УДК 32

Концепции кибергосударства и криптоанархии в теории и практике государственного управления

Косоруков Артем Андреевич

Кандидат политических наук, старший преподаватель,
Московский государственный университет имени М.В. Ломоносова,
119991, Российская Федерация, Москва, Ленинские горы, 1;
e-mail: Kosorukovmsu@mail.ru

Аннотация

Активное применение информационных технологий в сфере государственного управления трансформирует традиционное представление о государстве. Концепция кибергосударства позволяет сформировать новую теоретическую основу для переосмысления государственного управления в условиях формирования независимых киберюрисдикций, границы которых не совпадают с границами государственной правовой системы и не зависят от нее. Происходит столкновение государства, отстаивающего территориальный суверенитет, с экстерриториальным по своей природе информационным обществом, в анархическом пространстве которого образуются многочисленные сетевые взаимосвязи и центры власти. Укрепление виртуальных инструментов мониторинга и контроля за поведением граждан, создание их «цифровых двойников» способно, с одной стороны, обеспечить установление «тоталитарного» типа государственного управления, с другой стороны, основной целью кибергосударства является повышение эффективности государственного управления и построение «государства-как-платформы», позволяющей на основе единой облачной платформы и инфраструктуры совместного использования повысить качество оказания государственных услуг и в конечном итоге повысить степень социальной киберинклюзии. С концепцией кибергосударства тесно связана концепция криптоанархии, которая описывает практику неконтролируемой передачи информации в киберпространстве. Распространение криптотехнологий вынуждает государство отстаивать свой суверенитет и безопасность за счет создания заградительных барьеров на пути зашифрованной коммуникации. Подобные усилия не только снижают возможности применения криптотехнологий среди виртуальных сообществ, но и ограничивают свободу информации в киберпространстве.

Для цитирования в научных исследованиях

Косоруков А.А. Концепции кибергосударства и криптоанархии в теории и практике государственного управления // Теории и проблемы политических исследований. 2018. Том 7. № 4А. С. 9-19.

Ключевые слова

Кибергосударство, юрисдикция, суверенитет, электронные услуги, государство как платформа, криптоанархия, виртуальное сообщество, киберпреступность, государственный контроль, кибербарьер.

Введение

Развитие информационных технологий и масштабная компьютеризация общества в рамках «четвертой промышленной революции», постоянная смена и перетекание технологий из корпоративного сектора в сферу государственного и муниципального управления, в частности, внедрение электронных технологий и практики предоставления государственных и муниципальных услуг в электронном виде, а также оптимизация работы современных государственных служащих посредством многочисленных баз данных и облачных инструментов трансформируют традиционное представление о государстве и его функциях. Меняется сама система государственного управления, которая все больше перемещается в виртуальное пространство и отдаляется от личного взаимодействия с гражданами, характеризуется постоянным сокращением административных издержек, экономией материальных, финансовых и кадровых ресурсов, сокращением времени на обработку данных и принятие управленческих решения. Более того, развитие современных инновационных технологий и становление информационного общества обуславливает необходимость дальнейшего совершенствования системы государственного и муниципального управления, ее соответствия лучшим управленческим практикам корпоративного сектора. Все более актуальной в этой связи становится концепция кибергосударства, позволяющая сформировать новую теоретическую основу для переосмысления практической деятельности органов государственного управления.

Основная часть

В этих условиях зарубежные исследователи, пытаясь осмыслить происходящие изменения, все активнее применяют концепцию кибергосударства или «виртуального государства» в отношении современного этапа развития государственного управления [Ludlow, 2001]. Большой вклад в теоретико-методологическое осмысление концепции кибергосударства внес американский адъюнкт-профессор философии Питер Ладлоу. В 2005 году была переведена на русский язык и опубликована его работа «Криптоанархия, кибергосударства и пиратские утопии» [Ладлоу, 2005]. В данной работе речь идет о формировании особого киберпространства, размывающего власть правительственных структур и лежащие в их основе правовые нормы, и институты. Такое размывание усугубляется не только политикой государства относительно делегирования отдельных полномочий в сфере регулирования киберпространства на региональный и местный уровень, которые не обладает достаточными ресурсами и компетенциями, но и спецификой данного пространства, в рамках которого возникают независимые юрисдикции, границы которых не совпадают с границами правовой системой отдельного государства и порой охватывают весь мир (причем для их охвата недостаточны даже экстерриториальные границы правовой системы США, так как виртуальные юрисдикции в сети Интернет могут не базироваться в каком-либо конкретном государстве). Можно привести в качестве примера конфликт между двумя деловыми партнерами, которые совершают сделки в рамках киберпространства, но территориально находятся друг от друга в тысячах километрах и в разных государственных юрисдикциях. Возникает коллизия относительно юрисдикции, в пространстве которого данный конфликт может быть разрешен: являясь гражданами разных государств, деловые партнеры могут регистрировать свои компании и совершать деловые операции по всему миру, в том числе, используя виртуальные

адреса и юрисдикции, при этом правовые системы данных государств могут не сопрягаться на уровне наднациональных институтов или межгосударственных соглашений, усложняя достижение правового консенсуса.

В работах зарубежных исследователей киберпространство рассматривается как особая виртуальная сфера, которая не только формирует общественное представление о государстве, его институтах и механизмах управления, но и трансформирует саму сущность государственного управления в рамках требований информационного общества. Вместе с тем, зарубежные исследователи отмечают, что киберпространство в процессе встраивания в него государственных институтов характеризуется появлением ряда проблем правового и организационного характера, связанных с поддержанием в нем необходимой степени подотчетности и легитимности. Если электронное государство рассматривалось преимущественно как инфраструктура для предоставления физическим и юридическим лицам государственных и муниципальных услуг на базе современных интернет-технологий [Газизов, 2015], включая систему электронного документооборота, в рамках которой осуществлялась автоматизация всех управленческих процессов, то в отношении кибергосударства выдвигаются более высокие требования по повышению эффективности и интенсивности государственного управления, трансформации структуры и качества взаимоотношений между государством и обществом на базе информационно-коммуникационных технологий (в частности, перевода государственных услуг в электронный вид по умолчанию). Кроме того, одним из качественных результатов становления кибергосударства, выстраивания горизонтальных и координационных взаимоотношений с гражданским обществом является повышение уровня конструктивной и конструирующей гражданской активности (в частности, на основе открытой для сторонних разработчиков правительственной архитектуры), а также уровня доверия населения к органам государственной власти и местного самоуправления.

Однако концепция кибергосударства обладает рядом существенных проблем, усиливаемых в ходе ее практической реализации административными и политическими особенностями той или иной страны. Одной из проблем построения кибергосударства является появление виртуальных инструментов мониторинга и контроля за поведением граждан как в сети Интернет, так и в обычной жизни (через отслеживание финансовой и кредитной истории, видеонаблюдение и определение местоположения и др.). Базы персональных данных, системы идентификации и аутентификации, способствующие созданию «цифровых двойников» граждан, способны с технической точки зрения обеспечить установление «тоталитарного» типа государственного управления, нарушающего целый комплекс прав и свобод человека, включая право на неприкосновенность частной жизни.

Среди проблем построения кибергосударства, доставшихся «по наследству» от электронного государства, также можно указать проблему подготовки государственных и муниципальных служащих к использованию информационных технологий в своей практической деятельности. И здесь речь идет не только о профессиональной подготовке, но и моральной, ценностно-ориентационной основе их работы. Исключение из деятельности государственных служащих личного взаимодействия с гражданами и замена этой взаимосвязи автоматизированным процессом влечет за собой все большую формализацию своего места и роли в системе государственного управления и снижение общего уровня ответственности за совершаемые рутинные операции. Помимо этого, актуализируется проблема низкой мотивации государственных и муниципальных служащих к обучению новым профессиональным компетенциям в сфере информационных технологий и готовности применять их в своей работе,

которая усугубляется тем, что различные социальные и возрастные группы населения также обладают недостаточным уровнем информационных компетенций и имеют неравный уровень доступа к информационным системам государства.

Формирование кибергосударства приводит к постепенному смещению центра власти и общественной жизни в виртуальное пространство, характеризующееся достаточно высокой степенью анархии и критически зависящее от развития информационных сетей и баз данных. Многими аналитиками и экспертами подвергается сомнению возможность сохранения территориального (вестфальского) государственного суверенитета в условиях стирания границ между реальной и виртуальной властью, все более заметной реализации государственных полномочий в киберпространстве. Эта проблема отмечается не только на научно-исследовательском уровне, но и на уровне внешне- и внутриполитической деятельности современных государств. Так, в декабре 2017 года председатель КНР Си Цзиньпин публично представил свое мнение о суверенитете и безопасности в киберпространстве. В обращении к участникам Всемирной конференции по интернету китайский руководитель заявил о необходимости уважения суверенитета в киберпространстве на основе взаимовыгодного и равного сотрудничества между государствами [Си Цзиньпин призвал уважать суверенитет в киберпространстве, www].

Российский исследователь М.Ш. Шарифов в своей научно-исследовательской работе выделил несколько основных факторов, подрывающих суверенитет государства в киберпространстве [Шарифов, www]:

7) Виртуальность и условность параметров взаимодействия граждан и государства;
8) Сохраняющаяся анонимность участников или предоставление ими *недостоверных сведений о себе*;
9) Формирование трансграничной виртуальной идентичности у отдельных граждан и их сетевых сообществ;
10) Зависимость горизонтальной социальной стратификации от качества доступа к киберпространству, а не от территориальной принадлежности (при этом вертикальная социальная стратификация в большей мере начинает зависеть от уровня владения информационными компетенциями).

Очевидно, что проблема смещения центра власти и общественной жизни в киберпространство влечет за собой не только проблему трансформации государственного суверенитета к новым условиям, но и проблему определения границ юрисдикции государственных институтов. Такая категория, как юрисдикция, несомненно, связана с территориальными границами и верховенством права над определенной территорией и населением. Однако на современном этапе речь идет о снижении значимости территориального фактора для самоидентификации государства, определения государственной принадлежности граждан и юридических лиц. Для киберпространства вопрос территориальных границ значительно менее применим, чем для физического пространства. Общественные отношения формируются в рамках киберпространства вне зависимости от действительного местонахождения участников этих отношений.

В контексте усиления значимости киберпространства, выступающего критически важной средой дальнейшей эволюции государства, остро встает вопрос о столкновении территориального суверенитета государства с экстерриториальной природой информационного общества, в пространстве которого образуются многочисленные сетевые взаимосвязи и центры власти. Вместо факторов территории и населения социально-политическое пространство

государства кристаллизуется вокруг финансовых и информационных потоков в киберпространстве. Однако органы государственной власти не всегда могут получить контроль за информационными сетями и базами данных за пределами государственных границ, поэтому сосредотачиваются на контроле над той областью информационной инфраструктуры, которая находится внутри государственных границ и обслуживает взаимодействие с подавляющим большинством граждан данного государства.

Концепция кибергосударства в настоящее время не получила своего законодательного воплощения, однако ее отдельные положения нашли свое отражение в нормативно-правовой базе концепции электронного государства. Так, в Российской Федерации целью создания электронного государства выступило создание качественной и результативной системы взаимодействия государства, граждан и юридических лиц, включая поэтапное построение электронного правительства, внедрения механизмов электронного парламента и электронного правосудия. В этой связи концепция электронного государства в России подразумевает создание множества специализированных государственных автоматизированных систем, каждая из которых обслуживает то или иное государственное ведомство или учреждение (при том, что кибергосударство подразумевает интеграцию данных систем в рамках единой облачной платформы). Более того, концепция электронного государства продолжает активно реализовываться в рамках государственной программы «Информационное общество» на период 2011-2020 годы и Стратегии развития информационного общества в РФ на период 2017-2030 годы. Следует отметить, что на современном этапе нельзя говорить о построении в России полноценного электронного государства. Это обусловлено тем, что создание автоматизированных информационных систем, перевод многих государственных и муниципальных услуг в электронный вид носит пока номинальный, а не содержательно-смысловой характер. Система государственного управления пока не адаптировалась к современным информационным технологиям, различным рискам и угрозам, возникающим в связи с развитием информационных технологий в сфере финансов, средств массовой коммуникации, оборонной и разведывательной сфер и др.

В отличие от концепции электронного государства построение кибергосударства предполагает внедрение электронного формата предоставления всего спектра государственных и муниципальных услуг по умолчанию. Уходя от вспомогательной роли электронного формата оказания услуг населению, трансформация государственного управления в рамках концепции кибергосударства направлена на построение «государства-как-платформы» (единой государственной облачной платформы и информационной инфраструктуры совместного использования), характеризующейся оптимизацией численности и структуры государственного аппарата, виртуализацией рабочих мест государственных и муниципальных служащих, электронным документооборотом и управлением процессами прохождения дел, электронным мониторингом государственной инфраструктуры, повышением качества и защищенности взаимодействия между ведомствами, финансовой экономией за счет отказа от создания дублирующих информационных инфраструктур в отдельных ведомствах или регионах, оперативным принятием всего спектра управленческих решений, отсутствием посредников между человеком и его данными, выстраиванием индивидуальных траекторий в развитии и решении жизненных ситуаций, с которыми сталкивается человек (рождение ребенка, покупка автомобиля и др.) [Петров и др., 2018]. Если в рамках электронного правительства многофункциональные центры оказания государственных и муниципальных услуг брали на себя функцию предоставления услуг отдельным группам населения, не имеющим доступа или

не владеющими навыками работы с информационными порталами, то кибергосударство стремится преодолеть электронное неравенство, охватывая своими услугами все население за счет мобильных интернет-приложений. Переход к кибергосударству означает не только создание услуг, которые нужны гражданам и которые граждане хотят получать посредством электронных каналов связи, но и создание условий для киберинклюзии граждан, возможности доступа к услугам и развития соответствующих навыков использования информационных сервисов.

С концепцией кибергосударства тесно связана концепция криптоанархии. Термин криптоанархии разработал американский технический и политический писатель Тимоти Мэй [May, 2001]. Он использовал этот термин с целью характеристики последствий глобального применения шифровальных технологий, поддерживающих высокую степень анархичности и автономии киберпространства на фоне усилий различных государств по контролю над информационным пространством. Иными словами, к криптоанархии приводит практика неподконтрольной и практически недешифрируемой передачи информационных сообщений и данных в киберпространстве, в частности, совершения никем не контролируемых финансовых сделок и операций. Проблема имеет две стороны:

– Неконтролируемые коммерческие сделки, использующие упрощенные механизмы совершения финансовых операций в Интернет-пространстве и направленные на финансирование политической сферы;
– Формирование теневой экономики в киберпространстве, не поддающейся налоговому регулированию государства и снижающей возможности практической реализации данного признака государственного суверенитета.

По мнению Питера Ландлоу, который в своих работах также уделяет большое внимание проблеме криптоанархии [Ludlow, 1996], зашифрованная коммуникация в рамках киберпространства получает преимущество перед традиционными средствами и технологиями передачи информации, трансформируя административную и коммерческую практику, вынужденную адаптироваться к новым условиям через государственную политику депонирования ключей шифрования популярных мессенджеров и социальных сетей, а также легализации рынка криптовалют.

В рамках концепции криптоанархии получает дальнейшее развитие концепция виртуальных сообществ, выступающих в качестве сетей, включающих отдельных пользователей и их группы, которые могут находиться на любом физическом отдалении друг от друга и общаться в защищенных от государственного контроля режимах на различных интернет-платформах. Виртуальность этого взаимодействия определяется отсутствием вербального контакта между членами виртуального сообщества, которое имеет такие же признаки, как и обычное сообщество людей. В качестве исторических примеров устойчивых сообществ людей, объединенных только виртуальной связью, можно привести международные клубы и ассоциации, террористические и криминальные организации и т.д., взаимодействие внутри которых в настоящее время значительно усилилось благодаря переходу к использованию интернет-коммуникаций. Особенно важно отметить возросший потенциал таких виртуальных сообществ как террористические и криминальные организации, могущих бросить вызов государственному суверенитету отдельных стран и действующих достаточно безнаказанно вследствие несовершенства международных механизмов борьбы с ними и отсутствием согласованности в действиях ведущих держав.

Важным последствием криптоанархии, как уже было сказано, становится формирование

теневой политики и теневой экономики, которые не поддаются прямому регулированию и контролю со стороны государства или международных институтов. Более того, распространение идей криптоанархии и популяризация криптотехнологий повлекло за собой появление такого явления как киберпреступность. Киберпреступность следует рассматривать в качестве негативного уголовно-правового явления, связанного с применением информационных технологий и глобальных сетей передачи данных, нарушающих требования международного или национального права. В результате, актуальным и весьма целесообразным становится разработка особых правовых мер в отношении регулирования информационных взаимоотношений с использованием криптотехнологий как со стороны отдельных государств, так и на международном уровне. Важным оказывается в данном случае учет множества факторов, оказывающих влияние на обеспечение информационной безопасности в глобальном киберпространстве, в частности, необходимости разработки и совершенствования программных и аппаратных средств защиты информации (например, разработки отечественного программного обеспечения для работы государственных ведомств и коммуникации государственных служащих, внедрения практики депонирования ключей от информационных криптосистем у специализированных доверенных организаций).

Для российской действительности этот вопрос является особо острым. Криптоанархия в условиях правовых и организационных проблем в сфере государственного управления в России влечет за собой серьезные последствия, касающиеся нанесения ущерба государственному бюджету. Только за 2017 год ущерб от киберпреступлений в банковском секторе России составил более 1,3 млрд. долларов. Статистика демонстрирует негативную тенденцию увеличения количества киберпреступлений. С 2013 по 2016 год их количество увеличилось в 6 раз (с 11 тысяч в 2013 году до 66 тысяч в 2016 году), при этом эксперты прогнозируют дальнейший рост.

Здесь особенно ярко проявляется противоречие между идеалами криптоанархии и требованиями по защите государственного суверенитета, так как преступления в киберпространстве совершаются в России, как правило, с целью распространения экстремистской информации (2/3 преступлений в киберпространстве обладают экстремистской направленностью). Особую проблему также составляют преступления в киберпространстве, связанные с терроризмом: переход от одиночных спонтанных атак на отдельные государственные и корпоративные порталы к спланированным нападениям виртуальных преступных сообществ на объекты жизненно важной критической инфраструктуры, которые могут спровоцировать как техногенные аварии и экологические катастрофы, так и социально-политические потрясения.

Разработка и распространение корпорациями и исследовательскими организациями информационных систем на базе криптотехнологий во многом приводит к обострению противоречий между ними и представителями государственной власти, выступающими в защиту государственного суверенитета и национальной безопасности. Противоречие возникает также в связи с неконтролируемым распространением среди виртуальных сообществ криптотехнологий и стремлением со стороны кибергосударства реализовать свои суверенные полномочия, построить против них заградительные барьеры (например, проект «Золотой щит» или «Великий китайский файервол»), которые, согласно ежегодному исследованию свободы в Интернете «Freedom on the Net», могут представлять собой [Freedom on the Net Methodology, www]: 1) техническую блокировку определенных веб-страниц и мобильных приложений, доменов или IP-адресов на территории конкретной страны (используется тогда, когда прямая

юрисдикция или дешифрирование иностранных сайтов и мобильных приложений недоступны для властей); 2) удаление результатов поиска, когда частные компании, предоставляющие услуги поиска в сети Интернет, в рамках соглашений о сотрудничестве с тем или иным государством, скрывают нежелательные результаты поиска и снижают возможности популяризации и монетизации криптосервисов; 3) государственное регулирование работы Интернет-провайдеров с целью предотвращения распространения запрещенной или нежелательной информации. Подобные усилия не только снижают возможности применения криптотехнологий среди виртуальных сообществ, большинство из которых не связано с преступной деятельностью, но и вызывают оправданную критику, так как ограничивают свободу информации в киберпространстве и несут в себе элементы цензурирования.

Виртуальные сообщества, в свою очередь, используя криптотехнологии, стремятся преодолевать любые кибербарьеры, так как по своей природе отличаются от традиционных форм социальной интеграции использованием многочисленных каналов коммуникации и многовариантностью форм интеграции людей, отсутствием четких границ (относительно членства в виртуальном сообществе), а также множественностью целей и интересов участников виртуального сообщества, затрудняющих контроль над ними [Рыков, 2013]. На фоне вышеперечисленных особенностей виртуальных сообществ следует отметить повышение государственной активности, актуализирующей противоречия между суверенитетом кибергосударства и криптоанархией. Примером актуализации указанных противоречий можно считать российскую практику мониторинга социальных сетей и интернет-ресурсов органами государственной власти на предмет распространения экстремистских материалов (в Российской Федерации за распространение таких материалов предусмотрена административная и уголовная ответственность), а также оперативного реагирования (в течение 24 часов) на жалобы граждан в социальных сетях со стороны региональных властей с использованием различных автоматизированных инструментов, в частности, «Инцидент менеджмента». Более того, согласно принятым федеральным законам № 374 и 375 (пакет Яровой-Озерова) государство расширяет полномочия правоохранительных органов, выдвигает более жесткие требования к операторам мобильной связи и Интернета, обязывая их хранить телефонные записи, SMS и Интернет-трафик в течение 6 месяцев в своих дата-центрах.

Заключение

Однако рядом экспертов вполне корректно ставится вопрос о том, что усиление контроля над киберпространством становится заметным элементом политической повестки государства и инструментом поддержания политической стабильности несмотря на то, что изначально подобный контроль рассматривался исключительно в плоскости борьбы с терроризмом и экстремизмом.

Библиография

11. Газизов Р.Р. Перспективы развития технологий электронного государства в России // Ленинградский юридический журнал. 2015. №2 (40). С. 53-58.
12. К 2018 году потери РФ от киберпреступлений превысят 2 трлн рублей. URL: https://rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html
13. Киберпреступники за 2017 год нанесли 1,3 млрд ущерба банковской сфере РФ. URL: https://regnum.ru/news/2381125.html
14. Ладлоу П. Криптоанархия, кибергосударства и пиратские утопии. М.: Ультра. Культура, 2005. 239 с.

15. «Медиалогия» на PR+Forum. URL: http://www.mlg.ru/about/news/5780/
16. Петров М. и др. Государство как платформа. (Кибер)государство для цифровой экономики. Цифровая трансформация. М.: Центр стратегических разработок, 2018. URL: https://www.csr.ru/wp-content/uploads/2018/05/GOSUDARSTVO-KAK-PLATFORMA_internet.pdf
17. Постановление Правительства РФ от 28.01.2002 г. № 65 «О федеральной целевой программе «Электронная Россия (2002-2010 годы)».
18. Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 30.03.2018) «Об утверждении государственной программы Российской Федерации «Информационное общество (2011-2020 годы)».
19. Преступления в сфере компьютерной информации. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/
20. Рыков Ю.Г. Виртуальное сообщество как социальное поле: неравенство и коммуникативный капитал // Журнал социологии и социальной антропологии. 2013. Том XVI. №4. С. 44-60.
21. Си Цзиньпин призвал уважать суверенитет в киберпространстве. URL: https://ria.ru/world/20171203/1510097655.html
22. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы».
23. Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».
24. Федеральный закон от 06.07.2016 № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».
25. Число киберпреступлений в РФ с 2013 года выросло вшестеро. URL: http://www.interfax.ru/russia/589574
26. Шарифов М.Ш. Суверенная власть в киберпространстве и в сетевом пространстве. URL: https://www.sovremennoepravo.ru/m/articles/view/Суверенная-власть-в-киберпространстве-и-в-сетевом-пространстве
27. Юрий Чайка рассказал о борьбе с интернет-преступностью. URL: https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html
28. Freedom on the Net Methodology. URL: https://freedomhouse.org/report/freedom-net-methodology
29. Ludlow P. Crypto Anarchy, Cyberstates and Pirate Utopias. UK: A Bradford Book, 2001. 451 p.
30. Ludlow P. High Noon on the Electronic Frontier. Conceptual Issues in Cyberspace. USA: MIT Press, A Bradford Book, 1996. 558 p.
31. May T. True Nyms and Crypto Anarchy // True Names and the Opening of the Cyberspace Frontier. Tor, 2001. P. 33-87.

The concepts of cyber state and cryptoanarchy in the theory and practice of public administration

Artem A. Kosorukov

PhD in Political Science, Senior Lecturer,
Lomonosov Moscow State University,
119991, 1, Leninskie Gory, Moscow, Russian Federation;
e-mail: Kosorukovmsu@mail.ru

Abstract

The active use of information technologies in the sphere of public administration transforms the traditional concept of the state. The concept of a cyber state allows forming a new theoretical basis for rethinking public administration in the context of the formation of independent cyber jurisdictions, the boundaries of which do not coincide with the boundaries of the state legal system and do not depend on it. There is a clash of the state, which stands for territorial sovereignty, with an information society that is extraterritorial in nature, in the anarchic space of which numerous

network interconnections and centers of power are formed. Strengthening of virtual instruments for monitoring and controlling the behavior of citizens, creating their "digital counterparts" is capable, on the one hand, of establishing a "totalitarian" type of public administration, on the other hand, the main goal of the cyber state is to increase the efficiency of public administration and build a "state-platform, which allows to improve the quality of public services on the basis of a single cloud platform and shared infrastructure and, ultimately, to raise to be a degree of social cyber inclusion. The concept of cyber-state is closely connected with the concept of cryptoanarchy, which describes the practice of uncontrolled transmission of information in cyberspace. The proliferation of crypto-technologies forces the state to defend its sovereignty and security by creating barrage barriers in the way of encrypted communication. Such efforts also restrict freedom of information in cyberspace.

For citation

Kosorukov A.A. (2018) Kontseptsii kibergosudarstva i kriptoanarkhii v teorii i praktike gosudarstvennogo upravleniya [The concepts of cyber state and cryptoanarchy in the theory and practice of public administration]. *Teorii i problemy politicheskikh issledovanii* [Theories and Problems of Political Studies], 7 (4A), pp. 9-19.

Keywords

Cyber state, jurisdiction, sovereignty, electronic services, state as a platform, cryptoanarchy, virtual community, cybercriminality, state control, cyber barrier.

References

1. *Chislo kiberprestuplenii v RF s 2013 goda vyroslo vshestero* [The number of cybercrimes in the Russian Federation has grown sixfold since 2013]. Available at: http://www.interfax.ru/russia/589574 [Accessed 05/05/2018]
2. *Federal'nyi zakon ot 06.07.2016 № 374-FZ «O vnesenii izmenenii v Federal'nyi zakon «O protivodeistvii terrorizmu» i otdel'nye zakonodatel'nye akty Rossiiskoi Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeistviya terrorizmu i obespecheniya obshchestvennoi bezopasnosti»* [Federal Law of 06.07.2016 No. 374-FZ "On Amendments to the Federal Law" On Counteracting Terrorism "and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety"].
3. *Federal'nyi zakon ot 06.07.2016 № 375-FZ «O vnesenii izmenenii v Ugolovnyi kodeks Rossiiskoi Federatsii i Ugolovno-protsessual'nyi kodeks Rossiiskoi Federatsii v chasti ustanovleniya dopolnitel'nykh mer protivodeistviya terrorizmu i obespecheniya obshchestvennoi bezopasnosti»* [Federal Law of July 6, 2016 No. 375-FZ "On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety"].
4. *Freedom on the Net Methodology.* Available at: https://freedomhouse.org/report/freedom-net-methodology [Accessed 05/05/2018]
5. Gazizov R.R. (2015) Perspektivy razvitiya tekhnologii elektronnogo gosudarstva v Rossii [Prospects for the Development of Electronic State Technologies in Russia]. *Leningradskii yuridicheskii zhurnal* [Leningrad Law Journal], 2 (40), pp. 53-58.
6. *K 2018 godu poteri RF ot kiberprestuplenii prevysyat 2 trln rublei* [By 2018, Russia's losses from cybercrime will exceed 2 trillion rubles]. Available at: https://rg.ru/2016/10/01/reg-ufo/poteri-kiberprestuplenij-prevysiat-2-trln.html [Accessed 05/05/2018]
7. *Kiberprestupniki za 2017 god nanesli 1,3 mlrd ushcherba bankovskoi sfere RF* [Cybercriminals for 2017 inflicted 1.3 billion damage to the banking sector of the Russian Federation]. Available at: https://regnum.ru/news/2381125.html [Accessed 05/05/2018]
8. Ludlow P. (2001) *Crypto Anarchy, Cyberstates and Pirate Utopias*. UK: A Bradford Book.
9. Ludlow P. (1996) *High Noon on the Electronic Frontier. Conceptual Issues in Cyberspace.* USA: MIT Press, A Bradford Book.
10. Ludlow P. (2005) *Kriptoanarkhiya, kibergosudarstva i piratskie utopii* [Cryptoanarchy, cyber states and pirate utopias]. Moscow: Ul'tra. Kul'tura Publ.
11. May T. (2001) True Nyms and Crypto Anarchy. In: *True Names and the Opening of the Cyberspace Frontier*. Tor.

12. *«Medialogiya» na PR+Forum* ["Medialogy" at the PR + Forum]. Available at: http://www.mlg.ru/about/news/5780/ [Accessed 05/05/2018]
13. Petrov M. et al. (2018) *Gosudarstvo kak platforma. (Kiber)gosudarstvo dlya tsifrovoi ekonomiki. Tsifrovaya transformatsiya* [The state as a platform. (Cyber) state for the digital economy. Digital transformation]. Moscow: Tsentr strategicheskikh razrabotok Publ. Available at: https://www.csr.ru/wp-content/uploads/2018/05/GOSUDARSTVO-KAK-PLATFORMA_internet.pdf [Accessed 05/05/2018]
14. *Postanovlenie Pravitel'stva RF ot 28.01.2002 g. № 65 «O federal'noi tselevoi programme «Elektronnaya Rossiya (2002-2010 gody)»* [Resolution of the Government of the Russian Federation of 28.01.2002 No. 65 "On the Federal Target Program" Electronic Russia (2002-2010)"].
15. *Postanovlenie Pravitel'stva RF ot 15.04.2014 № 313 (red. ot 30.03.2018) «Ob utverzhdenii gosudarstvennoi programmy Rossiiskoi Federatsii «Informatsionnoe obshchestvo (2011-2020 gody)»* [Resolution of the Government of the Russian Federation of April 15, 2014 No. 313 (as amended on March 30, 2013) "On approval of the state program of the Russian Federation" Information Society (2011-2020)"].
16. *Prestupleniya v sfere komp'yuternoi informatsii* [Crimes in the field of computer information]. Available at: http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/ [Accessed 05/05/2018]
17. Rykov Yu.G. (2013) Virtual'noe soobshchestvo kak sotsial'noe pole: neravenstvo i kommunikativnyi kapital [Virtual community as a social field: inequality and communicative capital]. *Zhurnal sotsiologii i sotsial'noi antropologii* [Journal of Sociology and Social Anthropology], XVI, 4, pp. 44-60.
18. Sharifov M.Sh. *Suverennaya vlast' v kiberprostranstve i v setevom prostranstve* [Sovereign power in cyberspace and in the network space]. Available at: https://www.sovremennoepravo.ru/m/articles/view/Suverennaya-vlast'-v-kiberprostranstve-i-v-setevom-prostranstve [Accessed 05/05/2018]
19. *Si Tszin'pin prizval uvazhat' suverenitet v kiberprostranstve* [Xi Jinping called for respect for sovereignty in cyberspace]. Available at: https://ria.ru/world/20171203/1510097655.html [Accessed 05/05/2018]
20. *Ukaz Prezidenta RF ot 09.05.2017 № 203 «O Strategii razvitiya informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017-2030 gody»* [Presidential Decree No. 203 of May 9, 2017 "On the Strategy for the Information Society Development in the Russian Federation for 2017-2030".].
21. *Yurii Chaika rasskazal o bor'be s internet-prestupnost'yu* [Yuri Chaika spoke about the fight against Internet crime]. Available at: https://rg.ru/2017/08/24/iurij-chajka-rasskazal-v-briks-o-borbe-s-internet-prestupnostiu.html [Accessed 05/05/2018]