Якунина Анастасия Владимировна*,
магистрант кафедры государственного и административного права ФГАОУ ВО «Самарский национальный исследовательский университет имени академика С.П. Королева» (г. Самара)

ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ И РАЗВИТИЕ ПРАВОВОЙ ЗАЩИТЫ ОБЩЕСТВЕННЫХ ИНТЕРЕСОВ И ЦЕННОСТЕЙ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Развитие информационного общества, подобно промышленной революции, стало катализатором в системных изменениях в экономической, социальной, духовной и политической сферах. Еще в 20 веке американский социолог Д. Белл отметил, что в течение следующего столетия формирование новой социальной структуры, основанной на телекоммуникациях, станет критически важным для экономической и социальной жизни, для методов производства знаний и для природы всего человеческого труда. Влияние информационных технологий на экономику иногда сравнивают с предыдущими технологическими инновациями – электричеством и железными дорогами. Не стала исключением и правовая сфера.

Вопрос государственного суверенитета в области информации и телекоммуникаций проистекает как из объективных свойств Сети (трансграничный характер правовых отношений и т. д.), так и из субъективных факторов эволюционного развития управления системой доменных имен и их технической инфраструктуры (концентрация соответствующих полномочий в интернет-корпорации по присвоению имен и номеров).

Важным является выявление признаков противоречия между принципами стабильности, отказоустойчивости и свободы распространения информации в сети Интернет, а также государственного суверенитета и т.д., сохранение одно-полярной «квазимонополии» на средства и механизмы управления Интернетом, которые создают предпосылки для выработки на основе норм международного права новых организационных форм управления им.

Под государственным суверенитетом следует понимать конститутивное свойство политико-территориального образования осуществлять всю полноту государственной власти, юрисдикционного

верховенства и ответственности в пространственно-временном и личностном континууме сферы действия своей национально-правовой системы, а также его независимость как субъекта международного права для осуществления внешней политики и международных отношений.

Согласно позиции судьи А. Альвареса, изложенной в особом мнении по делу «О канале Корфу», суверенитет означает «совокупность прав и свойств, которыми Государство обладает на своей территории вплоть до исключения всех остальных Государств, а также в его отношениях с другими Государствами. Суверенитет наделяет Государства правами и возлагает обязанности»[1]. Он также выделил семь областей распространения государственного суверенитета: сухопутная, морская, речная, озерная, воздушная, полярная и территория плавучих островов[2].

Ограничение суверенитета возникает в случаях добровольного делегирования государством части его полномочий межправительственному органу, признания компетенции наднациональных органов или в случае применения чрезвычайных мер со стороны международного сообщества в соответствии с Уставом Организации Объединенных Наций (статья 7, пункт 2, статьи 39—51), общепринятыми нормами и принципами международного права.

Интернет, если оперировать на уровне образной модели взаимодействия некоторых традиционных сфер суверенного господства, является информационно-телекоммуникационным архипелагом, постоянно дрейфующим в трансграничном пространстве «открытое море - территориальные воды», искусственно образованный в результате, как правило, алгоритмизированных и подчиненных волевым действиям участников сетевого информационного обмена соединений в точке маршрутизации разнородных телекоммуникационных и компьютерных сетей и систем, интегрирующих в себе встроенные процессоры и контроллеры.

Согласно ч. 1 ст. 4 Конституции Российской Федерации суверенитет Российской Федерации распространяется на всю ее территорию. Данная норма отнюдь не должна толковаться как подразумевающая самоограничение со стороны носителя учредительной власти по сфере распространения государственного суверенитета РФ только физическими границами государства, как это определено в часть 1 ст. 67 Конституции Российской Федерации (территории субъектов Российской Федерации, внутренние воды и территориальное море, воздушное пространство над ними). Государственный

суверенитет с необходимостью распространяется и на идеальные сегменты национальных информационных пространств, которые соединены воедино во всемирную информационно-телекоммуникационную сеть Интернет.

Принадлежность части Интернета к российскому государству определяется следующими юридически значимыми обстоятельствами:

1) непосредственная локализация на территории страны возникающих, изменяющихся или прекращающихся и подлежащих нормативному урегулированию общественных отношений (через элементы сетевой инфраструктуры и т.д.);

2) тесная связь интернет-правоотношений с территорий Российской Федерации; в случае с доменами «.рф» и «.ru» — по месту нахождения регистратуры и регистраторов доменных имен, а также ввиду распространения последствий соответствующих правоотношений на Российскую Федерацию, ее частных и публичных субъектов (так называемая «Effects doctrine»)

3) притяжение к своей территориально-пространственной среде неопределенного круга лиц (субъектов) и объектов воздействия, включая их следующие виды:

– информационные посредники (статья 1253.1 Гражданского кодекса Российской Федерации) (операторы связи, владельцы сайтов, поисковых систем и т. д.) и другие лица, размещающие контент, предназначенный для населения Российской Федерации, то есть рассчитанный в основном на русскоязычных пользователей Интернета[3]. В послании Президента Российской Федерации лидерам стран G20 о новой концепции использования и защиты результатов творческой деятельности в глобальной сети к информационным посредникам отнесены также владельцы доменных имен.

Знак тождества между владельцами доменных имен и информационными посредниками по смыслу ст. 1253.1 ГК РФ уместен только в тех случаях, когда владелец доменного имени одновременно является администратором созданного на его основе интернет-сайта. Никакого противоречия здесь нет, поскольку указанное выше Послание опубликовано 7 ноября 2011 г., тогда как ст. 1253.1 ГК РФ введена в действие с 1 августа 2013 г., что позволило за это время отказаться от автоматического отнесения даже пассивных владельцев доменных имен к категории информационных посредников, т.е. от подчинения их режиму особого контроля со стороны и в интересах правообладателей результатов интеллектуальной деятельности без должных к тому оснований;

– национальная регистратура, регистраторы и администраторы доменных имен второго уровня в национальных доменах «.рф» и «.ru». Следует отметить, что еще в Доктрине информационной безопасности Российской Федерации к числу наиболее важных направлений в контексте реализации правовых методов обеспечения информационной безопасности Российской Федерации была отнесена разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, включая «определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории Российской Федерации, и правовое регулирование деятельности этих организаций». Однако с тех пор российское интернет-законодательство нисколько не обогатилось нормами, регулирующими статус как национальной регистратуры, так и аккредитованных ICANN регистраторов доменных имен в доменах «.ru» и «.рф»;

– средства виртуальной идентификации и индивидуализации, включая доменные имена в национальных доменах и т. д.;

– государственные и национальные символы, достопримечательности, объекты культурного наследия, географические названия, исторически памятные события и явления, прочно ассоциируемые и входящие в национально-культурную идентичность России, а также составляющих ее субъектов, местных сообществ и всего многонационального народа Российской Федерации.

В работе зарубежного исследователя Хайнта-Шелле фон Хейнега терминологический аппарат и постановка задач в значительной степени основаны на документах НАТО с с апеллированием к программным установкам, обнародованным и, по мнению автора, представляющими собой важные руководящие принципы для разработки общепринятых принципов и норм международного права с точки зрения обеспечения суверенитета стран в киберпространстве. Всё интернет-пространство фактически ассимилируется с концепцией государственной территории, становясь «обычным» объектом правового регулирования и сферы суверенного господства. Однако, авторами не предлагается конкретных методов или критериев для разграничения интернет-пространства сегментами мощного общественного доминирования отдельных государств, полагаясь почти исключительно на географический аспект соответствующих отношений.

Согласно Международной стратегии о киберпространстве, подписанной президентом США 16 мая 2011 года, «разработка стан-

дартов, регулирующих поведение государства в киберпространстве, не требует переработки законов и обычаев международного права». Ранее действующие международные законы, регулирующие поведение государств во времена мира или конфликта, также применяются к киберпространству.

Тем не менее, уникальные свойства, присущие сетевым технологиям, требуют дополнительной работы для уточнения того, как применяются эти стандарты и какие дополнительные интерпретации могут потребоваться для их восполнения»[4].

Средства обеспечения государственного суверенитета в области информации разнообразны: они могут быть юридическими, организационно-техническими, а также экономическими. Роль правовых средств заключается в обеспечении адекватного нормативно-правового регулирования информационной безопасности, которое отвечает всем вызовам развивающегося информационного общества. Организационно-технические мероприятия направлены на практическую реализацию мер информационной безопасности, а также на постоянное совершенствование элементов ее системы. Экономические меры призваны создать оптимальные экономические условия для реализации организационно-технических средств с точки зрения финансовых мер по их совершенствованию, а также для оптимального регулирования экономических процессов.

Сегодня суверенитет Российской Федерации в информационной сфере находится на крайне низком уровне. По мнению современных авторов, это связано с рядом факторов. Во-первых, это связано с большой долей импорта на внутреннем рынке информационно-коммуникационных технологий. Во-вторых, из-за большой доли импорта актуальной становится проблема кибершпионажа. В-третьих, законодательство Российской Федерации не ориентировано на обеспечение государственного суверенитета в информационной сфере. Обращая внимание на эту проблему, следует отметить, что конституционно-правовое закрепление государственного суверенитета является традиционным и не отвечает вызовам современного информационного общества[5].

Распространяя суверенитет России на всю ее территорию, Конституция Российской Федерации упускает распространение государственного суверенитета на национальное информационное пространство, в том числе в национальном сегменте глобальной сети Интернет. Сегодня все больше и больше экспертов сходятся во мнении, что во избежание утечки важной информации сеть Интер-

нет можно разделить на десятки отдельных и автономных сетей в пределах национальных границ.

Оценивая влияния средств обеспечения государственного суверенитета в информационной сфере на развитие информационного общества, необходимо отметить, что информационное общество существует и развивается на двух уровнях - национальном и международном.

Необходимость и всевозможные выгоды от развития информационного общества декларируются на обоих уровнях: в Стратегии развития информационного общества и в Уставе информационного общества. Территориальное различие Информационное общество Российской Федерации и глобального информационного общества не нуждается в дополнительных комментариях. Средства обеспечения государственного суверенитета в информационной сфере по-разному влияют на развитие национального и глобального информационного общества.

Уяснение основополагающей роли государственного суверенитета в регулировании информационного общества с точки зрения покрытия рисков информационной безопасности помогает выявить несколько концептуальных проблем. Первый вопрос: как мы можем обеспечить реальный (а не формальный) суверенитет государств в области информации и каков статус-кво на данный момент? Второй вопрос – оценить влияние этих средств на развитие информационного общества.

В первом случае обеспечение государственного суверенитета явно не противоречит развитию национального информационного общества. Действительно, защита от внешних компьютерных угроз не окажет существенного влияния на возможность развития внутреннего информационного общества. Ключевым моментом здесь является возможность развития национального информационного общества, поскольку в какой-то момент оно может быть не готово к полноценной реализации мер, обеспечивающих государственный суверенитет в информационной сфере. Эта неготовность выражается в скудном ассортименте элементов информационного общества с приставкой «отечественное» (отечественные информационные технологии, отечественная идеология и т.д.). В этой связи обеспечение суверенности будет «шагом вперед и двумя назад» в развитии информационного общества[6].

Во втором случае обеспечение государственного суверенитета в сфере информации и развитие глобального информационного об-

щества являются практически взаимоисключающими задачами. Это связано с практической невозможностью определенного государства сохранять контроль над информационной политикой в условиях глубокой интеграции в мировое информационное общество. Интересно отметить, что на сегодняшний день все настойчивее звучит призыв подвергнуть ревизии само понятие «суверенитет национального государства» в пользу глобализированного «объединенного суверенитета», обосновывая перспективность наднациональных (а не международных) структур и институтов.

Из всего вышесказанного вытекают отношения и взаимозависимость суверенитета государств с информационным обществом. С развитием информационного общества возрастают угрозы суверенитету государств, являющемуся фундаментальным элементом информационной безопасности. Меры по обеспечению суверенитета государств в свою очередь приводят к ограничению процессов, направленных на развитие информационного общества. Эти взаимосвязи и взаимозависимости являются сложной задачей для регулятора общественных отношений - задача найти золотую середину[7].

В результате информационного взрыва объем информации удваивается каждые два года, что в итоге может привести к подрыву государственного суверенитета государства. Так, в 2012 году объем сгенерированных данных составил 2,8 зетабайта, то к 2020 году он достигнет 40 зетабайт.

На сегодняшний день, Россия является одной из ведущих стран по количеству пользователей Интернета. Исторически интернет формировался как свободная среда информационного взаимодействия[8].

Сегодня Интернет в значительной степени изменил торговые, финансовые операции, политическую и социальную активность граждан, то есть ключевые сферы жизни каждого государства. В то же время принципы поствестфальского международного права не распространяются на Интернет.

Термин «кибервойны» стал широко использоваться лишь в самые последние годы. Следует четко разделять информационные и кибервойны. Информационные войны характеризуются информационными потоками, которые в первую очередь влияют на психику и человеческое сознание.

Информационные войны - это так называемые «контентные войны», проводимые с целью изменения массового, группового и ин-

дивидуального сознания, навязывания своей воли противникам и перепрограммирования их поведения.

Кибервойна - это целенаправленное разрушительное воздействие информационных потоков в виде программных кодов на физические объекты и их системы, их разрушение, нарушение функционирования или перехват управления ими.

Эти два типа войн ведутся в сетевом электронном пространстве, которые охватывают не только Интернет, но и закрытые государственные и военные сети, корпоративные и частные локальные сети.

Кибервойны тесно связаны с кибершпионажем, киберпреступностью и кибертерроризмом. В ближайшем будущем мы можем ожидать электронные войны третьего типа, которые объединяют информационные и кибернетические войны в некотором смысле, например, пси-войны, пси-шпионаж, телепатия, над которыми работала военная разведка ЦРУ и КГБ, нейровойны и так далее.

Основные особенности кибервойны:

– высокий уровень анонимности;

– неопределенность момента их начала;

– потенциальная бесследность;

– отсутствие в этих войнах привычных понятий, таких как «фронт» и «тыл»;

– чрезвычайная сложность их контроля государственными системами разведки и безопасности;

– отсутствие какой-либо международной нормативно-правовой базы.

Все эти характеристики позволяют сделать выводы об уникальном характере кибервойн относительно других видов военных операций, их особой опасности, возможности быстрого развязывания и трудности урегулирования.

Основными факторами, которые расширяют масштабы и увеличивают разрушительную силу использования кибер-оружия, являются:

– рост интернет адресов. В настоящее время на него приходится более 10 млрд IP адресов, а в 2020 году их будет не менее 50 млрд;

– появление «Бодинет». Переход к множественности подключений к общедоступным и внутренним сетям с одного устройства создает благоприятные условия для применения кибервооружений, кибертерроризма и кибершпионажа;

– активное развитие облачных вычислений. Их экономические достоинства могут превратиться в серьезные проблемы в области информационных технологий;

– кластерный характер современной технологической революции, особенно в робототехнике, 3D-печати, биотехнологии. Особые риски создает теснейшая интеграция информационных и биотехнологий.

В целом совокупность уже имеющихся фактов и сведений позволяет утверждать, что кибервойна США против остального мира, особенно против Китая, России и Ирана, уже началась. Для России кибероружие может стать реальным шансом дать ассиметричный ответ Западу на гонку высокоточных вооружений и стать одним из ключевых элементов достаточной национальной безопасности.

Таким образом, в связи с возможными кибервойнами, можно сделать следующие выводы:

1. Вмешательство США и их союзников в украинский кризис и события вокруг Сирии показывают, что на геополитических конкурентов России не распространяются моральные ограничения при реализации своих агрессивных планов против мирного населения. В том числе — использования информационного оружия для обоснования начала войны против суверенной страны, в обход международного права. В этой связи, развертывание российских кибервойск является важной и неотложной государственной задачей.

2. Информационный взрыв после публикации материалов Сноудена о ведущейся кибервойне США против России и других стран, применяемых технологиях и технических средствах, требует безотлагательной подготовки кадров, способных вести противоборство в киберпространстве.

3. Сдерживание кибервойны невозможно без развития всесторонних фундаментальных научных исследований.

Таким образом, подводя итог вышесказанному, можно сделать вывод, что государственный суверенитет в сети Интернет определяется как конститутивное свойство политико-территориального образования как верховного администратора национального информационного пространства и его информационно-телекоммуникационной инфраструктуры осуществлять всю полноту государственной власти, юрисдикционного верховенства и ответственности в целях охраны прав и законных интересов человека и гражданина, включая фундаментальное право на доступ к Интернету, а также в целях защиты конституционного строя, нравственности, здоровья населения, обеспечения обороны страны и безопасности государства.

Примечания

[1] Наумов В. Б. Интернет и государственный суверенитет // Тезисы доклада на I Всероссийской конференции «Право и Интернет: теория и практика». – 2016.

[2] См.: Сокерин К. В. Субъекты права на доменное имя // Юридический мир. – 2007. – № 4.

[3] См.: Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. – 2006. – № 52 (1 ч.). – Ст. 5496.

[4] Обращение Президента США // [Электронный ресурс]. - https://clck.ru/GfY8U

[5] См.: Тарасов А.М. Киберугрозы, прогнозы, предложения // Информационное право. – 2014. – № 3. – С. 11-15.Якунина Анастасия Владимировна,мвнуаря 1984 праваД.Е., Мязина Р.Г., Назарцев Е.И., Харитнов С.С., Ассистенты: Печегина Ю.С., Мам

[6] См.: Симонишвили Л. Р. Проблемы понимания «суверенитета государства» в современных условиях // Международное публичное и частное право. – 2014. – № 1. – С. 6-8.

[7] См.: Красинский, В. В. Государственный суверенитет: гносеологический аспект проблемы // Современное право. - 2015. – № 7. – С. 5-10.

[8] См.: Колин К.К., Урсул А.Д. Информация и культура. Введение в информационную культурологию. – М.: Изд-во «Стратегические приоритеты», 2015.