law Review - # 3 (76) - 1998 – p. 553-584.

85 MacLean D. Herding cats: Some conceptual tools for thinking about Internet governance // Internet Governance: a grand collaboration. An edited collection of papers. Edited by MacLean D. New York, 2004, p. 73-100.

86 Хрусталев М.А. Анализ международных ситуаций и политическая экспертиза. Очерки теории и методологии – М., 2008 – 320 с.

87 Internet Fragmentation: An Overview. World Economic Forum. 2016 https://www.weforum.org/reports/internet-fragmentation-an-overview.

88 UNCTAD Digital Economy Report 2021 https://unctad.org/webflyer/digital-economy-report-2021.

89 См. напр.: Capri A. Techno-Nationalism: What Is It And How Will It Change Global Commerce? Forbes. 20.12.2019 https://www.forbes.com/sites/alexcapri/2019/12/20/techno-nationalism-what-is-it-and-how-will-it-change-global-commerce/?sh=77705a7c710f.

90 Безопасность в Интернете достигается не запретами. Россия сегодня. 05.06.2019. https://1prime.ru/telecommunications_and_technologies/20190605/830039744.html.

91 См. напр.: International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World. US White House. 2011 https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

92 IP-адрес – уникальный адрес, которым должно обладать каждое устройство, подключаемое к Интернету. Текущая версия базового интернет-протокола IPv4 предполагает наличие ограниченного количества IP-адресов, что делает их потенциально оспариваемым ресурсом. Современные технологические решения в большинстве случаев позволяют обойти данное ограничение.

93 На основании Internet World Stats http://www.Internetworldstats.com.

94 См. WSIS-03/GENEVA/DOC/5-R. Всемирная встреча на высшем уровне по вопросам информационного общества. План действий. 12.12.2003 http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-R.pdf.

95 См. Заявление Совета глав государств-членов Шанхайской

организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 10.11.2020 https://www.fmprc.gov.cn/rus/zxxx/t1831178.shtml.

96 См. A/70/174 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 22.07.2015 https://daccess-ods.un.org/TMP/6949319.83947754.html.

97 См. В России вступил в силу «Закон о суверенном Рунете». РБК. 01.11.2019 https://www.rbc.ru/technology_and_media/01/11/2019/5dbb1cb49a7947777b009bd6; Global Initiative on Data Security. Ministry of Foreign Affairs of the People's Republic of China. 09.08.2020 https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml; EU Data Strategy. European Commission. 2020 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

98 Ritchell M. Egypt Cuts Off Most Internet and Cell Service. NY Times. 28.01.2011 https://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html.

99 Baraniuk C. Iran's Internet Blackout Reaches Four-Day Mark. BBC News. 20.11.2019 https://www.bbc.com/news/technology-50490898.

100 OECD Digital Economy Indicators. 2020. https://www.oecd.org/en/publications/oecd-digital-economy-outlook-2020_bb167041-en/full-report.html#section-1.

101 См. напр.: Доктрина информационной безопасности Российской Федерации https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html; Global Initiative on Data Security Ministry of Foreign Affairs of the Peoples Republic of China. 2020 https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1812951.shtml; EU Data Strategy. European Commission 2020 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

102 UNCTAD Digital Economy Report 2021.

103 Haas P. Epistemic Communities and International-Policy Coordination - Introduction //International Organization - 1992 - № 46 (1) - p. 1-35.

104 Franda M. Governing the Internet: The Emergence of an International Regime - Boulder: Lynne Rienner Publishers, 2001 – p. 215.

105 DNS (англ. Domain Name System — система доменных имён) — распределённая система (распределённая база данных),

способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить IP-адрес, или (в зависимости от запроса) другую информацию.

106 Contract Between ICANN and the United States Government for Performance of the IANA Function — 1998 http://www.icann.org/en/general/iana-contract-09feb00.htm; Memorandum of Understanding Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers — 1998.

107 IANA Naming Function Contract. 30 September 2016 https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

108 Там же.

109 Россия будет добиваться изменения системы управления Интернетом в мире // РБК 27.03.2017 http://www.rbc.ru/technology_and_media/27/03/2017/58d508179a7947d969c13c50

110 Carr M. Power Plays in Global Internet Governance //Millennium-Journal of International Studies - 2015 - T. 43 - №. 2 - p. 641.

111 Mueller M. The Internet and Global Governance: Principles and Norms for a New Regime / M.Mueller, J.Mathiason, H.Klein // Global Governance – 2007 – № 13 http://www.atypon-link.com/LRP/doi/abs/10.5555/ggov.2007.13.2.237

112 См. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

113 См. https://www.state.gov/declaration-for-the-future-of-the-internet

114 https://www.mfa.gov.cn/rus/mtfw/ce_cegw_chn/lxjzhzhdh/202407/t20240704_11448043.html

115 Там же

116 Денисов, И.Е. Китайская стратегия «больших данных»: реформа управления, инновации и глобальная конкуренция. М.: Издательство «МГИМО-Университет», 2023. 28 с. https://mgimo.ru/upload/iblock/522/ed8xn1kq6rg7ffp8z83iifh692z3qhfw/china-big-data-strategy.pdf

117 Там же.

118 Там же.

119 История развития Интернета в России // РИА Новости. URL: https://ria.ru/20240407/internet-1938028291.html

120 Там же.

121 Там же.

122 https://trends.rbc.ru/trends/industry/661011a39a79473fc8582c77

123 Там же.

124 https://www.rbc.ru/technology_and_media/11/12/2024/6759b4709a79472b45d8949e

125 https://issek.hse.ru/news/892383987.html

126 Там же.

127 https://smartcity.cnews.ru/news/top/2018-07-24_moskva_stala_liderom_rejtinga_oon_po_okazaniyu

128 https://национальныепроекты.рф/new-projects/ekonomika-dannykh/

129 Там же.

130 30 самых дорогих компаний Рунета 2025. Рейтинг Форбс. https://www.forbes.ru/biznes/531064-lidery-rejtinga-samyh-dorogih-kompanij-runeta-2025

131 Там же.

132 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-03/GENEVA/DOC/4-R. Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии - 12 декабря 2003 года - http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf

133 Итоговый документ международного семинара «Управление использованием Интернет». Кишинев, 2005 г. - http://www.rcc.org.ru/ru/news/documents/2005-01.doc

134 Нью-Делийская декларация ШОС. Нью Дели, 2023.

135 Астанинская декларация ШОС. Астана, 2024.

136 Там же.

137 Гуржий А. О программе ЮНЕСКО «Информация для всех» и участии в ней Российской Федерации (справка) // Официальный сайт программы ЮНЕСКО «Информация для всех» - http://www.ifap.ru/404.htm

138 Игнатов А.А. Управление Интернетом в повестке БРИКС // Вестник международных организаций: образование, наука, новая экономика. 2022. № 2.

139 Зиновьева Е. Что не так с глобальным цифровым договором // РСМД, 2024 https://russiancouncil.ru/analytics-and-comments/

analytics/chto-ne-tak-s-globalnym-tsifrovym-dogovorom/

140 Щёголев И. Весь наш Интернет уязвим к внешнему воздействию // РБК. 27.03.2017 http://www.rbc.ru/newspaper/2017/03/27/58d3bc559a79471ca8c1fbbd

141 В ходе голосования на площадке Генеральной Ассамблеи ООН были приняты решения, санкционировавшие создание ГПЭ и РГОС, Форума управления Интернетом, а также Форума ВВУИО.

142 Итоговый документ совещания высокого уровня Генеральной Ассамблеи, посвященного общему обзору хода осуществления решений Всемирной встречи на высшем уровне по вопросам информационного общества. Резолюция A/RES/70/125 // ООН – URL: https://docs.un.org/en/A/RES/70/125

143 Resolution 73 of the ITU Plenipotentiary Conference, Minneapolis, 1998 // Международный союз электросвязи – URL: https://www.itu.int/net/wsis/docs/background/resolutions/73.html

144 Resolution 56/183. World Summit on the Information Society // Международный союз электросвязи – Текст: электронный - URL: https://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002.pdf

145 Mathiason, J., Mueller, L.M., Klein, H. The Internet and Global Governance: Principles and Norms for a New Regime // Global Governance. Vol. 13. No 2. 2017. – P. 240.

146 Document WSIS-03/GENEVA/DOC/5-E Plan of Action // Правительство Республики Индия – URL: https://www.itu.int/net/wsis/docs/geneva/official/poa.html. Следует отметить, что Женевский план действий включает в себя гораздо более широкий перечень приоритетов, в общем смысле укладывающихся в такие области как развитие цифровой инфраструктуры и распространение цифровых компетенций/навыков; расширение доступности ИКТ в сельских регионах, образовательных, научных и культурных учреждениях; обеспечение всеобщего глобального доступа к телевидению и радио; развитие многоязычия на пространстве Интернета и т.д.

147 Report of the Working Group on Internet Governance // Working Group on Internet Governance – URL: https://www.wgig.org/docs/WGIGREPORT.pdf

148 Исходный текст: «Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making

procedures, and programmes that shape the evolution and use of the Internet.». См.: Report of the Working Group on Internet Governance // Working Group on Internet Governance – URL: https://www.wgig.org/docs/WGIGREPORT.pdf

149 Mathiason, J., Mueller, L.M., Klein, H. The Internet and Global Governance: Principles and Norms for a New Regime // Global Governance. Vol. 13. No 2. 2017. – P. 237 – 254.

150 Тунисская программа для информационного общества // Международный союз электросвязи – Текст: электронный - URL: https://www.itu.int/net/wsis/outcome/booklet/tunis-agenda_Cru.html

151 В ходе второго этапа ВВУИО особенно активно себя проявила делегация Китая, которая продавливала концепцию реформирования ICANN с целью исключения американского доминирования, в частности, создание «Глобального совета Интернета», функционирующего на многосторонней основе. См.: Galloway, T, He, B. China and Technical Global Internet Governance: Beijing's Approach to Multi-Stakeholder Governance within ICANN, WSIS and the IGF // China: An international Journal. Vol. 12. No. 3. 2014. – P. 72 – 93.

152 Полный список документов и перечень прошедших встреч доступен здесь: WSIS Implementation by Action Line // Международный союз электросвязи – URL: https://www.itu.int/net/wsis/c3/index.html

153 Нельзя не отметить, что за все время существования МСЭ чаще всего (2 раза) на пост Генерального секретаря избирались представители США (1960 – 1965 гг., Гросс, Г.; текущий Генеральный секретарь Богдан-Мартин Д., занимающая пост с 1 января 2023 г.). Из числа стран БРИКС только представители Индии (1965 – 1967 гг., Сарвате Манохар) и Китая (2015 – 2022 гг., Чжао Хоулинь) избирались на руководящий пост Союза. Можно упомянуть период руководства МСЭ Турэ Х. И. (2007 – 2014 гг.), уроженцем Мали, который получил инженерное образование в Советском Союзе и может считаться идейно близким к России. Отмечается близость позиций России и Китая в отношении роли МСЭ как центрального элемента системы управления Интернетом. Тем не менее, другие члены БРИКС – Индия и Бразилия – не поддержали предложенную Россией на Всемирной конференции по международной связи 2012 года концепцию, предусматривающую передачу МСЭ всех основных функций

управления киберпространством. См.: Sherman, J. Russia's War for Control of Global Internet Governance // SSRN – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4119863

154 ICT Development Index 2017 // Международный союз электросвязи – URL: https://www.itu.int/net4/ITU-D/idi/2017/index.html. Решение о приостановке компиляции Индекса: ICT Development Index – Background // Международный союз электросвязи – URL: https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/Background.aspx

155 Measuring digital development. Facts and figures 2022 // Международный союз электросвязи – URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

156 ITU Recommendations // Международный союз электросвязи – URL: https://www.itu.int/en/ITU-T/publications/Pages/recs.aspx

157 Исключением можно считать Регламент международной электросвязи, который считается внутренним регламентирующим документом МСЭ и является обязательным для всех стран-членов.

158 Argentina. Part 5 of the Chair's Paper // Международный союз электросвязи.

159 Тунисская программа для информационного общества // Международный союз электросвязи https://www.itu.int/net/wsis/outcome/booklet/tunis-agenda_Cru.html

160 UN General Assembly Resolution 60-252 - World Summit on the Information Society // ООН https://www.itu.int/en/ITU-D/Regional-Presence/UN/Documents/GA_Resolutions_ICTs/ares60d252_en.pdf

161 Short synthesis of written contributions and discussions // Internet Governance Forum https://web.archive.org/web/20081124220909/http://www.intgovforum.org/brief.htm.

162 Информационный доклад. Подготовлен секретариатом ФУИ // Форум управления Интернетом https://web.archive.org/web/20081112080700/http://www.intgovforum.org/cms/Substantive_1st_IGF/Summary.Final.07.11.2006.doc

163 Форум ООН по вопросам управления Интернетом. Есть ли у него будущее? // НАМИБ https://namib.online/2022/02/forum-oon-po-voprosam-upravlenija-internetom-est-li-u-nego-budushhee.

164 Так, например, в ходе 17-й встречи в Аддис-Абебе в качестве основных тем были заявлены: подключение всех людей к Интернету и защита прав человека; недопущение фрагментации

Интернета; управление данными и защита приватности; обеспечение безопасности, защиты и ответственности; передовые технологии, включая искусственный интеллект. В целом эти темы перекликаются с тематикой первой встречи Форума в 2006 г. Аддис-Абебские Послания ФУИ // Форум управления Интернетом https://www.intgovforum.org/en/filedepot_download/249/24459

165 Форум ООН по вопросам управления Интернетом. Есть ли у него будущее? // НАМИБ https://namib.online/2022/02/forum-oon-po-voprosam-upravlenija-internetom-est-li-u-nego-budushhee.

166 В соответствии с теоретической рамкой настоящего исследования, следует отметить, что, несмотря на свою значимость в качестве платформы для согласования многосторонних позиций, Форум не формирует вокруг себя самостоятельный международный режим и служит преимущественно переговорной площадкой. Маловероятно, что в будущем Форум сможет стать центральным институтом нового международного режима в рамках комплексного международного режима управления Интернетом в силу, прежде всего, слабой представленности интересов национальных правительств. Тем не менее, отмечается, что для России характерно позиционирование Форума как площадки для продвижения собственного видения проблемы обеспечения глобальной информационной безопасности. См.: Nocetti, J. Contest and Conquest: Russia and Global Internet Governance // Chatham House https://www.chathamhouse.org/sites/default/files/field/field_publication_docs/INTA91_1_07_Nocetti.pdf

167 Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения –Т. 64. № 12. 2020 - с. 25–32.

168 UN OEWG and GGE // Geneva Internet Platform https://dig.watch/processes/un-gge

169 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security // Dig Watch https://dig.watch/resource/un-gge-report-2010-res-a65201

170 Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения – Т. 64. № 12. 2020 - с. 27.

171 Письмо постоянных представителей Казахстана, Китая,

Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря // ООН https://docs.un.org/en/A/69/723

172 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // ООН https://docs.un.org/en/A/C.1/73/L.27/Rev.1

173 Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности // ООН https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/000/28/PDF/N2100028.pdf

174 К таковым принято относить применимость международного права к кибератакам в мирное время; контроль над распространением кибероружия; контроль над ИКТ двойного назначения; применимость Устава ООН к киберпространству, в частности, права на самооборону; применение превентивных мер и уведомление перед применением контрмер; атрибуция кибератак; координация ответственного поведения государств в киберпространстве; обеспечение прав человека в процессе применения новых норм и правил поведения в ИКТ-пространстве и т.д. Ромашкина Н.П. Проблема международной информационной безопасности в ООН // Мировая экономика и международные отношения –Т. 64. № 12. 2020 - с. 30.

175 Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности // ООН https://digitallibrary.un.org/record/3991743?v=pdf

176 https://d-russia.ru/oon-prinjala-proekt-konvencii-o-borbe-s-ikt-prestupnostju.html

177 Там же.

178 Толстухина А. Технологический суверенитет Европейского союза и его границы // Валдай, 2022 https://ru.valdaiclub.com/files/42559/

179 Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy // The European Council. Press release. 22.03.2021 https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

180 Толстухина А. Технологический суверенитет Европейского союза и его границы // Валдай, 2022 https://ru.valdaiclub.com/files/42559/

181 The Digital Transformation Strategy for Africa (2020-2030) https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

182 https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf

183 https://au.int/sites/default/files/documents/44005-doc-AU_Digital_Compact_V4.pdf.....

184 Там же.

185 https://eec.eaeunion.org/upload/medialibrary/ccc/Predlozheniya-po-formirovaniyu-tsifrovogo-prostranstva.pdf

186 Там же.

187 https://eec.eaeunion.org/upload/medialibrary/343/Strategicheskie-napravleniya-formirovaniya-tsifrovogo-prostranstva-EAES-_proekt_.pdf

188 http://kremlin.ru/acts/bank/43027

189 https://eec.eaeunion.org/news/v-eaes-nachalos-pereformatirovanie-tsifrovoy-povestki-/

190 https://www.kommersant.ru/doc/5571902

191 https://eec.eaeunion.org/news/eaes-i-asean-obmenyalis-opytom-v-sfere-tsifrovoy-transformatsii-/

192 Васина А.М., Дёмина Ю.А. Политика в целях развития в плановых и стратегических документах АСЕАН // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. № 4. с. 49–68.

193 Канаев Е.А., Королёв А.С. ЕАЭС и АСЕАН: результаты и перспективы сотрудничества //Мировая экономика и международные отношения – 2020 – Т. 64 – № 1 – с. 64-72 https://www.imemo.ru/index.php?page_id=1248&file=https://www.imemo.ru/files/File/magazines/meimo/01_2020/08-KANAEV.pdf

194 https://asean.org/wp-content/uploads/2021/10/Bandar-Seri-Begawan-Roadmap-on-ASEAN-Digital-Transformation-Agenda_Endorsed.pdf

195 Членами «Группы двадцати» являются 19 государств – Австралия, Аргентина, Бразилия, Россия, Индия, Китай, США, Великобритания, Италия, Франция, Канада, Мексика, Индонезия, Германия, Южная Корея, Япония, Саудовская Аравия, ЮАР и Турция. В работе форума принимает участие представитель Европейского союза.

196 Согласно результатам совместного исследования Центра исследований международных институтов РАНХиГС и Университета Торонто, в среднем «Группа двадцати» принимает

около 180 решений по итогам председательства, при этом показатель исполнения ключевых решений поддерживается на уровне 75%. См. Оценка исполнения обязательств // РАНХиГС https://www.ranepa.ru/ciir/gruppa-dvadtsati/otsenka-ispolneniya-obyazatelstv/ Более подробно методология оценки эффективности исполнения обязательств неформальных институтов глобального управления описана во введении к настоящему исследованию.

197 Другие задачи в рамках «Осакского трека» – формулирование правил регулирования электронной торговли, а также формирование рекомендаций по использованию данных в интересах содействия росту и развитию – были в дальнейшем выведены в рамки Всемирной торговой организации и ОЭСР соответственно. Таким образом, документ «не изменил баланса влияния» «двадцатки» на регулирование цифровой экономики. См.: Ларионова М.В., Шелепов А.В. Формирующиеся механизмы регулирования цифровой экономики. Риски и возможности для многосторонней системы глобального управления // Вестник международных организаций – 2021 – Т. 16 - № 1 – с. 41.

198 См.: G20 Digital Economy Ministers Meeting Ministerial Declaration https://g20.utoronto.ca/2020/2020-g20-digital-0722.html

199 См.: Декларация эр-риядского саммита лидеров «Группы двадцати» (21–22 ноября 2020 года) http://www.kremlin.ru/supplement/5585

200 См.: Римская декларация лидеров «Группы двадцати» (31 октября2021 года) http://www.kremlin.ru/supplement/5729

201 США, Великобритания, Канада, Япония, Италия, Франция, Германия.

202 См.: Ларионова М.В., Игнатов А.А., Попова И.М., Сахаров А.Г., Шелепов А.В. Десять лет БРИКС. Что дальше? М.: Дело – 2020 – с. 98.

203 См.: VII саммит БРИКС. Уфимская декларация http://static.kremlin.ru/media/events/files/ru/YukPLgicg4mqAQIy7JRB1HgePZrMP2w5.pdf

204 См: Сямэньская декларация руководителей стран БРИКС https://d-russia.ru/wp-content/uploads/2017/09/2017-09-05_BRICS_Declaration.pdf

205 См.: Terms of Reference (ToR) of BRICS Model E-Port Network http://www.brics.utoronto.ca/docs/170831-eport.html

206 См.: Декларация Бразилиа по итогам XI саммита государств –

участников БРИКС http://www.kremlin.ru/supplement/5458

207 См.: Стратегия экономического партнерства БРИКС до 2025 года https://www.economy.gov.ru/material/file/636aa3edbc0dcc2356ebb6f8d594ccb0/1148133.pdf

208 См.: Сямэньская декларация руководителей стран БРИКС https://d-russia.ru/wp-content/uploads/2017/09/2017-09-05_BRICS_Declaration.pdf

209 См.: Московская декларация XII саммита БРИКС http://www.kremlin.ru/supplement/5581

210 См.: Сямэньская декларация руководителей стран БРИКС https://d-russia.ru/wp-content/uploads/2017/09/2017-09-05_BRICS_Declaration.pdf

211 См.: BRICS E-commerce Cooperation Initiative http://www.brics.utoronto.ca/docs/170831-ecommerce.html

212 См.: Московская декларация XII саммита БРИКС http://www.kremlin.ru/supplement/5581

213 См.: Декларация Гоа http://www.kremlin.ru/supplement/5139

214 См.: Стратегия экономического партнерства БРИКС до 2025 года https://www.economy.gov.ru/material/file/636aa3edbc0dcc2356ebb6f8d594ccb0/1148133.pdf

215 Там же.

216 Welcome to ICANN! // ICANN https://www.icann.org/resources/pages/welcome-2012-02-25-en

217 Результаты анализа, представленные в данном параграфе, были опубликованы в соавторстве автором настоящего исследования в 2020 году. См.: Васильковский, С.А., Игнатов А.А. Управление Интернетом: системные диспропорции и пути их разрешения // Вестник международных организаций. Т. 15. №. 4. 2020 - с. 7-29.

218 Исходный текст: "...to provide an institutional home for and financial support for the Internet Standard process". См.: Cerf V. IETF and the Internet Society // Internet Society https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/

219 Internet Society Action Plan 2022 // Internet Society https://www.internetsociety.org/wp-content/uploads/2021/12/2022-ISOC-Action-Plan-EN.pdf

220 Lessig, L. Code is Law // Harvard Magazine https://www.

harvardmagazine.com/2000/01/code-is-law-html

221 Abbate, J. Inventing the Internet – The MIT Press. 2000 - p. 147.

222 Savage J. G. The politics of international telecommunications regulation – Routledge. 2019 – p. 240.

223 Global Digital Platform Power Index 2023 URL: https://www.dinarstandard.com/post/global-digital-platform-powerindex-2023

224 Там же.

225 Платформенная экономика в России: потенциал развития: аналитический доклад /

П37 Г.И. Абдрахманова, Л.М. Гохберг, А.В. Демьянова и др.; под ред. Л.М. Гохберга, Б.М. Глазкова, П.Б. Рудника, Г.И. Абдрахмановой; Нац. исслед. ун-т «Высшая школа экономики» – М.: ИСИЭЗ ВШЭ, 2023 - с. 72.

226 https://amp.rbc.ru/rbcnews/technology_and_media/22/01/2025/6790abbc9a7947c418ec83f1

227 Толстухина А. Американский Big Tech без правил. РСМД, 2022 https://russiancouncil.ru/analytics-and-comments/analytics/amerikanskiy-big-tech-bez-pravil/

228 Ковачич Л. Китайский Big Tech: от вольного развития к жёсткому регулированию // РСМД. 2022 https://russiancouncil.ru/analytics-and-comments/analytics/kitayskiy-big-tech-ot-volnogo-razvitiya-k-zhestkomu-regulirovaniyu/

229 И. Зуенко. Китай в эпоху Си Цзинпиня. Москва, АСТ, 2024 - с. 164.

230 Ковачич Л. Китайский Big Tech: от вольного развития к жёсткому регулированию // РСМД. 2022 https://russiancouncil.ru/analytics-and-comments/analytics/kitayskiy-big-tech-ot-volnogo-razvitiya-k-zhestkomu-regulirovaniyu/

231 Там же - с. 166.

232 UNTAD Digital Economy Report 2021 https://unctad.org/webflyer/digital-economy-report-2021

233 См., напр., Trump's TikTok Battle Heralds the Ugly Birth of a New Splinternet. Wired. 21.09.2020 https://www.wired.co.uk/article/tiktok-china-trump

234 The Splinternet of Things Threatens 5G's Potential. The Economist. 25.12.2019 https://www.economist.com/the-world-in/2019/12/25/the-splinternet-of-things-threatens-5gs-potential

235 Носетти Ж. Жизнь после Эдварда Сноудена: будущее управления

Интернетом. Коммерсантъ. https://www.kommersant.ru/doc/2448799

236 Е. Зиновьева. Проблема «цифрового вмешательства» в российско-американских отношениях. https://russiancouncil.ru/analytics-and-comments/analytics/problema-tsifrovogo-vmeshatelstva-v-rossiysko-amerikanskikh-otnosheniyakh/

237 Грибков Д.В. Защита от компьютерных атак является одной из основных задач // Интервью журналу «Национальная оборона».

238 Стратегия национальной безопасности Российской Федерации. Утв. указом президента № 400 от 02.07.2021.

239 https://news.un.org/ru/story/2023/01/1436692

240 Там же.

241 Основы государственной политики Российской Федерации в области международной информационной безопасности. Утв. указом президента № 213 от 12.04.2021.

242 Международная информационная безопасность: подходы России / Под ред. А.В. Крутских, Е.С. Зиновьевой. М.: МГИМО, 2022

243 Стратегия национальной безопасности Российской Федерации. Утв. указом президента № 400 от 02.07.2021.

244 Международная информационная безопасность: подходы России / Под ред. А.В. Крутских, Е.С. Зиновьевой. М.: МГИМО, 2022.

245 Грибков Д.В. Защита от компьютерных атак является одной из основных задач // Интервью журналу «Национальная оборона». 05.03.2024.

246 О принятии Конвенции ООН против киберпреступности // МИД РФ. https://www.mid.ru/ru/foreign_policy/news/1989289/

247 https://www.imemo.ru/news/events/text/nauchnaya-konferentsiya-zelenaya-povestka-v-sovremennoy-evrope

248 https://news.un.org/ru/story/2024/11/1458456

249 https://news.un.org/ru/story/2024/11/1458456

250 Окинавская Хартия глобального информационного общества - Окинава, 2000 http://www.ifap.ru/ofdocs/okinhar.htm

251 https://unctad.org/publication/digital-economy-report-2024

252 Волкова С.Г. Искуственный интеллект – ведущая прорывная технология // Цифровые международные отношения/ Под ред. Е.С. Зиновьевой, С.В. Шитькова. М.: МГИМО, 2023 - с. 20.

253 «Национальная стратегия развития искусственного интеллекта на период до 2030 года». Утв. Указом Президента Российской Федерации от 12.02.2024.

254 Там же.

255 https://yandex.ru/company/news/01-18-12-2023

256 http://kremlin.ru/events/president/news/72811

257 Указ президента РФ от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утверждённую этим указом».

258 Обновлённая концепция Конвенции ООН об обеспечении международной информационной безопасности 2023 // Совет Безопасности Российской Федерации http://www.scrf.gov.ru/media/files/file/P7ehXmaBUDOAAcATW2Rwa3yNK1bNAWl9.pdf

259 Указ президента РФ от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утверждённую этим указом».

260 Интервью официального представителя МИД России М.В. Захаровой журналу «Международная жизнь», 10 февраля 2024 года.

261 https://oecd.ai/en/ai-principles

262 См. напр.: Руководящие принципы ОЭСР по защите персональной информации https://www.oecd.org/digital/ieconomy/privacy-guidelines.htm

263 Shneiderman, B. Human-centered AI / B. Shneiderman — Oxford University Press, 2022 — p. 377.

264 G20 Ministerial Statement on Trade and Digital Economy // G20 Official Site — 2019.

265 https://www.g20.org/content/dam/gtwenty/gtwenty_new/document/G20-New-Delhi-Leaders-Declaration.pdf

266 United Nations Activities on Artificial Intelligence // International Telecommunication Union — 2020.

267 White Paper on Trustworthy Artificial Intelligence // Center for security

and emerging technology — 2021.

268 Estratégia Brasileira de Inteligência Artificial (EBIA) // Governo Federal — 2021.

269 National Strategy for Artificial Intelligence // The Government of the Republic of Korea.

270 Artificial intelligence act // European Parliamentary Research Service — 2023.

271 National Artificial Intelligence Research and Development Strategic Plan. 2023 Update // National Science and Technology Council — 2023.

272 Распоряжение правительства РФ от 19 августа 2020 г. № 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники на период до 2024 года» // Гарант.ру — 2020.

273 Стратегия научно-технологического развития Российской Федерации. Утв. указом президента № 145 от 28.02.2024.

274 Principles of the Ethical Use of Artificial Intelligence in the United Nations System // Chief Executive Board for Coordination — 2022.

275 ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения // Официальный сайт Федерального агентства по техническому регулированию и метрологии.

276 Волкова С.Г. Искуственный интеллект – ведущая передовая технология // Цифровые международные отношения / Под ред. Е.С. Зиновьевой, С.В. Шитькова. М., 2023 - с. 42.

277 https://www.un-ilibrary.org/content/books/9789211068870c001

278 https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f

279 Указ президента Российской Федерации от 15.02.2024 № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 года № 490 «О развитии искусственного интеллекта в Российской Федерации» и в Национальную стратегию, утверждённую этим указом».

280 https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

281 https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-

landmark-law

282 https://ria.ru/20230823/tszinpin-1891759909.html

283 ИИ в России 2023 – тренды и перспективы. Яков и Партнеры, Яндекс. Москва, 2023 - с. 32.

284 https://ethics.a-ai.ru

285 Волкова С.Г. Искусственный интеллект – ведущая передовая технология // Цифровые международные отношения / Под ред. Е.С. Зиновьевой, С.В. Шитькова. М., 2023 - с. 24.

286 https://digital-strategy.ec.europa.eu/en/library/hiroshima-process-international-guiding-principles-advanced-ai-system

287 https://rapsinews.ru/digital_law_news/20231030/309342102.html

288 https://www.ey.com/en_gl/insights/ai/g7-ai-principles-and-code-of-conduct

289 Recommendation of the Council on Artificial Intelligence. OECD, 2019 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

290 https://tass.ru/politika/19133985

291 Волкова С.Г. Искусственный интеллект – ведущая передовая технология // Цифровые международные отношения / Под ред. Е.С. Зиновьевой, С.В. Шитькова. М., 2023- с. 26.

292 https://tass.ru/politika/19133985

293 https://www.cnews.ru/news/top/2019-07-17_blokchejn_prineset_rossijskoj_ekonomike_16_trillionov

294 Волкова С.Г. Технологии распределённых реестров и блокчейн // Цифровые международные отношения / под ред. Е.С. Зиновьевой, С.В. Шитькова. М.: Аспект-Пресс, 2023.

295 https://ru.tradingview.com/markets/cryptocurrencies/dominance/

296 https://www.cbr.ru/content/document/file/132241/consultation_paper_20012022.pdf

297 https://news.un.org/en/story/2022/08/1124362

298 https://blogs.worldbank.org/psd/fear-uncertainty-and-doubt-global-regulatory-challenges-crypto-insolvencies

299 https://blogs.worldbank.org/psd/fear-uncertainty-and-doubt-global-regulatory-challenges-crypto-insolvencies

300 https://cointelegraph.com/news/imf-banning-crypto-not-effective-in-long-run

301 https://www.ledgerinsights.com/imf-xc-platform-tokenized-cross-border-payments/; https://cointelegraph.com/news/imf-cbdc-gets-feedback-from-crypto-community

302 https://eurasiangroup.org/files/uploads/files/06.Updated-Guidance-VA-VASP_rus.pdf

303 https://www.brics-pay.com

304 https://fortune.com/2023/06/25/dollar-reserve-currency-brics-brazil-russia-india-china-south-africa/

305 https://www.brics-pay.com/

306 https://www.pnp.ru/economics/v-eaes-predlozhili-sozdat-obshhuyu-kriptovalyutu.html

307 https://techcollectivesea.com/2022/10/28/crypto-trends-thailand-vietnam/

308 https://miuc.org/vs-big-data/

309 https://twitter.com/TheKanter/status/559034352474914816

310 https://www.oxfordreference.com/display/10.1093/acref/9780191803093.001.0001/acref-9780191803093-e-88

311 Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. Тунисская программа для информационного общества - 18 ноября 2005 года https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf

312 Лебедева Т.П. Каким быть глобальному управлению? // Вестник Московского университета – 2006 - № 1. Серия 21. Управление (государство и общество) https://cyberleninka.ru/article/n/kakim-byt-globalnomu-upravleniyu

313 Цыганков П.А. Мировая политика и её содержание // Международные процессы — 2005 - № 1(7) https://mgimo.ru/library/publications/26422/

314 Baird Z., Verhulst S. A New Model for Global Internet Governance // Governance in the 21st Century: The Partnership Principle, Alfred Herrhausen Society for International Dialogue https://www.markle.org/wp-content/uploads/2022/03/ahs_global_internet_gov.pdf

315 Kleinwächter W. Internet Co-Governance. Towards a Multilayer Multiplayer Mechanism of Consultation, Coordination and Cooperation (M3C3) // E–Learning – 2006 - № 3(3)

https://www.wgig.org/docs/Kleinwachter.pdf

316 Raboy M. The World Summit on the Information Society and its legacy for global governance // The international journal for communication studies, 2004 - № 3-4 (66) – p. 225–232.

317 Raboy M. The World Summit on the Information Society and its legacy for global governance // The international journal for communication studies, 2004 – № 3-4 (66) – p. 225–232.

318 Judge A. International Organization Networks // International Organization: A Conceptual Approach / Eds. Groom A., Taylor P. – L.: Pinter Publishers, 1978, p. 408.

319 Governance.com: democracy in the information age / Ed. by Kamarck C., Nye J. – Washington, D.C.: Brookings Institution Press, 2002 - p. 62.

320 Drezner D. The Global Governance of the Internet: Bringing the State Back In // Political Science Quarterly – 2004 – № 3 (119) http://www.danieldrezner.com/research/egovernance.pdf

321 https://cyberleninka.ru/article/n/mezhdunarodnoe-upravlenie-internetom-problemy-podhody-perspektivy

322 Цыганков П.А. Мировая политика и её содержание // Международные процессы — 2005 - № 1(7) https://mgimo.ru/library/publications/26422/

323 См. напр.: https://tass.ru/ekonomika/18806071

324 Malcolm J. Appraising the success of the Internet Governance Forum // Internet Governance Project – 21 November 2008 http://www.internetgovernance.org/pdf/MalcolmIGFReview.pdf

325 Comments of the Internet Governance Project on The Continued Transition of the Technical Coordination and Management of the Internet's Domain Name and Addressing System: Midterm Review of the Joint Project Agreement submitted to The National Telecommunications and Information Administration U.S. Department of Commerce - February 15, 2008 http://www.internetgovernance.org/pdf/IGP-JPA-08-comments.pdf

326 Mueller, L.M. Against Sovereignty in Cyberspace // International Studies Review. Vol. 22. № 4. 2019 – p. 779–801.

327 Balkanize // Merriam-Webster https://www.merriam-webster.com/dictionary/balkanize

328 Впервые с подобными заявлениями на правах председателя «Группы двадцати» в 2014 году выступила Австралия,

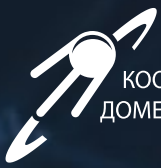
подразумевая необходимость оказания давления на российское руководство на фоне крымских событий; с осуждением подобных призывов выступил Китай и ряд других стран. После начала специальной военной операции России на территории Украины в феврале 2022 года в «двадцатке» вновь раздались призывы к отстранению представителей России от международных мероприятий в рамках председательства Индонезии – Джакарта заняла последовательную и непреклонную позицию и не поддалась давлению. В 2023 году схожую позицию заняла Индия.

329 Васильковский, С.А., Игнатов А.А. Управление Интернетом: системные диспропорции и пути их разрешения // Вестник международных организаций. Т.15. №. 4. 2020 – с. 21-23.

330 https://www.itu.int/net/wsis/outcome/booklet/declaration_Bru.html

331 www.internetworldstats.com

Международное управление Интернетом



Книга «Международное управление Интернетом» включает в себя анализ ключевых тенденций развития Интернета и системы управления сетью на современном этапе. Подробно изучена история развития Интернета, рассмотрено, как появлялись институты и механизмы управления сетью, проанализированы современные проблемы и вызовы в области управления Интернетом. Показано, как новые технологии, в том числе технологии искусственного интеллекта влияют на развитие Интернета и цифровой сферы в целом, а также институтов управления процессами глобальной цифровой трансформации.