Vestnik RUDN. International Relations
Вестник РУДН. Серия: МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ
2020 Vol. 20 No. 2 382—394
http://journals.rudn.ru/international-relations

DOI: 10.22363/2313-0660-2020-20-2-382-394

*Научная статья*

# Информационная политика и информационная безопасность КНР: развитие, подходы и реализация

**Т.И. Понька, М.С. Рамич, Ю. У**

Российский университет дружбы народов, Москва, Российская Федерация

Статья посвящена рассмотрению нового курса информационной политики Китайской Народной Республики, который стало проводить «пятое поколение» лидеров КНР после XVIII съезда Коммунистической партии Китая (КПК) в 2012 г. По итогам данного съезда КПК была выдвинута стратегия «Сильного сетевого государства», которая предполагает не только обеспечение кибербезопасности страны, но и использование сетевого потенциала для развития национальной экономики. Новая информационная политика КНР была вызвана резко возросшей ролью информационно-коммуникационных технологий в международных процессах и смещением фокуса международных отношений в Азиатско-Тихоокеанский регион. Основой информационной политики КНР является наличие наиболее современных технологий в ИТ-сфере и активное использование частных компаний для регулирования внешней и внутренней информационной безопасности. Актуальность данного исследования обусловлена возросшим научным интересом к опыту ведущих стран мира по вопросу регулирования в данной области. Китай является одним из лидеров в области научно-технических разработок и активно использует их для реализации задач в области внутренней и внешней политики. Уникальный сетевой ландшафт, который сформировался под влиянием государственной политики по контролю за публикуемым контентом и за счет разделения рынка цифровых услуг между тремя наиболее крупными информационными корпорациями (Baidu, Tencent и Alibaba), стал неотъемлемой частью системы обеспечения информационной безопасности страны и требует тщательного изучения. Целью статьи является выявление эволюции стратегии развития информационной политики КНР и ресурсов для ее реализации. Исследование информационной политики КНР проводится на внешнем и на внутреннем уровне. В статье также рассматриваются угрозы информационной безопасности КНР и проводится анализ подходов к ее обеспечению. Результатами исследования являются выводы, которые показывают роль и место информационной политики во внешней политике КНР, структуру системы обеспечения информационной безопасности и стратегические подходы к регулированию международных отношений в киберпространстве.

**Ключевые слова:** Китайская Народная Республика, информационная безопасность, кибербезопасность, информационная политика, киберпространство, Интернет, информационные технологии

**Благодарности:** Статья выполнена при поддержке гранта РФФИ № № 20-514-92001 ВАОН «Российско-вьетнамское сотрудничество в контексте современной геополитической ситуации в Восточной Азии».

**Для цитирования:** *Понька Т.И., Рамич М.С., У Ю.* Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2020. Т. 20. № 2. С. 382—394. DOI: 10.22363/2313-0660-2020-20-2-382-394

*Research article*

# Information Policy and Information Security of PRC: Development, Approaches and Implementation

**T.I. Ponka, M.S. Ramich, Y. Wu**
RUDN University, Moscow, Russian Federation

**Abstract.** The subject of the study is the new course of the PRC information policy, which was launched by the "Fifth generation" of the PRC leaders after the 18th Congress of the Chinese Communist Party in 2012. As a result, after the 18th Congress of the CPC was started the implementation of the "Strong cyberpower" strategy, which implies not only ensuring cyber security in the country, but also the usage of network resources to develop the national economy. China's new information policy was caused by the sharply increased role of information and communication technologies in international processes and the shift in the focus of international relations to the Asia-Pacific region. The PRC's information policy is based on the most advanced technologies in the IT sphere and the cooperation with private companies on regulating external and internal information security. The relevance of the research topic is due to the increasing role of ICT in international processes. In this context, the most important are the positions of the leading countries of the world to regulate this area, as well as the mechanisms and tools used by them. The People's Republic of China is one of the leaders in the field of scientific and technical developments and actively uses its achievements to accomplish tasks in the field of domestic and foreign policy. In this regard, the purpose of the study is to analyze and compare the development strategies of the PRC information policy and the resources that are necessary for their implementation. The unique network landscape, which was formed under the influence of government policy on control over published content and the sharing of digital services market among the three largest information corporations (Baidu, Tencent and Alibaba), has become an essential part of the country's information security system and requires detailed study. The purpose of the article is to identify the evolution of China's information policy development strategy and resources for its implementation. This article also discusses the threats to the information security of the People's Republic of China and analyzes the approaches to ensuring it. The results of the study are the conclusions that show the role and place of information policy in the PRC foreign policy, the structure of the information security system and strategic approaches to the regulation of international relations in cyberspace.

**Key words:** People's Republic of China, information security, cybersecurity, information policy, cyberspace, Internet, information technologies

**Acknowledgements:** The study was supported by the RFBR grant No. 20-514-92001 VAON "Russian-Vietnamese Cooperation in the Context of the Current Geopolitical Situation in East Asia".

**For citation:** Ponka, T.I., Ramich, M.S. & Wu, Y. (2020). Information Policy and Information Security of PRC: Development, Approaches and Implementation. *Vestnik RUDN. International Relations*, 20 (2), 382—394. DOI: 10.22363/2313-0660-2020-20-2-382-394

В настоящее время во многих странах мира осознали необходимость применения конструктивистской парадигмы к формированию внешней политики государства. Это связано с тем, что на политику государств стали оказывать большое влияние негосударственные акторы, такие как транснациональные компании, средства массовой информации и влиятельные исследовательские центры. А такие процессы, как глобализация и информатизация, вынуждают сами страны изобретать и применять новые подходы к решению своих внешнеполитических задач. Вместе со стремительным социально-экономическим подъемом стран Азиатско-Тихоокеанского региона фокус международных отношений смещается на Восток, вместе с этим возрастают роль и участие стран региона в формировании глобальной повестки дня.

Киберпространство в отличие от других пространств межгосударственного взаимодействия представляет собой искусственную виртуальную среду, с помощью которой соединены устройства, расположенные в различных государствах, и его структура может изменяться [Ebert, Maurer 2013]. Кроме того, именно киберпространство расширило возможности влияния негосударственных акторов на мировую политику, что, в свою

очередь, создало новые вызовы для обеспечения национальной безопасности стран мира [Nye 2011].

Уникальным отличием киберпространства как поля взаимодействия является то, что оно выступает не только инструментом влияния, но и само воздействует на более традиционные пространства межгосударственного взаимодействия [Sheldon 2014]. Более того, деятельность в киберпространстве обходится значительно дешевле, чем в других политических пространствах. Это обусловливается доступностью информационно-коммуникационных технологий и воспроизводимостью данных, находящихся в киберпространстве, что в значительной мере усложняет возможность уничтожения кибероружия или элементов влияния, таких как пропагандистские вебсайты и др. [Sheldon 2011]. Сайт может быть заблокирован или удален, однако нет никаких гарантий, что через пару часов он не появится во всемирной сети по новому адресу. КНР как одна из наиболее влиятельных стран в мире в значительной мере обеспокоена обеспечением «информационной безопасности». Это обусловлено тем, что ее родной регион стал полем для информационных столкновений [Кошурникова 2016].

Си Цзиньпин после своего вступления в должность Председателя КНР стал уделять особое внимание проблемам информационной безопасности. По итогам XVIII съезда КПК была выдвинута стратегия «Сильного сетевого государства», которая подразумевает не только обеспечение кибербезопасности страны, но и использование сетевого потенциала для развития национальной экономики. В настоящее время именно информационные технологии стали главным драйвером развития экономики КНР [Fei 2011: 186]. В апреле 2018 г., выступая на Национальной конференции по кибербезопасности и информатизации, Си Цзиньпин отметил, что Китай неизменно следует собственному пути регулирования сети Интернет и движется к цели становления «сильным сетевым государством»[1]. Это говорит о том, что руководство КНР уделяет особое внимание данной сфере и пытается использовать все возможные методы для повышения сетевого потенциала государства.

## Основы информационной политики КНР

КНР обладает всеми необходимыми условиями для становления «сильным сетевым государством», для этого у нее есть и ресурсы, и эффективная система государственных институтов. На данный момент Китай является крупнейшим в мире интернет-сообществом, количество активных пользователей внутри страны составляет 854 млн человек[2], что больше, чем количество пользователей в США и ЕС одновременно. Однако необходимо учитывать, что в процентном соотношении лишь 60,1 % жителей КНР являются пользователями Интернета, а остальные 39,9 % потенциально могут получить доступ к всемирной сети в ближайшее время. Кроме того, Китай обладает уникальным сетевым ландшафтом, на котором доминируют исключительно национальные компании. Это связано с очень жесткой цензурой со стороны китайского законодательства. Многие интернет-ресурсы, которые занимают большую часть западного рынка, не имеют доступа к китайскому Интернету.

Фундаментом для проведения информационной политики КНР выступают: правительственные концепции и инициативы, направленные на комплексное развитие ИТ-сферы в КНР, начиная с производства инновационного оборудования и заканчивая созданием современного программного обеспечения; представители крупного бизнеса в ИТ-сфере, которые слишком влиятельны на внутреннем рынке и не позволяют выйти на него

[1] Xijinping: Zizhu chuangxin tuijin wangluo qiangguo jianshe. 2018-04-21 [Выступления Председателя КНР Си Цзиньпина на Национальной конференции по кибербезопасности и информатизации 20—21 апреля 2018 г.] (на китайском языке) // Xinhuanet. URL: http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm (дата обращения: 05.01.2019).

[2] Asia Internet use, population data and Facebook statistics // Internet World Stats. URL: https://www.internetworldstats.com/stats3.htm (accessed: 08.01.2020).

новым игрокам; эффективные системы контроля Интернета, которые выступают своеобразным барьером для внешних акторов, стремящихся получить доступ к китайскому рынку. Новые технологии, такие как искусственный интеллект, облачные вычисления и анализ больших объемов данных (big data), при использовании сети 5G позволят придать новый импульс развитию информационно-коммуникационных технологий через внедрение систем умных городов, «Интернета вещей» и т. д. [Hong, Harwit 2020].

В 2010 г. Информационное бюро Государственного совета КНР опубликовало «Белую книгу» по основным положениям политики КНР в отношении регулирования Интернета. В данном документе уделялось особое внимание следующим направлениям: популяризации и распространению Интернета среди населения, повышению уровня доступности Интернета, гарантированию прав и свобод в интернет-пространстве, управлению Интернетом, обеспечению кибербезопасности и международного сотрудничества в этой области[3].

Следует отметить, что впервые китайское правительство поставило вопросы обеспечения информационной и кибербезопасности в один ряд с национальной безопасностью страны, был введен в оборот термин «Интернет-суверенитет». Таким образом, Китай обозначил исключительное право на регулирование своей внутренней сети, что было сделано ввиду усиления влияния внешних акторов — это касалось не только отдельных государств, таких как США, но и негосударственных структур [Lewis 2017]. Интернет-суверенитет необходим для того, чтобы в процессе развития цифровой среды можно было сконцентрироваться на вопросах материального благополучия и справедливого развития, не останавливаясь на вопросах обеспечения безопасности, конфиденциальности и борьбы за управление интернетом [Hong, Goodnight 2020].

Для реализации своей информационной политики КНР начала создавать современную технологическую базу. Для обеспечения себе лидерства в ИТ-сфере в 2016 г. в КНР приняли «Национальную стратегию информатизации и развития». Данная стратегия подразумевает, что к 2020 г. китайские технологии достигнут мирового уровня и будут конкурентоспособными на мировом рынке; к 2025 г. должна быть построена международная сеть мобильной связи, которая будет обеспечиваться передовыми технологиями и программным обеспечением, что позволит КНР повысить конкурентоспособность своей экономики и решить вопросы кибербезопасности; к середине XXI в. КНР должна стать «сильным сетевым государством» и оказывать значительное влияние на процесс информатизации во всем мире, опираясь на концепцию социализма с китайской спецификой[4]. Таким образом, Китай нацелен на лидерство как в сфере производства высокотехнологичной продукции, так и в сфере создания современного программного обеспечения. Данная стратегия объединила в себе идеи, которые были заложены в стратегических инициативах «Интернет плюс» и «Делай в Китае — 2025».

На данный момент на долю Китая приходится около 50 % всех интернет-платежей в мире и три четверти мирового рынка интернет-кредитования. Успех информационной политики КНР во многом был обеспечен популярностью смартфонов среди китайских пользователей, которые предпочитают пользоваться интернет-ресурсами через мобильные устройства[5]. Интернет стал основным пространством как для частного общения, так и для ведения бизнеса, а благодаря протекци-

[3] The Internet in China // Information Office of the State Council of the People's Republic of China. URL: http://www.scio.gov.cn/zxbd/nd/2010/Document/667385/667385.htm (accessed: 05.01.2019).

[4] Zhonggong zhongyang bangong ting guowuyuan bangong ting yinfa "guojia xinxi hua fazhan zhanlue gangyao" [Национальная стратегия информатизации и развития КНР] (на китайском языке) // Сайт Государственного совета КНР. URL: http://www.gov.cn/zhengce/2016-07/27/content_5095336.htm (дата обращения: 06.01.2019).

[5] Lee J. The rise of China's tech sector: The making of an internet empire // The Interpreter. 2015. URL: https://www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-making-internet-empire (accessed: 07.01.2019).

онистской политике китайского правительства и жесткой интернет-цензуре на внутреннем китайском рынке доминируют исключительно китайские компании, такие как Alibaba, Tencent и Baidu. Эти цифровые гиганты стараются занять возможные секторы рынка цифровых услуг посредством создания приложений и агрессивно вытесняют конкурентов.

Такое положение на китайском интернет-рынке называют «Троецарствием» по аналогии с классическим китайским романом XIV в.[6] Под «тремя царствами» подразумевают: Baidu, которая лидирует в поисковом сегменте (его часто называют «китайским Google»), Alibaba, которая контролирует сегмент электронной коммерции и постоянно увеличивает количество функционирующих площадок, а Tencent является лидером в области социальных медиа, владея крупнейшей в Китае социальной сетью WeChat и большим количеством платформ, предоставляющих развлекательные услуги. В таких условиях у зарубежных компаний нет возможности выйти на китайский рынок — их останавливает необходимость конкурировать с уже устоявшимися лидерами на рынке цифровых услуг и сложность адаптации к китайским законам и условиям ведения бизнеса. В то же время разделение рынка между несколькими крупными компаниями означает, что государству достаточно контролировать несколько компаний для эффективного управления большинством процессов в сети [Creemers 2017: 95].

Таким образом, КНР, поддерживая свои технологические стартапы и проводя политику жесткой интернет-цензуры, фактически изолировала свой внутренний рынок от иностранного вмешательства. Такие мировые гиганты, как Google, Facebook и Amazon не имеют прямого доступа к китайскому рынку. В первые годы после начала активных блокировок на территории Китая стали популярны VPN-сервисы (Virtual Private Network — виртуальная частная сеть), которые позволяли обойти запрет, используя специализированное программное обеспечение, но на данный момент сервисы обхода цензуры запрещены и полиция активно борется с использованием подобных приложений.

Для китайских компаний, лидирующих в сфере информационных технологий, приоритетным направлением является экспорт своих товаров и услуг для расширения своего влияния в мире. И в то время, когда США и страны Европы относятся с опасением к приобретению товаров и услуг, связанных с обеспечением информационной безопасности, развивающиеся страны в большинстве своем не разделяют эту точку зрения, особенно принимая во внимание, что Китай предлагает более выгодные условия и гарантии [Cheung 2018].

## Система обеспечения информационной безопасности КНР

В целях реализации своей информационной политики КНР необходимо обеспечить информационную безопасность. В «Национальной стратегии безопасности в киберпространстве КНР» информационная безопасность определяется как залог политической стабильности в стране. И для ее обеспечения необходимо защититься от любых видов вмешательства в политическую, социальную и культурную жизнь государства. Данная стратегия подразумевает не только деятельность, направленную на обеспечение кибербезопасности страны, но и на защиту законных прав своих граждан в сети Интернет[7]. В большинстве стран мира кибербезопасность достигается за счет безопасности компьютеров, сетей и данных, однако в Китае больший акцент делается именно на информационную безопасность [Heinl 2017: 139].

Китаю для обеспечения кибербезопасности необходимо добиться превосходства

[6] Yuan B.L. Kingmakers of China's Internet: Baidu, Alibaba and Tencent // Wall Street Journal. 21.10.2015. URL: https://www.wsj.com/articles/kingmakers-of-chinas-internet-baidu-alibaba-and-tencent-1445451143 (accessed: 07.01.2019).

[7] "Guojia wangluo kongjian anquan zhanlue" quanwen. 2016-12-27 [Национальная стратегия безопасности в киберпространстве] (на китайском языке) // Xinhuanet. URL: http://www.xinhuanet.com/politics/2016-12/27/c_1120196479.htm (дата обращения: 06.01.2019).

в производстве высокотехнологичного оборудования и вычислительных мощностей.

В 2016 г. было завершено строительство квантовой коммуникационной линии Пекин — Шанхай, которая, по заявлениям главы проекта профессора Пан Цзяньвэя, является устойчивой к хакерским атакам[8]. Основными спонсорами этого проекта выступили Центральный военный совет КНР и Торгово-промышленный Банк Китая (ICBC)[9]. Задача данной коммуникационной линии — обеспечить бесперебойную передачу зашифрованных данных.

Больших успехов КНР достигла и в рамках создания суперкомпьютеров — на сегодняшний день страна обладает наибольшим их количеством в мире (228 машин). Среди них «Тяньхэ» (Tianhe–1A), созданный Оборонным научно-техническим университетом Народно-освободительной армии Китая (НОАК) и остававшийся самым мощным суперкомпьютером с 2013 по 2015 г. В 2018 г. он был обновлен до версии «Тяньхэ–2» (Tianhe–2A) и сегодня занимает четвертое место в глобальном рейтинге. Необходимо отметить, что третье место в рейтинге принадлежит также китайскому суперкомпьютеру «Санвэй» (Sunway TaihuLight), который находится в Национальном центре суперкомпьютеров в г. Уси. На ноябрь 2019 г. из 500 самых мощных суперкомпьютеров мира в КНР находятся 45,6 %[10]. Таким образом, КНР уже обеспечила себе определенное лидерство в области цифровых технологий, создав все необходимое программное обеспечение для функционирования данного оборудования.

Подготавливая технологическую базу для обеспечения своей информационной безопасности, в Китае параллельно создается структура сотрудничества между государственными и негосударственными структурами для эффективного реагирования на все новые тенденции в киберпространстве.

Высшее руководство информационной политикой выполняет Центральный Военный Совет, кроме того, в данном процессе задействованы профильные министерства, такие как Бюро общественной информации и надзора за сетевой безопасностью, Министерство общественной безопасности, Министерство науки и технологий КНР и другие узконаправленные правительственные институты. Ключевым отличием от большинства стран мира является то, что в Китае большое влияние на реализацию информационной политики оказывает Коммунистическая партия Китая. Координирующую роль играет Центральная комиссия по киберпространству, в которую входят председатель КНР Си Цзиньпин, премьер Государственного совета КНР Ли Кэцян и главы профильных министерств и комиссий.

Главным государственным проектом в сфере обеспечения информационной безопасности является проект «Золотой щит». За его реализацию отвечает Бюро общественной информации и надзора за сетевой безопасностью. «Золотой щит» — это один из ведущих проектов КНР в области создания электронного правительства. За счет регулирования информации и создания благоприятного информационного фона данный проект позволяет повысить осведомленность граждан о назначении электронного правительства и улучшить их общее мнение на счет подобных инициатив [Wang, Lai 2015]. Поддержка населения страны обусловливает создание безопасного и благоприятного климата в киберпространстве КНР, который потенциально будет способствовать развитию всех отраслей социально-экономической жизни Китая.

Говоря об участии негосударственных структур в процессе регулирования киберпространства, стоит упомянуть о сотрудничестве правительства КНР с такими компаниями, как Huawei, Venustech, Qihu 360, Leadsec и Westone. Ресурсы данных компаний используются для обеспечения информационной

[8] Zhihao Z. Beijing-Shanghai quantum link a “new era” // China Daily. 30.09.2017. URL: http://www.chinadaily.com.cn/china/2017-09/30/content_32669593.htm (accessed: 10.01.2019).

[9] Moore M. China builds computer network impenetrable to hackers // The Telegraph. November 07, 2014. URL: https://www.telegraph.co.uk/news/worldnews/asia/china/11216766/China-builds-computer-network-impenetrable-to-hackers.html (accessed: 10.01.2019).

[10] TOP500 official website. URL: https://www.top500.org (accessed: 08.01.2020).

безопасности во время проведения крупномасштабных политических, экономических, культурных и спортивных мероприятий на территории КНР, что уже является одним из итогов действующего политического курса на информатизацию [Разумов 2017]. За счет сотрудничества с частными компаниями НОАК получает доступ к передовым разработкам в области ИКТ. Таким образом, развитие собственного инновационного потенциала рассматривается как одно из средств обеспечения кибербезопасности страны [Ибрагимова 2013: 181].

Обратной стороной такого сотрудничества становится недоверие к китайским технологическим компаниям в мире, что повсеместно становится причиной запрета их продукции в США, Австралии и странах Европы [Segal 2017: 18]. Необходимо отметить, что компания Huawei в 2016 г. представила «Белую книгу по кибербезопасности», которая потенциально может стать ориентиром развития других стран и компаний в данной области. Приоритетами развития эксперты Huawei считают понимание основных угроз глобальной цепи производства, исходящих из киберпространства, понимание и умение идентифицировать и устранить угрозу, а также создание внутренних и внешних структур для обеспечения работы всей системы[11].

Одним из элементов системы кибербезопасности должен стать эффективный файрволл (firewall), который будет обеспечивать безопасность внутри системы и от внешних угроз. Если переложить китайскую концепцию «гармоничного мира» на киберпространство, то ситуация, где все государства будут использовать единые протоколы защиты и станут участниками общего международного соглашения по нормам и правилам поведения в киберпространстве, полностью соответствовала бы данной концепции.

[11] Huawei Cyber Security White Paper // Huawei. June 2016. URL: https://www.huawei.com/en/about-huawei/cyber-security/whitepaper/huawei-cyber-security-white-paper-2016 (accessed: 11.01.2019).

## Внешняя информационная безопасность КНР

Еще одним важным аспектом обеспечения информационной безопасности КНР является обеспечение внешней безопасности страны. В свете роста экономики и влияния Китая в мире появляется все больше вопросов международной повестки дня, где сталкиваются интересы какого-либо государства и КНР. В последнее время обострились трения между КНР и США. В частности, одной из причин ухудшения отношений стали именно вопросы кибербезопасности и защиты интеллектуальной собственности. Это связано в том числе и с тем, что наиболее уязвимыми секторами экономики для кибератак являются финансовый сектор и сфера информационных технологий (ИКТ), в это же время развитие этих секторов повышает уровень готовности противостоять угрозам, исходящим из киберпространства [Makridis, Smeets 2019]. Именно поэтому Китай идет по пути создания максимально самодостаточной и защищенной информационной среды внутри страны, которая позволила бы защитить уязвимые сектора экономики от кибератак.

Разоблачения бывшего сотрудника ЦРУ Э. Сноудена в 2013 г. стали стимулом к активному развитию кибербезопасности в Китае [Schia, Gjesvik 2017: 3]. В частности, квантовая коммуникационная линия, о которой говорилось ранее, является одним из элементов данной системы. Политические круги и народ Китая резко негативно отреагировали на подобные действия со стороны США, что позволило китайскому правительству пойти на более решительные меры: был расширен штат сотрудников, занимающихся ручным фильтрованием информации в китайском Интернете, а также началось активное совершенствование компонентов искусственного интеллекта (ИИ-компонентов) «Золотого щита».

Таким образом, фильтрация информации происходит на трех уровнях:

— первый уровень — блокирование крупных внешних ресурсов, таких как крупные социальные медиа, новостные и прочие

электронные ресурсы, которые не согласны сотрудничать с правительством КНР, не соблюдают законы страны или в негативном свете представляют политику КНР и КПК. Его также называют «Великий китайский файрволл»;

— второй уровень — ИИ-алгоритмы, которые осуществляют мониторинг всех типов контента на предмет соответствия законодательству страны и осуществляют его оперативную блокировку;

— третий уровень — ручной мониторинг контента в сети Интернет работниками Бюро общественной информации и надзора за сетевой безопасностью.

Кроме того, некоторые западные исследователи приписывают КНР создание так называемой «50-фэневой армии» (wumaodan) — группы людей или ботов, которые занимаются публикацией проправительственной информации и дискредитацией пользователей, публикующих антиправительственный контент. Предполагается, что к участию в данном проекте привлекаются журналисты, блогеры и прочие медийные личности [King, Pan, Roberts 2017]. Работая над национальным файрволлом, Китай сталкивается с необходимостью сохранения баланса в отношении регулирования иностранного присутствия в китайском интернет-пространстве. Дилемма заключается в необходимости выбора между уменьшением идеологического контроля внутри страны или уменьшением возможностей для международного экономического сотрудничества [Lindsay 2015: 19].

Принимая во внимание все риски и возможности, КНР создает благоприятный информационный климат внутри страны и не дает воздействовать на него извне, в частности, тщательно фильтруются любые статьи и высказывания по поводу таких чувствительных для Китая вопросов, как Тайвань, Тибет и территориальные споры в Южно-Китайском море (ЮКМ). А в связи с началом торговой войны с США и продолжающимся информационным противостоянием между странами роль обеспечения кибербезопасности во внешней политике КНР возросла. Соперничество КНР и США ускоряет процесс милитаризации киберпространства, что становится причиной увеличения напряженности и вовлечения новых акторов в гонку вооружений в киберпространстве, создавая угрозу для сети Интернет, которая имеет существенное значение для развития глобализации [Антипов 2013: 43].

Американские исследователи воспринимают КНР как угрозу для США в киберпространстве. В докладе Центра стратегических и международных исследований (CSIS) говорится, что с 2006 г. Китай выступал агрессором в киберпространстве в 108 инцидентах в то время, когда на него было совершено всего 25 нападений, в свою очередь США выступали агрессором только в 9 случаях, а жертвой агрессии — в 117 случаях[12]. Необходимо отметить, что в данном случае имеется в виду общее количество инцидентов, а не только те, в которых задействованы США и КНР. Однако на основе данной информации можно сделать выводы, что Китай ведет агрессивную политику в киберпространстве и предпочитает наступательные действия. Учитывая, что данный аналитический центр предоставляет материалы правительству США, скорее всего, именно такой позиции придерживаются правящие круги в Вашингтоне.

Китайские специалисты, в свою очередь, считают, что агрессором выступают именно США: в частности, они утверждают, что США используют киберпространство для усиления своей гегемонии в мире и давления на Китай за счет ухудшения политической ситуации вокруг тем Тайваня, Тибета, Синьцзян-Уйгурского автономного района и спорных территорий в Южно-Китайском море[13]. Говоря о подобных инцидентах, необходимо помнить о сложности быстрого определения агрессора в киберпространстве,

[12] Significant Cyber Incidents // CSIS. URL: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity (accessed: 12.01.2019).

[13] Saalman L. New domains of crossover and concern in cyberspace // Stockholm International Peace Research Institute. July 26, 2017. URL: https://www.sipri.org/commentary/topical-backgrounder/2017/new-domains-crossover-and-concern-cyberspace (accessed: 20.01.2019).

поэтому на данный момент проблема атрибуции[14] стоит наиболее остро [Manson 2011].

Одним из способов косвенного определения агрессора является поиск государства, для которого результаты кибератаки наиболее выгодны, но никаких гарантий такой подход не дает. Если обратиться к общедоступным данным, то чаще всего появляются данные об атаках, в которых может быть заинтересована КНР. Речь идет о ряде кибератак на структуры, связанные с территориальными спорами КНР в ЮКМ. Наиболее примечательной является DDoS-атака на сайт Международного трибунала в Гааге в 2015 г., когда проходили слушания по делу Филиппин против Китая по вопросу регулирования территориальной принадлежности ряда островов в ЮКМ[15].

В свою очередь, КНР неизменно выступает за усиление роли ООН в урегулировании конфликтных ситуаций в рамках киберпространства. КНР была в числе государств, которые выступали за принятие международного документа о взаимном отказе от кибератак на стратегическую инфраструктуру. Здесь Китай солидарен с проектом конвенции, который был выдвинут Россией. Сущность данного проекта заключается во всеобъемлющем сотрудничестве стран мира по вопросу предупреждения преступлений в сфере высоких технологий. Однако данный проект столкнулся с резкой критикой со стороны США и ЕС, и на данный момент невозможность договориться и найти компромисс тормозит процесс принятия данной конвенции [Ватрушкин 2017].

КНР на данный момент способна в полной мере обеспечить свою кибербезопасность за счет наличия полного спектра необходимых для этого технологий, институтов и нормативно-правовой базы. Согласно китайскому законодательству, право регулировать Интернет на территории КНР имеют только китайские государственные структуры. Положения относительно регулирования Интернета в КНР сформулированы в «Законе КНР о безопасности сети Интернет», принятом в 2016 г. Там же отмечается, что все аспекты сетевой информации, касающиеся военной сферы, регулируются Центральным военным советом[16].

В высшем руководстве КНР ставят в один ряд понятия национальной и кибербезопасности, что неоднократно было отмечено в речах председателя КНР Си Цзиньпина. Проект «Золотой щит» является эффективным инструментом защиты от внешних информационных угроз, а также позволяет вести надзор за всем контентом, публикуемым на просторах китайского киберпространства. Вместе с этим, по некоторым данным, правительство КНР спонсирует деятельность групп лиц, публикующих контент, популяризирующий текущий политический курс. В этом процессе помимо обычных пользователей задействованы популярные медийные личности, блогеры, представители науки и культуры, которых можно охарактеризовать как «лидеров мнений» (Key Opinion Leaders).

На уровне технологий Китай спонсирует создание внутренней защищенной сети на основе квантового шифрования: первый участок — квантовая коммуникационная линия Пекин — Шанхай уже была введена в эксплуатацию. Также правительство активно сотрудничает с крупными компаниями-производителями высокотехнологичных продуктов внутри страны, а также с представителями

[14] Атрибуция кибератаки — совокупность технических методов и организационных мероприятий с целью установления злоумышленника или преступной группировки, стоящей за кибератакой или вредоносной кампанией. Обычно процесс атрибуции состоит из работы ИБ-специалистов, изучающих следы киберпреступления и выполняющих технический анализ взлома, а также следственных действий, проводимых правоохранительными органами на основании выводов аналитиков (Атрибуция кибератаки // Энциклопедия «Касперского». URL: https://encyclopedia.kaspersky.ru/glossary/cyber-attribution/ (дата обращения: 06.03.2019)).

[15] Tweed D. Chinese Hackers Hit U.S. Firms Linked to South China Sea Dispute // Bloomberg. March 16, 2018. URL: https://www.bloomberg.com/news/articles/2018-03-16/china-hackers-hit-u-s-firms-linked-to-sea-dispute-fireeye-says (accessed: 15.01.2019).

[16] Zhonghua renmin gongheguo wangluo anquan fa [Закон КНР о безопасности сети Интернет] (на китайском языке) // Офис комиссии по киберпространству КНР. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата обращения: 06.01.2019).

самых крупных социальных медиа в стране не только для контроля над Интернетом, но и для стимулирования развития экономики.

Вместе с тем очевидно, что КНР обладает и наступательным потенциалом в киберпространстве. Косвенными подтверждениями этого являются доклады западных аналитических центров по поводу сетевых атак на структуры, деятельность которых отвечает национальным интересам КНР; на уровне международного взаимодействия КНР выступает за создание единого международно-правового документа, регулирующего эту область, в котором будут учтены интересы всех стран на основе равенства и взаимности. Такой подход полностью отвечает концепции «гармоничного мира», которая является одной из доминирующих в курсе нынешнего поколения лидеров КНР.

Основным же соперником КНР в киберпространстве являются США. Корень противостояния лежит в изначально разном понимании того, что такое информационная безопасность и кибербезопасность. В США и Европе обычно используют термин «кибербезопасность» и уделяют больше внимания вопросам безопасности технической составляющей Интернета, в то время как в Китае ключевое внимание уделяется информационной безопасности — регулированию контента в рамках национальной сети и контролю за ее поступлениями извне [Булавин 2014]. Соперничество США и КНР в киберпространстве — это фактически борьба за лидерство в глобальной информационной среде, которая не ограничивается каким-либо одним аспектом и носит комплексный характер [Mori 2019].

## Заключение

Проведенный анализ позволяет сделать следующие выводы относительно современной информационной политики КНР.

1. Основная задача информационной политики Китая заключается в построении «сильного сетевого государства». Для этого необходимо обеспечить лидерство КНР как в производстве высокотехнологического оборудования, так и современного программного обеспечения для его функционирования. К настоящему моменту Китай уже занимает лидирующие позиции по данным показателям, в частности, он является обладателем мощных суперкомпьютеров «Тяньхэ–2» и «Санвэй», которые занимают третье и четвертое место в глобальном рейтинге, а также обладателем самого большого количества суперкомпьютеров в мире.

2. Перед правительством Китая, стремящегося стать «сильным сетевым государством», возникает задача создания благоприятных условий для развития национальной экономики за счет построения эффективной системы регулирования Интернета внутри страны и его защиты от внешнего воздействия. Для этого правительством КНР были созданы специализированные ведомства, приняты национальные стратегии развития и обеспечения безопасности в киберпространстве и выработана четкая позиция по вопросу международного регулирования киберпространства. Кроме того, был налажен диалог с крупнейшими национальными технологическими корпорациями.

3. Лидирующие позиции на китайском рынке цифровых услуг занимают три компании: Baidu, Tencent и Alibaba. Они ведут агрессивную политику в отношении других компаний на рынке, что в значительной мере усложняет процесс выхода иностранных компаний на китайский рынок. В то же время в Китае были воссозданы национальные аналоги всех необходимых сервисов для создания цифровой экономики, что говорит о позитивном влиянии таких действий.

4. Особое место в информационной политике КНР занимает информационная безопасность. В китайском понимании это означает одновременно и защиту ключевой инфраструктуры от кибератак, и фильтрацию контента в рамках внутренней сети. Во многом противоречия КНР и других стран мира связаны с тем, что Китай настаивает на исключительном праве на регулирование Интернета на территории страны, активно использует цензуру для фильтрации контента, запрещенного законодательством КНР и представляющего угрозу для имиджа страны и правящей партии.

5. Основным конкурентом КНР за лидерство в киберсфере являются США. Страны неоднократно обвиняли друг друга в кибершпионаже и атаках на внутреннюю инфраструктуру. После начала «торговой войны» ситуация только ухудшилась, и на данный момент не предвидится подписания какого-либо документа, регулирующего действия стран в киберпространстве.

КНР обладает всеми необходимыми ресурсами для использования цифровых технологий для стимулирования внутреннего развития и решения своих задач как во внутренней, так и во внешней политике. Определенные успехи информационной политики мы уже можем наблюдать, однако более отчетливо говорить о ее результатах можно будет после завершения ее первого этапа в 2025 г.

Поступила в редакцию / Received: 10.03.2020
Принята к публикации / Accepted: 25.04.2020

## Библиографический список

*Антипов К.В.* Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. 2013. № 6. С. 39—54.

*Булавин А.В.* О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. 2014. № 1. С. 27—31.

*Ватрушкин А.А.* Правовые основы обеспечения кибербезопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. Т. 31. № 6. С. 78—84.

*Ибрагимова Г.Р.* Стратегия КНР в киберпространстве: вопросы управления интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. Т. 6. № 19. С. 169—184.

*Кошурникова Н.А.* Особенности информационной политики современного Китая // Китай: история и современность: материалы IX международной научно-практической конференции «Китай: история и современность» 22—23 октября 2015. Екатеринбург: Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, 2016. С. 279—284.

*Разумов Е.А.* Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. Т. 98. № 4. С. 156—170.

*Cheung T.M.* The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities // Journal of Cyber Policy. 2018. Vol. 3. Iss. 3. P. 306—326. DOI: 10.1080/23738871.2018.1556720

*Creemers R.* Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century // Journal of Contemporary China. 2017. Vol. 26. Iss. 103. P. 85—100. DOI: 10.1080/10670564.2016.1206281

*Ebert H., Maurer T.* Contested Cyberspace and Rising Powers // Third World Quarterly. 2013. Vol. 34. Iss. 6. P. 1054—1074. DOI: 10.1080/01436597.2013.802502

*Fei G.* China's Cybersecurity Challenges and Foreign Policy // Georgetown Journal of International Affairs. International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity. 2011. P. 185—190.

*Heinl C.H.* New Trends in Chinese Foreign Policy: The Evolving Role of Cyber // Asian Security. 2017. Vol. 13. Iss. 2. P. 132—147. DOI: 10.1080/14799855.2017.1286160

*Hong Y., Harwit E.* China's Globalizing Internet: History, Power, and Governance // Chinese Journal of Communication. 2020. Vol. 13. Iss. 1. P. 1—7. DOI: 10.1080/17544750.2020.1722903

*Hong Y., Goodnight G.T.* How to Think about Cyber Sovereignty: The Case of China // Chinese Journal of Communication. 2020. Vol. 13. Iss. 1. P. 8—26. DOI: 10.1080/17544750.2019.1687536

*King G., Pan J., Roberts M.* How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument // American Political Science Review. 2017. Vol. 111. Iss. 3. P. 484—501.

*Lewis D.* China's Global Internet Ambitions: Finding Roots in ASEAN // ICS Occasional Papers. 2017. No. 14. P. 1—28.

*Lindsay J.R.* The Impact of China on Cybersecurity: Fiction and Friction // International Security. 2015. Vol. 39. No. 3. (Winter 2014/15). P. 7—47.

*Makridis C.A., Smeets M.* Determinants of Cyber Readiness // Journal of Cyber Policy. 2019. Vol. 4. Iss. 1. P. 72—89. DOI: 10.1080/23738871.2019.1604781

*Manson G.P*. Cyberwar: The United States and China Prepare For the Next Generation of Conflict // Comparative Strategy. 2011. Vol. 30. No. 2. P. 121—133. DOI: 10.1080/01495933.2011.561730

*Mori S.* US Technological Competition with China: The Military, Industrial and Digital Network Dimensions // Asia-Pacific Review. 2019. Vol. 26. No. 1. P. 77—120. DOI: 10.1080/13439006.2019.1622871

*Nye J.S. Jr*. Nuclear Lessons for Cyber Security // Strategic Studies Quarterly. 2011. Vol. 5. Iss. 4. P. 9—20.

*Segal A.* Chinese Cyber Diplomacy in a New Era of Uncertainty // Hoover Institution, Aegis Paper Series. 2017. Vol. 1703. P. 1—23.

*Schia N.N., Gjesvik L.* China's Cyber Sovereignty // Norwegian Institute of International Affairs Policy Brief Series. 2017. Vol. 2. P. 1—4.

*Sheldon J.B*. Deciphering Cyberpower: Strategic Purpose in Peace and War // Strategic Studies Quarterly. 2011. Vol. 5. Iss. 2. P. 95—112.

*Sheldon J.B*. Geopolitics and Cyber Power: Why Geography Still Matters // American Foreign Policy Interests. 2014. Vol. 36. No. 5. P. 286—293. DOI: 10.1080/10803920.2014.969174

*Wang F., Lai M.* Woguo dianzi zhengwu fazhan xianzhuang yu duice yanjiu [Исследование о современном состоянии и мерах развития электронного правительства Китая] // Renwen. 2015. No. 15. P. 198 (на кит. яз.).

## References

Antipov, K.V. (2013). Cyber Conflict in Sino-US Relations and the Search for Dialogue. *The Far Eastern Affairs*, 6, 39—54. (In Russian).

Bulavin, A.V. (2014). Concerning Approaches of the USA and China to Cybersecurity. *Society: Politics, Economics, Law*, 1, 27—31. (In Russian).

Cheung, T.M. (2018). The Rise of China as a Cybersecurity Industrial Power: Balancing National Security, Geopolitical, and Development Priorities. *Journal of Cyber Policy*, 3 (3), 306—326. DOI: 10.1080/23738871.2018.1556720

Creemers, R. (2017). Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century. *Journal of Contemporary China*, 26 (103), 85—100. DOI: 10.1080/10670564.2016.1206281

Ebert, H. & Maurer, T. (2013). Contested Cyberspace and Rising Powers. *Third World Quarterly,* 34 (6), 1054—1074. DOI: 10.1080/01436597.2013.802502

Fei, G. (2011). China's Cybersecurity Challenges and Foreign Policy. *Georgetown Journal of International Affairs. International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity*, 185—190.

Heinl, C.H. (2017). New Trends in Chinese Foreign Policy: The Evolving Role of Cyber. *Asian Security*, 13 (2), 132—147. DOI: 10.1080/14799855.2017.1286160

Hong, Y. & Goodnight, G.T. (2020). How to Think about Cyber Sovereignty: The Case of Chin. *Chinese Journal of Communication*, 13 (1), 8—26. DOI: 10.1080/17544750.2019.1687536

Hong, Y. & Harwit, E. (2020). China's Globalizing Internet: History, Power, and Governance. *Chinese Journal of Communication*, 13 (1), 1—7. DOI: 10.1080/17544750.2020.1722903

Ibragimova, G.R. (2013). China's Strategy in Cyberspace: The Issues Internet Governance and Information Security. *Security Index*, 2013, 19 (6), 169—184. (In Russian).

King, G., Pan, J. & Roberts, M. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review*, 111 (3), 484—501.

Koshurnikova, N.A. (2016). Specifics of Information Policy of China. *China: History and the Present. Materials of the IX International Scientific and Practical Conference "China: History and the Present"*, October, 22—23. Yekaterinburg: Ural Federal University named after the first President of Russia B.N. Yeltsin publ. P. 279—284. (In Russian).

Lewis, D. (2017). *China's Global Internet Ambitions: Finding Roots in ASEAN*. ICS Occasional Papers, 14, 1—28.

Lindsay, J.R. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security*, 39 (3), 7—47.

Makridis, C.A. & Smeets, M. (2019). Determinants of Cyber Readiness. *Journal of Cyber Policy*, 4 (1), 72—89. DOI: 10.1080/23738871.2019.1604781

Manson, G.P. (2011). Cyberwar: The United States and China Prepare For the Next Generation of Conflict. *Comparative Strategy*, 30 (2), 121—133. DOI: 10.1080/01495933.2011.561730

Mori, S. (2019). US Technological Competition with China: The Military, Industrial and Digital Network Dimensions. *Asia-Pacific Review,* 26 (1), 77—120. DOI: 10.1080/13439006.2019.1622871

Nye, J.S.Jr. (2011). Nuclear Lessons for Cyber Security. *Strategic Studies Quarterly*, 5 (4), 9—20.

Razumov, E.A. (2017) China's Cybersecurity Policy. *Russia and the Pacific*, 4 (98), 156—170. (In Russian).

Schia, N.N. & Gjesvik, L. (2017). China's Cyber Sovereignty. *Norwegian Institute of International Affairs Policy Brief Series*, 2, 1—4.

Segal, A. (2017). Chinese Cyber Diplomacy in a New Era of Uncertainty. *Hoover Institution, Aegis Paper Series*, 1703, 1—23.

Sheldon, J.B. (2011). Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly*, 5 (2), 95—112.

Sheldon, J.B. (2014). Geopolitics and Cyber Power: Why Geography Still Matters. *American Foreign Policy Interests,* 36 (5), 286—293. DOI: 10.1080/10803920.2014.969174

Vatrushkin, A.A. (2017). The Legal Framework for Cybersecurity of Russian Federation's Critical Infrastructure. *Eurasian Advocacy*, 6 (31), 78—84. (In Russian).

Wang, F. & Lai, M. (2015). Woguo dianzi zhengwu fazhan xianzhuang yu duice yanjiu [Research on the Current Situation and Measures of China's E-Government Development]. *Renwen*, 15, 198. (In Chinese).

**Сведения об авторах:** *Понька Татьяна Ивановна* — кандидат исторических наук, доцент кафедры теории и истории международных отношений Российского университета дружбы народов (e-mail: ponka-ti@rudn.ru).
*Рамич Мирзет Сафетович* — студент кафедры теории и истории международных отношений Российского университета дружбы народов (e-mail: ramich_ms@mail.ru).
*У Юйяо* — аспирант кафедры теории и истории международных отношений Российского университета дружбы народов (e-mail: 6166480@qq.com).

**About the authors:** *Ponka Tatyana Ivanovna* — PhD in History, Associate Professor, the Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University) (e-mail: ponka-ti@rudn.ru).
*Ramich Mirzet Safetovich* — Student, the Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University) (e-mail: ramich_ms@mail.ru).
*Wu Yuyao* — Postgraduate Student, the Department of Theory and History of International Relations, Peoples' Friendship University of Russia (RUDN University) (e-mail: 6166480@qq.com).