Зарубежный опыт. Международное сотрудничество

ПРОБЛЕМЫ МЕЖДУНАРОДНОГО ПРАВА В ОБЛАСТИ КИБЕРПРОСТРАНСТВА И ЦИФРОВОГО СУВЕРЕНИТЕТА НА ЕВРОПЕЙСКОМ И АЗИАТСКОМ ПРОСТРАНСТВЕ

Статья рекомендована к публикации членом редакционного совета М.В. Якушевым 23.03.2021.

Олимпиев Анатолий Юрьевич

Доктор исторических наук, кандидат юридических наук
Институт социальных наук, заведующий кафедрой теории и истории государства и права

Москва, Российская Федерация
a.olimpiev@yandex.ru

Стрельникова Ирина Александровна

Кандидат юридических наук, доцент
Национального исследовательского университета «Высшая школа экономики», факультет мировой экономики и мировой политики, департамент зарубежного регионоведения, научный сотрудник

Москва, Российская Федерация
irina.a.strelnikova@mail.ru

Аннотация

В представленной статье рассмотрены вопросы о роли в формировании международного права в отношении киберпространства. Авторы анализируют существующие проблемы в области международного права и управления в киберпространстве, раскрывают проблематику регламентации киберпространства и цифрового суверенитета, в основе которого лежит идея контроля и управления доступом к информации, коммуникациями, сетями и инфраструктурой в цифровой сфере со стороны публичной власти, на основе опыта Европы и Азии на европейском и азиатском пространстве; анализируется Китайско-российский кибер-альянс по цифровому суверенитету.

Ключевые слова

киберпространство, международное право, юрисдикция субъекта, кибербезопасность, цифровой суверенитет, либеральные институционалисты, киберлибертарианцы и государственники, Китайско-российский кибер-альянс, арбитраж, Международный уголовный суд

Введение

Фома Аквинский в своем великом труде «Сумма теологии» отмечал: «Закон есть установление разума для общего блага, совершаемое теми, кто заботится об общине» [1]. К сожалению, это высказывание не всегда резонирует с международным правом в киберпространстве. Отсутствие эффективных международно-правовых документов и механизма регулирования киберпространства продолжает вызывать острую полемику на многочисленных теоретических и политических дебатах, поскольку сложности в регламентации киберпространства затрудняют для субъектов процесс заключения соглашений и ведения их деятельности.

В спорах и научных дебатах главным образом участвуют те, кто считает, что государства и публичная власть должны играть более влиятельную роль в формировании международного права в отношении киберпространства, и те, кто настаивает на том, что киберпространство должно оставаться свободным и диффузным доменом [2]. Помимо академической среды, еще более острая полемика наблюдается между заинтересованными сторонами в международных кругах и институтах [3]. Все эти споры сводятся к одной ключевой мысли: отсутствие международно-правового режима в киберпространстве обусловлено сложностью определения юрисдикции

субъекта в киберпространстве. Это еще более осложняется тем фактом, что в последние годы в международных кругах активно продвигается идея цифрового суверенитета, в целях возвращения контроля над информацией, коммуникациями, данными и инфраструктурой, связанной с интернетом [4]. Следовательно, это создает более серьезные проблемы для формирования норм международного права в области кибербезопасности и киберпространства. В этой связи возникает вопрос: применимо ли вообще международное право к поведению государств в киберпространстве в эпоху цифрового суверенитета?

Данная статья направлена на анализ двух ключевых вопросов на примере европейского и азиатского регионов: 1) существующие проблемы в области международного права и управления киберпространством и 2) международное право в области киберпространства и цифрового суверенитета. Главный аргумент заключается в том, что сформировавшееся международное право по киберпространству не может эффективно применяться к государствам как субъектам суверенной и публичной власти, учитывая проблемы, возникающие в международном публичном праве, связанные с юрисдикцией, арбитражем, а также иными правовыми инструментами. Будущее международного права в киберпространстве также вряд ли будет применимо к поведению государств из-за усиливающейся тенденции продвижения норм цифрового суверенитета.

Самая большая сила ЕС и его государств-членов в Азиатском регионе — это его экономическое влияние. Азиатские государства и крупные внешние игроки, такие как США, сейчас также внимательно изучают переплетение экономических и технологических тенденций. Это имеет прямые последствия для Европы: больше нет соглашений о свободной торговле ЕС, а только о торговле, помощи в целях развития телекоммуникационного оборудования европейских компаний, о бизнесе или принятии европейских технических стандартов, о регулировании. Все эти примеры дают возможность ЕС и его государствам-членам укрепить свои стратегические интересы и ценности.

Как и Соединенные Штаты Америки и Япония, Европа обсуждает дальнейшую диверсификацию своих экономических отношений за пределами Китая в результате пандемии и более враждебной торговой атмосферы, созданной американо-китайской торговой войной. В то время как некоторая близкая переориентация на Европу и ее периферию возможны, многие из основных альтернатив для производства товаров высокой и низкой стоимости находятся в других частях Азии, включая Вьетнам, Индонезию, Малайзию, Индию, Тайвань и Южную Корею. Несколько стран Ассоциации государств Юго-Восточной Азии (АСЕАН) и Индия имеют все предпосылки, чтобы войти в число наиболее быстрорастущих крупных экономик мира уже в наступившем десятилетии.

Ограничения материально-технического потенциала в Юго-Восточной Азии начинают оказывать все большее влияние на европейскую устойчивость, технологический суверенитет и экономический рост, а также на то, как ЕС и его государства-члены видят предпочтительный как региональный, так и глобальный порядок.

Учитывая перечисленные выше зависимости и тенденции, которые разворачиваются в значительной степени за пределами прямого влияния Европы, важно понять, какая политика лучше всего укрепила бы способность ЕС действовать в Азии и, следовательно, способствовала бы увеличению Европейского стратегического суверенитета.

Существующие проблемы в области международного права и управления в киберпространстве

Идея регулирования киберпространства международным правом не является чем-то удивительно новым. Начиная с 1996 года, усилия по разработке международного права в отношении киберпространства уже постоянно предпринимались экспертами в области права и деловыми кругами. Существуют три доминирующие идеи о том, как киберпространство должно регулироваться международным правом: либеральные институционалисты, киберлибертарианцы и государственники. Либеральные институционалисты призывают к важности международного института и основанной на правилах многосторонности в управлении киберпространством. В то время как киберлибертарианцы [5] являются сторонниками идеи о том, что киберпространство должно оставаться свободным от тирании и любых репрессивных правил, которые могут препятствовать свободе интернета. Государственники [6] считают, что ответственность за разработку национального и международного права для управления киберпространством лежит

соответственно на государствах. Эти три основные идеи нашли свое отражение в развитии международного права в киберпространстве. Вместе с тем на сегодняшний день эффективно функционирующее международное право в киберпространстве до сих пор отсутствует из-за всё продолжающихся по этому поводу дебатов. Эти дебаты основываются на трех основных проблемах, возникающих в процессе формирования международного права в киберпространстве, связанных с ядром принципов и характеристик международного публичного права: юрисдикция, арбитраж и правовые инструменты.

Юрисдикция в международном праве, согласно мнению ряда зарубежных ученых [7], относится в основном к субъекту международного права (или субъектам международных отношений) и территориальности, в отношении которой право может быть формально применено. Субъекты права, или акторы в киберпространстве весьма разнообразны и размыты, поскольку они варьируются от государственных субъектов, крупных интернет-компаний, малых и средних предприятий, хакеров до частных лиц, не говоря уже о том, что интернет изначально также обеспечивает анонимность своим пользователям. Эти многочисленные субъекты также имеют свои собственные различные интересы и проблемы в отношении того, как должно регулироваться киберпространство. По-прежнему чрезвычайно сложно решить, какие субъекты права должны принимать решения в области международного права в киберпространстве, а также какие вопросы должны регулироваться. Многочисленные дебаты как в академических кругах, так и в политических были специально посвящены обсуждению киберпреступности [8]. Кроме того, международные субъекты до сих пор не пришли к согласию относительно статуса киберпространства: является ли оно глобальным достоянием, принадлежит ли оно территории отдельных суверенных государств или основано на их национальном происхождении [9]. В результате это создает серьезные проблемы для определения юрисдикции международного киберправа на сегодняшний день.

Сложность действующих лиц и вопросов, рассмотренных выше, создает дополнительные трудности в арбитраже и судопроизводстве. Международное публичное право требует четких механизмов урегулирования споров в арбитраже. В киберправе из-за многообразия его субъектов (участников отношений) до сих пор не достигнуто универсально согласованной правовой нормы о том, кто должен заниматься вопросами судопроизводства и урегулирования возникающих споров. В настоящее время уже существуют примеры арбитражей, которые заняты урегулированием вопросов в киберпространстве, но в основном они связаны с торговлей и преступностью, имеющими место на территории отдельных государств, в национальной правовой системе, а не на международном уровне [10]. Вместе с тем, не исключено, что в киберпространстве возможно создание и международного арбитража. Постоянный Третейский Суд в Гааге, вероятно, будет рассматриваться в качестве органа, выносящего решения по киберпространству, поскольку он уже имеет мандат по космическим, энергетическим и экологическим делам. В пользу этого умозаключения говорит также и то, что практика Постоянного Третейского Суда не сводится лишь к разбирательству в рамках межгосударственных споров. Нередко его производства подпадают под регулирование «факультативных регламентов по арбитражному разбирательству споров между двумя государствами (действует с 20 октября 1992 г.), между двумя сторонами, только одной из которых является государство (с 6 июля 1993 г.), с участием международных организаций и государств, между международными организациями и частными лицами (с 1 июля 1996 г.), примерными регламентами по арбитражному разбирательству споров, связанных с природными ресурсами и (или) окружающей средой (с 19 июня 2001 г.), и по арбитражному разбирательству споров, связанных с деятельностью в космосе (с 6 декабря 2011 г.)» [11]. Как справедливо в этой связи замечает И.В. Федоров: «Регламенты факультативны и придают особое значение диспозитивности и автономности сторон. Суд принял руководящие принципы для адаптации регламентов к разрешению споров из многосторонних соглашений и контрактов» [12]. Однако затронутая проблематика весьма обширна и многоаспектна и, безусловно, требует отдельного предметного исследования.

Международное право о киберпространстве и цифровом суверенитете: опыт Европы и Азии

Прежде чем приступить к непосредственному изучению опыта Европы и некоторых азиатских государств в контексте выработки государственной политики, государственного отношения к феномену киберпространства, построения систем кибербезопасности, а также урегулированию

отношений, возникающих между всеми субъектами в киберпространстве, отметим, в первую очередь, диаметрально противоположные взгляды представленных сторон на то, что следует относить к правам и свободам человека как таковым в рассматриваемом аспекте [13].

Так, учитывая колоссальное влияние интернета на коммуникацию, на социально-экономические, культурные и политические процессы в обществе, на иные ключевые сферы жизнедеятельности, право на доступ к Сети плавно вошло в международную систему прав человека. В 2007 году Советом Европы была принята Рекомендация «О мерах по укреплению общественной значимости Интернета» [14], в которой отмечалось, что полноценное и всемерное осуществление прав и свобод человека невозможно без наличия беспрепятственного доступа к интернету. Позднее, в 2014 году, эти положения получили развитие и были представлены уже в виде целого каталога принципов, провозгласивших запрет на принудительное прекращение доступа пользователя в интернет (за исключением наличия соответствующего судебного решения, в силу условий договора или иных законных оснований) и иные формы дискриминации по любым признакам, а также обеспечение ценовой и географической доступности Интернета вне зависимости от места проживания и уровня дохода пользователя.

Как справедливо замечает А.С. Шатилина: «наиболее тесным образом право на доступ к Интернету связано со свободой получения и распространения информации, гарантированной статьей 10 Конвенции о защите прав человека и основных свобод 1950 года» [15]. В связи с указанной нормой особый интерес представляет заявление, сделанное в 2011 году в ту пору Специальным докладчиком ООН Фрэнком Уильямом Ла Рю, о том, что невзирая на отсутствие пока признания наличия возможности подключения к Интернету в качестве одного из прав человека, государства, тем не менее, обязаны поощрять и содействовать возможности свободно высказывать свое мнение в Сети. Вместе с тем Ла Рю указал на недопустимость ограничения названной свободы, поскольку иное означало бы ущемление прав человека на образование, на участие в общественно-политической и иных сферах жизни социума, на мирные собрания и объединения.

В целом надо отметить, что Европа сегодня идет по пути не только признания права на доступ к интернету в качестве одного из прав человека, но и его конституирования. Так, к примеру, ныне комиссар Совета Европы по правам человека Дуня Миятович в бытность еще представителем ОБСЕ по вопросам свободы СМИ заявила: «Вклад интернета в развитие непосредственной демократии и реализацию свободы слова и СМИ позволяет говорить о том, что право доступа к интернету со временем может быть возведено в ранг конституционного» [16].

Судебная практика Европейского суда также идет по пути признания рассматриваемого права как одного из важнейших прав человека. В своих решениях Европейский суд, например, указывает: «искусственное создание барьеров для доступа к большому объему информации значительно ограничивает права интернет-пользователей и приводит к значительным косвенным последствиям» [17]; «Суд признает первостепенное значение прав пользователей Интернета, поскольку именно Интернет является важнейшим средством осуществления свободы выражения мнения» [18]; «Вмешательство в право заключенных на доступ к информации в целях получения образования есть вмешательство, которое не было необходимым в демократическом обществе» [19] и др.

В целом же согласимся с точкой зрения, согласно которой использование интернета не должно преследовать лишь одну какую-то определенную цель и, следовательно, может использоваться с учетом всевозможных образовательных, коммуникационных, развлекательных и иных интересов пользователей [20].

Другой подход к киберпространству в целом и интернет-отношениям в частности можно наблюдать в самом густонаселенном и интенсивно развивающемся регионе мира – Азии, которая сегодня является глобальным лидером по количеству персональных компьютеров и числу смартфонов, используемых населением. И если такие активные пользователи Сетью как Индия, Южная Корея или Япония хотя и применяют различные системы анализа активности интернет-пользователей, но все же непосредственную блокировку ресурсов не практикуют, то, к примеру, в КНДР и Туркменистане государство полностью контролирует интернет-сферу. Более того, в последних из названных государств власти сами определяют перечень разрешенных сайтов, которыми могут пользоваться лишь несколько десятков или сотен «избранных» людей: в силу занимаемой должности и исполняемых обязанностей, особого расположения со стороны верховного руководителя или иного привилегированного статуса или положения. Однако, подходы, применяемые в КНДР и Туркменистане, вряд ли следует использовать в качестве некой

«модели для сборки». Здесь, скорее, наибольший интерес представляет государственная политика в отношении киберпространства, проводимая в Китайской Народной Республике. Все-таки это государство с населением примерно в 1 млрд 400 млн человек, где почти 800 миллионов из них пользуются [21] интернетом, и которое с каждым днем все громче заявляет о себе как об одном из мировых лидеров не только в сфере политики, экономики и культуры, но теперь еще и в киберпространстве.

Так, правовое регулирование Интернета в Китае отнесено к компетенции отдела пропаганды Центрального комитета Коммунистической партии Китая, Министерства науки и технологий, а также Министерства общественной безопасности. В свою очередь за непосредственный мониторинг Интернета отвечает Комиссия по управлению киберпространством.

Как отмечает А.С. Шатилина: «Сегодня в Китае действует собственная система фильтрации интернет-контента, именуемая «Золотой щит», которая также известна под неофициальным названием «Великий китайский файрвол» [15]. Цель этой системы состоит в обеспечении пользователя идеологически верной информацией и ограничении либо блокировке доступа к ряду иностранных сайтов, социальных сетей и иных интернет-ресурсов, например: Google, Facebook, YouTube, Twitter, WhatsApp, Instagram, Pinterest и др. Строго говоря, китайский подход заключается в непризнании права на доступ к интернету в качестве права человека как такового.

Представляется, что такое отношение во многом продиктовано идеей сохранения цифрового суверенитета государства, а значит и идеей обеспечения высокого уровня национальной безопасности. Ведь чем больше прав публичная власть предоставляет пользователям Сетью, чем меньше управляет доступом к ней и чем меньше контролирует информационные потоки, коммуникации и инфраструктуру в цифровой сфере, тем больше киберпространство того или иного государства подвержено как внутренним, так и внешним угрозам. Надо сказать, что в последние годы идея о необходимости укрепления цифрового суверенитета государств приобретает в мире все больше сторонников. При этом особый всплеск популярности этой идеи можно было наблюдать после широких договоренностей России и Китая о сотрудничестве в киберпространстве; после нашумевших дел Сноудена и Wikileaks; а также после стремительного подъема четырех крупнейших мировых ИТ-компаний: Google, Apple, Facebook и Amazon, именуемых для простоты также как GAFA.

Вообще, взгляды политического руководства России и Китая на то, каким образом должно развиваться киберпространство, и каким образом оно должно контролироваться, очень во многом совпадают. Подтверждением единства взглядов стало подписанное странами в мае 2015 года двустороннее соглашение о сотрудничестве в сфере обеспечения международной информационной безопасности. В документе, к примеру, говорится об укреплении доверия и «совместном продвижении норм международного права для обеспечения государственной и международной информационной безопасности», в частности под эгидой площадок соответствующих международных организаций: ООН, ОБСЕ, МСЭ. В последующие годы вплоть до сегодняшнего дня такое взаимодействие двух государств только ширится [22], что, неудивительно, вызывает беспокойство у других крупнейших «игроков» глобального киберпространства [23].

Так, например, в киберстратегии Департамента безопасности США основным оппонентом североамериканского государства называется именно Россия, которая «значительно продвинулась в развитии своих кибервозможностей и стратегий». Также в документе отмечается: «Российские акторы незаметны в своей кибербразведке и очень часто определить их намерения довольно сложно. Китай присваивает интеллектуальную собственность глобального бизнеса в пользу китайских компаний, чем подрывает конкурентоспособность США». Таким образом, Соединенные Штаты Америки открыто заявляют о своем видении глобальной кибернетической конъюнктуры и воспринимают Россию и Китай в качестве основных оппонентов, конкурентов и источников угроз собственной безопасности.

В этой связи не приходится удивляться сближению российской и китайской точек зрения на складывающиеся сегодня проблемы и вызовы в киберпространстве. Тем не менее, представляется, что киберсоюз России и Китая сегодня в большей степени необходим именно Российской Федерации, и подписанное соглашение в этом смысле видится весьма логичным, учитывая смещение фокуса на сотрудничество нашей страны с восточными партнерами из-за дипломатической и экономической блокады в отношениях с партнерами западными.

Китай же в настоящее время в определенном смысле является примером для России, как минимум в вопросах осуществления контроля и надзора за Интернетом, интернет-цензуры и последующей блокировки нежелательных ресурсов. Вспомнить хотя бы недавнюю историю с многочисленными попытками Роскомнадзора заблокировать деятельность социальной сети Telegram на территории России, впрочем, неудачными, поскольку эта сеть продолжает активно развиваться, а многие российские государственные органы теперь считают хорошим тоном вести свой канал на названном ресурсе. Тот же Роскомнадзор является весьма активным пользователем Telegram. Неоднократно в отечественных медиа также разворачивались дискуссии о необходимости запрета YouTube, Instagram, Twitter и некоторых других ресурсов, однако далее разговоров дело не заходило. Тем не менее, определенный посыл со стороны властей в отношении информационно-телекоммуникационной сферы и киберпространства достаточно красноречив и понятен.

Схожую мысль (о взятии на вооружение китайского подхода) в 2017 году выразил советник Президента России Герман Клименко: «Путь один — это китайский вариант. Китай менее щепетилен к мнению общества, они оценили угрозу и ограничили интернет. Если интернет ограничен, то обеспечить безопасность легче» [24].

В целом надо сказать, что в России кибербезопасность рассматривается как неотъемлемый элемент системы национальной безопасности. Соответствующие положения, подтверждающие подобный подход государства, нашли свое закрепление в многочисленных стратегических нормативных правовых актах: «Стратегия национальной безопасности» [25], «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы» [26], «Доктрина информационной безопасности Российской Федерации» [27], «Концепция внешней политики Российской Федерации» [28], Федеральный закон «Об информации, информационных технологиях и о защите информации» [29] и др.

Основной посыл поименованных документов заключается в недопустимости вмешательства во внутренние дела, посягательства на суверенитет, территориальную целостность и независимость государств, в том числе в сфере информационных технологий [30]. Примечательно, что подобный подход практически дословно перекликается с официальной позицией Китая, отраженной в его «Международной стратегии сотрудничества в киберпространстве». Таким образом, оба государства последовательно отстаивают идею о цифровом суверенитете как одном из важнейших элементов национальной безопасности.

Представляется, что возможности российско-китайского сотрудничества сегодня выходят на новый уровень. Уже выработан достаточно эффективный алгоритм взаимодействия в рамках ООН, ШОС, БРИКС [31]; развивается сотрудничество и обмен опытом между оборонными ведомствами двух стран; совершенствуется работа Российско-китайской подкомиссии по связи и информационным технологиям; ведется постоянный диалог на экспертном уровне.

Подобный сценарий и тренд на укрепление позиций России и Китая в киберпространстве вызывает обеспокоенность не только у США, как уже отмечалось выше, но и у европейских государств, в том числе в связи с астрономическим ростом GAFA, из-за которого Европейский Союз был вынужден пересмотреть свою цифровую экосистему, о чем будет рассказано дальше по тексту.

Однако прежде отметим, что сложившаяся сегодня ситуация однозначно задает новый климат в области международно-правового регулирования сферы киберпространства. Тенденции, наметившиеся в сфере цифрового суверенитета, на самый серьезный уровень поднимают вопросы неизбежного ограничения свободы в киберпространстве, и тем самым подрывают потенциал существующего международного права в области кибербезопасности. Это связано с тем, что цифровой суверенитет потенциально создаст фрагментированное киберпространство, поскольку оно будет глубоко регулироваться самими государствами на территориальной национальной основе. Идея цифрового суверенитета приведет к отключению глобального интернета, как это и постепенно начинает происходить сейчас. В результате это затруднит возможность международным субъектам прийти к согласию по выработке эффективного международно-правового регулирования и инструментария в отношении киберпространства. Это также затруднит возможность рассмотрения дел о киберпреступлениях уполномоченными органами публичной власти, поскольку цифровой суверенитет укоренен в принципах невмешательства. С другой стороны, если эта идея цифрового суверенитета позволит международным акторам прийти к соглашению о формулировании нового международного киберправа, то само право, по-видимому, будет доминировать и определяться интересами публичной власти с их идеями

цифрового суверенитета за счет негосударственных субъектов, таких как коммерческие компании, отдельные граждане и гражданское общество в целом.

В то время как многие из нас склонны считать, что многосторонний мировой порядок закончился, и государство, как актор, уже не имеет былого значения в нынешнюю эпоху суперплатформ, все же полномочия по выработке правовой политики по-прежнему остаются за государством. Правительства играют решающую роль в распределении ресурсов даже в цифровом пространстве и определении правил игры с помощью изменений в правовой политике.

Итак, перед государствами европейского континента, в частности, главным действующим «лицом» – Европейским Союзом, помимо уже упомянутой проблемы России и Китая, проблемы GAFA и постоянных попыток США влиять на внутреннюю политику ЕС, также стоит множество иных проблем в кибернетической сфере, которые предстоит решить уже в самое ближайшее время.

Это, во-первых, выработка единых правил и способов противодействия хакерским атакам, которых только за 2020 год, по словам [32] Верховного представителя Союза по иностранным делам и политике безопасности Жозепа Борреля, было совершено более 450 по основным системам Евросоюза, включая кластеры финансов, энергетики, здравоохранения, фармацевтики и др.

Во-вторых, упорядочивание, в первую очередь в правовом поле, единого европейского рынка криптовалюты и криптоактивов. Здесь надо отметить, что правовое регулирование и регламентация всего спектра отношений, возникающих в данной сфере, требует существенных финансовых затрат и принятия соответствующих скоординированных мер как на национальном уровне, так и на международном. Однако, к таким шагам сегодня готовы далеко не все государства-участники ЕС.

Наконец, в-третьих, проблема политико-организационного характера, заключающаяся в необходимости соблюдения принципа единогласия при принятии решений. Данное требование распространяется на решения, принимаемые в рамках некогда одного из трех столпов Евросоюза, введенных Маастрихтским договором 1 ноября 1993 года, и именуемого «Общая внешняя политика и политика безопасности». Европейский Союз стоит на том, что подобная практика, предусматривающая согласование и осуществление государствами ЕС совместных внешнеполитических действий на основе единогласно принятых решений, развивает опыт «европейского политического сотрудничества».

Что касается первой из поименованных проблем, то надо сказать, что Европейский Союз уже предпринял определенные действия для ее устранения. Так, в декабре 2020 года Еврокомиссия представила новую киберстратегию ЕС, предусматривающую повышение устойчивости жизненно важных инфраструктур, противодействие кибератакам извне, в том числе путем наложения т.н. киберсанкций. К слову, впервые киберсанкции со стороны Евросоюза были применены в июле и октябре того же 2020 года в отношении восьми физических и четырех юридических лиц из России, Китая и Северной Кореи [33].

Как отметил Вице-президент Европейской комиссии по защите европейского стиля жизни Маргаритис Схинас: «Мы наблюдаем систематические атаки на нашу инфраструктуру здравоохранения, на критически важные функции Европейского Союза, на наши учреждения. По-моему, наши люди всё больше осознают, что это новое поле опасности, что угрозы исходят с меняющегося ландшафта» [34].

Новая европейская киберстратегия восприняла и развила соответствующие положения таких программ Евросоюза как «Формирование цифрового будущего Европы», «План экономического восстановления Европы» и «Стратегия совместной безопасности ЕС», и провозгласила, что новый документ направлен на укрепление сотрудничества с партнёрами по всему миру в деле популяризации «глобального, открытого, стабильного и безопасного киберпространства, основанного на законах, правах человека, фундаментальных свободах и демократических ценностях». Стоит отметить, что приведенная цитата была дословно заимствована из национальной киберстратегии Соединенных Штатов Америки.

В частности, европейская стратегия действий в киберпространстве предполагает следующие основные инициативы:

совершенствование правил безопасности сетей и информационных систем таким образом, чтобы уровень устойчивости к кибератакам в ключевых сферах жизнедеятельности (лечебные учреждения, энергетические сети, транспортные пути сообщения), а также единых центрах

хранения данных, исследовательских центрах, облачных сервисах, правительственных ИТ-системах и пр. был достаточным, чтобы все критические функции оставались работоспособными;

создание центров безопасности, работу которых в значительной степени будет обеспечивать искусственный интеллект, призванный не только обнаруживать малейшие признаки, указывающие на возможную угрозу кибератаки, но и осуществлять проактивные действия для раннего обнаружения и подавления таких угроз;

создание «Объединенного киберотдела Европейского Союза» в целях совершенствования взаимных действий по выявлению кибератак и ответу на них;

в сотрудничестве с институтами ООН и иными международными партнерами развитие международных норм и стандартов по защите прав человека и фундаментальных свобод онлайн;

во взаимодействии со странами третьего мира и заинтересованными международными организациями создание «кибердипломатической сети» для продвижения европейских ценностей и европейского видения того, каким образом должно формироваться и развиваться киберпространство, и как себя следует в нем вести;

противодействие злонамеренному поведению третьих стран в киберпространстве,и создание в этих целях рабочей группы киберразведки в составе Центра разведки ЕС;

реализация программы «Цифровых инновационных хабов», которые должны способствовать поиску «киберталантов» - людей, которые смогли бы, «опережая время», обеспечивать и развивать кибербезопасность в ЕС.

Впрочем, по оценкам Еврокомиссии претворение в жизнь положений киберстратегии должно обойтись налогоплательщикам на период до 2027 года не менее чем в 4,5 млрд евро, с чем, вероятно, согласятся не все страны-участницы.

Говоря о второй проблеме, прежде всего, отметим, что феномен криптовалюты, криптоактивов до сих пор остается весьма загадочным явлением для обывателя. Это, в свою очередь, создает определенные трудности для более оперативного принятия законов, регулирующих этот своеобразный рынок. Европейские ценности, как уже было отмечено выше, строятся не только на принципе единогласия правительств государств-членов ЕС при принятии соответствующих решений, но также и на одобрении гражданами конкретных законопроектов или иных правил, которые непосредственно отразятся на их жизни. Таким образом, первоочередная задача государств состоит в том, чтобы объяснить людям суть конкретного явления, затем обозначить опосредуемые им проблемы и опасности и предложить инструменты для их нивелирования либо полной ликвидации.

Надо сказать, что Европейский Союз прошел в этом направлении большой путь и проделал значительную работу, что, в конечном счете, выразилось в предложенном Еврокомиссией 24 сентября 2020 года проекте «Регламента рынка криптоактивов» [35], содержащего предполагаемые законодательные правила регулирования в рассматриваемой сфере.

Любопытно отметить, что до 2019 года в ЕС превалировало мнение о том, что проблема криптоактивов является нишевой проблемой, которая не требует к себе пристального внимания в силу ее «местечковости» и крайне небольшого тогда размера глобального рынка криптоактивов. Однако два года назад, после объявления о публичном предложении поддерживаемого компанией Facebook стейблкоина [36] Libra, европейские аналитики пришли к выводу о том, что данная социальная сеть и другие гиганты мировой ИТ-индустрии имеют потенциальную возможность захватить весь мировой рынок криптоактивов и установить собственные правила для всех, в том числе и для ЕС. Таким образом, международное право и международные стандарты и требования в рассматриваемой сфере de facto могли быть сформированы частными компаниями.

Во избежание подобного сценария Еврокомиссия приняла во внимание имевшийся на тот момент в мировой международной практике опыт законодательного регулирования рынка криптоактивов, а также выводы Рабочей группы G7 по стейблкоинам, которая в октябре 2019 года заявила, что «ни один глобальный проект стейблкоина не должен начинать работу до тех пор, пока не будут должным образом выполнены соответствующие законодательные, нормативные и надзорные требования» [37].

Предложенный Еврокомиссией для обсуждения Регламент должен быть окончательно обсужден к середине 2022 года и в 2023 году вступить в силу. Важно подчеркнуть, что Европейский Союз намерен максимально распространить выработанные им к сегодняшнему дню правила

регулирования рынка криптоактивов. Это планируется делать не только в рамках двусторонних и многосторонних межгосударственных отношений, не только в контексте сотрудничества с крупными международными организациями и транснациональными корпорациями, но и в рамках многочисленных военных и гражданских миссий ЕС, проводимых по всему миру.

В целом надо отметить, что сфера киберпространства и применяемые в ней инструменты и технологии совершенствуются с молниеносной скоростью, и решения, принимаемые законодателями, попросту не поспевают за ними. На момент вступления в силу закон уже является устаревшим по отношению к достижениям ИТ-сферы. В этой связи, учитывая несомненную международную, глобальную повестку рассматриваемой в настоящей статье проблематики, законодателям придется проявить недюжинную прозорливость в деле эффективной международно-правовой регламентации всего спектра правоотношений, возникающих в киберпространстве, принимая также во внимание имеющийся сегодня в мире спрос на укрепление цифрового суверенитета государств.

Заключение

Вопрос о том, применяется ли международное право к поведению государств в киберпространстве и как сделать его применение наиболее эффективным, по-прежнему остается дискуссионным и вызывает острую полемику. Он базируется на трех ключевых аспектах международного права: юрисдикция, арбитраж, правовые инструменты. В перспективе наметившаяся тенденция ко все более широкому распространению норм цифрового суверенитета потенциально может привести к тому, что будущее международное право в киберпространстве будет дополнено нормами, регламентирующими цифровой суверенитет в ущерб интересам иных негосударственных субъектов. В любом случае нормы международного права, регулирующие отношения в киберпространстве, нуждаются в пересмотре и совершенствовании.

Идеальным сценарием, ведущим к созданию высоконадежных, отвечающих высоким стандартам, более открытых рамок среди партнеров-единомышленников, конечно, стало бы развитие киберпартнерства и кибердипломатии между европейскими государствами, в первую очередь Европейским Союзом, и «законодателями мод» в ИТ-сфере на азиатском континенте, прежде всего, Китаем. Однако в силу разницы менталитетов, исповедуемых ценностей, опыта государственного строительства, взгляда на основные права и свободы человека и, безусловно, обстоятельств объективной социально-экономической и политической реальностей, как видится, в ближайшей перспективе симбиоза мнений и действий между указанными сторонами ожидать не приходится.

Однако стоит отметить, что некоторые подвижки в русле «огосударствления» киберпространства (в том смысле, что публично-властные органы стремятся к получению больших возможностей по управлению Интернетом и цифровыми сетями, а в некоторых случаях установлению разрешительного режима пользования отдельными его сегментами) Евросоюза сегодня отчетливо видны, и, более того, даже прослеживаются определенные тенденции, выражающиеся, например, в отказе от подхода laissez-faire, установлении жестких нормативных и надзорных требований для всех «игроков» европейского рынка криптоактивов, фактическом запрете на участие в нем нерезидентов ЕС и др. В этом смысле думается, что и основополагающие принципы и ценности ЕС, провозглашающие право человека пользоваться Интернетом важнейшим средством осуществления свободы выражения мнения, могут в не столь далеком времени быть пересмотрены в контексте некоторого ограничения такого права в пользу обеспечения национальной безопасности заинтересованных государств во всех сферах их деятельности.

Литература

1. Аквинский Ф. Сумма теологии. М., 2019, с. 33. (Aquinas F. The Amount of theology. M., 2019, p. 33.) (In Russ.)
2. Barlow, John. 1996. “A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation (February 1996), http://homes.eff.org/-barlow/Declaration-Final.html. (accessed 12.12.2020).

3. Opinio Juris. 2019. France Declaration on International Law in Cyberspace. https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed 15.12.2020)
4. Gueham, Farid. 2017. Digital Sovereignty – Steps Towards a New System of Internet Governance. Paris: Fondapol.
5. Barlow, John. 1996. "A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation (February 1996), http://homes.eff.org/-barlow/Declaration-Final.html. 10.
6. Lewis, James A. 2010. "Sovereignty and the Role of Government in Cyberspace", Brown Journal of World Affairs, 16(2): 55-65.
7. Cali, Basak. 2015. International Law for International Relations. New York: Palgrave Macmillan.
8. Rid, T. and Buchanan, B. 2014. "Attributing Cyber Attacks", Journal of Strategic Studies, 38(1-2), pp.4-37.
9. Liaropoulos, Andrew. 2017. "Cyberspace Governance and State Sovereignty", in Democracy and an Open-Economy World Order, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.
10. Kittichaisaree, Kriangsak. 2017. Public International Law of Cyberspace. New York: Springer.
11. Официальный сайт Постоянного Третейского Суда [Электронный ресурс] URL: http://www.pca-cpa.org/showpage.asp?pag_id=1188 (дата обращения 10 марта 2021 г.)
12. Федоров И.В. Развитие квазимеждународных форм третейского судопроизводства // Российский юридический журнал. 2012. N 4. С. 118 - 121.
13. Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. №1. С. 261-269.
14. Рекомендация Комитета министров Совета CM/Rec(2007) 16 о мерах по повышению ценности Интернета как общественной службы.
15. Шатилина А.С. Права человека в Интернете: проблема признания права на доступ к Интернету // Прецеденты Европейского суда по правам человека. 2018. N 1. С. 38 - 45.
16. OSCE media freedom representative calls on governments to recognize access to the Internet as a human right. OSCE Press release 16 July 2011 // http://www.osce.org/fom/81006.
17. Постановление Европейского суда по делу "Ахмет Йилдырым против Турции" (Ahmet Yildirim v. Turkey) от 18 декабря 2012 г., жалоба N 3111/10. См.: Прецеденты Европейского суда по правам человека. 2016. N 6.
18. Решение Европейского суда по делу "Яман Акдениз против Турции" (Yaman Akdeniz v. Turkey) от 11 марта 2014 г., жалоба N 20877/10.
19. Постановление Европейского суда по делу "Янковскис против Литвы" (Jankovskis v. Lithuania) от 17 января 2017 г., жалоба N 21575/08 // Бюллетень Европейского суда по правам человека. 2017. N 6.
20. Левова И., Шуклин Г., Винник Д. Права интернет-пользователей: Россия и мир, теория и практика. 2013. С. 37.
21. Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности // Китай в мировой и региональной политике. История и современность. 2018. Т.23. №.23. С. 223-237.
22. Россия и Китай будут сотрудничать в сфере блокировки запрещенной информации // Официальный сайт издания «Коммерсантъ» [Электронный ресурс] URL: https://www.kommersant.ru/doc/4118750 (дата обращения 9 марта 2021 г.); Чжан Х. Вперед вместе с Россией: отношения наших стран не подвержены влиянию чрезвычайных ситуаций и внешнего вмешательства // Официальный сайт издания «Российская газета» [Электронный ресурс] URL: https://rg.ru/2020/10/08/otnosheniia-rossii-i-kitaia-ne-podverzheny-vliianiiu-chrezvychajnyh-situacij.html (дата обращения 9 марта 2021 г.); Русско-китайская киберзащита // Официальный сайт издания «Газета.ру» [Электронный ресурс] URL: https://www.gazeta.ru/tech/2015/05/06/6670173/Russia_China_infobezopasnost.shtml (дата обращения 8 марта 2021 г.)
23. Куликова А. Киберпакт Китая и России: есть ли повод для беспокойства? // Официальный сайт «Russia Direct» [Электронный ресурс] URL: http://www.pircenter.org/media/content/files/13/14358794450.pdf (дата обращения 9 марта 2021 г.)
24. Герман Клименко предложил ограничить в России интернет, как в Китае // Официальный сайт издания «Ведомости» [Электронный ресурс] URL:

https://www.vedomosti.ru/technology/news/2017/01/26/675045-klimenko-internet (дата обращения 9 марта 2021 г.)
25. Указ Президента РФ от 31 декабря 2015 г. N 683 "О Стратегии национальной безопасности Российской Федерации" / Собрание законодательства Российской Федерации от 4 января 2016 г. N 1 (часть II) ст. 212
26. Указ Президента РФ от 9 мая 2017 г. N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" / Собрание законодательства Российской Федерации от 15 мая 2017 г. N 20 ст. 2901
27. Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" / Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074
28. Указ Президента РФ от 30 ноября 2016 г. N 640 "Об утверждении Концепции внешней политики Российской Федерации" / Собрание законодательства Российской Федерации от 5 декабря 2016 г. N 49 ст. 6886
29. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" / Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448
30. Молчанов Н.А., Матевосова Е.К. Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. N 1. С. 133 - 141.
31. Столетов О.В. Проблема правового регулирования международной информационной и кибербезопасности в современной мировой политике // Российский журнал правовых исследований. 2018. Т.5. № 1. С. 66-72.
32. В ЕС представили новую Стратегию кибербезопасности // Официальный сайт издания «Экономическая правда» [Электронный ресурс] URL:https://www.epravda.com.ua/rus/news/2020/12/16/669259/ (дата обращения 6 марта 2021 г.)
33. ЕС представил новую Стратегию кибербезопасности // Официальный сайт информационного агентства «Интерфакс». [Электронный ресурс] URL: https://www.interfax.ru/world/741613 (дата обращения 5 марта 2021 г.)
34. Обновлённая стратегия кибербезопасности Евросоюза // Официальный сайт информационного агентства «EURONEWS». [Электронный Ресурс] URL: https://ru.euronews.com/2020/12/16/eu-commission-cyber-security (дата обращения 6 марта 2021 г.)
35. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 // COM/2020/593 final.
36. Стейблкоин – это криптовалюта, привязанная к другим активам, таким, например, как доллар или евро. В сущности, это цифровые активы, предназначенные для имитации курса фидуциарных (фиатных) валют. Они позволяют пользователям дешево и быстро обмениваться стабильной валютой в любой точке мира. Токены электронных денег и токены, привязанные к активам, являются стейблкоинами.
37. G7 Working Group on Stablecoins: Investigating the impact of global stablecoins. October 2019. [Электронный ресурс], URL:https://www.bis.org/cpmi/publ/d187.pdf (дата обращения 8 марта 2020 года).

PROBLEMS OF INTERNATIONAL LAW IN THE FIELD OF CYBERSPACE AND DIGITAL SOVEREIGNTY IN THE EUROPEAN AND ASIAN SPACE

Olimpiev, Anatoly Yuryevich

Doctor of historical sciences, candidate of legal sciences
Institute of social sciences, head of Department of theory and history of state and law
Moscow, Russian Federation
a.olimpiev@yandex.ru

Strelnikova, Irina Aleksandrovna

Candidate of legal sciences, associate professor
National Research University "Higher School of Economics", Faculty of world economy and international affairs, School of international regional studies, research fellow
Moscow, Russian Federation
irina.a.strelnikova@mail.ru

Abstract

The article deals with the role of international law in the formation of cyberspace. The authors analyze the existing problems in the field of international law and governance in cyberspace, reveal the problems of regulation of cyberspace and digital sovereignty, which is based on the idea of control and management of access to information, communications, networks and infrastructure in the digital sphere by public authorities, based on the experience of Europe and Asia in the European and Asian space; the Chinese-Russian cyber Alliance on Digital sovereignty is analyzed. The unfolding situation in the field of digital sovereignty raises questions of freedom in cyberspace, as well as undermines the potential of modern international law in the field of cybersecurity, which makes it necessary to modify the existing legal regime.

Keywords

Cyberspace, international law, subject jurisdiction, cybersecurity, digital sovereignty, liberal institutionalists, cyberlibertarians and statesmen, Chinese-Russian Cyber Alliance, Arbitration, International Criminal Court

References

1. Akvinskij F. Summa teologii. M., 2019, s. 33. (Aquinas F. The Amount of theology. M., 2019, p. 33.
2. Barlow, John. 1996. “A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation (February 1996), http://homes.eff.org/-barlow/Declaration-Final.html. (accessed 12.12.2020).
3. Opinio Juris. 2019. France Declaration on International Law in Cyberspace. https://opiniojuris.org/2019/09/24/frances-declaration-on-international-law-in-cyberspace-the-law-of-peacetime-cyber-operations-part-i/ (accessed 15.12.2020)
4. Gueham, Farid. 2017. Digital Sovereignty – Steps Towards a New System of Internet Governance. Paris: Fondapol.
5. Barlow, John. 1996. “A Declaration of the Independence of Cyberspace, Electronic Frontier Foundation (February 1996), http://homes.eff.org/-barlow/Declaration-Final.html. 10.
6. Lewis, James A. 2010. “Sovereignty and the Role of Government in Cyberspace”, Brown Journal of World Affairs, 16(2): 55-65.
7. Cali, Basak. 2015. International Law for International Relations. New York: Palgrave Macmillan.
8. Rid, T. and Buchanan, B. 2014. “Attributing Cyber Attacks”, Journal of Strategic Studies, 38(1-2), pp.4-37.
9. Liaropoulos, Andrew. 2017. “Cyberspace Governance and State Sovereignty”, in Democracy and an Open-Economy World Order, ed. George Bitros & Nicholas Kyriazis. Cham: Springer.
10. Kittichaisaree, Kriangsak. 2017. Public International Law of Cyberspace. New York: Springer.
11. Oficial'nyj sajt Postoyannogo Tretejskogo Suda [Elektronnyj resurs] URL: http://www.pca-cpa.org/showpage.asp?pag_id=1188 (data obrashcheniya 10 marta 2021 g.)
12. Fedorov I.V. Razvitie kvazimezhdunarodnyh form tretejskogo sudoproizvodstva // Rossijskij yuridicheskij zhurnal. 2012. N 4. S. 118 - 121.

13. Danel'yan A.A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva // Obrazovanie i pravo. 2020. №1. S. 261-269.
14. Rekomendaciya Komiteta ministrov Soveta CM/Rec(2007) 16 o merah po povysheniyu cennosti Interneta kak obshchestvennoj sluzhby.
15. Shatilina A.S. Prava cheloveka v Internete: problema priznaniya prava na dostup k Internetu // Precedenty Evropejskogo suda po pravam cheloveka. 2018. N 1. S. 38 - 45.OSCE media freedom representative calls on governments to recognize access to the Internet as a human right. OSCE Press release 16 July 2011 // http://www.osce.org/fom/81006.
16. OSCE media freedom representative calls on governments to recognize access to the Internet as a human right. OSCE Press release 16 July 2011 // http://www.osce.org/fom/81006.
17. Postanovlenie Evropejskogo suda po delu "Ahmet Jildyrym protiv Turcii" (Ahmet Yildirim v. Turkey) ot 18 dekabrya 2012 g., zhaloba N 3111/10. Sm.: Precedenty Evropejskogo suda po pravam cheloveka. 2016. N 6.
18. Reshenie Evropejskogo suda po delu "YAman Akdeniz protiv Turcii" (Yaman Akdeniz v. Turkey) ot 11 marta 2014 g., zhaloba N 20877/10.
19. Postanovlenie Evropejskogo suda po delu "YAnkovskis protiv Litvy" (Jankovskis v. Lithuania) ot 17 yanvarya 2017 g., zhaloba N 21575/08 // Byulleten' Evropejskogo suda po pravam cheloveka. 2017. N 6.
20. Levova I., SHuklin G., Vinnik D. Prava internet-pol'zovatelej: Rossiya i mir, teoriya i praktika. 2013. S. 37.
21. Isaev A.S. Rossijsko-kitajskoe vzaimodejstvie po voprosam obespecheniya informacionnoj bezopasnosti // Kitaj v mirovoj i regional'noj politike. Istoriya i sovremennost'. 2018. T.23. №.23. S. 223-237.
22. Rossiya i Kitaj budut sotrudnichat' v sfere blokirovki zapreshchennoj informacii // Oficial'nyj sajt izdaniya "Kommersant" [Elektronnyj resurs] URL: https://www.kommersant.ru/doc/4118750 (data obrashcheniya 9 marta 2021 g.); CHzhan H. Vpered vmeste s Rossiej: otnosheniya nashih stran ne podverzheny vliyaniyu chrezvychajnyh situacij i vneshnego vmeshatel'stva // Oficial'nyj sajt izdaniya «Rossijskaya gazeta» [Elektronnyj resurs] URL: https://rg.ru/2020/10/08/otnosheniia-rossii-i-kitaia-ne-podverzheny-vliianiiu-chrezvychajnyh-situacij.html (data obrashcheniya 9 marta 2021 g.); Russko-kitajskaya kiberzashchita // Oficial'nyj sajt izdaniya «Gazeta.ru» [Elektronnyj resurs] URL: https://www.gazeta.ru/tech/2015/05/06/6670173/Russia_China_infobezopasnost.shtml (data obrashcheniya 8 marta 2021 g.)
23. Kulikova A. Kiberpakt Kitaya i Rossii: est' li povod dlya bespokojstva? // Oficial'nyj sajt «Russia Direct» [Elektronnyj resurs] URL: http://www.pircenter.org/media/content/files/13/14358794450.pdf (data obrashcheniya 9 marta 2021 g.)
24. German Klimenko predlozhil ogranichit' v Rossii internet, kak v Kitae // Oficial'nyj sajt izdaniya «Vedomosti» [Elektronnyj resurs] URL: https://www.vedomosti.ru/technology/news/2017/01/26/675045-klimenko-internet (data obrashcheniya 9 marta 2021 g.)
25. Ukaz Prezidenta RF ot 31 dekabrya 2015 g. N 683 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii" / Sobranie zakonodatel'stva Rossijskoj Federacii ot 4 yanvarya 2016 g. N 1 (chast' II) st. 212
26. Ukaz Prezidenta RF ot 9 maya 2017 g. N 203 "O Strategii razvitiya informacionnogo obshchestva v Rossijskoj Federacii na 2017 - 2030 gody" / Sobranie zakonodatel'stva Rossijskoj Federacii ot 15 maya 2017 g. N 20 st. 2901
27. Ukaz Prezidenta RF ot 5 dekabrya 2016 g. N 646 "Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii" / Sobranie zakonodatel'stva Rossijskoj Federacii ot 12 dekabrya 2016 g. N 50 st. 7074
28. Ukaz Prezidenta RF ot 30 noyabrya 2016 g. N 640 "Ob utverzhdenii Koncepcii vneshnej politiki Rossijskoj Federacii" / Sobranie zakonodatel'stva Rossijskoj Federacii ot 5 dekabrya 2016 g. N 49 st. 6886
29. Federal'nyj zakon ot 27 iyulya 2006 g. N 149-FZ "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" / Sobranie zakonodatel'stva Rossijskoj Federacii ot 31 iyulya 2006 g. N 31 (chast' I) st. 3448

30. Molchanov N.A., Matevosova E.K. Konceptual'no-politicheskij i formal'no-yuridicheskij analiz Parizhskogo prizyva k doveriyu i bezopasnosti v kiberprostranstve i rossijskie iniciativy v oblasti mezhdunarodnogo prava // Aktual'nye problemy rossijskogo prava. 2020. N 1. S. 133 - 141.
31. Stoletov O.V. Problema pravovogo regulirovaniya mezhdunarodnoj informacionnoj i kiberbezopasnosti v sovremennoj mirovoj politike // Rossijskij zhurnal pravovyh issledovanij. 2018. T.5. № 1. S. 66-72.
32. V ES predstavili novuyu Strategiyu kiberbezopasnosti // Oficial'nyj sajt izdaniya «Ekonomicheskaya pravda» [Elektronnyj resurs] URL:https://www.epravda.com.ua/rus/news/2020/12/16/669259/ (data obrashcheniya 6 marta 2021 g.)
33. The EU presented a new Cybersecurity Strategy // Official website of the Interfax news agency. [Electronic resource] URL: https://www.interfax.ru/world/741613 (date of treatment March 5, 2021)
34. Obnovlyonnaya strategiya kiberbezopasnosti Evrosoyuza // Oficial'nyj sajt informacionnogo agentstva «EURONEWS». [Elektronnyj Resurs] URL: https://ru.euronews.com/2020/12/16/eu-commission-cyber-security (data obrashcheniya 6 marta 2021 g.)
35. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 // COM/2020/593 final.
36. Stejblkoin – eto kriptovalyuta, privyazannaya k drugim aktivam, takim, naprimer, kak dollar ili evro. V sushchnosti, eto cifrovye aktivy, prednaznachennye dlya imitacii kursa fiduciarnyh (fiatnyh) valyut. Oni pozvolyayut pol'zovatelyam deshevo i bystro obmenivat'sya stabil'noj valyutoj v lyuboj tochke mira. Tokeny elektronnyh deneg i tokeny, privyazannye k aktivam, yavlyayutsya stejblkoinami.
37. G7 Working Group on Stablecoins: Investigating the impact of global stablecoins. October 2019. [Electronic resource], URL: https: //www.bis.org/cpmi/publ/d187.pdf (date of appeal March 8, 2020).