THE CONFRONTATION OF THE SPHERES OF POWER IN THE MANAGEMENT OF THE INFORMATION SPACE

Alexander V. Fedorov

Bauman Moscow State Technical University, Moscow, Russia.
E-mail: fedorov-av@bmstu.ru

ABSTRACT

The article deals with the problem of Internet governance in the context of international information security, which is quite new for political theory and international law, on a systematic basis.

The advanced development of the technical base of the Internet, the attitude of the absolute majority of users to it as to new, powerful means of communication, without taking into account the conceptually inherent threats and risks, including political and even military ones, sharply complicate the creation of an international system of control over its use. Considered as a generalized concept, the Internet still does not have a clear definition. At the same time, even "advanced" Internet users rarely go beyond the knowledge that these resources, being included in open information networks and using the capabilities of public global communication networks, allow the storage, processing and exchange of information in a telecommunication mode. The question of who and how controls this process is not of interest to many. This uncertainty of the Internet environment is actively used by a number of states and IT corporations to solve their problems at the expense of the common good and public safety. Moreover, attempts to build a system of law in the Internet space as the development of the existing system of international security meets with resistance.

As a result of the analysis of the practice of building an Internet governance system based on the principle of multistakeholderism, the presented article shows that this component of global communication in its current form, although it is caused by natural social and technical processes, acts in the interests of the United States and carries the potential of threats to peoples and countries. whose government policy does not allow Washington to classify them as "democratic" and "friendly". The recent Twitter revolutions are examples of this. Among the goals of their organizers today are the states of the Caspian region and the South of Russia. Accompanying and facilitating globalization, the Internet creates new opportunities and new, including strategic, risks. There are still no international legal mechanisms to prevent them. The development of the latter is an urgent task of modern law and diplomacy.

KEYWORDS

Internet; international information security; cyber security; political process.

ПРОТИВОБОРСТВО СФЕР СИЛЫ В ВОПРОСАХ УПРАВЛЕНИЯ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Федоров Александр Валентинович

Московский государственный технический университет им. Н.Э. Баумана, Москва, Россия.
E-mail: fedorov-av@bmstu.ru

АННОТАЦИЯ

В статье на системной основе рассматривается достаточно новая для политической теории и международного права проблема управления Интернетом в контексте международной информационной безопасности.

Опережающее развитие технической базы Интернета, отношение к нему абсолютного большинства пользователей как к новому, обладающему большими возможностями средству связи, без учета концептуально заложенных в нем угроз и рисков, в том числе политического и даже военного характера, резко осложняют работу по созданию международной системы контроля над его использованием. Рассматриваемый как обобщенное понятие, Интернет до сих пор не имеет четкого определения. При этом даже «продвинутые» интернет-пользователи редко идут дальше знания того, что эти ресурсы, будучи включены в открытые информационные сети и использующие возможности глобальных сетей связи общего пользования, позволяют в телекоммуникационном режиме осуществлять хранение, обработку и обмен информацией. Вопрос о том, кто и как контролирует этот процесс, интересует не многих. Такая неопределенность интернет-среды активно используется рядом государств и IT-корпораций для решения своих задач в ущерб общему благу и общественной безопасности. Мало того, попытки построить систему права в Интернет-пространстве как развитие существующей системы международной безопасности встречает сопротивление.

Как результат анализа практики строительства системы управления Интернетом на основе принципа мультистейкхолдеризма в представленной статье показывается, что эта составляющая глобальной коммуникации в нынешнем виде, хотя и вызвана к жизни естественными социальными и техническими процессами, действует в интересах США и несет в себе потенциальную угрозу народам и странам, чья государственная политика не позволяет Вашингтону отнести их к разряду «демократических» и «дружественных». Примерами тому стали недавние «твиттер-революции». В числе целей их устроителей и сегодня значатся государства Каспийского региона и Юг России. Сопровождая глобализацию и способствуя ей, Интернет порождает новые возможности и новые, в том числе стратегические, риски. Для их предотвращения пока нет международно-правовых механизмов. Выработка последних – актуальная задача современного права и дипломатии.

КЛЮЧЕВЫЕ СЛОВА

Интернет; международная информационная безопасность; кибербезопасность; политический процесс.

ВВЕДЕНИЕ

В общественном сознании существует устоявшееся мнение, что именно Интернет[1] последние два десятилетия формирует глобальное информационное пространство. Это утверждение достаточно спорно и требует отдельного рассмотрения. Однако, вне всякого сомнения, существующая под этим именем глобальная информационно-телекоммуникационная структура – знаковое явление постиндустриализма. Став феноменом организации социальной и во многом производственной коммуникации, Интернет оказывает значительное влияние на общественное бытие (а постепенно и на общественное сознание, воздействуя на образование, науку и культуру, формируя поколения Y и Z), становится частью этого бытия[2], формируя темпоральность информационного общества. И вопрос доступа к управлению им имеет политическое значение.

После «цветных революций», получивших еще названия «твиттер»- и «фейсбук»-революций, политическое значение Интернета мало у кого вызывает сомнение. С сожалением надо признать, что этот «революционный процесс» еще не завершен и, несколько отхлынув от берегов Средиземного моря, тофлеровская «третья волна»[3] все еще держит в напряжении многие страны мира.

Государства Каспийского региона и республики Юга России, вероятно, в наибольшей степени подвержены исходящей от нее угрозе, поскольку остаются постоянным раздражителем для государств – фактических владельцев социальных сетей[4] и заказчиков, проводимых через них (будем называть вещи своими именами) информационно-психологических операций, направленных, в частности, на разжигание межнациональной розни в Киргизии, антирусских настроений в Казахстане, поддержку очагов национализма и религиозного экстремизма, а то и просто терроризма на Северном Кавказе и в Поволжье. Сейчас многие уже забыли, что такое «сайт Кавказ». Это хорошо, но ему на смену пришли другие интернет-ресурсы, проповедующие исламский фундаментализм и насилие, и несущие угрозы целостности страны. В условиях постоянной информационной войны уже много

[1] Под термином Интернет в целях данной статьи будем понимать совокупность технических, программных и информационных ресурсов хранения, передачи и обработки информации, действующих на базе открытых телекоммуникационных сетей, использующих протоколы TCP/IP и адресную систему DNS.

[2] Значимость интернета подтверждается масштабами его использования. На 30 июня 2020 г. число пользователей сети по данным сайта Internet World Stats (URL:http://www.internetworldstats.com/stats.htm) составило 4 833 521 806 при населении планеты в 7 796 949 710 человек, что составляет 62,0% жителей Земли. По Европе и Северной Америке этот показатель еще выше – 87,2% и 90,3% соответственно.

[3] Элвин Тоффлер выразил мысль о том, что мир постепенно формируется тремя волнами технологических инноваций, которые, как высокий прилив, нельзя остановить. Первой была сельскохозяйственная революция, второй – промышленная. Третья волна – информационная революция – предвещает новый образ жизни, что, утверждает Тоффлер, будет просто замечательно, правда, в том случае, если мы удержимся на гребне этой волны (Тоффлер).

[4] Следует отметить (и это является политической основой ситуации), что практически все значимые элементы этой архитектуры Интернета и подавляющее большинство социальных сетей всегда являлись и остаются юридическими лицами США и как таковые имеют определенные обязательства перед своим государством, даже если в уставных и регистрационных документах они значатся общественными и открытыми или имеющими международные органы управления. Надо, однако, признать, что это сложилось исторически, никакие признаки злого умысла со стороны Вашингтона, Пентагона и американских спецслужб в этом аспекте не выявлены.

лет живет Исламская республика Иран. Дополнительный импульс придают факты кибератак (в частности, признанное всеми как акт войны применение вируса Stuxnet против ядерных объектов Ирана в 2010 году), которые наглядно демонстрируют, что информационные войны и Интернет – это уже не абстрактные сценарии футурологов, но вполне реальная практика.

Только принимаемые руководством этих государств меры, может быть, где-то не оптимальные, где-то опирающиеся на традиционные и даже архаичные стороны национальных менталитетов народов региона, но решительные и твердые меры не позволяют разжечь пожары, на которые так рассчитывают авторы «твиттер-революций», декларирующие свою историческую миссию носителей демократии. Между тем один из основных «исполнителей» – Твиттер[1], как показывает его конфликт с Минюстом России, сам далек от демократических норм. Защитники подобных действий, опираясь в своих заявлениях на Всеобщую декларацию прав человека, никогда не упоминают, что в ней есть Статья 29, говорящая об обязанностях человека по отношению к обществу и государству и возможности ограничения прав, когда его деятельность несет ущерб миру и безопасности.

Почти 20 лет вопрос контроля над Интернетом, управления его структурами находится на первых позициях повестки дня мирового сообщества, непосредственно связанных с вопросами безопасности и развития. Без понимания существующих здесь взаимосвязей и возникающих противоречий нельзя адекватно оценить уровень угроз, исходящих от глобальной сети, а также объем рисков государств, не предусматривающих в своем правовом поле и своей международной политике механизмов противодействия первым и управления вторыми. Далее мы не будем останавливаться на составе и взаимоотношениях органов управления Интернетом и его элементами. Они не так просты и включают в себя, как институированные, так и общественные структуры. Предполагается, что это читателю известно (Курбалиа, 2010; Зиновьева, 2011; Федоров, Зиновьева, 2017).

ПРОБЛЕМА УПРАВЛЕНИЯ ИНТЕРНЕТОМ

Определение понятия «управление Интернетом» стало предметом политических и научных дебатов с 2003 года, проявившись как проблема в ходе Всемирной встречи (Женева, 2003 г. – Тунис, 2005 г.) на высшем уровне по вопросам информационного общества. Дискуссия развивалась на фоне эпохального для Интернет-сообщества события – новой стадии развития всемирной паутины, которую Т. О'Рейли назвал Web 2.0, определив 7 ключевых принципов, нового – политического – этапа в развитии всемирной сети, из которых, в частности, следует, что:

– Интернет становится ключевой платформой политического дискурса;

[1] Владельцем системы «Твиттер» является компания Twitter Inc., юридическое лицо штата Калифорния (США), главный офис которой находится в Сан-Франциско (штат Калифорния). Twitter Inc. также имеет серверы и офисы в Сан-Антонио (штат Техас) и Бостоне (штат Массачусетс). В России официального представительства не имеет.

– его развитие, в частности рост проприетарных баз данных, ведет к свободному движению информации и использованию ее в политических целях, формирует коллективное сознание пользователей сети;

– упрощение механизмов и технологий использования социальных медиа способствует быстрому проникновению политики в публичную сферу;

– распространение политического контента с помощью различных приложений формирует пользовательский опыт в политике (O'Reilly, 2005).

Архитектура Интернета и Всемирной паутины эпохи Web 2.0 таковы, что пользователи, преследуя свои собственные «эгоистичные» интересы, автоматически как побочный продукт создают коллективные ценности. У О'Рейли это звучит как «пользователи добавляют ценность», то есть формируют глобальную базу данных, на основе которой ведется, в том числе политический дискурс.

С этого момента всемирная сеть окончательно получила – и это было публично декларировано на встрече в Тунисе – политическое звучание и свое место в международной политической повестке дня.

Поскольку мы стремимся применить общие понятия политологии к изучению управления Интернетом, то определим глобальное управление в соответствии с широко используемым в теории международных отношений (Zürn, 2018), понимая его как «трансграничное осуществление властных полномочий, через существующие государственные и общественные механизмы в соответствии с общепринятыми нормами и правилами и настолько, насколько это отвечает общим интересам и потребностям». Это довольно широкое определение подразумевает отнесение к субъектам управления, кроме правительств и официальных структур государства, межправительственные механизмы, частные организации, гражданское общество, договоренности и инициативы, а также их смешанные формы.

Управление Интернетом происходит с позиций различных сфер силы. Сфера силы, как она представляется в статье, – это больше, чем просто группа стейкхолдеров-единомышленников, ссылки на которые часто встречаются в литературе по Интернету, или государств одного политического лагеря, стоящих на общих позициях в отношении видения роли Интернета в политике. Она может реализовываться через разнообразие субъектов, таких как государства, национальные правительственные и межправительственные организации, научные и образовательные организации, институты гражданского общества, частный сектор, многосторонние форумы и пр. В соответствии с приведенным определением глобального управления, сферы силы – это совокупность государств, меж- или надгосударственных образований, функциональных или технократических органов, объединенных единым пониманием и исполнением назначения и роли Интернета в общественном развитии, а также совокупность норм и нормативных предписаний, обеспечивающих правовую сторону деятельности обозначенных органов. Такой подход не является уникальным, но в

нашем случае он позволяет свести все конкурирующие и претендующие на контроль над Интернетом стороны к двум идеальным типам: либеральной и государственнической сферам. Как идеальные типы, они не предназначены для точного представления реальных сил, но скорее представляют собой абстракцию этой реальности, позволяющую использовать ее как инструмент анализа.

Более консолидированная и исторически контролирующая техническую составляющую Интернета либеральная сфера (представлена в первую очередь США, их союзниками, поддерживающими их межгосударственными, общественными, бизнес- и прочими не связанными с государством структурами гражданского общества) исходит из необходимости всячески ограничивать в управлении сетью роль государства, делая ставку на частную инициативу и идею свободы информации.

Сторонники второй силы – государственнической сферы, в основном приверженцы идеи государственного суверенитета[1] и основанной на праве всеобщей безопасности в информационном пространстве – подчеркивают необходимость государственного контроля над Интернетом, межправительственности в решениях и договоренностях, а также недопустимости преобладания в ее системах управления американских, как это есть сейчас, институтов и частных акторов. Ее основными представителями можно рассматривать Россию, Китай, страны ШОС, частично БРИКС и их союзников, и единомышленников.

Сторонники либеральной сферы видят в Интернете возможность формирования наднационального пространства, которое должно в основном управляться за счет частного саморегулирования на основе добровольного участия и предметной экспертизы. Его институты должны быть гибкими и ориентированными на негосударственные заинтересованные стороны (стейкхолдеров), в то время как роль государства должна ограничиваться обеспечением безопасности и, когда необходимо, контролем за соблюдением правил. Здесь идеологи либеральной сферы реализуют идею В. Гумбольда: государство есть зло, но зло необходимое, его прерогативы должны быть ограничены посредством права. Их социальная цель – стимулировать развитие Интернета, предоставляя частным лицам, фирмам и организациям гражданского общества как можно больше свободы. Как стейкхолдеры воспринимаются межправительственные организации того же либерального толка, ориентированные на достижение той же цели. В основе идеологии – западный либерализм, сочетание свободного рынка и плюралистического мышления гражданского общества. В этом смысле как лозунг сторонников либеральной сферы можно привести позицию М. Кастельса, что широкое распространение

[1] Вслед за сторонниками этой силы воздержимся в данной работе от дискуссии по вопросу о том, что в настоящее время следует понимать под термином «государственный суверенитет» и применимости его классического – боденовского – значения к современности, в том числе с учетом наличия такой международной структуры как Совет безопасности ООН с его легитимным правом применения силовых акций в отношении членов ООН на фоне их суверенного равенства.

социальных сетей на базе Интернета и их использование государствами следует рассматривать как источник новых возможностей для развития и разрешения современных глобальных проблем, масштаб которых несоизмерим с возможностями и ресурсами отдельно взятого государства. Интернет и социальные медиа дают возможности формирования глобального гражданского общества и глобальных дискуссий. Публичная дипломатия в таком контексте рассматривается не как дипломатия государства, но как народная дипломатия, которая создает основу для национальной публичной дипломатии и действует поверх межгосударственных отношений, основываясь на общих подходах (Castells, 2008).

Сторонники государственнической сферы – государственники – видят в Интернете не только возможность и инструмент решения новых проблем посредством новых форм, но и канал реализации угроз интересам государства, средство деструктивного воздействия на общество и личность, инструмент информационного противоборства. Поэтому он должен регулироваться государствами, а также межправительственными органами и институтами. Негосударственные стейкхолдеры (фирмы, гражданское общество или эксперты) должны в лучшем случае иметь консультативную роль. Социальная цель этой сферы, считают ее сторонники, состоит в защите суверенитета государства и основных, традиционных для его общества ценностей, предотвращения использования какими-либо государственными или международными акторами полученной ими через принадлежащие им, или контролируемые ими, интернет-базируемые социальные сети, возможностью влиять на общественное сознание, отношения и политику других стран. Лежащая в основе идеологии идея – это мир, в котором правительства, получившие власть посредством механизмов демократии, принимают решения в рамках внутренней политики на основании национальных законов без внешнего вмешательства и ограничений и заключают международные соглашения на основе провозглашенных Уставом ООН отношений суверенного равенства.

Государственническая сфера охватывает государства, которые выступают за регламентацию управления Интернетом на основе международных договоров, то есть традиционного международного права, хотя их противники и видят в этом желание таких стран, как Китай и Россия, поддерживать посредством глобальной сети внутреннее, по их мнению, авторитарное правление, а также стремление развивающихся стран иметь большее влияние в мире.

Вместе с тем обе сферы воспринимают западные государства (в первую очередь США) как доминирующие в управлении Интернетом. Только либеральная сфера стремится сохранить это как статус-кво, а государственническая – изменить.

Надо отметить, что когда мы говорим о «приверженцах» или «сторонниках» либеральной, или государственнической сфер, то имеем в виду лишь штамп для выражения позиций государств и других субъектов в отношении альтернативных способов организации управления Интернетом. Это ничего не говорит об их позициях по отношению к другим вопросам, и эту характеристику не следует

путать с формальным членством или принадлежностью к какому-либо сообществу. Практика трех десятилетий существования Интернета и основанных на нем социальных и прочих (финансовых, библиотечных, торговых и др.) сетей показывает применимость метода типичных сфер для выявления стабильности, непрерывности и постепенности изменений в кажущейся динамичной системе в условиях неурегулированной политики в информационной сфере в целом. Такой подход помогает понять, что под поверхностью динамизма, основополагающие социальные цели, институциональные предпочтения и нормы остаются относительно стабильными и структурированы вдоль линии противоречий между двумя сферами власти.

Различие этих сфер наиболее ярко демонстрируется в дискуссиях о «многосторонности» и «смене режима» управления сетью, в частности переноса вопроса от форума мультистейкхолдеров к установленному правовому международному учреждению – Международному Союзу Электросвязи (МСЭ) – или новому международному институту – специальному комитету ООН.

Технологически защитники либеральной сферы консультациям или переговорам на государственном или правительственном уровне предпочитают частные встречи специалистов или форумы с участием многих заинтересованных сторон, не имеющих официальной государственной аккредитации. Нельзя сказать, что они являются противниками формальных институтов, но поддерживают их, главным образом, для того, чтобы иметь дело с основными носителями государственных властных полномочий, таких как обеспечение безопасности. Однако среди них они по идеологическим соображениям предпочитают (а точнее, другие и не рассматривают) организации западной ориентации, такие как Совет Европы или ОЭСР.

Сторонники же государственнической сферы нацелены на создание иной институциональной структуры, в которой не доминируют крупные и мощные западные монополии, отдавая предпочтение государствам на основе равного представительства и предлагая выработать (опять же на формальной основе, т.е. в рамках норм существующей международной правовой системы) международный режим управления сетью. Реализацию своей позиции они видят в признании нормативности политически легитимного межгосударственного контроля над Интернетом. Предпочтительным институциональным местом проведения подобных инноваций государственниками рассматривается ООН и ее специализированные органы, такие как МСЭ.

РАЗВИТИЕ ПРАВОВОЙ БАЗЫ ИНТЕРНЕТА

В отношении норм (понимаемых как общие стандарты надлежащего поведения акторов с заданной идентичностью), показательной стала дискуссия по вопросу о том, что должно лежать в основе развития правой базы Интернета: укрепление прав человека и свободы выражения мнений или информационная безопасность и международное право. В контексте проблемы управления

Интернетом эта коллизия норм в большей степени обусловлена социальной практикой и некими выводимыми из нее общими принципами.

Дискуссии на эту тему начались в рамках Всемирной встречи на высшем уровне по информационному обществу (ВВУИО), прошедшей в два этапа: в Женеве в 2003 и в Тунисе в 2005 году; продолжились на Всемирной конференции по международным телекоммуникациям (ВКИТ-12) 2012 года и в четвертой Группе правительственных экспертов ООН по вопросам достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности (ГПЭ), работавшей в период 2014–2015 годов на основании одноименной резолюции 70 сессии ГА ООН 2013 года. Обсуждения продолжаются до сих пор, в том числе в рамках рассмотрения вопроса актуальности Будапештской Киберконвенции Совета Европы 2001 года.

Впервые конфликт позиций проявился на Первой Встрече ВВУИО в 2003 году (Всемирная встреча, 2003). Ее ключевыми темами стали разработка норм и принципов управления Интернетом, а также определение самого понятия «управление Интернетом». Здесь впервые официально группа ориентированных на суверенитет государственных и независимых участников бросила вызов существующей американо- ориентированной системе управления. Компромиссом стало учреждение Форума ООН по управлению Интернетом (UN Internet Governance Forum (IGF)) как «новой площадки для многостороннего политического диалога» заинтересованных сторон. Его эффективность подверглась резкой критике на следующей встрече ВВУИО и до сих пор вызывает сомнения.

Что касается институтов, то уже в начале конференции ВВУИО в Женеве выявилось существование различных точек зрения на сложившийся статус-кво. Ориентированная на США система управления включала множество довольно формальных технических органов, таких как: ICANN, целевая группа по разработке Интернета (IETF), частные субъекты и пр. (См. Федоров &Зиновьева, 2017). Идею их сохранения и развития как независимых, основанных на гражданском обществе без прямого государственного участия и контроля над структурами в системе управления Интернетом, а по сути признания статус-кво фактического контроля Вашингтона над всеми структурами ядра сети, продвигали США, западные и поддерживающие их страны. Формирующееся контрдвижение, возглавляемое Китаем, Россией, Бразилией, Южной Африкой, поддерживаемое МСЭ и Еврокомиссией, выдвинуло идею межправительственной модели управления с опорой на решения и в рамках ООН, подчеркивая важность политической власти и ее связи с суверенитетом и экономическим развитием. Позже в 2014 г., когда нынешний Генеральный секретарь МСЭ Хоулинь Чжао избирался на этот пост, именно такой лозунг во многом обеспечил ему поддержку стран – сторонников государственнической сферы, в том числе России, и в конечном итоге победу на выборах. К сожалению, он не был реализован.

Хотя изначально Интернет развивался по американской модели, односторонний надзор США за ICANN, существовавший в то время, все больше

превращался в источник конфликта. Это привело к столкновениям в ходе ВВУИО за власть над ICANN между США, с одной стороны, и европейскими государствами, с другой. Европейская комиссия предложила «новую модель сотрудничества» как «более прочную демократическую, транспарентную и многостороннюю основу, с более сильным акцентом на интересах государственной политики всех правительств». Она подверглась жесткой критике со стороны США. В качестве уступки давлению сторонников государственнической сферы принципы участия заинтересованных сторон в управлении Интернетом были расширены, в частности распространены на правительства. Однако после значительных дипломатических усилий и из опасений торжества таких стран, как Китай, Саудовская Аравия и Иран, продвигавших идею повышения киберсуверенитета, европейские и другие «демократические» страны сдали свои позиции и пошли на компромисс. Либеральный принцип «демократии между собой не воюют» сработал.

Если относительно институтов имелись значительные расхождения, то по поводу норм спорили существенно меньше. Тем не менее угроза стабильности возникла. Так, в заявлении китайского представителя прозвучал призыв «подчеркнуть социальную ответственность и обязательства» в области управления Интернетом. В отличие от китайцев сторонники либеральной сферы выразили озабоченность по поводу угроз свободе информации, якобы возникающих в случае, если пройдет инициатива государственников, и подчеркнули необходимость обеспечить выполнение принципов открытости и свободы выражения мнений, закрепленное во Всеобщей Декларации прав человека, вновь забыв про ее 29 статью. Тунисская программа для информационного общества и сопутствующее тунисское обязательство (Всемирная встреча, 2005) завершили процесс ВВИО компромиссом. Принятая Программа подчеркивает, что «вопросы государственной политики являются суверенным правом государств» (статья 35a) и привлекают внимание к «равной роли и ответственности правительств» (статья 68). И тут же узаконивает существующие структуры (статья 55) и, в частности, приверженность многосторонности, подчеркивает роль (Статья 35b, c) частных субъектов и гражданского общества. Создание Форума по управлению Интернетом (Internet Governance Forum– IGF) отмечается как учреждение новой площадки для обсуждения деэскалации, но не разрешение противоречий. Его слабый институциональный потенциал не ограничил полномочия ICANN или других технических органов. Таким образом, новизна IGF состояла лишь в большем вовлечении негосударственных субъектов в процессы управления. Тем не менее его создание уже показывает наметившиеся тенденции в конфликте между либеральной и государственнической сферами.

Что касается норм, то ВВУИО лишь продемонстрировала признаки конфликта. Тунисские итоговые документы не содержат конкретных формулировок по спорным вопросам, допуская их различные толкования заинтересованными сторонами. Однако в отличие от более ранних дискуссий, в которых особое внимание уделялось приверженности «демократическому»

управлению Интернетом, уже в первых пунктах Тунисской программы Информационного общества указывается как на опору на основные нормы либерализма.

В итоге после ВВУИО либеральная сфера еще более консолидировалась, несмотря на проявившиеся противоречия в позиции, в частности между акцентом на государственный контроль США и ответственностью частного сектора. Однако государственническая сфера также сохранила решимость. Усилия демократических стран БРИКС, в частности Бразилии и Южной Африки, возможно, внесли бы свой вклад в повышение ответственности правительств в области управления интернетом, если бы их поддержали европейские государства. Однако стремление повысить роль частных субъектов и озабоченность по поводу расширения прав и возможностей стран государственнической сферы заставило европейцев в качестве институционального компромисса присоединиться к США и настаивать на закреплении принципа участия всех заинтересованных сторон. Этот шаг успешно предотвратил попытки дробления Интернета на Всемирной конференции по международным телекоммуникациям 2012 года (WCIT-12).

К началу WCIT-12 (World Conference) действовавшие Регламенты Международной Электросвязи (устанавливающие общие принципы обеспечения и функционирования международной электросвязи, услуги и международные средства их предоставления), признавались устаревшими и непригодными для борьбы с растущими угрозами терроризма, киберпреступностью, кибервойной и кибершпионажем. Вопрос их обновления рассматривался как технический, и большинство предлагаемых изменений не вызывало споров. Однако дискуссия пошла по другому сценарию. Внепланово сторонники либеральной и государственнической сфер открыли дебаты по вопросам об институтах (роль ООН, в систему учреждений которой входит МСЭ, в управлении Интернетом) и нормах (баланс между правами человека и безопасностью). Что касается институтов, то спор возник по поводу того, в какой степени управление Интернетом должно быть поставлено под контроль ООН. В то время как приверженцы либеральной сферы хотели сохранить ограниченную роль МСЭ, сторонники государственнической сферы добивались полной замены существующей модели и предоставления МСЭ дополнительных полномочий по регулированию сети. Россия и ее сторонники предложили, кроме того, предоставить государствам-членам равные права на управление в части имен и номеров, что должно было на деле изменить подотчетность ICANN. У сторонников либеральной сферы это, конечно же, вызвало обеспокоенность, поскольку принятие такого рода предложения привело бы к замене мультистейкхолдерской модели.

Относительно норм в области прав человека и государственного контроля контента интернет-сообщений приверженцы государственнической сферы представили предложение о том, что правительства должны иметь право определять, как маршрутизировать национальный интернет-трафик, чтобы

повысить безопасность информации. По оценке представителей либеральной сферы, это оправдывало бы интернет-цензуру во имя национальной безопасности.

Процесс пересмотра ITRs обострился при принятии сопутствующих документов: в принятом проекте Резолюции 3 государственники добились заявления участников WCIT-12, что «все правительства должны играть равную роль, а также разделить ответственность за международное управление Интернетом и за обеспечение стабильности, безопасности и непрерывности существующего интернета». Либералы увидели в этом повышение роли МСЭ и перевод управления сетью на межправительственный уровень и подрыв принципа мультистейкхолдеризма.

В итоге WCIT-12 55 стран (среди которых Австралия, Канада, государства-члены ЕС, Индия, Япония, Новая Зеландия и США) не подписали пересмотренный договор. Это привело к созданию двух институциональных структур: одна для государств-подписантов и другая для тех государств, которые остались на старых ITRs 1988 года. Такой результат многие характеризовали как раскол МСЭ и первый этап фрагментации управления Интернетом в конкретном секторе.

Большинство исследователей, за исключением военных и аналитиков спецслужб, до 2015 г. не обращали особого внимания на такую проблему, как международная информационная безопасность (МИБ). В национальные делегации на переговорах по этой теме включались только представители государственных ведомств, но никогда не представители научных и политических кругов. Хотя российская сторона, поддерживаемая Китаем, ШОС, БРИКС, ОДКБ и др. не западными структурами, с 1999 г. на всех уровнях заявляла, что информационное общество не может существовать без информационной безопасности и кибербезопасность – это часть проблемы МИБ, реакции на международном уровне практически не было. Не было ее и в научных исследованиях. Даже в резолюции «Достижения в области информатизации и телекоммуникации в контексте международной безопасности», ежегодно с 1999 г. принимаемой Генассамблеей ООН, говорилось только о МИБ и никогда о «кибербезопасности».

И вдруг в 2015 г. все, как по команде, обратили внимание на то, что МИБ стала глобальной проблемой, а Генеральная Ассамблея ООН (ГА ООН) поручила пятой (заметим, уже пятой – первая была созвана в 2004 г.) профильной Группе правительственных экспертов ООН написать доклад о том, как международное право применяется к использованию информационно-коммуникационных технологий (ИКТ)[1] государствами. Поскольку ГПЭ создавалась по резолюциям Первого комитета ГА ООН (Вопросы разоружения и международной

[1] Термин изначально считался неудачными, но компромиссным между «информационным оружием», предлагавшимся российской стороной и «кибертехнологии», на котором настаивали западники (значения термина «технология» в русском и английском языках сильно отличаются – русскому значению больше соответствует английское «know haw», что ни в коем случае не может обозначать новый вид оружия). Даже при его рассмотрении на первой профильной ГПЭ ООН в 2005 г. было признано допустимым на национальном уровне использовать другие более привычные термины. В России в государственных документах используется вариант «информационные и коммуникационные технологии» с той же аббревиатурой ИКТ или привычное «информационное оружие», определения которого во все военные словари мира включены еще в 80-х годах прошлого века и практически идентичны, чего нельзя сказать о «кибероружии».

безопасности), то рассмотрение темы велось в контексте предотвращения применения ИКТ в войне и в целях войны, то есть в контексте гуманитарного права и разоруженческих договоров.

Между тем еще в 2013 г. третья ГПЭ согласилась с тем, что международное право, и в частности Устав ООН, применимы к использованию ИКТ государствами, не упоминая про других акторов, оставляя их вне правового пользователя, хотя это те самые стейкхолдеры, которые по убеждению либералов должны нести основную нагрузку в управлении Интернетом, то есть киберпространством. Четвертая ГПЭ в 2015 г. не только подтвердила эту позицию, но сформулировала добровольные и необязательные нормы ответственного поведения государств[1]. Однако, по оценке руководителя американской делегации в ГПЭ М. Маркофф, который в настоящее время исполняет обязанности координатора по кибервопросам Госдепартамента США, доклад ГПЭ ООН 2015 года является вершиной «прогресса, достигнутого в отчетах ГПЭ» (Markoff, 2021). Новых результатов последующие ГПЭ не получили. Видимо, вершина была действительно достигнута и дальше идти было уже не надо.

Конфликт проявился, когда сторонники либеральной (США и государства ЕС) и государственнической сферы (страны СНГ, БРИКС и некоторые развивающиеся страны) разошлись во мнениях как по вопросу институирования, так и норм управления Интернетом. Что касается институтов, то приверженцы либеральной сферы, опираясь на упомянутые результаты работы ГПЭ ООН, полагали возможным применить существующее международное право к кибербезопасности, не создавая новый режим. Приверженцы же государственнической сферы предпочитали разработать новый обязательный межправительственный режим с новыми управленческими институтами и инициировать соответствующий переговорный процесс в рамках ООН. Движителем таких переговоров они видели ГПЭ ООН по МИБ.

Что касается норм, то сторонники либеральной и государственнической сфер разошлись в видении того, что конкретно следует понимать под применением существующего международного права по таким вопросам, как право на самооборону, контрмеры, и гуманитарное право. Этого ждали от ГПЭ 2017 г., но согласовать позиции и добиться консенсуса не удалось. Приверженцы государственнической сферы видели во включении права на самооборону попытку узаконить возмездие с помощью других видов вооружений, включая ОМУ. Особенно проблематичной для них оказалась формулировка в проекте итогового доклада, приравнивающая деструктивное использование ИКТ государствами к вооруженному нападению, как-то определяется в статье 51 Устава ООН (Право на

[1] Доклад четвертой ГПЭ ООН в 2016 г. был поддержан саммитами «G7» и «G20», которые тем самым включили указанные нормы в международной право, а Президент Б.Обама в декабре того же года в своем последнем указе использовал этот факт в качестве основания для введения санкций против России за нарушения международного права в информационном пространстве. За основу принятых Правил были взяты соответствующие положения обамовской Стратегии для киберпространства 2011 г., хотя еще в 2006 г. в решении профильной Группы экспертов ШОС были предложены и формулированы в более общем виде «Правила поведения в информационном пространстве» для всех акторов информационного пространства, а не только государств.

самооборону). Мало у кого вызывало сомнение, что США при необходимости будут использовать такое прочтение международного права в качестве оправдания для нанесения ответных ударов в случаях обвинений в кибершпионаже со стороны таких стран, как Иран или Северная Корея. Учитывая решение сентябрьского 2014 г. саммита НАТО в Уэльсе[1], такая перспектива виделась более чем реальной, к тому же Пентагон назвал информационное пространство самостоятельным «полем боя» еще в 1996 г. (Menoher, 1996). Опасение вызывало также то, что ссылка на контрмеры косвенно признала бы право на взаимность кибератак. Это позволило бы ввести санкции и наказание в обход Совета Безопасности ООН. Кроме того, статья 51 сама по себе не предполагает мирного урегулирования конфликтов, поскольку признание права на оборону при кибернападении де-факто легитимирует войну в информационном пространстве.

Разногласия обострились после того, как некоторые сторонники либеральной сферы стали отказываться от своей поддержки применимости международных норм. Подобное отступление было неприемлемо для Вашингтона. В своем выступлении в Государственном департаменте накануне заключительной встречи ГПЭ в 2017 г. эксперт США заявила, «что те, кто не желает подтвердить применимость международно-правовых норм и принципов, считают, что их государства могут действовать в киберпространстве или через киберпространство для достижения своих политических целей без каких-либо ограничений или ограничений на свои действия. Это опасная и неприемлемая точка зрения, и я категорически отвергаю ее» (Markoff, 2021). В чей адрес было направлено это обвинение, остается только догадываться[2].

Расхождения во взглядах между приверженцами двух сфер стали для пятой ГПЭ непреодолимыми. Попытка адептов либеральной сферы укрепить существующий режим информационной безопасности потерпела неудачу. Точно так же и попытка приверженцев государственнической сферы создать новый режим. Отсутствие консенсуса и непринятие итогового доклада оказались фатальным для обоих лагерей.

Еще одним проявлением противоречий между сферами власти в подходах к контролю над деятельностью в информационном пространстве стало принятие первым комитетом ГА ООН в 2018 году сразу двух противоречащих друг другу резолюции по МИБ, представленных США и Россией. Резолюция Соединенных Штатов (139 голосов «за») призывала к созданию новой ГПЭ для изучения норм и обсуждения того, как международное право применяется к киберпространству (UNGA). Российская резолюция (109 голосов «за») устанавливает Рабочую группу открытого состава (РГОС) по дальнейшему рассмотрению норм, включенных в

[1] Пункт 72 Заявления по итогам встречи на высшем уровне в Уэльсе (обнародовано главами государств и правительств, участвующими в заседании Североатлантического союза в Уэльсе - 4-5 сентября 2014) приравнивает кибернападение к акту агрессии и определяет, что «киберзащита является частью одной из основных задач НАТО – коллективной обороны» и приводит к введению в действие статьи 5.

[2] Выступление правительственного эксперта США само по себе очень интересное и хорошо прорисовывает все перипетии публичной деятельности дипломатов. Не вызвало бы удивления, если бы такую речь произнес российский или китайский эксперт. Но то, что это произнесла представлявшая США во всех ГПЭ ООН М.Маркофф, оставляет только один вопрос: читают ли материалы Госдепа в дипломатических ведомствах других стран.

итоговый доклад четвертой ГПЭ ООН, и модели регулярного институционального диалога в рамках ООН (UNGA. A/C.1/73/L.27/Rev.1.). Эта новая попытка сторонников государственнической сферы создания альтернативы ГПЭ в чем-то была созвучна WCIT-12. Критика такого шага сводилась к тому, что это была лишь попытка создать конкурентный режим с переносом дебатов на новые места / новое место проведения – РГОС, когда они признаны бесплодными на других площадках (ГПЭ). Мало того, многие аналитики сходятся в том, что РГОС изначально не имела перспектив: срок ее деятельности на год короче ГПЭ[1], что позволяло в решениях последней нивелировать нежелательные для западников и реализованные в РГОС инициативы государственников, а открытый состав гарантирует непринятие решения, не выгодного сторонникам либеральной сферы. Хотя исход этих событий пока не ясен, тем не менее это, по крайней мере, указывает на то, что конфликт между сторонниками либеральной и государственнической сфер продолжается.

Последним направлением, на котором проявилось противостояние либеральной и государственнической сфер, стала борьба с преступностью и правоохранительная деятельность в информационной сфере. Это направление объективно смыкается с вопросом управления Интернетом, поскольку основная масса информационных правонарушений совершается в глобальных сетях или с их использованием, и борьба с ними непосредственно затрагивает вопросы управления Интернетом и установления в нем правовых норм.

Киберпреступность уже к началу века стала глобальной проблемой и рассматривается различными международными институтами. Однако Европейская конвенция о киберпреступности (Conventionon Cybercrime) является единственным юридически обязывающим и, возможно, самым важным международным документом в этой области[2].

Не все государства-члены СЕ ратифицировали конвенцию – Россия отказалась даже подписать его. Первая и, по сути, главная причина состоит в том, что к Конвенции можно только присоединиться, высказанное при этом мнение едва ли будет услышано. Россия не участвовала в ее разработке и даже не получила приглашение сделать это. Соответственно, ее позиция ни по субстантивным, ни по частным вопросам в документе учтена не была. Текст же документа подготовлен так, что внести в него изменения практически невозможно: правки могут вносить только участники Конвенции (т.е. после ратификации); процедура внесения правок сложна, многоступенчата и требует согласия не только всех участников Конвенции, но европейских органов вплоть до Еврокомиссии; оговорки

[1] В 2020 г. он был продлен еще до 2025 года.

[2] Совет Европы является региональной межправительственной организацией, включает 47 государств-членов, в том числе все государства ЕС и Россию. США, Канада, Япония и ряд других стран имеют статус наблюдателя. Однако Будапештская конвенция явно была разработана с целью глобального охвата и в настоящее время имеет более чем 60 участников.

допускаются только при ратификации и депонировании ратификационных грамот, и только по 9 пунктам 9 статей.

Россия высказывала ряд серьезных замечаний, наиболее обсуждаемым из которых является неприемлемость положения, допускающего «посредством компьютерной системы на своей территории получать доступ к компьютерным данным, расположенным на территории другой Стороны» без информирования компетентных органов страны владельца соответствующих ресурсов (статья 32b). История международных отношений знает и менее значительные основания для вмешательства во внутренние дела других стран. Примечательно, что США при ратификации Конвенции заявили, что резервируют за собой право самостоятельного решения о ее исполнении в каждом конкретном случае.

С момента подписания Киберконвенции прошло почти 20 лет. Она остается единственным правовым документом в этой области, но ее эффективность и исполняемость не оценивались. Очевидно, что в нынешних условиях роста криминализации информационной сферы она морально устарела и покрывает далеко не все поле информационных преступлений. В этой ситуации Россия выступила с инициативой создать новый, альтернативный режим под эгидой ООН, который отражал бы приверженность международному праву, в том числе суверенному равенству стран, как-то определяет Устав ООН, не отрицая при этом защиты прав человека, незыблемой для СЕ.

Страны государственнической сферы с 1998 г. предлагают заключить в рамках ООН международные договоры в области борьбы с киберпреступностью и информационной безопасности. Лидеры БРИКС на саммите 2017 года коллективно заявили, о «необходимости универсального нормативного обязательного документа по борьбе с преступным использованием ИКТ под эгидой ООН» (BRICS. 9th BRICS Summit).

Во исполнении своей инициативы Россия предложила ГА ООН в 2017 году проект Конвенции ООН о Сотрудничестве в борьбе с информационными преступлениями (StatementbyForeignMinister). В принятой по этому вопросу 88 голосами «з» в ноябре 2018 года резолюции ГА ООН (UNGA. A/C.3/73/L.9/Rev.1.) сторонники государственнической сферы вновь подчеркнули роль ООН в борьбе с киберпреступностью. Однако, как и предложенный Россией в 2011 г. к широкому обсуждению проект Концепции Конвенции о международной информационной безопасности, этот проект был практически проигнорирован сторонниками либеральной сферы.

По понятным причинам большинство участников Будапештской конвенции восприняли эти попытки как ненужные или преждевременные в свете существующей структуры и необходимости значительного времени и усилий для переговоров по новому соглашению на глобальном уровне. Резолюция 2018 года подверглась резкой критике со стороны представителя США за предпринятую в ней попытку «политизировать, поляризовать и подорвать» существующую политику (US Department of State).

Что касается норм, то усилия государственников подчеркивают их приверженность информационному суверенитету, территориальной целостности и невмешательству, хотя точное значение этих понятий в отношении сети пока нигде не определено. Напротив, сторонники либеральной сферы высказывают опасения по поводу возможности якобы навязать государствам контроль над Интернетом через договор о глобальной сети (UNGA. GA/DIS/3560). Считая принципиальным соблюдение в Интернете упоминающихся в Будапештской Конвенции прав человека, таких как свобода слова или свобода мнений, они упрекают своих оппонентов в ограниченности их уважения указанных прав и замене его ссылками на «стабильность и безопасность общества» или необходимость суверенитета (International Strategy 2017). При этом ревнители прав человека, как всегда, забывают о статье 29 Всеобщей декларации.

Однако подход государственнической сферы после арабской весны и цветных революций находит все более широкую поддержку в мире. У либералов же этот подход вызывает опасения, что за ним стоит нацеленность на введение контроля контента и обхода таким образом конституционалистских принципов (читай: «священной» для американцев Первой поправки к Конституции США), хотя нельзя не признавать, что это сокращает и их возможности воздействия на общество через информационное пространство, где не последнее место сегодня занимают контролируемые теми же либералами социальные сети, которые не только опираются на доступный и лишенный суверенности Интернет, но и были серьезным инструментом для устроителей тех же «весен» и «революций».

ДИСКУССИИ И ВЫВОДЫ

Столь длинный обзор событий и решений последних 20 лет был необходим, поскольку в российской публичной сфере вопрос информационной безопасности как бы есть и как бы нет. Активная индоктринация российского общественного мнения идеей кибербезопасности создала убеждение в том, что информационное пространство – это Интернет, а у многих и того уже – социальные сети. При этом вопрос, что такое Интернет, не имеет строгого ответа даже у многих специалистов. И тем не менее Интернет – реальность. С ним связаны огромные экономические и политические проблемы. В данной статье, конечно, мы не и пытались их решить: это вопрос не сегодняшний – мы лишь хотели бы дать «пищу для размышлений».

Проведенный анализ противоречий в международном дискурсе по вопросам норм и институтов системы управления Интернетом как ключевым на сегодня элементом глобальной информационной сферы и стоящими за ним решениями в области МИБ показывает, что противоречия эти сводятся к антагонизму двух принципиально различных подходов к использованию возможностей глобальной сети, потенциалу решаемых с ее помощью задач бизнеса, политического и информационного доминирования, социального регулирования. Две конкурирующие сферы силы – либеральная и государственническая, как мы их

обозначили, – характеризующиеся фундаментально разными социальными целями, в своем противоборстве, ограничивая или превознося роль государства в управлении глобальной сетью, предпринимают постоянные попытки подстроить систему управления ею и нормативировать ее деятельность так, чтобы максимально обеспечивать достижение своих политических целей. Поскольку управление Интернетом по большому счету пока не нормативировано, эти противоречия пока не влекут за собой коллизии правовых норм. Пока не определено, какие нормы применимы к управлению Интернетом. ГПЭ ООН по МИБ, обсуждая этот вопрос, не сумела опуститься в правовом пространстве глубже Устава ООН. В этой ситуации нормативной неопределенности, две различные сферы силы, конструируя систему управления сетью, которая могла бы обеспечить их интересы в глобальном информационном пространстве, опираются на различные системы норм, исходящие из различных институтов: либералы, как правило, из области прав человека, государственники – из коллективных прав общества. Таким образом, длящиеся почти три десятилетия споры сводятся к ставшим классическими еще со времен Великой французской революции и пока неразрешенным дилеммам: что является определяющим, интересы человека как части общества или общества как совокупности людей; что важнее: права человека в обществе или безопасность общества, реализующего права человека; индивид через свои права представляет интересы общества или общество через право представляет интересы индивида, и насколько общественные институты, в первую очередь государство, представляют общество; в какой степени интересы государства направлены на общее благо.

Сложившийся (или установленный, так как отвечает интересам контролирующего его основные структуры государства) характер управления Интернетом, основанный на идее мультистейкхолдеризма и характеризующийся низкой степенью легитимности и публичности, отсутствием сильного ядра (или его расположением вне сети), институционализации урегулирования споров и множащимися формальными и неформальными площадками для рассмотрения вопросов организации контроля над ним – это действующие факторы, которые в теории должны были бы способствовать быстрой фрагментации системы управления глобальными информационными ресурсами. Однако такой фрагментации не видно. Создание в ООН в 2018 году по российской инициативе Рабочей группы открытого состава, в противовес ставшей традиционной, но занявшей проамериканскую позицию Группе правительственных экспертов, демонстрирует разве что решимость государственников и также не обещает существенных дивидендов.

Конфликт между двумя сферами силы не ограничивается проанализированными здесь случаями. Мы не коснулись ситуации в ОБСЕ в 2014–2016 годах, когда были разработаны «добровольные» меры безопасности, позволяющие на деле контролировать поведение государств в информационной сфере, в АСЕН, стремящейся с подачи американцев копировать ОБСЕ, деятельности ШОС и БРИКС, представляющих в этой дискуссии половину

человечества. Но и рассмотренное можно трактовать как индикаторы широкого противоборства на пути защиты и оспаривания существующих норм управления Интернетом и его институтами. Россия предложила принять Конвенцию о международной информационной безопасности в 2011 году (Conventionon International Information). Государства-члены ШОС продвигали в ГА ООН кодекс поведения в области информационной безопасности (A/69/723). Кроме того, Китай организовал ежегодную Всемирную конференцию по вопросам Интернета, ориентированную на выработку глобальных норм управления сетью.

Однако либеральная сфера испытывает вызовы не только извне, но и изнутри. Особенно после разоблачений Сноудена в 2013 году, когда конфликты в таких областях, как конфиденциальность данных, бросили вызов монополии США и американских компаний. Передача в 2016 г. функций управления пространством имен и адресов Интернета – критической технологической процедурой, обеспечивающей функционирование Интернета на глобальном уровне, – от ICANN, частной некоммерческой организации, имеющей контрактные отношения с правительством США, к ее дочерней фирме (Public Technical Identifiers)[1] не решила проблемы с подотчетностью и международной легитимностью сложившейся системы управления сетью, оставив правительству США существенные рычаги влияния. Однако, как и ранее, государства, ключевые субъекты формирующегося глобального режима международной информационной безопасности, не имеют возможности влиять на принимаемые решения. Эти вызовы не приводят к ослаблению либерального курса. Несмотря на поддержку со стороны либеральной сферы инициатива NETmundial провалилась, но лигитимировала концепцию мультистейкхолдеризма. Либеральная сфера адаптируется или даже укрепляется, реагируя на вызовы, и тем самым предотвращает фрагментацию управления Интернетом. Однако либеральная сфера страдает от двух несоответствий.

Во-первых, существует сильная зависимость либералов от частного саморегулирования, мягкое право и дискурсивные многосторонние процессы не заменяют публичное международное право. В результате либеральная сфера сильна в отношении технической власти, но слаба в легитимной политической власти. Необходимость в последней, однако, все больше ощущается по мере того, как управление Интернетом набирает политическое и экономическое значение. Фирма Microsoft призывает принять международный документ, адресованный правительствам (Цифровая Женевская конвенция) и обязывающий их принять нормы, необходимые для защиты гражданского населения в Интернете в мирное время. Однако он с большой сдержанностью рассматривается Германией, государством, которое обычно выступает с позиций многосторонности и

[1]Данная организация формально независима от Министерства торговли США (для выполнения своих функций ей не требуется одобрения Министерства торговли США), но при этом зарегистрирована в США, штат Калифорния и не имеет права выводить инфраструктуры адресного пространства Интернета за пределы штата. Работа PTI будет прекращена в том случае, если Министерство торговли США расторгнет контактные отношения с ICANN

международного права. При этом практически все игнорируют аналогичную инициативу Норникеля, с которой тот выступил еще в 2017 г.

Во-вторых, меняется либеральное отношение к призыву государственников рассматривать интернет-коммуникации при нынешней системе управления ими как потенциального носителя угрозы извне для внутренней стабильности государства и общества. В течение долгого времени либералы расценивали этот аргумент как троянского коня для «нелиберальных и недемократических» государств, оправдывающий возможность отключения Интернета и цензуру. Для государственников нынешняя система норм и институтов, напротив, является еще одним примером того, как небольшое число западных государств доминирует в информационной сфере с помощью глобализации и ее средствами эту глобализацию поддерживает. Их основной аргумент заключается в том, что нынешняя система управления Интернетом глубоко вторгается не только в информационное пространство страны, но и в законные внутренние социальные отношения и внутренние законы государства. Даже среди западных государств наблюдается растущая тенденция к введению законодательства, направленного на криминализацию явных нарушений внутреннего законодательства, борьбу с террористической пропагандой и дезинформацией, особенно когда она мешает работе государственных и общественных институтов и экономике. Опасения либеральной сферы в этом отношении звучат все более похоже на те, что принадлежат государственникам. Это ослабляет либеральное сопротивление ограничению свободы выражения мнений в угоду законным внутригосударственным интересам.

Противоречия в отношении управления Интернетом – это нечто большее, чем классический межгосударственный спор. Это фундаментальный ценностный конфликт между различными сферами власти, относительно того, каким образом должны быть организованы глобальные сети и каким образом следует осуществлять управление ими, памятуя Кастельса и его «власть в сети».

Для МИБ попытки маскировки политических решений, принимаемых органами управления Интернетом, реализующими политические интересы только одной страны, представляют серьезную опасность. 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 бы при участии всех заинтересованных сторон, поскольку ни одно государство не в состоянии обеспечить информационную безопасность и сохранить связность Интернета как глобальной системы без многостороннего сотрудничества. Безопасность должна быть единой и неделимой не только в Европе, но и в информационном пространстве. И государства, как основные политические институты общества, должны занимать в этой системе особое место и нести

основную ответственность, обладая соответственно большими правами и уравновешивая складывающуюся систему сфер власти.

Постепенно это понимание входит в сознание и технических специалистов и политиков.

СПИСОК ЛИТЕРАТУРЫ

Зиновьева, Е.С. (2011). *Международное управление интернетом: конфликт и сотрудничество.* Москва: МГИМО-Университет. 169 с.

Курбалийя, Й. (2010). *Управление Интернетом*. Москва: Координационный центр национального домена сети Интернет. 208 с.

Тоффлер, Э. (2004). *Третья волна*. Москва: АСТ. 781 с.

Федоров, А.В., Зиновьева, Е.С. (2017). *Информационная безопасность: политическая теория и дипломатическая практика*. Москва: МГИМО-Университет. 357 с.

A/69/723. Letter Addressed to the Secretary-General. Retrieved from https://digitallibrary.un.org/record/786846

BRICS. 9th BRICS Summit – BRICS Leaders Xiamen Declaration. Xiamen, Retrieved from http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf

Castells, M. (2008). The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The Annals of the American Academy of Political and Social Science*, *616*, 78-93. https://doi.org/10.1177/0002716207311877

Convention on International Information Security. Retrieved from http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Convention on Cybercrime. Budapest: ETS No 185. Retrieved from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

International Strategy of Cooperation on Cyberspace Retrieved from http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

Markoff, M.G. Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://2017-2021.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/index.html

Menoher, P.E.Jr. (1996). Lieutenant General, the U.S. Army Deputy Chief of Staff for Intelligence. «Force XXI: Redesigning the Army Through Warfighting Experiments» Military Intelligence Professional Bulletin, *2*. Retrieved from https://fas.org/irp/agency/army/mipb/1996-2/menoher1.htm

Public Technical Identifiers (PTI). IANA Naming Function Contract. 30 September 2016. Retrieved from https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

O'Reilly, T. (2005). What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software. *Oreilly.com*. Retrieved from http://oreilly.com/web2/archive/what-is-web-20.html

Statement by Foreign Minister Sergey Lavrov at the 72nd Session of the UN General Assembly. (21 September) New York, NY: United Nations. Retrieved from http://www.mid.ru/en/vizity-ministra/asset_publisher/ICoYBGcCUgTR/content/id/2870898

UN GA. A/C.1/73/L.37. Advancing Responsible State Behaviors in Cyberspace in the Context of International Security. Retrieved from http://undocs.org/A/C.1/73/L.37

UN GA. GA/DIS/3560. Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race. Retrieved from https://www.un.org/press/en/2016/gadis3560.doc.htm

UN GA. A/C.3/73/L.9/Rev.1.Countering the Use of Information and Communications Technologies for Criminal Purposes. Retrieved from http://undocs.org/A/C.3/73/L9/Rev.1

UN GA. A/C.1/73/L.27/Rev.1. Developments in the Field of Information and Telecommunications in the Context of International Security Retrieved from http://undocs.org/A/C.1/73/L.27/Rev.1.UN GA. A/C.3/73/L.9/Rev.1

US Department of State. Explanation of Vote on a Third Committee Resolution on Countering the Use of Information and Communication Technologies for Criminal Purposes. Bureau of Public Affairs. Retrieved from http://www.state.gov/misc/415.htm/remarks/8803

World Conference on International Telecommunications (WCIT-12). Retrieved from https://www.itu.int/en/wcit-12/Pages/default.aspx

World Summit on the Information Society, (2003) Declaration of Principles: Building the Information Society: a global challenge in the new Millennium. Dokument WSIS-03/GENEVA/DOC/4-E. 12 December 2003. Retrieved from http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

World Summit on the Information Society (2005). Dokument WSIS-05/TUNIS/DOC/7-E. TUNIS COMMITMENT. 18 Novembe 2005. Retrieved from http://www.itu.int/wsis/docs2/tunis/off/7-E.pdf

Zürn, M. (2018). *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford: Oxford University Press. Retrieved from https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198819974.001.0001/oso-9780198819974

Для цитирования: Федоров, А.В. (2021). Противоборство сфер силы в вопросах управления в информационном пространстве. *Caspium Securitatis: журнал каспийской безопасности*, *1*(2), 11-34.

DOI 10.21672/2713-024X-2021-2-1-011-034

REFERENCES

Zinovieva, E.S. (2011). *International Internet Governance: Conflict and Cooperation.* Moscow: MGIMO-University. 169 p. (In Russian)

Kurbaliyya, Y. (2010). *Internet Management*. Moscow: Coordination center for the national Internet domain, 208 p. (In Russian)

Toffler, E. (2004). *Third wave*. Moscow: AST. 781 p. (In Russian)

Fedorov, A.V. & Zinovieva, E.S. (2017). *Information security: political theory and diplomatic practice*. Moscow: MGIMO-University. 357 p. (In Russian)

A/69/723. Letter Addressed to the Secretary-General, Retrieved from https://digitallibrary.un.org/record/786846

BRICS. 9th BRICS Summit – BRICS Leaders Xiamen Declaration. Xiamen, Retrieved from: http://www.mea.gov.in/Uploads/PublicationDocs/28912_XiamenDeclaratoin.pdf

Castells, M. (2008). The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance. *The Annals of the American Academy of Political and Social Science*, *616*, 78-93. https://doi.org/10.1177/0002716207311877

Convention on International Information Security. Retrieved from http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666

Convention on Cybercrime. Budapest: ETS No 185. Retrieved from http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

International Strategy of Cooperation on Cyberspace Retrieved from http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm

Markoff, M.G. *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*. Retrieved from https://2017-2021.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/index.html

Menoher, P.E.Jr. (1996). Lieutenant General, the U.S. Army Deputy Chief of Staff for Intelligence. «*Force XXI: Redesigning the Army Through Warfighting Experiments» Military Intelligence Professional Bulletin*. *2*. Retrieved from https://fas.org/irp/agency/army/mipb/1996-2/menoher1.htm

Public Technical Identifiers (PTI). IANA Naming Function Contract. 30 September 2016. Retrieved from https://www.icann.org/iana_pti_docs/151-iana-naming-function-contract-v-30sep16

O'Reilly, T. (2005). What Is Web 2.0. Design Patterns and Business Models for the Next Generation of Software. *Oreilly.com*. Retrieved from http://oreilly.com/web2/archive/what-is-web-20.html

Statement by Foreign Minister Sergey Lavrov at the 72nd Session of the UN General Assembly. (21 September) New York, NY: United Nations Retrieved from http://www.mid.ru/en/vizity-ministra/asset_publisher/ICoYBGcCUgTR/content/id/2870898

UN GA. A/C.1/73/L.37. Advancing Responsible State Behaviors in Cyberspace in the Context of International Security. Retrieved from http://undocs.org/A/C.1/73/L.37

UN GA. GA/DIS/3560. Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race. Retrieved from https://www.un.org/press/en/2016/gadis3560.doc.htm

UN GA. A/C.3/73/L.9/Rev.1. Countering the Use of Information and Communications Technologies for Criminal Purposes, Retrieved from http://undocs.org/A/C.3/73/L.9/Rev.1

UN GA. A/C.1/73/L.27/Rev.1. Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from http://undocs.org/A/C.1/73/L.27/Rev.1. UN GA. A/C.3/73/L.9/Rev.1.

US Department of State. Explanation of Vote on a Third Committee Resolution on Countering the Use of Information and Communication Technologies for Criminal Purposes. Bureau of Public Affairs. Retrieved from http://www.state.gov/misc/415.htm/remarks/8803

World Conference on International Telecommunications (WCIT-12). Retrieved from https://www.itu.int/en/wcit-12/Pages/default.aspx

World Summit on the Information Society, (2003) Declaration of Principles: Building the Information Society: a global challenge in the new Millennium. Retrieved from: http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf

World Summit on the Information Society (2005). Dokument WSIS-05/TUNIS/DOC/7-E. TUNIS COMMITMENT. 18 Novembe 2005. Retrieved from http://www.itu.int/wsis/docs2/tunis/off/7-E.pdf

World Summit on the Information Society (2005). Dokument WSIS-05/TUNIS/DOC/7-E. TUNIS AGENDA FOR THE INFORMATION SOCIETY. 18 Novembe 2005. Retrieved from http://www.itu.int/wsis/docs2/tunis/off/6-E.pdf

For citation: Fedorov, A.V. (2021). The Confrontation of the Spheres of Power in the Management of the Information Space. *Caspium Securitatis: Journal of Caspian Safety & Security*, *1*(2), 11-34.

DOI 10.21672/2713-024X-2021-2-1-011-034