УДК 327

Павел ШАРИКОВ

Наталья СТЕПАНОВА

ПОДХОДЫ США, ЕС И РОССИИ К ПРОБЛЕМЕ ИНФОРМАЦИОННОЙ ПОЛИТИКИ

Аннотация. Статья посвящена сравнительному анализу подходов Соединённых Штатов Америки, европейских государств и России по вопросам государственного регулирования информационной политики. Авторы ставят перед собой цель на конкретных примерах и политических шагах исследовать эволюцию таких понятий, как нейтральность сети, конфиденциальность информации, стратегия в сфере информационной безопасности. В новую информационную эпоху важнейшим ресурсом международного влияния является информация, что требует иного подхода в политическом регулировании. При этом политические системы стран Западной цивилизации более гибко реагируют на подобные вызовы современности. В ЕС и США сохраняются сильные политические традиции демократии, верховенства закона и гражданского общества. В Российской Федерации подобные вызовы имеют иной эффект.

Ключевые слова: США, ЕС, Россия, информационная политика, информационная безопасность, нейтральность сети, конфиденциальность.

Многие текущие события свидетельствуют о том, что современные международные отношения переживают очередной период турбулентности. Колоссальную роль при этом играет информационная революция и повсеместное распространение информационных технологий. Исследователи обращают внимание на социальные процессы, происходящие под влиянием информационной революции. В наиболее популярных теориях второй половины XX в., объясняющих современные социальные процессы, применяется термин “постиндустриальное общество”. Так, один из его первых идеологов Д. Белл говорит о том, что продукт, производимый в постин-

© **Шариков Павел Александрович** – ведущий научный сотрудник, Институт США и Канады РАН. **Адрес:** 121069, Россия, Москва, Хлебный переулок д. 2/3. **E-mail:** pasha.sharikov@gmail.com

Степанова Наталья Владиславовна – научный сотрудник, Институт США и Канады РАН. **Адрес:** 121069, Россия, Москва, Хлебный переулок д. 2/3. **E-mail:** nathalienaz@yandex.ru

Исследование выполнено при финансовой поддержке РГНФ в рамках научно-исследовательского проекта “Проблема электронной разведки в современной системе международной безопасности”, проект № 15-37-01203.

DOI: <http://dx.doi.org/10.15211/soveurope220197383>

дустриальном обществе, имеет принципиально новые качества по сравнению с тем, что производилось в обществах индустриальных и доиндустриальных [Bell, 1973: 116]. Э. Тоффлер утверждал, что средства массовой информации усиливают демасификацию общества, что влечёт за собой “огромный скачок объема информации, которой обмениваются люди друг с другом, и поэтому общество становится информационным” [Toffler, 1980: 182–183]. Очевидно, что вопросы регулирования сферы информации становились политическими приоритетами, однако большие сложности возникали в связи с особенностями информационных ресурсов в современном мире.

В современной мировой политике информация представляет собой одновременно важнейший ресурс, инструмент международного влияния и среду взаимодействия. При этом информация обладает рядом уникальных свойств, отличающих её от материальных ресурсов. Прежде всего – неотчуждаемость: передача или обмен информацией в большинстве случаев не подразумевает её отчуждение у одного субъекта в пользу другого. Безопасность информации подразумевает гарантию сохранения её определенных свойств – объективность, доступность, целостность, конфиденциальность, оперативность и др. Информационные ресурсы состоят из двух взаимодополняемых элементов – содержание и инфраструктура. Особое значение вопросы информационной политики приобрели в 1990-е гг., когда распространение информационных технологий приобрело революционный характер.

Учитывая стратегическое значение информационных ресурсов в современном мире, проблема безопасности информации стала приоритетом внутривластного регулирования и международных отношений. Очевидно, что применить к информации те же методы регулирования, что и в отношении прочих ресурсов, невозможно. Проблема осложняется тем, что производство и потребление информации в значительно большей степени индивидуально по сравнению с промышленными товарами и другими ресурсами. Информационная революция существенно расширила политические и экономические возможности индивидов в глобальном масштабе, что стало одним из наиболее сложных вызовов государственному суверенитету. В частности, британские исследователи утверждают, что “взаимодействие через интернет позволяет гражданам самостоятельно выполнять функции, которые ранее выполняло государство” [Micklethwait, Wooldridge, 2015].

К началу XXI века влияние информационной революции было уже настолько заметным, что требовало реакции политических систем для обеспечения безопасности. Принимаемые каждым государством меры в области регулирования сферы информации обусловлены внутренними политическими и правовыми традициями. Вместе с тем, учитывая усилившиеся возможности индивидов, возможности государственного регулирования и обеспечения безопасности информационных ресурсов крайне ограничены.

Особое значение имеет защита конфиденциальности информации. Учитывая во многом индивидуальный характер производства и потребления информации, обеспечение безопасности информационных ресурсов на уровне каждого индивида – особая задача для государства. Именно при разработке мер по обеспечению безопасности частной информации особенно ярко проявляются проблемы, обусловленные чрезмерным или недостаточным контролем и вмешательством со стороны государства. Современные информационные и интернет-технологии позволяют получить

практически исчерпывающую информацию об индивидах. Колоссальное количество информации можно получить, анализируя данные о деятельности в социальных сетях. При несанкционированном доступе угрозы могут исходить от недобросовестных пользователей, коммерческих компаний, и даже государственных структур.

Проблема информационной безопасности актуальна не только на национальном уровне, но и в международных отношениях. Глобальное информационное пространство открыло возможности информационного взаимодействия между различными акторами: индивидами, негосударственными акторами системы международных отношений, государственными деятелями. Особенности информационных ресурсов не позволяют применить те же нормы международного права, что и в отношении физически осязаемых пространств – воздушного, морского, наземного и космического.

Эти тенденции ставят новые задачи перед государством в сфере защиты национального суверенитета. Так или иначе, информационная революция коснулась всех стран, и всегда реакция государства основывалась на правовых и политических традициях. Подобно тому, как политические традиции верховенства права и неприкосновенности частной собственности стали важным фактором британского лидерства среди промышленно развитых государств, именно политические особенности стали заметным фактором американского превосходства в глобальном мире в информационную эпоху. Политический подход к регулированию информационных ресурсов в странах Запада и в первую очередь в Соединённых Штатах Америки заметно отличается от российского, что сыграло определённую роль в развитии двустороннего кризиса отношений между Россией и США, а также многими странами Запада. В условиях глобализации внутривнутриполитические изменения неизбежно приводят к появлению противоречий между субъектами международных отношений. Политическое руководство разных стран применяет различные методы защиты национального суверенитета, включая информационные ресурсы. Информационная асимметрия, а также различный подход к государственному регулированию информационных ресурсов во внешней политике стали дополнительными факторами в развернувшемся кризисе российско-американских отношений.

Американский опыт политического регулирования информации

Регулирование сферы информации стало приоритетом американской государственной политики раньше, чем в других странах. Это связано с тем, что именно США стали эпицентром информационной революции во второй половине XX века.

После экономического бума 1990-х гг., когда администрация У. Клинтона стремилась извлечь максимум экономической выгоды от информационно-технологической революции, произошло резкое усиление государственного контроля. Приоритетом администрации Дж. Буша-мл. было противодействие терроризму, что требовало усиления государственного контроля над информационными ресурсами. Такие меры вызвали мощные протесты со стороны гражданского общества, под влиянием которых эти решения были пересмотрены при администрации президента Б. Обамы.

Традиции индивидуализма определили генеральный подход американской политической системы к вызовам информационной эпохи. Ключевой вызов заклю-

чался в том, чтобы гарантировать равные возможности производства и потребления информации каждому индивиду.

В этой связи администрация Б. Обамы приняла “net neutrality” – принцип “нейтральности сети”¹, в основу которой были положены работы в области права американского профессора права Тима Ву. Американский правовед утверждал, что интернет должен развиваться согласно принципу равенства, который выражается в том, что все информационные сети должны стремиться обеспечить равный доступ всех пользователей к любому цифровому контенту [Wu, 2003: 146]. Принцип нейтральности сети подразумевает, что поставщики услуг связи, политические организации обязаны гарантировать равный доступ пользователей к производству и потреблению информации. Безопасность информации достигается через гарантию безопасности инфраструктуры при том, что политические или коммерческие структуры почти не контролируют содержание создаваемой и передаваемой информации.

В современном мире американский информационный потенциал заметно превосходит информационные ресурсы других стран. Вместе с тем представляется, что принцип нейтральности сети не связан с гегемонией Соединённых Штатов. Во-первых, специфика информационных ресурсов предполагает значительную асимметрию, т.е. возможность нанесения заметного ущерба при отсутствии превосходства. Во-вторых, информация является важным, но не единственным фактором, определяющим мощь государств в современном мире. В США действительно наблюдалась определённая эйфория после окончания холодной войны, однако уже президент Б. Обама признал, что однополярному миру, а соответственно и американской гегемонии не суждено состояться. Этот тезис нашел отражение в Стратегии национальной безопасности США 2010 г. [The US National Security Strategy, 2010] и в других доктринальных документах. В-третьих, в отношениях с европейскими союзниками проблемы “нейтральности сети” нет, даже на фоне появляющихся противоречий в других областях.

Президент Д. Трамп принял решение отменить [With net neutrality repeal., 16.12.17] принцип “нейтральности сети”, чем спровоцировал волну протестов со стороны предприятий информационно-технологического комплекса. В мае 2018 г. вопрос об отмене решения Трампа был вынесен на голосование в резолюции Сената. С минимальным отрывом [S.J.Res.52, 16.05.18] принцип нейтральности сети был поддержан, что говорит о том, что данная проблема остаётся приоритетной в информационной политике США. Вместе с тем перспектива принятия этой резолюции в Палате Представителей менее оптимистична, как и одобрение президента. Тем не менее очевидно, что сторонники “свободного интернета” продолжают оказывать давление на власть.

Принцип “сетевого нейтралитета” предполагает отсутствие монополии на распространение информации. Исходя из того, что львиная доля информационного взаимодействия происходит в цифровой сфере, принцип “сетевого нейтралитета” прежде всего ориентирован на “посредников” – провайдеров телекоммуникационных услуг. Они обязаны обеспечить равное распространение информации в отношении каждого пользователя. Отмена данного принципа позволит монополизиро-

¹ “Net neutrality”, в русскоязычной литературе также встречается перевод “сетевой нейтралитет”.

вать инструменты информационного обмена в первую очередь в пользу тех, кто обладает масштабными финансовыми ресурсами. Если этот принцип не соблюдается, сеть не может оставаться нейтральной.

Отход от глобалистской информационной политики в администрации Д. Трампа отражён и в Национальной стратегии кибербезопасности, опубликованной в сентябре 2018 г. В частности, в ней признаётся, что “США вовлечены в долгосрочное соперничество в киберпространстве против стратегических противников, государств-изгоев и криминальных сетей” [The US National Cyber Strategy, 2018]. В связи с этим, американское правительство намерено предпринимать самые решительные действия для обеспечения национальной кибербезопасности. Судя по всему, именно этой логикой руководствовалась администрация Д. Трампа, принимая решение об отмене “нейтральности сети”. Ещё в период предвыборной кампании Д. Трамп утверждал, что одной из серьёзных политических проблем современной Америки, препятствующих её развитию, являются “фальшивые новости” и “пост-правда”.

Практика политики “сетевого нейтралитета” в Европе

Примечательно, что проблема нейтральности сети возникла в Европе гораздо позже и оказалась гораздо менее резонансной, чем в Соединённых Штатах [Cave, Crocioni, 2007]. Во многом это связано с тем, что в европейских государствах сложилась полноценная нормативно-правовая база, способная регулировать рыночные аспекты таким образом, чтобы принцип “сетевого нейтралитета” соблюдался практически повсеместно. Приоритеты европейской политики регулирования информации имеют определённую уникальную специфику, однако во многом схожи с американскими. Прежде всего, информационная политика европейских стран развивается на нескольких уровнях: на национальном и на уровне структур Европейского Союза.

Дискуссии о целесообразности и эффективности применения принципа “нейтральности сети” в Европейском Союзе ведутся с первой половины 2000-х гг. Многие исследователи скептически относятся к данному принципу. Ряд исследователей полагал, что он противоречит действующему в ЕС антимонопольному законодательству и что его принятие нанесёт ущерб интересам потребителей [Cave, Crocioni, 2007]. Тем не менее большинство европейских государств используют принцип нейтральности сети при выработке информационной политики и стратегии кибербезопасности.

Стратегия кибербезопасности Великобритании [The UK National Cyber Security Strategy 2016–2021] утверждает следующие принципы обеспечения кибербезопасности: “неукоснительно защищать и продвигать наши основополагающие ценности. Они включают в себя демократию, верховенство закона, свободу, открытое и подотчётное правительство и другие органы власти, человеческие права, свободу слова, обеспечение и защиту частной жизни граждан Великобритании”.

Стратегия национальной безопасности в цифровой сфере Франции¹ также ставит во главу угла “безопасное киберпространство для субъектов предпринимательской деятельности любого размера, а также частных лиц, она провозглашает наме-

¹ French National Digital Security Strategy. URL: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (дата обращения: 04.10.2018).

рение принять меры по обеспечению безопасности, а также меры по устранению дефектов”. Французское правительство также заявляет о переходе к стратегии цифровой автономии с целью обеспечения внутренней безопасности, что является ярчайшим примером интернет-фрагментации.

В стратегии в сфере кибербезопасности Германии говорится о том, что “безопасность инфраструктуры требует большей защищенности информационно-технологических систем, используемых гражданами, а также малыми и средними организациями. Пользователям необходимы меры, предпринимая которые они могут использовать киберпространство безопасным образом”. В то же время власти Германии утверждают, что “в мировом киберпространстве безопасность может достигаться только через координированные действия на национальном и международном уровне”. Национальная стратегия в сфере кибербезопасности Испании признает, что существующие в ней угрозы сводятся не только к национальным государствам, но исходят от многих других акторов. “Основными принципами в сфере кибербезопасности являются ведущая роль государств, а также согласованность действий; взаимная ответственность; пропорциональность, рациональность и эффективность; международное сотрудничество как продолжение основных принципов Национальной стратегии безопасности”.

Большинство, если не все страны – члены ЕС провозглашают демократические принципы государственного регулирования интернета и национальной зоны киберпространства. Все европейские страны уделяют первоочередное внимание защите индивидуальных, нежели государственных интересов в цифровом пространстве. Все национальные стратегии в сфере кибербезопасности затрагивают как угрозы инфраструктуре, так и борьбу с пропагандой и распространением вредоносной информации из-за рубежа. На глобальном уровне Европа сталкивается с двойной интернет-фрагментацией – как на национальном уровне, так и на уровне институтов Европейского Союза. При этом, если общий подход к регулированию информационных источников является одинаковым, некоторые отличия всё-таки остаются.

Региональный европейский подход к информационной политике предполагает обеспечение гарантий нейтральности в сфере доступа к информации.

Орган европейского регулирования в сфере цифровых коммуникаций (The Body of European Regulators for Electronic Communication, BEREC) активно вовлечён в обеспечение “сетевой нейтральности” с 2010 г. В 2015 г. Европейский парламент и Совет приняли Директиву (ЕС) 2015/2120, в которой излагаются основные правила обеспечения равного доступа к трафику, предоставляемому интернет-провайдерами, и соблюдения вытекающих из него прав конечных пользователей. В 2016 г. BEREC принял основные принципы национального регулирования европейских правил “сетевой нейтральности” [BEREC Guidelines, 30.08.2016]. Таким образом, в каждой стране – члене ЕС существуют регулирующие органы, контролирующие рынок и способные оценить управление трафиком, коммерческие практики и соглашения и обеспечить соблюдение Директивы 2015/2120. Данные органы также обеспечивают соответствие качества услуг, предоставляемых интернет-провайдерами, технологическим возможностям. В соответствии с 5 статьей Директивы национальные регулирующие органы предоставляют ежегодные отчеты о соблюдении правил “открытого интернета” в Европейскую комиссию и BEREC. Публичный характер установленных в 2016 г. принципов наглядно подтверждается проведе-

Современная Европа, 2019, №2

нием предварительной дискуссии, в которой любой интернет-пользователь мог высказать свои предложения. Более 500 тыс. европейцев поддержали принцип нейтральности сети¹.

Определённое воздействие на европейскую политику в области нейтральности сети оказало решение администрации Д. Трампа отменить указанный принцип. Европейский парламент направил письмо в Конгресс США, в котором высказал глубокую озабоченность тем, что новое законодательство будет иметь глобальный эффект и ударит по нормам нейтральности сети, совсем недавно установленным в Европе [Europe Urges US to Block Trump on Net Neutrality, 22.01.2018]. Сомнению подверглась и будущая национальная политика Великобритании, которая после брекзита свободна устанавливать собственные “правила игры” и потенциально выйти из Директивы 2015/2120. Однако на территории Соединённого Королевства продолжает действовать национальный контролирующий орган², более того – правительство приняло на себя Обязательства по предоставлению услуг в зоне всеобщего охвата (Universal Service Obligation), гарантирующего широкополосный доступ в интернет со скоростью не ниже 10 Мбит/с каждому дому и предприятию³. Представляется, что Великобритания и в дальнейшем будет следовать принципу нейтральности сети.

Ключевым элементом информационной политики является определение пределов государственного контроля. Особое значение данное направление имеет для защиты конфиденциальных данных пользователей. Данное направление также всегда являлось приоритетом информационной политики в Европе. С этой целью в ЕС был принят Общий Регламент по защите данных [General Data Protection Regulation], принятый в 2016 г. и вступивший в силу 25 мая 2018 года.

Регламент предоставляет различные гарантии неприкосновенности конфиденциальной и частной информации европейских пользователей. Особое внимание в регламенте уделяется ответственности предоставляющих информационные услуги компаний перед пользователями. В частности, одним из основных положений регламента является ответственность компаний перед пользователями в сфере защиты конфиденциальных данных. Компании обязаны в ответ на запросы пользователей сообщать, каким образом они получают и защищают информацию пользователей.

Перспективы “сетевого нейтралитета” в России

Примечательно, что конфликт России и стран Запада во многом разворачивается в информационной сфере. Более того, решения в области регулирования сферы информации в российском внутривнутриполитическом процессе нередко провоцируют негатив в отношениях России и Запада.

Различный подход к информационному регулированию уже приводил к возникновению противоречий в отношениях между ними.

¹ SaveTheInternet.eu. URL: <https://savetheinternet.eu> (дата обращения: 04.10.2018).

² What is Ofcom? URL: <https://www.ofcom.org.uk/about-ofcom/what-is-ofcom> (дата обращения: 04.10.2018).

³ Broadband Universal Service Obligation: consultation on design. URL: <https://www.gov.uk/government/consultations/broadband-universal-service-obligation-consultation-on-design> (дата обращения: 04.10.2018).

Российская политическая система также адаптируется к новым условиям, однако присущий ей патернализм препятствует тем сценариям развития, которые происходят на Западе. Под влиянием информационной революции российское политическое руководство усиливает государственный контроль над сферой информации.

Российская информационная политика во многом фокусируется на содержании информации, передаваемой посредством телекоммуникационных сетей. Многие разработанные законодательные нормы заключаются в разработке государственных стандартов, которым должны соответствовать данные, размещаемые и передаваемые в российском сегменте сети Интернет. Разработанная в 2015 г. норма о локализации данных свидетельствует о том, что в российском правовом поле понимание феномена “информация” не учитывает особенностей этого ресурса и воспринимает его как физический объект, находящийся в юрисдикции государственного суверенитета.

Органы государственного управления обладают широкими полномочиями. В большинстве доктринальных документов интересы государства противопоставляются интересам граждан. В частности, Доктрина информационной безопасности в редакции 2016 г.¹ сохраняет триаду интересов личности, общества и государства, принятую еще в редакции 2000 г.², однако положения, касающиеся интересов личности, практически исчезли: сохранились только формулировки, касающиеся интересов государства.

В Доктрине 2016 г. декларируется, что “стратегическими целями обеспечения информационной безопасности... являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры”. При этом основные угрозы связаны с деятельностью иностранных субъектов. Утверждается, что “возможности трансграничного оборота информации всё чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности”³.

Характерный для российской политической системы консерватизм подразумевает широкие полномочия государственных органов, в том числе в отношении информационной сферы. В соответствии с российскими политическими традициями индивидуальное производство и потребление информационных ресурсов ограничивается, а государственный контроль усиливается. Применение информационных ресурсов в целях защиты национального суверенитета в России имеет не меньшее значение, но совершенно иную природу, чем в США и Европе, в силу чего и появляются политические противоречия.

¹ Доктрина информационной безопасности Российской Федерации. URL: <http://www.scrf.gov.ru/security/information/document5/> (дата обращения: 04.10.2018).

² Доктрина информационной безопасности Российской Федерации (утратила силу). URL: <http://base.garant.ru/182535/#friends#ixzz4tECPhvyL> (дата обращения: 04.10.2018).

³ Доктрина информационной безопасности Российской Федерации. URL: <http://www.scrf.gov.ru/security/information/document5/> (дата обращения: 04.10.2018).

С таким подходом российским технологическим компаниям намного сложнее оставаться нейтральными от политических процессов. Это уже проявлялось во многих инцидентах. Наиболее ярким примером является эпизод с социальной сетью “Телеграм”. Весной 2018 г., после отказа сети “Телеграм” предоставить ключи шифрования органам государственной безопасности, Роскомнадзор принял решение заблокировать интернет-адреса, через которые обслуживалась социальная сеть. Проблема заключалась в том, что выполнить требования властей было технически невозможно, а интернет-адреса зачастую совпадали с теми, которые обслуживали и другие интернет-сервисы. В результате действий Роскомнадзора было заблокировано порядка 20 миллионов интернет-адресов, включая те, что обслуживали такие популярные сервисы, как Amazon, Google и т.д. Данный конфликт подтверждает тезис о чрезмерном вмешательстве российских государственных структур в регулирование информационного взаимодействия.

Большое беспокойство вызывает тесное сотрудничество ряда российских сайтов с государственными органами. В частности, об этом свидетельствует преданный огласке запрос польского пользователя российской сети “ВКонтакте” о собственных персональных данных [Is Russian social media giant VKontakte..., 30.08.2018]. Социальная сеть была вынуждена ответить на запрос пользователя, учитывая, что в противном случае была бы подвергнута большому штрафу из-за принятого Регламента о защите данных.

Выяснилось, что сеть “ВКонтакте” имеет доступ к колоссальному количеству информации, более того, ход многих недавних судебных дел свидетельствует о том, что “ВКонтакте”, а также ряд других крупных компаний передают информацию в правоохранительные органы, пренебрегая судебной процедурой.

Большой проблемой, являющейся “раздражителем” в отношениях России и Запада, являются обвинения в распространении пропаганды. В то время как пропаганда была востребованным инструментом идеологического противоборства в период холодной войны, в основе нынешнего кризиса нет идеологического конфликта. При этом активно применяется пропаганда, возможности которой заметно усилены технологическими решениями XXI века. Примечательно, что если Российская стратегия противодействия влиянию Запада заключается в ограничении доступа российских пользователей к информации из-за рубежа, то в Европе действуют иным образом.

В целях противодействия российским “фальшивым новостям” в структуре ЕС была создана специальная рабочая группа “по противодействию российской дезинформации” (EU vs Disinformation campaign). Не ограничивая доступ европейских пользователей к информации из российских источников, на специальном сайте публикуются опровержения фактам, которые размещаются в российском информационном пространстве, в особенности на иностранных языках. Данный подход соответствует практике “сетевого нейтралитета”. Воздерживаясь от оценок, представленных на сайте по конкретным кейсам, очевидно, что подобная мера свидетельствует о тяжелейшем кризисе доверия между Россией и Европой.

Более того, к сожалению, в последние годы российские власти предпринимают усилия для ужесточения информационной политики. В результате принятого комплекса мер происходит заметное ограничение взаимодействия граждан России с внешним миром. Подобная информационная автаркия негативно отражается на самых разных аспектах внешней и внутренней политики России.

* * *

Регулирование информации стало приоритетом государственной политики практически во всех странах. Соединённые Штаты во многом были пионерами в данной сфере, учитывая, что именно там влияние информационной революции стало ощущаться раньше, чем в других странах. Американская информационная политика формировалась во многом стихийно, под влиянием уникальных факторов, однако в настоящее время уже можно выделить ряд основных направлений регулирования. Среди них: гарантия конфиденциальности, создание условий равной конкуренции в сфере производства информации, информационная безопасность.

Европейская информационная политика во многом складывалась под влиянием американской. Наиболее эффективные элементы американского опыта регулирования сферы информации широко используются в Европе, в определённом смысле даже опережая Соединённые Штаты. Именно потребительский спрос обеспечил революционное развитие информационных технологий в США, поэтому интересы потребителей остаются центральным объектом регулирования американской информационной политики. Аналогичного подхода придерживается и Европа. Европейская политика гарантии конфиденциальности обеспечивает широкую свободу индивидам в информационном пространстве. Большой интерес представляет принцип “нейтральности сети”, дискуссия относительно которого продолжается в США в настоящее время. Вместе с тем европейская информационная политика наталкивается на проблему бюрократии структур Европейского Союза. В целом нейтральность сети не может рассматриваться как некий статус или специфическая характеристика – скорее, это процесс, целью которого является развитие конкурентоспособности и инновационная деятельность как рынка, так и общества в целом. Пример информационной политики США, ЕС и России доказывает тезис о том, что при наличии противоречий между США и ЕС их основной подход тем не менее близок и кардинально отличается от российского.

Информационное направление становится приоритетным и для российской политики. При этом оно характеризуется более жёстким государственным контролем. Это проявляется, в первую очередь, в принимаемых законодательных нормах о полномочиях специальных служб. Если на Западе нейтральность сети не увязывается с проблематикой конфиденциальности информации, то в России эти направления связаны в тугой узел. Российские органы государственной безопасности зачастую подвергаются критике за пренебрежение судебной процедурой для получения доступа к частной информации россиян. Проводимая в России политика контроля и ограничения доступа пользователей к информации как извне, так и изнутри является, по мнению критиков, аналогом “железного занавеса” времён холодной войны, а также дополнительным раздражителем в отношениях России и Запада. Заметный урон проводимая политика наносит и российскому имиджу, нарушая беспрепятственное информационное взаимодействие на уровне гражданского общества.

References

Bell D. (1973) *The coming of post-industrial society: A venture of social forecasting*, Basic Books, New York, NY, USA.

Cave M. and Crocioni P. (2007) Does Europe Need Network Neutrality Rules?, *International Journal of Communication*, no. 1, pp. 669–679.

- Micklethwait J. and Wooldridge A. (2015) *The Fourth Revolution: The Global Race to Reinvent the State*, Penguin Books, New York, NY, USA.
- Toffler A. (1980) *The Third Wave*, Bantam Books, New York, NY, USA.
- Wu T. (2003) Network Neutrality, Broadband Discrimination, *Journal of Telecommunications and High Technology Law*, vol. 2, pp. 141–176.
- (2016) “BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules. 30.08.2016”, available at: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules.
- (2018) “Europe Urges US to Block Trump on Net Neutrality. Light Reading, 22.01.2018”, available at: <https://www.lightreading.com/net-neutrality/europe-urges-us-to-block-trump-on-net-neutrality/d/d-id/739892>.
- “EU vs Disinformation campaign”, available at: <https://euvsdisinfo.eu/about>.
- (2015) “General Data Protection Regulation. Council of the European Union, 11.06.2015”, available at: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.
- (2011) “International Strategy for Cyberspace. The White House, May 2011”, available at: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
- (2018) “Is Russian social media giant VKontakte sidestepping the GDPR? One user is trying to find out. Advox, 30.08.2018”, available at: <https://advox.globalvoices.org/2018/08/30/is-russian-social-media-giant-vkontakte-sidestepping-the-gdpr-one-user-is-trying-to-find-out>.
- “Net Neutrality. President Obama's Plan for a Free and Open Internet”, available at: <https://obamawhitehouse.archives.gov/net-neutrality>.
- (2018) “S.J.Res.52 – A joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to ‘Restoring Internet Freedom’. 115th Congress (2017–2018), 16.05.18”, available at: <https://www.congress.gov/bills/115th-congress/senate-joint-resolution/52>.
- (2015) “Statement by the President on the USA FREEDOM Act. June 02, 2015”, available at: <https://obamawhitehouse.archives.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act>.
- (2016) “The UK National Cyber Security Strategy 2016–2021”, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
- (2018) “The US National Cyber Strategy. The White House, 2018”, available at: <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.
- (2010) “The US National Security Strategy. The White House, 2010”, available at: <http://nssarchive.us/NSSR/2010.pdf>.
- (2017) “With net neutrality repeal, Trump notches first real deregulatory action. The Hill, 16.12.17”, available at: <http://thehill.com/opinion/white-house/365187-with-net-neutrality-repeal-trump-notches-first-real-deregulatory-action>.

US, Europe and Russia Approaches to the Problem of the Information Policy

Authors: Sharikov P., Leading Researcher, Institute for the US and Canadian Studies. **Address:** 2/3 Khlebnyy pereulok, Moscow, Russia, 121069. **E-mail:** pasha.sharikov@gmail.com

Stepanova N., Researcher, Institute for the US and Canadian Studies. **Address:** 2/3 Khlebnyy pereulok, Moscow, Russia, 121069. **E-mail:** nathalienaz@yandex.ru

Abstract. The article is dedicated to the comparative analysis of the US, EU and Russia approaches to the state regulation of the information policy. The authors' main aim is to study the evolution of such notions as net neutrality, confidentiality of information and the information security strategy. In the new information age, information is the most precious resource for international influence. This requires different norms of political regulation. At the same time, political systems of Western countries are more flexible in responding to those challenges. The EU and the US maintain strong political traditions of democracy, the rule of law and civil society. Such challenges lead to a different outcome in the Russian Federation.

Key words: USA, EU, Russia, information policy, information security, net neutrality, confidentiality.

DOI: <http://dx.doi.org/10.15211/soveurope220197383>