

ГОСУДАРСТВО И ОБЩЕСТВО / STATE AND SOCIETY

Архитектура концепции киберсуверенитета КНР (по материалам докладов Всемирной интернет-конференции «Киберсуверенитет: теория и практика»)

© 2023

DOI: 10.31857/S013128120026886-5

Янькова Александра Дмитриевна

Аспирант НИУ ВШЭ, стажер-исследователь Центра комплексных европейских и международных исследований НИУ ВШЭ (адрес: 119017, Москва, ул. Малая Ордынка, д. 17).
ORCID: 0000-0002-7209-9818. E-mail: ayankova@hse.ru

Статья поступила в редакцию 22.06.2023.

Аннотация:

Современный Китай исходит из установки, что без сетевой безопасности невозможна безопасность национальная. Государство выстраивает свою кибердиплотию с опорой на традиционные доминанты внешней политики — неизблемость границ, невмешательство во внутренние дела, уважение суверенитета. Распространение национального суверенитета на цифровую среду естественным образом повлекло за собой создание концепции киберсуверенитета, ставшей неотъемлемой частью китайской «дискурсивной силы» и краеугольным камнем подхода КНР к глобальному управлению Интернетом. Пекин, недовольный нынешним несправедливым, по его мнению, цифровым миропорядком и обеспокоенный необходимостью обеспечения всеобъемлющего контроля над внутренними сетями, выступает за институциональную реформу сложившейся системы глобального управления киберпространством. За последние два десятилетия государство превратилось из реципиента в создателя и пропагандиста кибернорм. Кейсы китайского нормативного предпринимательства привлекают все большее количество сторонников, в первую очередь среди развивающихся стран. Олицетворением конкурентной стратегии КНР на этом направлении стал ряд крупных инициатив, включая Всемирную интернет-конференцию, идею создания «сообщества единой судьбы человечества в киберпространстве» и «Цифровой шелковый путь». Целью этих инициатив является не просто информирование международной аудитории о намерении Китая придерживаться киберсуверенитета во всех внешнеполитических делах, но также они содержат призыв официально закрепить данный принцип в качестве подтверждения права государственных субъектов управлять Интернетом по своему усмотрению. В статье на основе первичных источников предпринята попытка проследить истоки концепции киберсуверенитета КНР, проанализировать ее эволюцию, институциональное оформление, целеполагание, наполнение и ограничения, а также с помощью объектно-ориентированной архитектуры представить ее в виде трехуровневой системы.

Ключевые слова:

Киберсуверенитет, кибербезопасность, кибернормы, управление Интернетом, глобальное управление, Китай.

Благодарности:

Автор выражает благодарность своему научному руководителю Василию Борисовичу Кашину, директору Центра комплексных европейских и международных исследований (ЦКЕ-МИ) НИУ ВШЭ, к.полит.н., за содействие в написании статьи.

Для цитирования:

Янькова А.Д. Архитектура концепции киберсуверенитета КНР (по материалам докладов Всемирной интернет-конференции «Киберсуверенитет: теория и практика») // Проблемы Дальнего Востока. 2023. № 4. С. 99–112. DOI: 10.31857/S013128120026886-5.

Незыблемость границ, уважение суверенитета и невмешательство во внутренние дела — столпы текущей внешней политики Китая — наилучшим образом отвечают его собственным национальным интересам, таким как безопасность, территориальная целостность, экономическое развитие и благоприятная международная обстановка. Кибердипломатия КНР также унаследовала эти принципы. С того момента, как положение о неприкосновенности государственных границ естественным образом распространилось на цифровое пространство, киберсуверенитет стал частью дискурсивной силы Китая.

Исходя из того, что сетевая безопасность является неотъемлемой частью национальной безопасности, КНР считает сохранение киберсуверенитета залогом собственного выживания и независимости внутренней политики. Значение этого вопроса заставляет Китай искать конкурирующую стратегию в подходах к глобальному управлению киберпространством. Китай недоволен нынешним киберпорядком и стремится изменить статус-кво в цифровом пространстве в свою пользу с помощью международной институциональной реформы¹.

Пекин осознает, что нынешнюю мировую «войну ценностей» выиграет тот, кто предложит наиболее привлекательную модель жизни. Страны мирового большинства, чувствительные к идеям неокOLONиализма и желающие быть услышанными, неохотно принимают цифровую гегемонию США и открыты к альтернативам. Выступающий за равенство в киберпространстве и вариативность моделей государственного управления Интернетом Китай готов ее предоставить.

Целью данной статьи является комплексный анализ китайского понимания киберсуверенитета. Предпринята попытка найти истоки концепции, проследить ее эволюцию, выявить целевую аудиторию, институциональное оформление и ограничения, а также при помощи объектно-ориентированной архитектуры визуализировать концепцию в виде трехуровневой системы (рис. 1). Среди первичных источников стержневыми представляются три версии доклада Всемирной интернет-конференции 2019, 2020 и 2021 гг. «Киберсуверенитет: теория и практика», еще не подвергавшиеся сравнительному анализу в научной литературе.

Нормативное регулирование киберсуверенитета КНР

Впервые понятие «киберсуверенитет», или «сетевой суверенитет» (网络主权), появляется в пятой части Белой книги «Состояние Интернета в Китае», опубликованной пресс-канцелярией Государственного совета в 2010 г.² Согласно документу, Китай признает Интернет частью национальной инфраструктуры и подчеркивает свое суверенное право осуществлять над ним юрисдикцию. Вероятно, тогда это было отражением новой политики активной фильтрации негативной информации в Интернете и продолжением кампании против Google³. Новая концепция явилась развитием уже существовавшей на тот момент идеи «информационного суверенитета» (信息主权), предполагающей способ-

¹ 韩瑞霞, 徐剑. 网络主权视域下当前互联网治理的主要问题, 成因及监管对策 [Хань Жуйся, Сюй Цзянь. Основные проблемы, причины и регулятивные контрмеры текущего управления Интернетом с точки зрения киберсуверенитета] // 南京邮电大学学报 (社会科学版). 2020年. 第22期. 第42页.

² 中国互联网状况 (白皮书) [Состояние Интернета в Китае (Белая книга)] // 中国政府网. 08.06.2010. URL: https://www.gov.cn/zhengce/2010-06/08/content_2615774.htm (дата обращения: 07.06.2023).

³ 浅析Google退出中國市場事件 [Краткий анализ ухода Google с китайского рынка] // 國家政策研究基金會. 07.04.2010. URL: <https://www.npf.org.tw/3/7253> (дата обращения: 10.08.2023).

ность страны защищать и контролировать любую информацию на своей территории⁴. Потребность в юридическом закреплении новой концепции на уровне международных институтов была обусловлена растущей гегемонией США и необходимостью поддерживать безопасность внутреннего режима в КНР.

Иллюстрацией конкурирующей стратегии, которую Китай использует в сфере глобального управления киберпространством, и отправной точкой для выхода идеи киберсуверенитета на новый уровень стала Всемирная интернет-конференция. Мероприятие было призвано стать площадкой для продвижения повестки дня Пекина по широкому кругу вопросов, касающихся управления Интернетом, — от кибербезопасности до новых технологий — с упором на сотрудничество и международные обмены⁵.

Конференция была организована Государственной канцелярией интернет-информации КНР, находящейся под прямой юрисдикцией Руководящей группы ЦК КПК по информатизации и безопасности в Интернете. Основным спонсором мероприятия стало государство в лице КПК, хотя финансовую поддержку оказал также ряд международных институтов — Департамент ООН по экономическим и социальным вопросам, Международный союз электросвязи (МСЭ), Всемирная организация интеллектуальной собственности (ВОИС), Всемирная Ассоциация GSM⁶.

На первой Всемирной интернет-конференции 19 ноября 2014 г. Генеральный секретарь ЦК Си Цзиньпин впервые официально объявил миру о китайском видении концепции киберсуверенитета. Он подчеркнул, что тенденции развития информационной эпохи создают новые вызовы для суверенитета и национальной безопасности, которая невозможна без безопасности сетевой⁷.

Мероприятие было рассчитано на международную аудиторию. Среди иностранных участников конференции присутствовали делегаты от Интернет-корпорации по присвоению имен и номеров (ICANN), ведущих хайтек-компаний, включая Microsoft, Facebook⁸, Apple, Intel, Amazon, Samsung и др., правительств иностранных государств, включая Россию⁹. Высокий уровень мероприятия способствовал расширению отраслевой дискуссии с национального уровня до области международного совместного управления, что, вероятно, и было целью Китая с 2010 г.

Однако формальная попытка склонить на свою сторону участников из стран Запада не увенчалась успехом. Проект «Декларации Учжэнь» столкнулся с серьезной критикой и в результате не был ни подписан, ни опубликован. По сообщениям СМИ, в последний день мероприятия о декларации речи не шло. Участники получили текст до-

⁴ 杨泽伟. 国际法析论: 第3版 [Ян Цзэвэй. Анализ международного права: 3-е издание]. 北京: 中国人民大学出版社, 2012年. 第247页.

郭玉军. 网络社会的国际法律问题研究 [Го Юйцзюнь. Исследование международно-правовых проблем в онлайн-сообществе] // 武汉: 武汉大学出版社, 2010年. 第 433 页.

⁵ 郑振宇. 改革开放以来我国互联网治理的演变历程与基本经验 [Чжэн Чжэнью. Эволюция и базовый опыт управления Интернетом в Китае со времен реформ и открытости] // 马克思主义研究, 2019年. 第1期. 第59页.

⁶ Михалевиц Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // Вестник Российского университета дружбы народов. Серия: Политология. 2021. № 2(23). С. 254–264. DOI: 10.22363/2313–1438–2021–23–2–254–264

⁷ 习近平. 让互联网发展成果惠及13亿中国人民 [Си Цзиньпин. Пусть достижения развитого Интернета принесут пользу 1,3 миллиардам китайцев] // 2014世界互联网大会新闻官网. 19.11.2014. URL: http://www.cac.gov.cn/2014–11/19/c_1113314465.htm (дата обращения: 07.06.2023).

⁸ Компания Meta Platforms Inc., реализующая свои продукты – социальные сети Facebook и Instagram, признана экстремистской и запрещена на территории Российской Федерации.

⁹ 2014世界互联网大会新闻官网 [Официальный сайт новостей Всемирной интернет-конференции]. 19.11.2014. URL: <http://www.wicnews.cn/index.shtml> (дата обращения: 07.06.2023).

кумента в распечатанном виде на английском языке только ночью. Многие из делегатов на тот момент уже покинули место проведения конференции. Остальные должны были успеть ознакомиться с текстом и внести изменения до утра. Согласно скриншотам электронной версии документа и китайским источникам, он состоял из девяти пунктов, повторяющих ключевые тезисы позиции КНР¹⁰. Неудача этого эксперимента с нормативным творчеством указывает на то, что Китай на тот момент еще испытывал трудности с использованием многосторонних форматов для продвижения выгодных для себя нормативных изменений.

Вторая по счету конференция прошла под лозунгом важности кибербезопасности на фоне возросшей после терактов в Париже в 2015 г. угрозы экстремизма и связанной с этим всеобщей обеспокоенностью, а также волны обвинений КНР со стороны США в диверсиях и кибершпионаже. Ошибки прошлого года были приняты во внимание — фокус конференции отныне был сосредоточен на проблемах не столько всего международного сообщества, сколько развивающихся стран. Регулярно звучали призывы к борьбе с растущим цифровым неравенством и кибергегемонией, что, вероятно, было замаскированной критикой западноцентричного подхода¹¹.

Си Цзиньпин предоставил более обстоятельную характеристику киберсуверенитета, определив его как принцип суверенного равенства, применяемый к киберпространству и подразумевающий право наций на независимое управление Интернетом. Председатель призвал страны уважать вариативность моделей управления цифровым пространством, включая модель с использованием государственного контроля. Идея киберсуверенитета вновь была тесно привязана к национальной безопасности: с китайской точки зрения киберпространство превратилось в пятую «границу» (新疆域) государства в дополнение к границам сухопутным, морским, воздушным и космическим¹². Тем самым оно расширило сферу государственного управления.

Си Цзиньпин выдвинул «четыре принципа» и «пять предложений» для развития и управления глобальным Интернетом. Киберсуверенитет был поставлен во главу списка как фундаментальный принцип, без которого остальные не будут иметь значения¹³. Данная позиция была подтверждена Международным симпозиумом по кибербезопасности, организованным в 2016 г. совместно Китаем и ООН¹⁴, и рядом документов, включая «Международную стратегию взаимодействия в киберпространстве» (2017), Белые книги «Совместная работа по созданию сообщества единой судьбы в киберпространстве» (2022) и «Киберуправление Китая в новую эпоху на основе верховенства закона» (2023).

¹⁰ China Delivers Midnight Internet Declaration — Offline // *The Wall Street Journal*. November 21, 2014. URL: <https://www.wsj.com/articles/BL-CJB-24963> (дата обращения: 07.06.2023).

¹¹ 乌镇倡议 [Декларация Учжэнь] // 新华网. 18.12.2015. URL: http://www.xinhuanet.com/politics/2015-12/18/c_1117512543.htm (дата обращения: 08.06.2023).

¹² 刘晗, 叶开儒. 网络主权的分层法律形态 [Лю Хань, Е Кайжэ: Иерархическая правовая форма киберсуверенитета] // 华东政法大学学报. 2020年. 第4期. 第80页.

¹³ 习近平在第二届世界互联网大会开幕式上的讲话 (全文) [Выступление Си Цзиньпина на церемонии открытия Второй Всемирной интернет-конференции (полный текст)] // 中国共产党新闻网. 16.12.2015. URL: <http://cpc.people.com.cn/n1/2015/1216/c64094-27937316.html> (дата обращения: 08.06.2023).

¹⁴ 联合国网络安全国际研讨会在北京举行 [Международный симпозиум ООН по кибербезопасности состоялся в Пекине] // 外交部. 11.07.2016. URL: https://www.fmprc.gov.cn/web/wjtb_673085/zjjg_673183/jks_674633/jksxwlb_674635/201607/t20160711_7666933.shtml (дата обращения: 08.06.2023).

Системный взгляд на концепцию киберсуверенитета КНР

Важными вехами стали шестая, седьмая и восьмая Всемирные интернет-конференции 2019, 2020 и 2021 гг., организованные Государственной канцелярией интернет-информации КНР. Мероприятия были посвящены построению «сообщества единой судьбы человечества» в цифровом пространстве и завершили публикацией докладов «Киберсуверенитет: теория и практика» (网络主权: 理论与实践)¹⁵, «Киберсуверенитет: теория и практика (версия 2.0)» (网络主权: 理论与实践 (2.0版))¹⁶, «Киберсуверенитет: теория и практика (версия 3.0)» (网络主权: 理论与实践 (3.0版))¹⁷.

Три версии документа, содержащие исчерпывающую характеристику понятия киберсуверенитета, стали олицетворением попыток КНР впервые его концептуализировать. В данном разделе представлен сравнительный анализ документов, позволивший сформировать максимально полную картину китайского видения концепции киберсуверенитета, представить ее в виде трехуровневой системы и визуализировать с помощью метода построения объектно-ориентированной архитектуры.

Над всеми докладами работали эксперты из Уханьского университета, Китайского института современных международных отношений и Шанхайской академии общественных наук. Во второй и третьей версиях документа список участвующих в его создании организаций расширился за счет Академии общественных наук КНР, Университета Цинхуа, Университета Фудань, Нанкинского университета и Университета международного бизнеса и экономики. В редактировании второй версии доклада приняли участие также представители Ассоциации кибербезопасности Китая, представляющей собой совокупность академических институтов, частных лиц и крупнейших хайтек-компаний страны. В третьей версии доклада представлен список авторов. Примечательно, что среди них присутствует Николас Цагуриас, профессор Шеффилдского университета (Великобритания).

Основной тезис документов состоит в том, что киберсуверенитет — это естественное распространение национального суверенитета на киберпространство. В качестве юридического обоснования приводится Устав ООН, закрепляющий принцип суверенного равенства и являющийся базовой нормой, регулирующей все аспекты современных международных отношений, включая цифровой. Киберсуверенитет распространяется на инфраструктуру информационно-коммуникационных технологий (ИКТ), модели управления, общество, организации, отдельных лиц, а также на все данные и информацию. Границы распространения киберсуверенитета определяются как сухопутными, морскими и воздушными границами государства, так и границами Сети — национального сегмента глобального киберпространства (рис. 1). Несмотря на то, что киберсреда является нематериальным (невещным) пространством, оно функционирует благодаря физической инфраструктуре — сетевому оборудованию, расположенному на территории страны, включая территорию посольств и консульств, и попадающему под ее юрисдикцию¹⁸.

Основополагающие права стран в цифровом пространстве во всех версиях доклада совпадают (рис. 1). Они соответствуют ключевым полномочиям, накладываемым

¹⁵ 网络主权: 理论与实践 [Киберсуверенитет: теория и практика] // 世界互联网大会. 21.10.2019. URL: https://cn.wicinternet.org/2019-10/21/content_36224822.htm (дата обращения: 10.06.2023).

¹⁶ 网络主权: 理论与实践 (2.0 版) [Киберсуверенитет: теория и практика (версия 2.0)] // 世界互联网大会. 15.10.2020. URL: https://cn.wicinternet.org/2020-10/15/content_36225577.htm (дата обращения: 10.06.2023).

¹⁷ 网络主权: 理论与实践 (3.0 版) [Киберсуверенитет: теория и практика (версия 3.0)] // 世界互联网大会. 28.09.2020. URL: https://cn.wicinternet.org/2021-09/28/content_36222995.htm (дата обращения: 10.06.2023).

¹⁸ Ковригин Д.Э. Границы государственного суверенитета национального сегмента киберпространства // *Власть*. 2023. № 1. С. 125. DOI: 10.31171/vlast.v31i1.9473

национальным суверенитетом: независимость, равенство, юрисдикция, самооборона. Расширяясь на киберпространство, они приобретают новое значение. Независимость в сети предполагает право государства функционировать и решать все внутренние вопросы, связанные с Интернетом, без вмешательства внешних сил. Например, формулировать соответствующую политику и законы, создавать организационные структуры и определять операционные модели в соответствии с собственными пожеланиями. Под равенством понимается право стран на равноценное участие в формулировании глобальных норм и стандартов, а также на справедливое распределение цифровых ресурсов, что подразумевает отказ от кибергегемонии. Право осуществлять юрисдикцию подразумевает в данном случае возможность государственного контроля над поступающей и исходящей информацией, включая управление контентом и общественным мнением на сайтах, форумах, блогах, в социальных сетях, а также регулирования поведения пользователей и привлечения их к ответственности.

Право на самооборону в Сети предполагает, что суверенное государство вправе проводить наращивание своего киберпотенциала и принимать законные меры для защиты границ, прав и интересов в киберпространстве от посягательств извне, в частности от распространения вредоносной информации, использования Интернета для осуществления подрывной деятельности, краж и кибертерроризма. Из прав вытекают обязанности, предполагающие невмешательство во внутренние дела и недопущение содействия подобному вмешательству со стороны прочих сил, включая экстремистские и сепаратистские группировки.

Третья версия документа существенно шире предыдущих. В ней впервые появляется пометка о том, что государства могут самостоятельно и по-разному «определять свой суверенитет и представления о пороге его нарушения». Также добавляется новое определение киберсуверенитета как «атрибута международного права» и «юридически обязывающего принципа и правила». Вводится характеристика проявлений суверенитета на разных уровнях киберпространства: физическом, логическом, информационном и социальном. Классификация уровней, вероятно, взята из труда Дэвида Кларка «Характеристика киберпространства: прошлое, настоящее, будущее» (*Characterizing Cyberspace: Past, Present and Future*, 2010)¹⁹.

На физическом уровне суверенитет предполагает право стран на государственное регулирование и защиту своей физической цифровой инфраструктуры, например технологических центров, точек передачи данных, хранилищ данных. На логическом уровне — право принимать и вводить в действие необходимые технические регламенты или стандарты, использовать соответствующее ПО и алгоритмы. На информационном уровне (или уровне контента) — право регулировать распространение контента, хранящегося на территории государства, ограничивать распространение информации, наносящей ущерб безопасности или общественным интересам, запрещать зарубежным организациям фабриковать и искажать факты. На социальном уровне — право осуществлять юрисдикцию над интернет-пользователями и платформами, создавать подходящую социальную среду, поддерживать свою модель управления Интернетом и участвовать в совершенствовании глобальной системы управления киберпространством.

Все документы завершаются разделом «Киберсуверенитет на практике», содержащим эталонные примеры работы КНР над популяризацией идеи киберсуверенитета. В первой версии документа эксперты рассматривают исключительно вклад ООН в обеспечение киберсуверенитета, ссылаясь на отчеты Группы правительственных экспертов от 2013 и 2015 гг. Во второй версии расширяются временные рамки, появляются упоминания Всемирной встречи на высшем уровне по вопросам информационного общества 2003 г., саммита G-20 2015 г. и саммита БРИКС 2016 г. Впервые для подтверждения ки-

¹⁹ Clark D. *Characterizing Cyberspace: Past, Present and Future*. MIT/CSAIL: Political Science Department Press, 2010. P. 15.

тайской позиции используется опыт отдельных стран — ЕС, Вьетнама и России. В качестве подтверждения успешного применения концепции киберсуверенитета на практике Китай приводит вьетнамский закон о кибербезопасности 2018 г., вступивший в силу в этом же году в ЕС Общий регламент по защите данных (принят в 2016 г.) и российский закон о «суверенном Интернете» 2019 г.

Красной нитью через все тексты проходит идея о возможности создания системы обеспечения гарантий киберсуверенитета как на государственном, так и на глобальном уровне. Китай не предлагает конкретных механизмов, но, анализируя международный опыт, рассуждает о том, какие пути могут оказаться эффективными (рис. 1). Помимо технических средств обеспечения информационной безопасности (физических, аппаратных, программных, аппаратно-программных, криптографических) Китай призывает к созданию законодательной базы, институциональных механизмов и воспитанию соответствующих кадров. На внутригосударственном уровне большое значение для КНР имеет реализация Закона о кибербезопасности и связанная с ним нормотворческая деятельность, на глобальном — разработка международного законодательства, касающегося претензий стран на киберсуверенитет, и создание развитой системы диалоговых площадок.

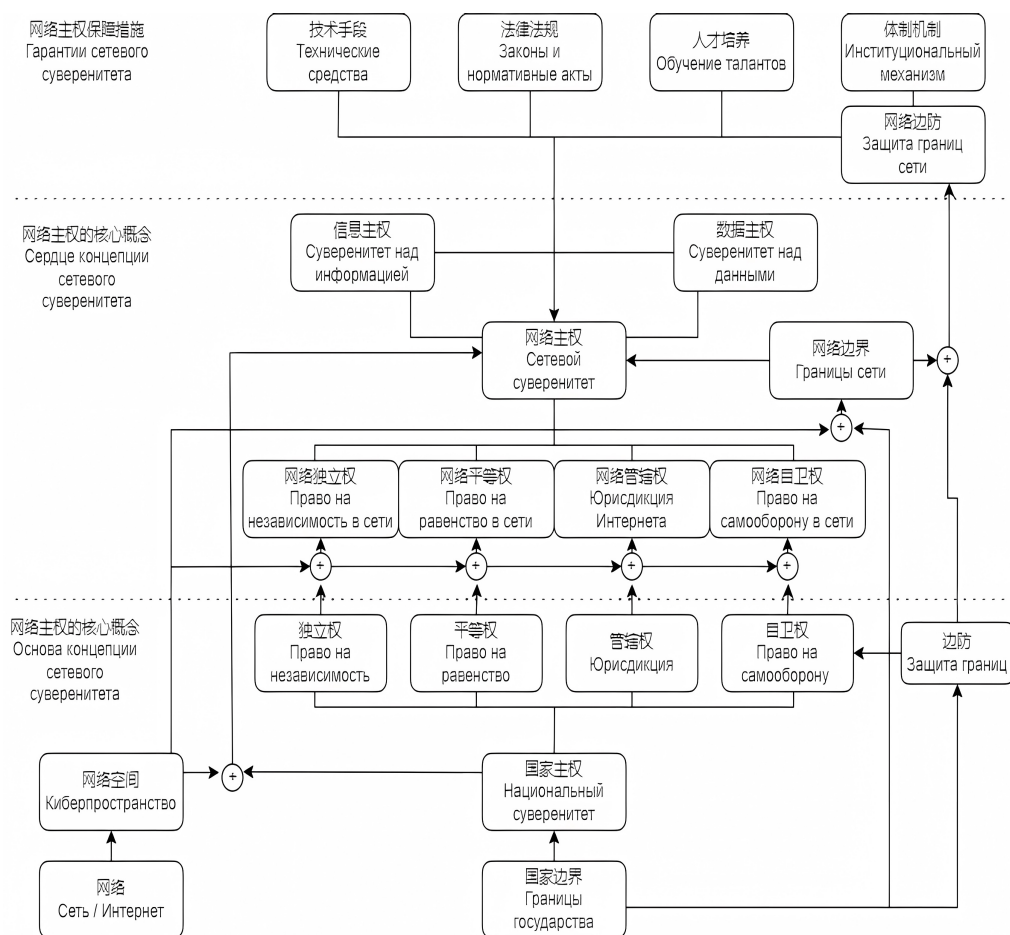


Рис. 1. Архитектура концепции киберсуверенитета КНР
Figure 1. Architecture of the PRC's Cyber-Sovereignty Concept

Источник: составлено автором.

Киберсуверенитет как альтернатива для развивающихся стран

Согласно официальной позиции, Китай утверждает, что нынешняя система управления важными интернет-ресурсами построена несбалансированно²⁰. Государство выступает за справедливое распределение цифровых дивидендов, продвигает позицию о том, что существующий миропорядок ставит средних и мелких игроков в уязвимое и невыгодное положение. Потребность в нормотворчестве Китай объясняет фрагментацией цифрового пространства и дефицитом доверия.

В 2017 г. МИД КНР опубликовал «Международную стратегию взаимодействия в киберпространстве», подчеркивающую уже ставшие традиционными для этой страны доминанты²¹. Примечательно, что документ содержит призыв не только к продвижению идеи киберсуверенитета через существующие международные диалоговые площадки (Форум по вопросам управления Интернетом, Всемирный экономический форум, Всемирная конференция по международной электросвязи, ICANN 50 и др.), но и к их осторожной реформе.

Концепция киберсуверенитета, заложенная в Стратегии, резко контрастирует с западноцентричным подходом США, ЕС и других развитых стран, построенном на основе мультистейкхолдеризма и идее свободы потоков информации²². Из-за подобного противоречия поиск Китаем международной поддержки изначально сталкивался с серьезным сопротивлением. Так, в 2011 г. западный блок стран отверг «Международный кодекс поведения в области информационной безопасности», ориентированный на киберсуверенитет, предложенный Китаем совместно с Россией и рядом государств — членов ШОС и Совет Безопасности ООН. В 2012 г. на Всемирной конференции по международной электросвязи против резолюции КНР о применимости международных правил телекоммуникаций к Интернету решительно выступили США и большинство западных стран. Документы были восприняты как потенциальный инструмент влияния авторитарных режимов и попытка навязать государствам централизованный подход к управлению киберпространством²³. В 2014 г. по той же причине на первой Всемирной интернет-конференции была отклонена упомянутая выше «Декларация Учжэнь».

Неудачи заставили Китай изменить приоритетные направления своей внешней политики. Фокус сместился на страны мирового большинства, в том числе Россию. Целеполагание при этом не поменялось: задачей все так же являлось вовлечение в свою орбиту как можно большего количества игроков. Китайский подход привлекателен для многих развивающихся кибердержав и стремящихся к этому статусу развивающихся стран, не входящих в западный блок и не желающих признавать лидерство США в вопросах управления киберпространством²⁴. Среди них — Россия, Белоруссия, Казахстан, Киргизия, Таджикистан, Узбекистан, Туркменистан, Пакистан, Бразилия, Камбоджа, Иран, Бангладеш, Аф-

²⁰ 中国关于网络空间国际规则的立场 [Позиция Китая в отношении международных правил в киберпространстве] // 外交部. 04.2023. URL: https://www.fmprc.gov.cn/web/wjlb_673085/zjzg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml (дата обращения: 17.06.2023).

²¹ 网络空间国际合作战略 [Международная стратегия взаимодействия в киберпространстве] // 新华社. 01.03.2017. URL: https://www.gov.cn/xinwen/2017-03/01/content_5172262.htm (дата обращения: 17.06.2023).

²² Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // *Вестник международных организаций*. 2021. № 3(16). С. 7–33. DOI: 10.17323/1996-7845-2021-03-01

²³ Hitchens T., Goren N. International Cybersecurity Information Sharing Agreements. Maryland: Center for International & Security Studies, 2017. P. 44.

²⁴ Stephen M. China's New Multilateral Institutions: A Framework and Research Agenda // *International Studies Review*. 2020. Vol. 23. No. 4. Pp. 827–829.

ганистан, Саудовская Аравия, Египет, Южная Африка, Зимбабве, Джибути, Уганда, отчасти Индия, страны АСЕАН и др. Наиболее активными игроками выступают Россия, Бразилия и государства — члены ШОС. Существует также группа «неопределившихся» развивающихся стран, которые еще не касались в своих высказываниях темы киберсуверенитета из-за отсутствия у них адекватного технологического потенциала.

Китай ведет работу с обеими группами государств, в первую очередь с помощью международных организаций. Например, активно развивается деятельность по линии БРИКС, где Китай выступает лидером и инициатором дискуссий. Принципы равенства и невмешательства во внутренние дела соответствуют общему курсу БРИКС на инклюзивность и вариативность, что позволяет Китаю без осуждения продвигать свои модели управления на международную аудиторию. В 2016 г. после саммита БРИКС при поддержке КНР вышла «Декларация Гоа», подчеркивающая, что развитие ИКТ должно происходить на основе принципов международного права, включая невмешательство во внутренние дела²⁵. Известно, что в ходе своего второго председательства в организации в 2017 г. Китай разрабатывал межгосударственное соглашение по киберсуверенитету и собирал Рабочую группу БРИКС по вопросам безопасности в сфере использования ИКТ для обсуждения вопросов управления Интернетом²⁶. В том же году КНР выступила с инициативой принятия Плана действий БРИКС по инновационному сотрудничеству на 2017–2020 гг. и предложила партнерам создать Институт БРИКС по изучению «сетей будущего». Приверженность Плану была закреплена в Сямьньской декларации руководителей стран БРИКС, Институт продолжает действовать по сей день.

В продвижении своей позиции Китай делает упор на трансрегиональные сетевые площадки и структуры управления. В 2014 г. в Афро-азиатской консультативно-правовой организации по инициативе КНР была создана рабочая группа для обсуждения суверенитета и сотрудничества в киберпространстве. В 2020 г. была запущена «Инициатива Китая и АСЕАН по созданию партнерства в области цифровой экономики», содержащая пункт об «уважении суверенитета в киберпространстве»²⁷. В 2021 г. Китайско-африканский форум по развитию и сотрудничеству в Интернете завершается «Инициативой по совместному созданию китайско-африканского сообщества единой судьбы в киберпространстве» — ее предполагалось строить «на основе уважения суверенитета и политики отдельных стран в Интернете»²⁸. В том же году Китай и Лига арабских государств обнародовали «Китайско-арабскую инициативу по сотрудничеству в области безопасности данных», подчеркивающую приверженность киберсуверенитету и отказ от заключения соглашений, ущемляющих киберсуверенитет третьих стран²⁹. В 2022 г. была принята схожая инициатива сотрудничества в области безопасности данных «Китай + пять стран

²⁵ 网络主权: 理论与实践 (3.0 版) [Киберсуверенитет: теория и практика (версия 3.0)] // 世界互联网大会. 28.09.2020. URL: https://cn.wicinternet.org/2021-09/28/content_36222995.htm (дата обращения: 10.06.2023).

²⁶ China to push 'sovereign' Internet vision at BRICS Summit // *India Today*. March 2, 2017. URL: <https://www.indiatoday.in/world/story/china-internet-vision-facebook-twitter-brics-summit-963464-2017-03-02> (дата обращения: 13.07.2023).

²⁷ 中国—东盟关于建立数字经济合作伙伴关系的倡议 [Инициатива Китая и АСЕАН по созданию партнерства в области цифровой экономики] // 外交部. 12.11.2020. URL: https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202011/t20201112_9869261.shtml (дата обращения: 17.06.2023).

²⁸ 中非互联网发展与合作论坛综述 [Резюме Китайско-африканского форума по развитию и сотрудничеству в Интернете] // 世界互联网大会. 03.09.2021. URL: https://cn.wicinternet.org/2021-09/03/content_36314600.htm (дата обращения: 17.06.2023).

²⁹ 中阿数据安全合作倡议 [Китайско-арабская инициатива по сотрудничеству в области безопасности данных] // 外交部. 29.03.2021. URL: https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202103/t20210329_9180823.shtml (дата обращения: 17.06.2023).

Центральной Азии» с Казахстаном, Киргизией, Таджикистаном, Узбекистаном и Туркменистаном³⁰. В конце года была опубликована Белая книга «Совместная работа по созданию сообщества единой судьбы в киберпространстве», фиксирующая важность популяризации китайского подхода к международному праву в Интернете³¹.

С 2015 г. инструментарий Китая расширился за счет создания новой геополитической инициативы «Цифровой шелковый путь» (数字丝绸之路), нацеленной на реформирование глобального цифрового порядка. В случае участия в инициативе Китай предлагает развивающимся странам цифровые продукты и услуги по конкурентным ценам, инвестиции в их ИКТ-инфраструктуру, совместные технологические проекты и исследовательские программы³². Взамен государство получает уменьшение технологической зависимости от Запада, новые рынки для своих хайтек-компаний и распространение китайских правовых стандартов, в том числе киберсуверенитета, уважение к которому вынесено в список пятнадцати общих принципов «Цифрового шелкового пути»³³. К инициативе официально присоединилось 16 стран. Более 40 государств, отдельные компании и организации, например АСЕАН, участвуют в ней без подписания меморандума. Спрос на доступные китайские технологии и инвестиции способствует популяризации концепции киберсуверенитета, стратегически важной для КНР.

* * *

Китай, как лидер молодых кибердержав, превращается в серьезного конкурента, способного бросить вызов устоявшейся гегемонии США в цифровом пространстве. Помимо того, что у КНР самое большое количество интернет-пользователей в мире, высокий уровень проникновения Интернета и развитый рынок товаров ИКТ, государство ведет активную деятельность по реформированию цифрового миропорядка. Среди инструментов правового регулирования Китая — международные организации, двухсторонние договоренности и национальные инициативы, в первую очередь Всемирная интернет-конференция и «Цифровой шелковый путь». Усиление влияния на глобальный Интернет помогает Пекину сохранять безопасность внутреннего режима от деструктивного влияния извне и продвигать интересы экономической политики.

Занимаясь правовым регулированием, Китай не просто заявляет международному сообществу о своем решительном намерении придерживаться киберсуверенитета во всех внешнеполитических делах, но призывает институционально закрепить данный принцип как подтверждение права государственных субъектов управлять Интернетом по своему усмотрению. Такая позиция оказывается привлекательной для ряда развивающихся стран, видящих в ней возможность бросить вызов кибергегемонии США или нуждающихся в китайских цифровых инвестициях.

Деятельность Китая в качестве создателя и пропагандиста кибернорм, начатая в 2010-х гг., стала более целостной, но элемент диссонанса в ряде вопросов сохраняется. К примеру, серьезная политическая поддержка Всемирной интернет-конференции и фор-

³⁰ «中国 + 中亚五国» 数据安全合作倡议 [Инициатива сотрудничества в области безопасности данных «Китай + пять стран Центральной Азии»] // 中国政府网. 09.06.2022.

URL: https://www.gov.cn/xinwen/2022-06/09/content_5694775.htm (дата обращения: 17.06.2023).

³¹ 携手构建网络空间命运共同体 (白皮书) [Совместная работа по созданию сообщества единой судьбы в киберпространстве (Белая книга)] // 中国政府网. 07.11.2022. URL: https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm (дата обращения: 17.06.2023).

³² Jing Cheng, Jinghan Zeng. “Digital Silk Road” as a Slogan Instead of a Grand Strategy // *Journal of Contemporary China*. 2023. Vol. 32. No. 142. P. 2.

³³ “数字丝路”建设将成全球发展新引擎 [Строительство «Цифрового шелкового пути» станет новым двигателем глобального развития] // 中国政府网. 09.09.2019. URL: https://www.gov.cn/xinwen/2019-09/09/content_5428411.htm (дата обращения: 18.06.2023).

мат управления его повесткой «сверху вниз» противоречит традиционному пониманию многосторонности. Призывы к «открытости и свободе киберпространства» в докладе «Киберсуверенитет: теория и практика (версия 3.0)» отчетливо контрастируют с заявлениями о необходимости строгого контроля за потоками информации. Потребность в защите государственного суверенитета в «Международной стратегии взаимодействия в киберпространстве» плохо стыкуется с призывом к созданию единых кибернорм на глобальном уровне. Также во всех документах присутствует конструктивная неопределенность отношений границ территории и виртуального пространства.

Этот диссонанс вкупе с фундаментальными расхождениями в подходах к киберсуверенитету стран мирового большинства во главе с КНР и Россией и стран коллективного Запада во главе с США может привести к дипломатическому тупику. Камнем преткновения в спорах чаще всего становится вопрос киберсуверенитета. Вероятно, положительную динамику может придать поэтапное дипломатическое согласование его определения и реальных, а не популистских различий в позициях. Китайский подход обусловлен соображениями национальной безопасности и внутрисударственной стабильности, в то время как страны Запада, особенно ЕС, обеспокоены скорее свободным развитием своей цифровой экономики и правами человека, такими как конфиденциальность³⁴. Позиции противоречат друг другу не так кардинально, как принято считать. Осознание этого может послужить толчком к преодолению противоречий.

Литература

- Дегтерев Д.А., Рамич М.С., Пискунов Д.А. Подходы США и КНР к глобальному управлению киберпространством: «новая биполярность» в «сетевом обществе» // *Вестник международных организаций*. 2021. № 3(16). С. 7–33. DOI: 10.17323/1996–7845–2021–03–01
- Ковригин Д.Э. Границы государственного суверенитета национального сегмента киберпространства // *Власть*. 2023. № 1. С. 124–129. DOI: 10.31171/vlast.v3i1i.9473
- Михалевич Е.А. Концепция киберсуверенитета Китайской Народной Республики: история развития и сущность // *Вестник Российского университета дружбы народов. Серия: Политология*. 2021. № 2(23). С. 254–264. DOI: 10.22363/2313–1438–2021–23–2–254–264
- Clark D. Characterizing Cyberspace: Past, Present and Future. MIT/CSAIL: Political Science Department Press, 2010. 18 p.
- Hitchens T., Goren N. International Cybersecurity Information Sharing Agreements. Maryland: Center for International & Security Studies, 2017. 140 p.
- Jing Cheng, Jinghan Zeng. “Digital Silk Road” as a Slogan Instead of a Grand Strategy // *Journal of Contemporary China*. 2023. Vol. 32. No. 142. Pp. 1–16. DOI: 10.1080/10670564.2023.2222269
- Stephen M. China's New Multilateral Institutions: A Framework and Research Agenda // *International Studies Review*. 2020. Vol. 23. No. 4. Pp. 807–834. DOI: 10.1093/isr/viaa076
- 习近平在第二届世界互联网大会开幕式上的讲话 (全文) [Выступление Си Цзиньпина на церемонии открытия Второй Всемирной интернет-конференции (полный текст)] // 中国共产党新闻网. 16.12.2015. URL: <http://cpc.people.com.cn/n1/2015/1216/c64094-27937316.html> (дата обращения: 08.06.2023).
- 郭玉军. 网络社会的国际法律问题研究 [Го Юйцзюнь. Исследование международно-правовых проблем в онлайн-сообществе] // 武汉: 武汉大学出版社, 2010年. 725页.
- 乌镇倡议 [Декларация Учжэнь] // 新华网. 18.12.2015. URL: http://www.xinhuanet.com/politics/2015-12/18/c_1117512543.htm (дата обращения: 08.06.2023).
- 中国—东盟关于建立数字经济合作伙伴关系的倡议 [Инициатива Китая и АСЕАН по созданию партнерства в области цифровой экономики] // 外交部. 12.11.2020. URL: https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202011/t20201112_9869261.shtml (дата обращения: 17.06.2023).

³⁴ Stephen M. China's New Multilateral Institutions: A Framework and Research Agenda // *International Studies Review*. 2020. Vol. 23. No. 4. Pp. 830–834.

- “中国 + 中亚五国” 数据安全合作倡议 [Инициатива сотрудничества в области безопасности данных «Китай + пять стран Центральной Азии»] // 中国政府网. 09.06.2022.
URL: https://www.gov.cn/xinwen/2022-06/09/content_5694775.htm (дата обращения: 17.06.2023).
- 网络主权: 理论与实践 [Киберсуверенитет: теория и практика] // 世界互联网大会. 21.10.2019.
URL: https://cn.wicinternet.org/2019-10/21/content_36224822.htm (дата обращения: 10.06.2023).
- 网络主权: 理论与实践 (2.0 版) [Киберсуверенитет: теория и практика (версия 2.0)] // 世界互联网大会. 15.10.2020. URL: https://cn.wicinternet.org/2020-10/15/content_36225577.htm (дата обращения: 10.06.2023).
- 网络主权: 理论与实践 (3.0 版) [Киберсуверенитет: теория и практика (версия 3.0)] // 世界互联网大会. 28.09.2020. URL: https://cn.wicinternet.org/2021-09/28/content_36222995.htm (дата обращения: 10.06.2023).
- 中阿数据安全合作倡议 [Китайско-арабская инициатива по сотрудничеству в области безопасности данных] // 外交部. 29.03.2021.
URL: https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202103/t20210329_9180823.shtml (дата обращения: 17.06.2023).
- 刘晗, 叶开儒. 网络主权的分层法律形态 [Лю Хань, Е Кайжу. Иерархическая правовая форма киберсуверенитета] // 华东政法大学学报. 2020年. 第4期. 第67–82页.
- 网络空间国际合作战略 [Международная стратегия взаимодействия в киберпространстве] // 新华社. 01.03.2017. URL: https://www.gov.cn/xinwen/2017-03/01/content_5172262.htm (дата обращения: 17.06.2023).
- 中国关于网络空间国际规则的立场 [Позиция Китая в отношении международных правил в киберпространстве] // 外交部. 01.04.2023.
URL: https://www.fmprc.gov.cn/web/wjb_673085/zjzg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml (дата обращения: 17.06.2023).
- 中非互联网发展与合作论坛综述 [Резюме Китайско-африканского форума по развитию и сотрудничеству в Интернете] // 世界互联网大会. 03.09.2021. URL: https://cn.wicinternet.org/2021-09/03/content_36314600.htm (дата обращения: 17.06.2023).
- 习近平. 让互联网发展成果惠及13亿中国人民 [Си Цзиньпин. Пусть достижения развитого Интернета принесут пользу 1,3 миллиардам китайцев] // 2014世界互联网大会新闻官网. 19.11.2014.
URL: http://www.cac.gov.cn/2014-11/19/c_1113314465.htm (дата обращения: 07.06.2023).
- 携手构建网络空间命运共同体 (白皮书) [Совместная работа по созданию сообщества единой судьбы в киберпространстве (Белая книга)] // 中国政府网. 07.11.2022.
URL: https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm (дата обращения: 17.06.2023).
- 中国互联网状况 (白皮书) [Состояние Интернета в Китае (Белая книга)] // 中国政府网. 08.06.2010.
URL: https://www.gov.cn/zhengce/2010-06/08/content_2615774.htm (дата обращения: 07.06.2023).
- 郑振宇. 改革开放以来我国互联网治理的演变历程与基本经验 [Чжэнь Чжэнью. Эволюция и базовый опыт управления Интернетом в Китае со времен реформ и открытости] // 马克思主义研究, 2019年. 第1期. 第58–67页.
- 韩瑞霞, 徐剑. 网络主权视域下当前互联网治理的主要问题, 成因及监管对策 [Хань Жуйся, Сюй Цзянь. Основные проблемы, причины и регулятивные контрмеры текущего управления Интернетом с точки зрения киберсуверенитета] // 南京邮电大学学报 (社会科学版). 2020年. 第22期. 第41–52页.
- 杨泽伟. 国际法析论: 第3版 [Ян Цзевэй. Анализ международного права: 3-е издание]. 北京: 中国人民大学出版社, 2012年. 247页.

Architecture of China's Cyber Sovereignty Concept (Based on the Reports World Internet Conference "Sovereignty in Cyberspace: Theory and Practice")

Alexandra D. Yankova

Ph.D. student at the HSE University, Research Assistant, Centre for Comprehensive European and International Studies, National Research University Higher School of Economics (address: 17/1, Malaya Ordynka Str., Moscow, 119017, Russian Federation). ORCID: 0000-0002-7209-9818.
E-mail: ayankova@hse.ru

Received 22.06.2023.

Abstract:

Modern China shares the position that national security is impossible without network security. The state builds cyber diplomacy based on the traditional dominants of its foreign policy — inviolability of borders, non-interference, respect for sovereignty. Naturally expanding into the digital space, the last of them has acquired a new form of cyber-sovereignty, become an integral part of the Chinese discursive force and the cornerstone of the PRC's approach to global Internet governance. Beijing, not satisfied with the current unfair digital world order and concerned about the need to ensure constant control over internal networks for the regime security, advocates institutional reform of the existing system of global cyberspace governance. Over the past two decades, the state has turned from a recipient into a creator and propagandist of cyber norms. The cases of Chinese regulatory entrepreneurship attract an increasing number of supporters, primarily among developing countries. Several major initiatives, including the World Internet Conference, the Community with a Shared Future in Cyberspace, the Digital Silk Road, have become the personification of China's competitive strategy in this direction. All of them aim to convey to an international audience a concrete message about China's intention to adhere to cyber sovereignty in all foreign policy affairs and a call to formalize this principle as a confirmation of the state's right to manage the Internet at their discretion. Based on primary sources, the article attempts to trace the origins of the PRC's cyber sovereignty concept, analyze its evolution, institutional design, goal setting, content, limitations, and using the construction of an object-oriented architecture to present it as a three levels system, visualized for a better understanding of the links between levels.

Key words:

Cyber sovereignty, cybersecurity, cyber-norms, Internet governance, global governance, China.

Acknowledgements:

The author expresses gratitude to her supervisor, Vasily B. Kashin, Ph.D. (Political Sciences), Director of the Centre for Comprehensive European and International Studies (CCEIS) at the HSE University, for his assistance.

For citation:

Yankova A.D. Architecture of China's Cyber Sovereignty Concept: Based on the Reports World Internet Conference "Sovereignty in Cyberspace: Theory and Practice" // Far Eastern Studies. 2023. No. 4. Pp. 99–112. DOI: 10.31857/S013128120026886-5.

References

- Clark D. Characterizing Cyberspace: Past, Present and Future. MIT/CSAIL: Political Science Department Press, 2010. 18 p.
- Degtarev D.A., Ramich M.S., Piskunov D.A. Podhody SSHA i KNR k global'nomu upravleniyu kiberprostranstvom: "novaya bipolyarnost'" v "setevom obshchestve" [U.S. & China Approaches to Global Internet Governance: "New Bipolarity" in Terms of "The Network Society"]. *Vestnik mezhdunarodnykh organizatsij*. 2021. Vol. 16. No. 3. Pp. 7–33. DOI: 10.17323/1996–7845–2021–03–01. (In Russ.)
- Hitchens T., Goren N. International Cybersecurity Information Sharing Agreements. Maryland: Center for International & Security Studies, 2017. 140 p.
- Jing Cheng, Jinghan Zeng. "Digital Silk Road" as a Slogan Instead of a Grand Strategy. *Journal of Contemporary China*. 2023. Vol. 32. No. 142. Pp. 1–16. DOI: 10.1080/10670564.2023.2222269
- Kovrigin D.E. Granicy gosudarstvennogo suvereniteta nacional'nogo segmenta kiberprostranstva [The boundaries of state sovereignty of the national segment of cyberspace]. *Vlast'*. 2023. No. 1. S. 124–129. DOI: 10.31171/vlast.v31i1.9473. (In Russ.)
- Mihalevich E.A. Konceptiya kibersuvereniteta Kitajskoj Narodnoj Respubliki: istoriya razvitiya i sushchnost' [The concept of cyber sovereignty of the PRC: the history of development and essence]. *Vestnik Rossijskogo universiteta družby narodov. Seriya: Politologiya*. 2021. Vol. 23. No. 2. Pp. 254–264. DOI: 10.22363/2313–1438–2021–23–2–254–264. (In Russ.)
- Stephen M. China's New Multilateral Institutions: A Framework and Research Agenda. *International Studies Review*. 2020. Vol. 23. No. 4. Pp. 807–834.
- 习近平在第二届世界互联网大会开幕式上的讲话 (全文) [Xi Jinping's speech at the opening ceremony of the Second World Internet Conference (full text)]. 中国共产党新闻网. 16.12.2015. URL: <http://cpc.people.com.cn/n1/2015/1216/c64094–27937316.html> (accessed: 08.06.2023). (In Chin.)

- 郭玉军. 网络社会的国际法律问题研究 [Guo Yujun. Research on International Legal Issues in the Online Society]. 武汉: 武汉大学出版社, 2010年. 725页. (In Chin.)
- 乌镇倡议 [The Wuzhen Initiative]. 新华网. 18.12.2015. URL: http://www.xinhuanet.com/politics/2015-12/18/c_1117512543.htm (accessed: 08.06.2023). (In Chin.)
- 中国—东盟关于建立数字经济合作伙伴关系的倡议 [China-ASEAN Initiative on Establishing a Digital Economy Partnership]. 外交部. 12.11.2020. URL: https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202011/t20201112_9869261.shtml (accessed: 17.06.2023). (In Chin.)
- “中国 + 中亚五国” 数据安全合作倡议 [“China + Five Central Asian Countries” Data Security Cooperation Initiative]. 中国政府网. 09.06.2022. URL: https://www.gov.cn/xinwen/2022-06/09/content_5694775.htm (accessed: 17.06.2023). (In Chin.)
- 网络主权: 理论与实践 [Sovereignty in Cyberspace: Theory and Practice]. 世界互联网大会. 21.10.2019. URL: https://cn.wicinternet.org/2019-10/21/content_36224822.htm (accessed: 10.06.2023). (In Chin.)
- 网络主权: 理论与实践 (2.0 版) [Sovereignty in Cyberspace: Theory and Practice (Version 2.0)]. 世界互联网大会. 15.10.2020. URL: https://cn.wicinternet.org/2020-10/15/content_36225577.htm (accessed: 10.06.2023). (In Chin.)
- 网络主权: 理论与实践 (3.0 版) [Sovereignty in Cyberspace: Theory and Practice (Version 3.0)]. 世界互联网大会. 28.09.2020. URL: https://cn.wicinternet.org/2021-09/28/content_36222995.htm (accessed: 10.06.2023). (In Chin.)
- 中阿数据安全合作倡议 [China-LAS Cooperation Initiative on Data Security]. 外交部. 29.03.2021. URL: https://www.mfa.gov.cn/web/ziliao_674904/1179_674909/202103/t20210329_9180823.shtml (accessed: 17.06.2023). (In Chin.)
- 刘晗, 叶开儒. 网络主权的分层法律形态 [Liu Han, Ye Kairu. Hierarchical legal form of Network Sovereignty]. 华东政法大学学报. 2020年. 第4期. 第67–82页. (In Chin.)
- 网络空间国际合作战略 [International Strategy of Cooperation on Cyberspace]. 新华社. 01.03.2017. URL: https://www.gov.cn/xinwen/2017-03/01/content_5172262.htm (accessed: 17.06.2023). (In Chin.)
- 中国关于网络空间国际规则的立场 [China's Positions on International Rules-making in Cyberspace]. 外交部. 01.04.2023. URL: https://www.fmprc.gov.cn/web/wjwb_673085/zjzg_673183/jks_674633/zclc_674645/qt_674659/202110/t20211012_9552671.shtml (accessed: 17.06.2023). (In Chin.)
- 中非互联网发展与合作论坛综述 [Summary of the China-Africa Internet Development and Cooperation Forum]. 世界互联网大会. 03.09.2021. URL: https://cn.wicinternet.org/2021-09/03/content_36314600.htm (accessed: 17.06.2023). (In Chin.)
- 习近平: 让互联网发展成果惠及13亿中国人民 [Xi Jinping: Let the achievements of Internet development benefit 1.3 billion Chinese people]. 2014世界互联网大会新闻官网. 19.11.2014. URL: http://www.cac.gov.cn/2014-11/19/c_1113314465.htm (accessed: 07.06.2023). (In Chin.)
- 携手构建网络空间命运共同体 (白皮书) [Jointly Build a Community with a Shared Future in Cyberspace (White paper)]. 中国政府网. 07.11.2022. URL: https://www.gov.cn/zhengce/2022-11/07/content_5725117.htm (accessed: 17.06.2023). (In Chin.)
- 中国互联网状况 (白皮书) [The Internet in China (White paper)]. 中国政府网. 08.06.2010. URL: https://www.gov.cn/zhengce/2010-06/08/content_2615774.htm (accessed: 07.06.2023). (In Chin.)
- 郑振宇. 改革开放以来我国互联网治理的演变历程与基本经验 [Zheng Zhenyu. The evolution and basic experience of Internet governance in my country since China's reform and opening-up]. 马克思主义研究, 2019年. 第1期. 第58–67页. (In Chin.)
- 韩瑞霞, 徐剑. 网络主权视域下当前互联网治理的主要问题, 成因及监管对策 [Han Ruixia, Xu Jian. The main problems, causes and regulatory countermeasures of current Internet governance under the perspective of network sovereignty]. 南京邮电大学学报 (社会科学版). 2020年. 第22期. 第41–52页. (In Chin.)
- 杨泽伟. 国际法析论: 第3版 [Yang Zewei. Analysis of International Law: 3rd Edition]. 北京: 中国人民大学出版社, 2012年. 247页. (In Chin.)