

Научная статья

УДК 342.72

doi:10.21685/2307-9525-2021-9-3-6

**ПРАВА ЧЕЛОВЕКА, КИБЕРБЕЗОПАСНОСТЬ,
БОРЬБА С ТЕРРОРИЗМОМ (ОПЫТ КИТАЯ)****Владислав Георгиевич Романовский¹, Динара Алиевна Абубекерова²**^{1, 2}Пензенский государственный университет, Пенза, Россия¹up406@mail.ru,²dinar.abubekerova2011@yandex.ru

Аннотация. *Актуальность и цели.* Проблемы и риски государственного регулирования интернет-пространства – актуальная тема для большинства современных стран. В связи с этим особый интерес вызывает правовая модель обеспечения цифрового суверенитета, созданная в Китайской Народной Республике. Основная цель – анализ китайской модели обеспечения кибербезопасности. В частности, подробно проанализирован Закон КНР от 7 ноября 2016 г. «О кибербезопасности», предъявляющий специальные требования к созданию и функционированию интернет-сетей на территории государства. Представлен также опыт расширительного толкования законодательства о государственной тайне и его применения в отношении вопросов программирования, распространения информации в сети Интернет. *Материалы и методы.* В связи с тем, что именно китайский опыт определяется как наиболее эффективный в государственном регулировании национальной кибербезопасности, в основу статьи был положен сравнительно-правовой метод исследования. *Результаты.* Представлены особенности проекта «Золотой щит», базирующегося на создании собственной технологической базы, разработке национальных продуктов (мессенджеров, социальных сетей, приложений, интернет-энциклопедии и др.). Показано, что в его основу заложен принцип суверенитета киберпространства, вытекающего из ключевых положений о государственном суверенитете. Одна из ключевых целей проекта – противодействие террористическим угрозам. Отмечено, что расширительное толкование понятия государственной тайны активно применяется для введения ограничений на использование зарубежных программных продуктов, установления запретов на информационную активность пользователей в сети. *Выводы.* Обозначены риски подобной фрагментации и суверенизации Интернета. Один из базовых недостатков – значительные финансовые затраты на реализацию национальных правил в киберпространстве.

Ключевые слова: права человека, кибербезопасность, противодействие терроризму, Китай, «Великий китайский файрвол», государственное регулирование, Интернет

Финансирование: исследование выполнено по гранту Президента Российской Федерации для государственной поддержки молодых российских ученых – кандидатов наук в рамках научного проекта № МК-390.2021.

Для цитирования: Романовский В. Г., Абубекерова Д. А. Права человека, кибербезопасность, борьба с терроризмом (опыт Китая) // Электронный научный журнал «Наука. Общество. Государство». 2021. Т. 9, № 3. С. 57–67. doi:10.21685/2307-9525-2021-9-3-6

Original article

**HUMAN RIGHTS, CYBERSECURITY,
COUNTERTERRORISM (PRACTICES IN CHINA)****Vladislav G. Romanovsky¹, Dinara A. Abubekerova²**^{1, 2}Penza State University, Penza, Russia¹up406@mail.ru²dinar.abubekerova2011@yandex.ru

Abstract. *Background.* The problems and risks of state regulation of the Internet space is a relevant topic for most modern states. In this regard, the legal model for ensuring digital sovereignty created in the People's Republic of China is of particular interest. The key aim is to analyze the Chinese cybersecurity model. The Law of the People's Republic of China dated 7 November 2016 "On Cybersecurity" is investigated, which imposes special requirements for creating and operating the Internet networks on the territory of the state. The practices of broad interpretation of the legislation on state secrets and its application in terms of programming and disseminating information on the Internet are also presented. *Materials and methods.* Due to the fact that the Chinese practices are defined as the most effective ones in the state regulation of national cybersecurity, the article is based on the comparative legal research method. *Results.* The features of the Golden Shield Project (the Great Firewall) built on creating internal technological capabilities and developing national products (messaging, social networks, applications, Internet encyclopedias, etc.) are presented. The article shows that the project rests on the principle of cyberspace sovereignty arising from the key provisions on state sovereignty. A key objective of the project is countering terrorist threats. It is indicated that the broad interpretation of the concept of state secrets is actively used to impose restrictions on using foreign software products, to establish bans on information activity of users on the network. *Conclusions.* The risks of such fragmentation and sovereignization of the Internet are outlined. One of the basic disadvantages is the significant financial costs of implementing national cyberspace regulations.

Keywords: human rights, cybersecurity, counterterrorism, China, the Great Firewall, government regulation, the Internet

Acknowledgments: the research was carried out under the grant of the President of the Russian Federation for state support of young Russian scientists – candidates of sciences – within the research project no MK-390.2021.

For citation: Romanovsky V.G., Abubekrova D.A. Human Rights, Cybersecurity, Counterterrorism (Practices in China). *Elektronnyy nauchnyy zhurnal "Nauka. Obshchestvo. Gosudarstvo"* = *Electronic scientific journal "Science. Society. State"*. 2021;9(3):57–67. (In Russ.). doi:10.21685/2307-9525-2021-9-3-6

В настоящее время сетевые технологии все больше пронизывают различные аспекты социальной жизни человека. Киберпространство становится основой информационного обмена. Благодаря новым технологиям происходит взаимодействие гражданина с органами государственной и муниципальной власти, интернет-экономика отвоёвывает себе место в мировом товарообмене, поиск деловых партнеров, личные знакомства осуществляются через мессенджеры и различные социальные сети.

Зависимость каждого из нас от мировой паутины все активнее проявляется в аддикции от распространения новых технологических решений информационного обмена. Нетрудно увидеть, что нанесение урона критической инфраструктуре не требует военного вмешательства и диверсионных атак. Для этого достаточно провести хакерское нападение на компьютеры той или иной компании, чтобы приостановить деятельность конкретной отрасли народного хозяйства. Исходя из осознания таких угроз каждое государство обеспокоено созданием эффективной системы кибербезопасности.

Необходимо отметить, что массовое распространение социальных сетей и мессенджеров внесло серьезные коррективы в стратегию и тактику информационного обмена. Еще недавно подчеркивалась высокая роль телевидения и печатных СМИ, сейчас влияние на умы граждан происходит через формирование поисковой повестки в различных интернет-программах. Изменение ситуации учитывается не только государствами, но и различными деструктивными элементами – экстремистскими и террористическими организациями. Несколько лет назад (в 2011 г.) Аль-Каида (запрещена в Российской Федерации) попыталась разместить онлайн-журнал под названием *Inspire* («Вдохновляй»), но его распространение было быстро заблокировано [1]. Неудачный опыт пропаганды собственных идей был учтен сподвижниками радикального движения. Попытки создания подобных журналов были прекращены. Появление его в мировой сети привело бы

к быстрой блокировке, что не позволило бы осуществлять необходимую агитацию для пополнения рядов сторонников.

Распространение социальных сетей изменило ситуацию. Следствием стала мгновенная передача информации, подчиненная системе хэштегов, выполняющих роль поисковика и объединителя сторонников по интересам. Крупные технологические компании не остаются в стороне от противодействия террористическим угрозам: выявляют и блокируют доступ к противоправному контенту. Однако быстрая заливка файлов обуславливает их моментальное тиражирование и распространение. Сайты стали неудобными, поскольку их блокировка весьма эффективна. Иное дело аккаунты в социальных сетях и телеграмм-каналы. Хэштег становится своеобразным ключом доступа для адептов террористической идеи. Кроме того, внесение специальных ошибок в хэштег минимизирует их блокировку. Например, вместо всем понятного слова «терроризм» публикуется хэштег «#терроизм», который собирает в считанные минуты значительное число получателей необходимых сведений. Данный пример лишь иллюстрирует возможности обхода. Практика же показывает очень искусные модели хэштегирования для обхода систем блокировок.

В качестве примера эффективной модели фильтрации в сети Интернет нередко приводится китайский проект «Золотой щит», или, как его именуют в иностранных источниках, «Великий китайский файрвол» (Great Firewall of China) [2]. Его юридической вершиной можно считать Закон КНР от 7 ноября 2016 г. «О кибербезопасности», предъявляющий специальные требования к созданию и функционированию интернет-сетей на территории государства. В основу его построения положен принцип сетевой безопасности, фильтрации контента, ограниченности доступа к запрещенным данным [3]. Иными словами, в пределах одного государства произошла фрагментация Интернета, к которому стали стремиться многие страны. Китайский опыт также прельщает некоторые демократические страны, заявляющие о защите своего информационного суверенитета.

«Золотой щит» показателен еще и тем, что это – относительно успешный пример выстраивания границ в киберпространстве. Значимый момент заключается в том, что оно осуществлялось не только введением запрещающих и ограничивающих правил, но и созданием специальной технологической базы [4]. Например, подавляющее большинство американцев являются пользователями сети Facebook. Запрет ее (блокировка) приведет к полному обрушению выстроенных социальных связей. КНР, запретив на своей территории использование Facebook, приложило усилия к созданию своих социальных сетей, которыми выступает мессенджер WeChat, социальные сети QQ, Sina Weibo (перечень далеко не исчерпывающий). Каждая из них призвана восполнить тот вакуум, который произошел в результате запрета зарубежных продуктов – Instagram, Twitter, Tumblr, Pinterest. В то же время каждый китайский продукт имеет ограниченное распространение, охватывая только территорию собственного государства, некоторые соседние государства Азиатского региона. Единственным исключением можно считать сервис для создания и просмотра коротких видео TikTok.

В России ведется подобная работа. Так, создан видеохостинг Rutube, управляемый холдингом «Газпром-медиа», но его перспективы оцениваются пока весьма скромно. В СМИ Rutube в связи с отсутствием оригинального контента именуют «складом перезаливов»¹. Даже при полном запрете в нашей стране иностранных сервисов Rutube вряд ли сможет выполнить функции того же YouTube ввиду территориальной ограниченности. В условиях информационной открытости фрагментация Интернета не имеет перспектив. Тем более такая политика будет иметь катастрофический характер для развивающихся экономик и представленных незначительным числом пользователей (в сравнении с числом пользователей технологических гигантов).

¹ «Склад перезаливов»: что ждет российский видеохостинг Rutube. URL: https://www.gazeta.ru/tech/2021/04/02/13544858/rutube_future.shtml (дата обращения: 19.06.2021).

Одновременно с этим Китай целенаправленно обеспечивал индустриальную независимость в построении собственных сетей, а также «точек входа» – дата-центров. Для сравнения – в России значительный объем трафика (особенно внешнего) связан с использованием сервисов компании Google. Так, более половины всего российского трафика связано с просмотром и загрузкой видео, две трети объема которого приходится на использование сервиса YouTube. Каждый провайдер нацелен на облегчение и удешевление своих услуг, что привело к установке и эксплуатации серверов Google Global Cache. Отказ от них в России не только приведет к удорожанию услуг связи, но и будет иметь иные негативные последствия. К тому же замена не произойдет одновременно и потребует серьезных финансовых вливаний. Общий объем затрат исчисляется десятками миллиардов долларов. В нашей стране не самая лучшая финансовая ситуация для такого революционного шага.

В Китае проводится целенаправленная политика отказа от анонимности в Интернете. Это имеет как свои плюсы, так и минусы. В числе положительных моментов можно указать на минимизацию кибермошенничества, в числе отрицательных – самоцензура при публикации материалов и разрешительный порядок практически на любой вид деятельности в мировой сети [5]. Нельзя забывать, что КНР – социалистическое государство с провозглашением коммунистической идеологии в качестве государственной. Однако некоторые новеллы, например отказ от анонимности, поддерживаются странами (а также рядом компаний, оказывающих коммуникационные услуги) вне зависимости от идеологических основ построения государственности [6]. К тому же в Китае действует «Интернет-полиция», внимательно отслеживающая распространяемый контент, а также формирующая общественное мнение в необходимом для Коммунистической партии Китая направлении [7].

Перейдем к характеристике Закона КНР «О кибербезопасности». Он был принят на 24-м заседании Постоянного комитета 12-го Всекитайского собрания народных представителей Китайской Народной Республики 7 ноября 2016 г., обнародован 1 июня 2017 г. (дата вступления в силу); подписан Председателем Китайской Народной Республики Си Цзиньпином, состоит из двух разделов, разделенных на семь глав. Основные цели закона обозначены следующим образом:

- обеспечение кибербезопасности;
- суверенитет киберпространства;
- защита национальной безопасности и социальных общезначимых интересов;
- защита законных прав и интересов граждан, юридических лиц и других организаций;
- содействие здоровому развитию экономической и социальной информатизации.

На сайте энциклопедии, где представлен текст Закона, опубликованы также краткие комментарии к основным положениям нормативного акта. В частности, при толковании принципов подчеркивается значение суверенитета киберпространства как «естественного продолжения и выражения национального суверенитета страны в киберпространстве»¹. Есть ссылка и на высказывание Генерального секретаря ЦК Коммунистической партии Китая Си Цзиньпина о распространении закрепленного в Уставе ООН международного принципа суверенного равенства на киберпространство. Содержанием этого элемента принципа будут права государства самостоятельно выбирать путь развития Интернета, модель управления, государственную политику в отношении Интернета и равное участие в управлении международным киберпространством.

Закон применяется ко всей технологической цепочке Интернета – от строительства и эксплуатации сетей до их использования, а также к надзору и управлению сетевой безопасностью.

¹ 中华人民共和国网络安全法. URL: <https://baike.baidu.com/item/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95/16843044?fr=aladdin> (дата обращения: 19.06.2021).

Во главу угла поставлено государство, которое: 1) формулирует и реализует стратегии сетевой безопасности; 2) устраняет риски и угрозы кибербезопасности, защищает критически важную информационную инфраструктуру; 3) пропагандирует цивилизованное поведение в Интернете, а также способствует распространению основных социалистических идей; 4) осуществляет международное сотрудничество, создает многостороннюю, демократичную и прозрачную сеть и систему управления ею.

Статья 12 Закона предусматривает, что все граждане и организации при использовании Интернета должны соблюдать Конституцию, законы, общественный порядок, уважать социальную этику, не должны создавать угрозу безопасности сети и не должны использовать Интернет для создания угроз национальной безопасности, чести и законным интересам граждан, для подстрекательства к свержению государственной власти, социалистического строя, не должны подстрекать к расколу страны, подрыву национального единства, содействовать терроризму, экстремизму, этнической ненависти и дискриминации, распространению насилия, нецензурной лексики и порнографии, изготавливать и распространять ложную информацию, нарушать экономический и социальный порядок, ущемлять репутацию и неприкосновенность частной жизни, авторские права и другие права и законные интересы граждан и организаций. Статья 13 специально нацеливает на создание безопасных сетевых продуктов для несовершеннолетних. Статья 14 обязывает пользователей сообщать о выявлении противоправного контента в соответствующие государственные органы, при этом обеспечивается конфиденциальность личности информатора.

Глава 2 Закона посвящена обеспечению сетевой безопасности. Государство разрабатывает и обновляет национальные и отраслевые стандарты сетевой безопасности, которые являются обязательными для исполнения. Провозглашается политика государства, нацеленная на поощрение системы общественных услуг сетевой безопасности (ст. 17), а также развитие технологий защиты и использования сетевых данных, инноваций, способствующих экономическому и социальному развитию (ст. 18). Гражданам должны предоставляться услуги по обучению основам кибербезопасности, обязанности по предоставлению которых возлагаются на местные органы власти. Средства массовой информации должны обеспечивать целевую рекламу и просвещение общества по сетевой безопасности, а образовательные организации должны разрабатывать специальные образовательные программы среднего и высшего образования, связанные с безопасностью в Интернете.

Провайдеры обязаны:

- защищать сети от вмешательства, разрушения или несанкционированного доступа;
- предотвращать утечки или кражи или подделки сетевых данных;
- создавать собственные системы внутренней безопасности;
- принимать технические меры по предотвращению компьютерных вирусов, сетевых атак и сетевых вторжений, которые угрожают сетевой безопасности;
- принимать технические меры для мониторинга и записи состояния работы сети и инцидентов сетевой безопасности, а также хранить соответствующие сетевые журналы не менее шести месяцев в соответствии с установленными правилами;
- классифицировать данные, осуществлять резервное копирование и шифрование важных данных.

Иные обязанности провайдеров могут устанавливаться законами и административными актами.

В соответствии со ст. 22 Закона «О кибербезопасности» поставщики сетевых продуктов и услуг не должны создавать вредоносные программы, а при их обнаружении им необходимо немедленно принять меры по исправлению положения, своевременно уведомить пользователей и сообщить об этом в соответствующие компетентные органы. Если предоставление услуг связано со сбором персональных данных, то поставщик должен уведомить об этом пользователей и получить их согласие.

Статья 27 устанавливает запрет на оказание любой помощи тем, кто участвует в противоправной деятельности в Интернете. Статья 28 Закона предусматривает обязанность операторов сетей оказывать техническую поддержку и помощь правоохранительным органам в обеспечении национальной безопасности и расследовании преступлений в соответствии с законом.

Дополнительные обязанности устанавливаются для операторов сетей, относящихся к критической информационной инфраструктуре. К тому же они должны принимать все меры, чтобы персональные и иные важные данные собирались и генерировались только на территории Китайской Народной Республики. В случае необходимости предоставления таких данных за границу в силу потребностей бизнеса должна проводиться оценка безопасности такой передачи, если иное не предусмотрено законом.

Закон о кибербезопасности определяет режим оборота персональных данных. Так, при их сборе и обработке должны раскрываться цель, объем, методы такой деятельности. Запрещается собирать личную информацию, не имеющую отношения к предоставляемым услугам (ст. 41). Операторы сети не имеют права раскрывать, подделывать или уничтожать личную информацию, которую они собирают; они не должны предоставлять такую информацию иным субъектам без согласия самого лица. О факте потери или утечки персональных данных должны быть уведомлены как сами пользователи, так и государственные органы.

Каждый оператор сети должен сформировать систему отчетности по жалобам в рамках информационной безопасности (ст. 49). В соответствии со ст. 51 государство создает систему мониторинга сетевой безопасности, раннего предупреждения об угрозах и информационного уведомления пользователей. Национальный департамент кибербезопасности и информатизации должен координировать деятельность соответствующих отделов для проведения сбора необходимой информации, ее анализа и уведомления о кибербезопасности, а также публиковать информацию о мониторинге кибербезопасности и раннем предупреждении об угрозах в едином порядке в соответствии с установленными правилами. Статья 58 Закона о кибербезопасности допускает введение государством временных ограничений в использовании сетевых коммуникаций. Глава VI посвящена административной ответственности за нарушения данного закона.

Китайский «Золотой щит» является эффективной моделью контроля сетевого пространства, что признается экспертами многих стран. Но здесь следует учитывать и возможности тотального контроля государства за многими проявлениями частной жизни собственных граждан [8]. Именно сочетание многих факторов обуславливает общие принципы функционирования «Золотого щита». Между тем технологические особенности киберпространства допускают обход вводимых границ. Показательно обращение к сайтам американских туристических компаний, специализирующихся на организации отдыха в Китае: практически везде есть специальный раздел, посвященный советам об обходе «Золотого щита» и получении доступа к привычным для американцев Facebook, Instagram и Twitter. Пошаговые инструкции рассчитаны на неподготовленных пользователей, предлагают варианты использования Proху-сетей, приложений VPN (Virtual Private Network), браузеров Tor и FreeBrowser.

Павел Дуров, основатель мессенджера Telegram, является также организатором «Цифрового сопротивления» – децентрализованного движения, нацеленного на отстаивание прав и свобод в цифровом пространстве. Впервые о нем было заявлено в 2018 г., когда Роскомнадзор пытался заблокировать мессенджер на территории Российской Федерации. После снятия всех официальных претензий к Telegram в 2020 г. Павел Дуров объявил о переориентировании движения на Иран и Китай. Технология борьбы с ограничениями связана с перенаправлением Proху-сетей на Китай и Иран, чтобы пользователи этих стран могли обходить вводимые запреты [9].

В то же время нельзя указывать, что только государства задействованы в механизме ограничений и запретов во Всемирной паутине. Технологические гиганты

также участвуют в фильтрации контента и используют ее для достижения максимальной прибыли. Монетизация коммуникационных услуг многими признается как глобальная угроза свободе информационного обмена. Сооснователь Интернета Тим Бернерс-Ли представил «Контракт для сети»¹, в котором обозначил принципы взаимодействия государства, компаний и граждан².

Для правительств:

- предоставление доступа к Интернету для всех;
- доступность Интернета в любое время, основанная на его открытости и конкуренции. Любые ограничения должны соответствовать общим правилам о защите прав человека;
- уважение и защита фундаментальных основ конфиденциальности граждан в Интернете и соблюдения прав на данные, обеспечение использования Интернета свободно, безопасно и без страха.

Для компаний:

- обеспечение технологической базы для свободного Интернета, в том числе гарантированного для меньшинств (создание удобных интерфейсов, учет интересов различных групп в формировании корпоративных политик, поддержка общественных сетей);
- гарантии конфиденциальности и защиты персональных данных, обеспечиваемые предоставлением четких объяснений сбора личной информации, минимизацией сбора самих данных, поддержкой корпоративной подотчетности;
- разработка технологий, которые поддерживают лучшее в человечестве и бросают вызов худшему. Интернет, действительно, является общественным благом, в котором люди превыше всего.

Для граждан:

- быть творцами и соавторами в Интернете, активно участвовать в формировании контента;
- создавать сильные сообщества, уважающие гражданский дискурс и человеческое достоинство;
- бороться за Интернет – открытый, глобальный, общедоступный ресурс для людей во всем мире сейчас и в будущем.

Анализ двух систем, представленных официальной государственной политикой Китая и активным гражданским обществом в лице Т. Бернерса-Ли, показывает наличие точек соприкосновения. Иной вопрос – различия в подходах. Китайская модель основана на этатистском подходе. Закон КНР «О кибербезопасности» богат на общие формулировки о возможностях государства в обеспечении именно собственного суверенитета в сетевом пространстве. Это предопределяет особенности публичного регулирования. Например, американское законодательство также богато на запреты и ограничения в сети Интернет. После теракта 2001 г. Патриотический Акт (принят осенью 2001 г.) и Акт о свободе (принят летом 2015 г.) установили дополнительные обязанности для провайдеров по сотрудничеству со спецслужбами в целях противодействия террористическим угрозам. Однако на протяжении всего времени в судебных инстанциях периодически возникают иски, поданные против официальных лиц государства, с обвинениями в превышении регуляторных полномочий. Наибольшая общественная значимость придавалась, в частности, таким делам, как «Мэйфилд против Соединенных Штатов»³, «Ларри Клейман против Обамы»⁴, «Доу против Мукаси»⁵ и др. Подобные иски трудно представить в Китайской Народной Республике. К тому же китайское

¹ Contract for the Web. A global plan of action to make our online world safe and empowering for everyone. URL: <https://contractfortheweb.org/> (дата обращения: 19.06.2021).

² Contract for the Web. URL: <https://9nrane41lq4966uwmjcfggv-wpengine.netdna-ssl.com/wp-content/uploads/Contract-for-the-Web-3.pdf> (дата обращения: 19.06.2021).

³ Mayfield v. United States. URL: <https://caselaw.findlaw.com/us-9th-circuit/1499231.html>

⁴ Memorandum Opinion. URL: <https://assets.documentcloud.org/documents/4267780/42df8218-70d7-4c17-9b6e-2704fdb37315.pdf> (дата обращения: 19.06.2021).

⁵ Doe v. Mukasey, 2d Cir., Dec. 15, 2008. URL: https://www.aclu.org/sites/default/files/pdfs/safefree/doev_mukasey_decision.pdf (дата обращения: 19.06.2021).

законодательство постоянно использует широкие формулировки, открывающие поле для толкования именно органам власти, а не гражданам для защиты собственной свободы в Интернете. К тому же Закон «О кибербезопасности» – далеко не единственный в регулировании Всемирной паутины. В апреле 2010 г. принят Закон КНР об охране государственной тайны, в рамках которого провозглашена обязанность операторов соблюдать положения о государственных секретах.

Статья 28 данного Закона закрепляет, что все интернет-операторы и поставщики услуг обязаны:

- 1) сотрудничать с государственными органами при проведении расследования;
- 2) прекратить передачу проблемных данных, вести записи и делать отчеты о таких случаях;
- 3) удалять информацию, когда это необходимо в целях защиты государственной тайны.

Статья 9 Закона, представляя понятие государственной тайны, включает в ее содержание различные аспекты политической и общественной деятельности страны, в том числе секреты народного экономического и социального развития (например, аудиторские заключения, которые имеют значение для иностранных инвесторов [10]), секреты науки и техники, секреты деятельности политических партий. Практика применения Закона об охране государственной тайны уже указывала на то, что государственные органы достаточно вольно трактовали обязанность по защите государственных секретов, предъявляя требования к иностранным технологическим гигантам. Некоторые правила касаются даже стандартных программных пакетов Microsoft [11]. Подобная политика фильтрации лишь усиливается после принятия Закона «О кибербезопасности».

Фрагментации Всемирной паутины с разделением ее на «национальные кварталы» наносит очередной урон с помощью технологий будущего. Ранее указывались возможности обхода введенных ограничений. Сейчас есть глобальная угроза разрушения киберграниц с помощью космического Интернета, активно внедряемого Илоном Маском. Его амбициозный проект «Starlink» набирает обороты: увеличивается число космических спутников, позволяющих охватить все большую территорию Земли, снижается цена предоставления услуги, облегчается технологический доступ. Китайская Народная Республика вначале отнеслась к идее спутникового Интернета весьма настороженно. Официальные лица высказывались об обеспечении суверенитета в космическом пространстве, вплоть до уничтожения летательных объектов. Однако сложность реализации такой идеи привела к пересмотру позиции и включению в мировую гонку технологий. В настоящее время провозглашен собственный проект – Galaxy Space. Учитывая успехи в продвижении инноваций, можно уверенно предположить, что Китай разработает собственную программу космического Интернета.

Таким образом, Китайская Народная Республика путем создания «Золотого щита» продвинула собственную концепцию распространения государственного суверенитета на киберпространство. Его основные постулаты заключаются в формировании национальной правовой базы, обеспечивающей достижение собственных интересов, минимизирующей внешнее влияние на китайское общество. К тому же именно «Золотой щит» рассматривается как наиболее эффективная модель противодействия кибертерроризму, негативные последствия которого расширяются по мере распространения цифровых технологий. Кстати, в российском уголовном праве отсутствует специальный состав преступления, что многими исследователями оценивается отрицательно [12–19]. Следует признать, что условное противоборство государства и технологических гигантов стало проявляться в различных странах. Так, Германия также стала активно продвигать идею государственного регулирования сетевых технологий [20]. Подобные тенденции видны и в правотворческой политике нашего государства. Исходя из этого китайский опыт весьма интересен для отечественного законодателя, поскольку позволит учесть как плюсы, так и минусы этатистской модели регулирования.

Список литературы

1. Романовский Г. Б., Кулешова Г. П., Капитонова Е. А. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // *Всероссийский криминологический журнал*. 2020. Т. 14, № 1. С. 156–165.
2. Fry J. D. Privacy, predictability and Internet surveillance in the U.S. and China: better the devil you know? // *University of Pennsylvania Journal of International Law*. 2015. Vol. 37. P. 419–501.
3. Quinn J. A Peek over the Great Firewall: a breakdown of China's new cybersecurity law // *SMU Science and Technology Law Review*. 2017. Vol. 20, № 2. P. 407–436.
4. Stevenson C. Breaching the Great Firewall: China's Internet Censorship and the quest for freedom of expression in a connected world // *Boston College International & Comparative Law Review*. 2007. Vol. 30, № 2. P. 531–558. URL: <https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1074&context=iclr>
5. Kissel T. K. License to Blog: Internet Regulation in the People's Republic of China // *Indiana International & Comparative Law Review*. 2007. Vol. 17, № 1. P. 229–268. URL: <https://mckinneylaw.iu.edu/iiclr/pdf/vol17p229.pdf>
6. Lee J.-A., Liu C.-Y. Real-name registration rules and the fading digital anonymity in China // *Washington International Law Journal*. 2016. Vol. 25, № 1. P. 1–34. URL: <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1717&context=wilj>
7. Zheng H. Regulating the Internet: China's law and practice // *Beijing Law Review*. 2013. Vol. 4, № 1. P. 37–41. URL: https://www.researchgate.net/publication/271293880_Regulating_the_Internet_China's_Law_and_Practice
8. Безрукова О. В., Капитонова Е. А., Кулешова Г. П. [и др.]. Терроризм, права человека и демократические ценности в России и за рубежом. М. : Юрлитинформ, 2019. 232 с.
9. Романовский Г. Б., Романовская О. В. Права человека и борьба с терроризмом: зарубежный опыт. М. : Проспект, 2021. 192 с.
10. Barber P. Bull in the China market: the gap between investor expectations and auditor liability for Chinese financial statement frauds // *Duke Journal of Comparative & International Law*. 2013. Vol. 24. P. 349–402. URL: <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1402&context=djcil>
11. Cheung A. S. Y. The business of governance: China's legislation on content regulation in cyberspace // *International Law and Politics*. 2005. Vol. 38, № 1. P. 1–38. URL: https://www.nyujilp.org/wp-content/uploads/2013/02/38.1_2-Cheung.pdf
12. Паненков А. А. Кибертерроризм как реальная угроза национальной безопасности России // *Право и кибербезопасность*. 2014. № 1. С. 12–19.
13. Услинский Ф. А. Кибертерроризм в России: его свойства и особенности // *Право и кибербезопасность*. 2014. № 1. С. 6–11.
14. Чернядзева Н. А. О международных подходах правового регулирования борьбы с кибертерроризмом // *Информационное право*. 2016. № 2. С. 26–29.
15. Бельский А. И., Якимова В. И. Кибертерроризм как один из наиболее опасных видов международного терроризма // *Российский следователь*. 2020. № 5. С. 66–70.
16. Антонян Е. А., Аминов И. И. Блокчейн-технологии в противодействии кибертерроризму // *Актуальные проблемы российского права*. 2019. № 6. С. 167–177.
17. Данильченко Э. Д. Правовая основа противодействия правоохранительных органов кибертерроризму // *Транспортное право*. 2015. № 4. С. 27–32.
18. Паненков А. А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России // *Военно-юридический журнал*. 2014. № 4. С. 3–13.
19. Чжэн И. Сотрудничество РФ и КНР в борьбе с кибертерроризмом // *Вестник Московского государственного областного университета*. 2018. № 2. С. 204–213.
20. Adamski H. Hassreden (Hate Speech) im internet. Zum streit um das Netzwerkdurchsetzungsgesetz (NetzDG) // *Gesellschaft. Wirtschaft. Politik*. 2018. № 1. S. 135–142.

References

1. Romanovsky G.B., Kuleshova G.P., Kapitonova E.A. Legal Framework for Countering Cyberterrorism in Russia and Abroad from the Social and Political Perspective. *Vserossiyskiy kriminologicheskii zhurnal = All-Russian Criminology Journal*. 2020;14(1):156–165. (In Russ.)

2. Fry J.D. Privacy, Predictability and Internet Surveillance in the U.S. and China: Better the Devil You Know? *University of Pennsylvania Journal of International Law*. 2015;37: 419–501.
3. Quinn J.A. Peek over the Great Firewall: A Breakdown of China's New Cybersecurity Law. *SMU Science and Technology Law Review*. 2017;20(2):407–436.
4. Stevenson C. Breaching the Great Firewall: China's Internet Censorship and the Quest for Freedom of Expression in a Connected World. *Boston College International & Comparative Law Review*. 2007;30(2):531–558. Available at: <https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1074&context=iclr>
5. Kissel T.K. License to Blog: Internet Regulation in the People's Republic of China. *Indiana International & Comparative Law Review*. 2007;17(1):229–268. Available at: <https://mckinneylaw.iu.edu/iiclr/pdf/vol17p229.pdf>
6. Lee J.-A., Liu C.-Y. Real-Name Registration Rules and the Fading Digital Anonymity in China. *Washington International Law Journal*. 2016;25(1):1–34. Available at: <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1717&context=wilj>
7. Zheng H. Regulating the Internet: China's Law and Practice. *Beijing Law Review*. 2013;4(1):37–41. Available at: https://www.researchgate.net/publication/271293880_Regulating_the_Internet_China's_Law_and_Practice
8. Bezrukova O.V., Kapitonova E.A., Kuleshova G.P. [et al.]. *Terrorizm, prava cheloveka i demokraticheskie tsennosti v Rossii i za rubezhom = Terrorism, Human Rights and Democratic Values in Russia and Abroad*. Moscow: Yurlitinform, 2019:232. (In Russ.)
9. Romanovsky G.B., Romanovskaya O.V. *Prava cheloveka i borba s terrorizmom: za-rubezhnyy opyt = Human Rights and Fight against Terrorism: Foreign Practices*. Moscow: Prospekt, 2021:192. (In Russ.)
10. Barber P. Bull in the China Market: The Gap between Investor Expectations and Auditor Liability for Chinese Financial Statement Frauds. *Duke Journal of Comparative & International Law*. 2013;24:349–402. Available at: <https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1402&context=djcil>
11. Cheung A.S.Y. The Business of Governance: China's Legislation on Content Regulation in Cyberspace. *International Law and Politics*. 2005;38(1):1–38. Available at: https://www.nyujilp.org/wp-content/uploads/2013/02/38.1_2-Cheung.pdf
12. Panenkov A.A. Cyberterrorism as a Real Threat to the National Security of Russia. *Pravo i kiberbezopasnost = Law and Cybersecurity*. 2014;(1):12–19. (In Russ.)
13. Uslinskiy F.A. Cyberterrorism in Russia: Properties and Features. *Pravo i kiberbezopasnost = Law and Cybersecurity*. 2014;(1):6–11. (In Russ.)
14. Chernyadieva N.A. On International Approaches to Legal Regulation of Fight against Cyberterrorism. *Informatsionnoe pravo = Information Law*. 2016;(2):26–29. (In Russ.)
15. Belskiy A.I., Yakimova V.I. Cyberterrorism as One of the Most Dangerous Types of International Terrorism. *Rossiyskiy sledovatel = Russian Investigator*. 2020;(5):66–70. (In Russ.)
16. Antonyan E.A., Aminov I.I. Blockchain Technologies in Countering Cyberterrorism. *Aktualnye problemy rossiyskogo prava = Topical Issues in Russian Law*. 2019;(6):167–177. (In Russ.)
17. Danilchenko E.D. Legal Framework for Law Enforcement Agencies to Counter Cyberterrorism. *Transportnoe pravo = Transport Law*. 2015;(4):27–32. (In Russ.)
18. Panenkov A.A. System of Cybercrimes Included in Terrorist Activity (Cyberterrorism) as a Real Threat to the External and Internal Contours of the National Security in Russia. *Voenno-yuridicheskiy zhurnal = Military Law Journal*. 2014;(4):3–13. (In Russ.)
19. Chzhen I. Cooperation between the Russian Federation and the People's Republic of China in Fight against Cyberterrorism. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta = Bulletin of Moscow State Region University*. 2018;(2):204–213. (In Russ.)
20. Adamski H. Hassreden (Hate Speech) im internet. Zum Streit um das Netzwerkdurchsetzungsgesetz (NetzDG). *Gesellschaft. Wirtschaft. Politik*. 2018;(1):135–142.

Информация об авторах / Information about the authors

В. Г. Романовский – кандидат юридических наук, доцент кафедры уголовного права, Пензенский государственный университет, 440026, г. Пенза, ул. Красная, 40.

Д. А. Абубекерова – ассистент кафедры уголовного права, Пензенский государственный университет, 440026, г. Пенза, ул. Красная, 40.

V.G. Romanovsky – Candidate of Law, Associate Professor of the sub-department of Criminal Law, Penza State University, 40 Krasnaya street, Penza, 440026.

D.A. Abubekerova – Assistant of the sub-department of Criminal Law, Penza State University, 40 Krasnaya street, Penza, 440026.

Авторы заявляют об отсутствии конфликта интересов / The authors declare no conflict of interests

Поступила в редакцию / Received 21.06.2021

Поступила после рецензирования и доработки / Revised 29.07.2021

Принята к публикации / Accepted 25.08.2021