DOI: 10.22394/2073-2929-2024-02-148-158

СПЕЦИАЛЬНОСТЬ: 5.5.4

EDN: LICZPV

Международный аспект политики информационной безопасности КНР

Семенов Б. Р.
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (Северо-Западный институт управления), Санкт-Петербург, Российская Федерация
e-mail: bsemenov-13@edu.ranepa.ru

РЕФЕРАТ

В статье рассмотрен международный аспект политики информационной безопасности Китая. В связи с тем что информационная сфера становится все более значимой в отношениях между государствами, обращение к политике одного из ведущих международных акторов — Китайской Народной Республики — является востребованным и актуальным. Опыт Китая в обеспечении информационной безопасности может быть востребован и в других государствах, включая Российскую Федерацию.

Цель. Цель работы — охарактеризовать международный аспект политики информационной безопасности Китая и раскрыть особенности взаимодействия КНР с другими странами в этой области.

Задачи. Провести обзор ключевых международных документов, обеспечивающих международную информационную безопасность КНР, а также внутреннего законодательства страны в этой сфере. Рассмотреть вопрос противостояния КНР и США в информационном пространстве.

Методы. В работе используется исторический метод для изучения развития системы информационной безопасности КНР, анализ документов для обзора внутреннего и внешнего законодательства Китая в сфере информационной безопасности, а также сравнительный анализ для сопоставления подходов различных стран в сфере кибербезопасности.

Результаты. По итогам проведенного исследования можно выделить следующие ключевые результаты.

В контексте Шанхайской организации сотрудничества (ШОС) КНР демонстрирует стремление к совместному развитию норм международного права в области информационной безопасности, а также активно участвует в создании соглашений о сотрудничестве в этой сфере, что подчеркивает роль государства как сторонника многополярного мира в киберпространстве.

В рамках взаимодействия со странами БРИКС Китай нацелен на углубление сотрудничества в области информационной безопасности через ряд инициатив и соглашений, направленных на разработку общих подходов и стандартов. Это сотрудничество способствует созданию единой системы защиты в информационной сфере среди стран БРИКС, укрепляя их позиции в международном информационном пространстве.

В отношениях с США взаимодействие КНР характеризуется конкуренцией и противостоянием, особенно в контексте кибербезопасности. Это включает в себя различия в подходах к регулированию информационного пространства и кибершпионаже. Тем не менее существующие противоречия и конфликты подчеркивают необходимость диалога и сотрудничества для разработки общих международных правил поведения в киберпространстве, что может способствовать обеспечению международной информационной безопасности и стабильности.

Выводы. Международный аспект политики информационной безопасности КНР раскрывает разнообразные формы взаимодействия с другими странами, каждая из которых имеет свои особенности. Эти взаимоотношения формируют многоуровневую систему международной

информационной безопасности, в которой КНР играет ключевую роль, стремясь к созданию сбалансированного и безопасного информационного пространства.
Ключевые слова: международная информационная безопасность, «Золотой щит», кибербезопасность, международное сотрудничество, кибершпионаж, технологическое развитие, Китайская Народная Республика
Для цитирования: Семенов Б. Р. Международный аспект политики информационной безопасности КНР // Евразийская интеграция: экономика, право, политика. 2024. Т. 18. № 2. С. 148–158. https://doi.org/10.22394/2073-2929-2024-02-148-158. EDN: LICZPV

International Aspect of PRC Information Security Policy

Boris R. Semenov
Russian Presidential Academy of National Economy and Public Administration (North-West Institute of Management), Saint Petersburg, Russian Federation
e-mail: bsemenov-13@edu.ranepa.ru

ABSTRACT
This article examines the international aspect of China's information security policy. Due to the fact that the information sphere is becoming increasingly important in relations between states, the appeal to the policy of one of the leading international actors — the People's Republic of China — is in demand and relevant. China's experience in ensuring information security may be in demand in other countries, including the Russian Federation.
Aim. The purpose of the article is to characterize the international aspect of China's information security policy and to reveal the specifics of China's interaction with other countries in this area.
Tasks. To achieve this goal was conducted a review of key international documents ensuring the international information security of the People's Republic of China, as well as the country's domestic legislation in this area. Also the issue of confrontation between China and the United States in the information space was considered.
Methods. The study employs the historical method to examine the development of China's information security system, document analysis to review China's domestic and international legislation in the field of information security, and comparative analysis to compare the approaches of different countries in the field of cybersecurity.
Results. The conducted research highlights the following key outcomes: In the context of the Shanghai Cooperation Organization (SCO), China demonstrates a commitment to the joint development of international legal norms in the field of information security, as well as actively participates in the creation of cooperation agreements in this area, emphasizing the state's role as an advocate for a multipolar world in cyberspace. Within the framework of interactions with the BRICS countries, China aims to deepen cooperation in the field of information security through a series of initiatives and agreements aimed at developing common approaches and standards. This cooperation contributes to the creation of a unified protection system in the information sphere among the BRICS countries, strengthening their positions in the international information space. In relations with the United States of America, the interaction of China is characterized by competition and confrontation, especially in the context of cybersecurity. This includes differences in approaches to regulating the information space and cyber espionage. Nonetheless, existing contradictions and conflicts underscore the need for dialogue and cooperation to develop common international rules of behavior in cyberspace, which can contribute to ensuring international information security and stability.
Conclusions. The international aspect of the China's information security policy reveals various forms of interaction with other countries, each with its unique features. These relationships form a multi-

level system of international information security, in which the PRC plays a key role, aiming to create a balanced and secure information space.
Keywords: International Information Security, "Golden Shield", Cybersecurity, International Cooperation, Cyber Espionage, Technological Development, People's Republic of China
For citing: Semenov B. R. International Aspect of PRC Information Security Policy // Eurasian Integration: Economic, Law, Politics. 2024. Vol. 18. No. 2. P. 148–158. (In Russ.)
https://doi.org/10.22394/2073-2929-2024-02-148-158. EDN: LICZPV

Введение

Участие страны в обеспечении международной информационной безопасности (МИБ) представляет собой один из ключевых принципов для Китайской Народной Республики (КНР). В связи с высоким экономическим ростом и укреплением позиции Китая на международной арене все чаще возникает конфликт интересов государства с другими странами. Особенно напряжены отношения Китая с Соединенными Штатами, что связано с проблемой кибербезопасности и защиты интеллектуальной собственности, в частности, уязвимостью секторов финансовых корпораций и информационных технологий. Вместе с тем их совершенствование и развитие позволяют противодействовать кибершпионажу со стороны иностранных агентов. Таким образом, правительство Китая заявляет о единоличном управлении собственным информационным пространством [10, с. 80], что подразумевает создание защищенной от кибератак информационной структуры.

Вопросы национальной безопасности в киберпространстве Китая активно изучаются американскими специалистами, например Д. Линдси [11] и Д. Вентре[1]. Их научные труды направлены на теоретическое обоснование работы государственного аппарата КНР в сфере информационного пространства.

В контексте китайских исследований следует отметить труды Ф. Биньсина [15] и В. Гуйфана [16]. Эти авторы также осуществляют сравнительный анализ подходов КНР и США к вопросам информационной безопасности, акцентируя внимание на анализе американской системы безопасности.

В российском научном дискурсе данная тематика представлена работами таких авторов, как Г. Ибрагимова [4], К. Антипов [1] и А. Булавин [2]. Они предлагают общий анализ системы кибербезопасности КНР, основываясь в большей степени на исследованиях зарубежных авторов.

В работе используются исторический метод для исследования развития системы информационной безопасности КНР, традиционный анализ документов для обзора внутренней и внешней законодательной базы Китая в сфере информационной безопасности, описательный метод для рассмотрения противостояния между КНР и США в информационном пространстве. Также использованы общенаучные методы синтеза, обобщения и аналогии.

Отметим, что стремительные технологические изменения, которые привели к созданию глобальных высокоскоростных сетей, как считает китайское руководство, являются потенциальной угрозой и могут подорвать национальный суверенитет. Поэтому необходимо установить определенный международный порядок информационного взаимодействия и обмена на паритетных началах. Среди приоритетных задач, стоящих перед страной в связи с встраиванием в глобальные сети, исследователи выделяют: запрет информации, которая не соответствует нормам и жизненным принципам китайского населения и расшатывает национально-культурные устои; блокировку доступа к сведениям о работе государственных структур; выработку жесткой системы правил, которые регулируют доступ к иностранным источникам [5, с. 25–26].

Одним из ключевых приоритетов, выделенных исследователями, также является защита интеллектуальной собственности, которая критически важна для стимулирования инноваций и экономического развития. Китай — страна с одним из самых высоких уровней валового внутреннего продукта в мире. В этой связи китайские технологии являются частой целью при краже интеллектуальной собственности,

[1] *Ventre D.* Artificial Intelligence, Cybersecurity and Cyber Defence [Электронный ресурс]. URL: https://www.wiley.com/en-us/Artificial+Intelligence%2C+Cybersecurity+and+Cyber+Defence-p-9781786304674 (дата обращения: 26.09.2023).

и усилия по укреплению механизмов защиты являются необходимыми для защиты технологических активов страны.

Кроме того, китайское правительство стремится регулировать поток информации в стране, особенно контент, который считается вредным для национальной безопасности или социальной стабильности. Это привело к развитию сложной системы интернет-цензуры и наблюдения, которая критикуется различными правозащитными группами за ограничение свободы слова и выражения. Несмотря на актуализацию внутренней безопасности в информационной сфере, Китай проявляет высокую активность в реализации международной информационной безопасности, участвуя в разработке политики в разных форматах, включая международные организации.

Несмотря на внешние и внутренние вызовы, Китай продолжает преследовать свою цель стать глобальным лидером в области информационных технологий и вкладывает значительные средства в развитие передовых технологий, таких как искусственный интеллект, квантовые вычисления и сети 5G. Эти усилия имеют потенциал изменить глобальный информационный ландшафт и могут иметь значительные экономические и стратегические последствия для Китая и всего мира.

Анализ международно-правовой базы КНР в области информационной безопасности

Первым официальным и вступившим в законную силу 1 июня 2017 г. законодательным актом, который регламентирует действия КНР в области кибербезопасности, является Стратегия международного сотрудничества в киберпространстве[1] (Ministry of Foreign Affairs of People's Republic of China). В соответствии с документом необходимо защитить интересы страны и национальный суверенитет, что подразумевает право определения модели государственной политики в сети Интернет; предупредить разногласия в киберпространстве; осуществить совместное управление киберпространством, в котором ООН станет главным инструментом; устранить цифровой разрыв между развитыми и развивающимися странами за счет обеспечения всеобщего доступа. В этой связи основными озвученными в Стратегии задачами становятся невмешательство сторонних государств во внутреннюю жизнь Китая, создание свода международных правил поведения в киберпространстве, защита прав и интересов граждан, разработка площадок для обмена «киберкультурой» [3, с. 128–129].

По словам ученых, в Китае также существует несколько формообразующих международных документов, обеспечивающих международную информационную безопасность [9, с. 129–130].

1. *Заявление глав государств — членов Шанхайской организации сотрудничества (ШОС) по международной информационной безопасности* (15 июня 2006 г.), диктующее необходимость обеспечения информационной безопасности на региональном и международном уровне, а также исследование концепций, которые направлены на укрепление безопасности глобальных информационных и телекоммуникационных систем[2].

2. *Соглашение между правительствами государств — членов ШОС о сотрудничестве в области международной информационной безопасности* (2 июня 2011 г.), в котором выработаны главные направления сотрудничества (выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, противодействие угрозам использования информационно-коммуникационных технологий в террористических целях, противодействие информационной преступности, содействие обеспечению безопасного, стабильного функционирования и интернационализации управления глобальной сетью Интернет и др.)[3].

Кроме того, по заявлению Генерального секретаря ШОС Ч. Мина, в 2023 г. обеспечение информационной безопасности и реагирование на вызовы и угрозы в Интернете были официально выделены

[1] Стратегия международного сотрудничества в киберпространстве [Электронный ресурс] // Xinhua (сайт). URL: http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.html (дата обращения: 28.06.2023).

[2] Заявление глав государств — членов ШОС по международной информационной безопасности (г. Шанхай, 15.06.2006) [Электронный ресурс] // Информационное агентство ИнфоРос (сайт). URL: http://infoshos.ru/ru/?id=94 (дата обращения: 15.01.2023).

[3] Соглашение между правительствами государств — членов ШОС о сотрудничестве в области международной информационной безопасности (02.06.2011) [Электронный ресурс]. URL: https://docs.cntd.ru/document/902289626 (дата обращения: 15.01.2023).

в отдельное направление работы Региональной антитеррористической структуры Шанхайской организации сотрудничества (РАТС ШОС). По утверждению Генерального секретаря, в 2022 г. в рамках РАТС ШОС были определены совместные меры по противодействию современным вызовам и угрозам со стороны международных террористических организаций, было подписано 42 соответствующих документа. Помимо этого, принимались последовательные меры по недопущению использования сети Интернет в террористических, сепаратистских и экстремистских целях на пространстве ШОС[1].

3. *Соглашение между правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности* (30 апреля 2015 г.), в котором среди основных направлений сотрудничества указаны создание каналов связи и контактов в целях совместного реагирования на угрозы в сфере МИБ, взаимодействие в разработке и продвижении норм международного права в целях обеспечения национальной безопасности и МИБ, разработка и осуществление необходимых совместных мер доверия, способствующих обеспечению МИБ, обмен информацией о законодательстве государств Сторон по вопросам обеспечения ИБ, содействие научным исследованиям в области обеспечения МИБ и др.[2]

4. Закон *«Об управлении деятельностью зарубежных неправительственных организаций внутри страны»* (28 апреля 2016 г.), указывающий на обязательную регистрацию и контроль зарубежных неправительственных организаций министерством общественной безопасности Китая [9, с. 129–130].

5. *Ташкентская декларация 15-летия Шанхайской организации сотрудничества* (24 июня 2016 г.), настаивающая на углублении практического сотрудничества по реализации Соглашения между правительствами государств — членов ШОС о сотрудничестве в области обеспечения МИБ[3].

6. *Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства* (25 июня 2016 г.) о необходимости совместных усилий в целях развития информационного пространства, обеспечения его безопасности, наращивания практического диалога и сотрудничества в этой области[4].

7. *Стратегия международного сотрудничества в киберпространстве* (2 марта 2017 г.) об интернет-суверенитете и отказе от гегемонии в Интернете, недопущении вмешательства во внутренние дела других государств с использованием ИКТ [9, с. 130].

8. *Циндаоская декларация Совета глав государств — членов Шанхайской организации сотрудничества* (10 июня 2018 г.) о создании системы мониторинга вероятных угроз в киберпространстве и противодействия им [9, с. 130].

В качестве одной из наиболее важных предпосылок к развитию информационной безопасности в КНР отмечается деятельность Эдварда Сноудена, экс-сотрудника Центрального разведывательного управления (ЦРУ) и Агентства национальной безопасности (АНБ) США. Его разоблачения вызвали негативную реакцию со стороны Китая, в результате чего был увеличен штат сотрудников, ответственных за фильтрацию и обработку данных в китайской сети Интернет, и началось улучшение элементов искусственного интеллекта «Золотого щита» [7, с. 388].

В Китае информационные данные проходят трехуровневую фильтрацию. На первом этапе происходит блокировка крупных электронных ресурсов, которые нарушают китайские законы, отказываются сотрудничать или демонстрируют политику государства в негативном ключе. На втором уровне используются алгоритмы искусственного интеллекта, проверяющие соответствие информационных данных законодательству КНР и, в противном случае, осуществляющие их блокировку. Третий этап подразумевает

---

[1] Генсек Чжан Мин: информационная безопасность стала отдельным направлением работы РАТС ШОС [Электронный ресурс] // Российское информационное агентство. URL: https://ria.ru/20230704/shos-1882050269.html (дата обращения: 25.03.2024).

[2] Соглашение между правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности (30.04.2015) [Электронный ресурс]. URL: https://docs.cntd.ru/document/420283259 (дата обращения: 28.01.2023).

[3] Ташкентская декларация 15-летия Шанхайской организации сотрудничества (29.01.2023) [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/5094 (дата обращения: 04.09.2022).

[4] Совместное заявление Президента Российской Федерации и Председателя Китайской Народной Республики о взаимодействии в области развития информационного пространства (25.06.2016) [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/5099 (дата обращения: 29.01.2023).

ручную обработку интернет-контента сотрудниками Бюро общественной информации и надзора за сетевой безопасностью [7, с. 388–389].

По замечанию зарубежных исследователей и журналистов, особым явлением в киберпространстве Китая стала «50-центовая армия», или «Умаодан». Она состоит из китайских блогеров и участников форумов (преимущественно студентов), которые осуществляют проправительственную деятельность в интернет-сети, положительно отзываясь о политике страны, ее правительстве и партии. За каждый пост автор получает пять мао (цзяо), что приравнивается к пятидесяти центам[1]. Руководство страны тем самым стремится сохранить баланс в вопросе контроля зарубежного присутствия в информационном пространстве Китая. Это, по словам ученых, порождает проблему выбора между ослабеванием внутреннего идеологического контроля и снижением эффективности внешнеэкономического сотрудничества [7, с. 389].

50-центовая армия является частью более широкой стратегии Китая по контролю за общественным мнением в киберпространстве. Правительство разработало сложную систему интернет-цензуры и наблюдения, чтобы сохранить свое влияние на информационный поток в стране. Руководство страны утверждает, что такие меры необходимы для поддержания социальной стабильности и национальной безопасности.

Вместе с тем использование оплачиваемых комментаторов для формирования общественного мнения не уникально для Китая и было замечено и в других странах. Это подчеркивает необходимость более широкой дискуссии об этике онлайн-поведения и потенциальном влиянии таких практик на общественный дискурс.

Здесь также необходимо отметить, что в международных масштабах беспрецедентным на тот момент стал принятый 7 ноября 2016 г. *Закон КНР о кибербезопасности*, согласно которому руководство Китая получает право на регулирование китайской интернет-сети. Срок хранения опубликованной информации на территории Китая составляет не менее полугода. К этим же мерам относится проект «Золотой щит», который с 2004 г. блокирует нежелательный для государства контент в информационном поле, а также спонсируемая руководством публикационная активность лиц, высказывающих положительное мнение о проводимой КНР политике [8, с. 159–160].

Участие КНР в разработке международной политики информационной безопасности

КНР играет значимую роль в разработке международной политики информационной безопасности, активно участвуя в различных международных форматах и инициативах. Эти платформы предоставляют Китаю возможность продвигать свои предложения и инициативы, направленные на укрепление международной информационной безопасности, а также выражать свою позицию в вопросах регулирования поведения государств в информационном пространстве. Приведем конкретные примеры.

1. *Глобальная инициатива по безопасности данных (2020 г.).*

В сентябре 2020 г. Китай объявил о глобальной инициативе по стандартам безопасности данных. Ключевые тезисы инициативы:

- Китай призывает другие страны объективно и разумно относиться к безопасности данных и прилагать усилия к обеспечению открытости, безопасности и стабильности глобальной цепочки поставок ИКТ. Вместе с этим страны должны противодействовать деятельности в сфере ИКТ, которая наносит ущерб ключевым инфраструктурным объектам других стран или нацелена на кражу важных данных из этих стран;
- Китай призывает мировое сообщество принять действия для предотвращения массовой слежки и незаконного сбора персональных данных граждан других государств. Поставщики продуктов и услуг ИКТ должны предотвращать создание так называемых «закладок» в своих продуктах и услугах, которые могут позволить незаконно получать данные;

[1] *Fareed M.* China Joins a Turf War [Электронный ресурс] // The Guardian. 22.09.2008. URL: https://www.theguardian.com/media/2008/sep/22/chinathemedia.marketingandpr (дата обращения: 15.07.2023).

- предприятия должны соблюдать законы стран, в которых они ведут свою деятельность, в то же время странам не следует в принудительном порядке требовать от отечественных предприятий хранить на их собственной государственной территории данные, созданные или полученные ими за рубежом;
- необходимо уважать суверенитет и право на управление данными других стран и отказаться от приобретения данных, хранящихся в других странах, через частные компании или частных лиц. Инициатива призывает разные страны удовлетворять потребности в получении трансграничных данных путем правовой помощи или через другие соответствующие каналы[1].

2. *Участие в Группе правительственных экспертов (ГПЭ) ООН.*

С 2004 по 2016 г. ООН организовала пять ГПЭ, в которых участвовали эксперты из 15–25 государств-членов, включая пять постоянных членов Совета Безопасности. Четвертая ГПЭ в 2015 г. достигла консенсуса о применимости международного права, в частности Устава ООН, к киберпространству и включила в свой окончательный отчет список из одиннадцати добровольных, необязательных норм ответственного поведения государств в киберпространстве, а также явное упоминание четырех принципов международного права (гуманность, необходимость, пропорциональность и различие), применимых к поведению государств в киберпространстве[2].

3. *Ежегодные встречи Всемирной интернет-конференции WIC.*

С 2014 г. Китай проводит ежегодные встречи Всемирной интернет-конференции, которые дают представление о глобальном видении Пекина в области управления Интернетом и цифрового суверенитета. В 2022 г. Китай заявил о преобразовании площадки в международную организацию с целью более действенного участия в управлении Интернетом как глобальной технической системой и как средой распространения информации[3].

4. *Инициативы в рамках БРИКС:*

- 2013 г., Дурбан, Южная Африка. В рамках этого саммита странами-участницами была признана необходимость сотрудничества в области кибербезопасности. На саммите была принята Декларация eThekwini, в которой подчеркивалась важность «вклада и участия в мирном, безопасном и открытом киберпространстве, разработке общепринятых норм, стандартов и практик»[4].
- 2015 г., Уфа, Россия. На саммите в Уфе в 2015 г. лидеры БРИКС учредили Рабочую группу по безопасности в использовании ИКТ с целью «разработки практического сотрудничества для решения общих проблем безопасности в использовании ИКТ» и «обмена информацией и кейс-стади по политике и программам в области ИКТ». В том же году был подписан Меморандум о взаимопонимании по сотрудничеству в науке, технологиях и инновациях, что способствовало расширению механизмов взаимодействия и созданию новых совещательных форматов в рамках обмена опытом в сфере регулирования киберпространства[5].

В целом эти инициативы и события иллюстрируют активное участие Китая в разработке и продвижении международной политики в области кибербезопасности, демонстрируя его стремление к совместной работе и обмену опытом.

---

1 *Tiezzi S.* China's Bid to Write the Global Rules on Data Security [Электронный ресурс] // The Diplomat. 10 September 2020. URL: https://thediplomat.com/2020/09/chinas-bid-to-write-the-global-rules-on-data-security/ (дата обращения: 15.01.2024).

2 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security № A/70/174. United Nations General Assembly. 22 July 2015 [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement (дата обращения: 15.01.2024).

3 *Li J.* China's World Internet Conference goes international as Beijing seeks to promote its own vision of global cyberspace. South China Morning Post. 3 July 2022 [Электронный ресурс]. URL: https://www.scmp.com/tech/big-tech/article/3185151/chinas-world-internet-conference-goes-international-beijing-seeks (дата обращения: 15.01.2024).

4 V BRICS Summit Ethekwini Declaration BRICS and Africa: Partnership for Development, Integration and Industrialisation. Durban, South Africa. 27 March 2013 [Электронный ресурс]. URL: http://brics2022.mfa.gov.cn/eng/hywj/ODS/202203/t20220308_10649513.html (дата обращения: 15.01.2024).

5 Меморандум о сотрудничестве в сфере науки, технологий и инноваций между Правительством Федеративной Республики Бразилии, Правительством Российской Федерации, Правительством Республики Индии, Правительством Китайской Народной Республики и Правительством Южно-Африканской Республики. 23.03.2015 [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru). URL: http://pravo.gov.ru/proxy/ips/?docview&page=1&print=1&nd=102369530&rdk=0&&empire= (дата обращения: 15.01.2024).

Противостояние КНР и США

Повышенное внимание к кибербезопасности со стороны руководства страны также было спровоцировано напряженными отношениями с США, вызванными торговой войной и обострившимися в ходе информационного противостояния, которое, по оценке экспертов, развивается в китайско-американских отношениях с 2009 г. Во время обсуждения в американском конгрессе применения КНР информационных технологий действующий на тот момент президент Барак Обама заявил, что кибератаки являются «одним из наиболее серьезных вызовов экономике и национальной безопасности США» [1, с. 41].

Корень конфликта кроется не просто в двусторонних, направленных на нанесение урона действиях, но и в принципиально разных подходах даже в вопросе, затрагивающем терминологию. Так, в США и европейских странах обычно используется термин «кибербезопасность», означающий в основном обеспечение безопасности архитектуры Интернета. Например, Б. Шнайер, американский специалист по технологиям безопасности, определяет кибербезопасность как важнейший компонент защиты информации и систем от несанкционированного доступа и атак. Его концепция связана с повышением устойчивости систем к угрозам, поддержанием конфиденциальности, целостности и доступности информации[1]. В КНР, как и в России, наиболее употребительным термином является «информационная безопасность», что означает регулирование, или ограничение, распространения нежелательной информации [2, с. 28]. Так, в соответствии с Указом Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» информационная безопасность страны определяется как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[2].

В целом позиция американского правительства о прозрачном контроле над интернет-сетью не пользуется одобрением со стороны китайского руководства. Кроме того, Пекин обвиняет США в милитаризации информационного пространства и присутствии во внутренних сетях Китая [2, с. 29]. Именно американское руководство, по мнению Китая, усиливает гегемонию в мире за счет киберпространства, осложняя политическую ситуацию вокруг вышеназванных, острых для страны тем [7, с. 389].

Руководство США имеет противоположную точку зрения, настаивая на том, что КНР несет в себе потенциальную угрозу для страны в интернет-пространстве. Исследователи ссылаются на доклад Центра стратегических и международных исследований (CSIS, Центр), в котором приводятся следующие сведения: зафиксировано 108 случаев агрессивной политики Китая в информационном поле и 25 нападений на страну; агрессивное поведение со стороны США наблюдалось лишь в 9 случаях, в то время как страна подвергалась сторонним атакам 117 раз. Несмотря на то, что в указанном примере приведено общее количество случаев, КНР ведет себя гораздо более агрессивно по сравнению с США [7, с. 389]. Однако с китайской точки зрения такая статистика не отражает истинного положения вещей, а является искажением реальной действительности.

Сотрудники Центра предполагают, что в ряде кибератак заинтересован сам Китай, особенно в части вопросов, касающихся территориального конфликта в Южно-Китайском море. Так, в 2015 г., когда состоялись слушания по вопросу «совладения» или «совместного освоения» зон архипелага Спратли между Филиппинами и Китаем [6, с. 126], была проведена кибератака на сайт Международного трибунала в Гааге [7, с. 389]. Вместе с тем ученые отмечают и наступательный характер киберстратегии Соединенных Штатов, действия которых провоцируют антиправительственные настроения в Китае, в том числе по вопросам Тибета и Синьцзяна [1, с. 42].

Информационную безопасность, отмечают эксперты, КНР способна обеспечить с помощью существующих на данный момент технологий, учреждений и нормативно-правовой базы. Так, страна занимается раз-

---

[1] *Schneier B.* Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. March 2015. W. W. Norton & Company. P. 7–8.

[2] Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://pravo.gov.ru/proxy/ips/?docbody=&firstDoc=1&lastDoc=1&nd=102417017 (дата обращения: 18.09.2023).

работкой внутренней защищенной сети, в основе которой лежит квантовое шифрование. Подтверждением служит запуск квантовой коммуникационной линии «Пекин — Шанхай», являющейся первым участком сети. Обеспечению кибербезопасности способствует также сотрудничество с внутренними организациями, которые производят высокотехнологичные продукты, и ведущими медиакомпаниями [7, с. 390–391].

Заключение

Современный мир сталкивается с беспрецедентными вызовами в сфере информационной безопасности, которые требуют глобального сотрудничества и скоординированных действий. Анализ политики Китайской Народной Республики в этой области демонстрирует активное участие страны в международном регулировании и развитии международных норм и стандартов кибербезопасности. Отходя от строго национального уклонения в политике информационной безопасности, Китай проявляет стремление к формированию многополярного мира в информационном пространстве, что представляет особый интерес для мирового сообщества.

Международное сотрудничество. Китай не только активно участвует в различных международных организациях и платформах, но и предлагает инициативы, направленные на разработку и укрепление международных норм и стандартов в области кибербезопасности. Среди наиболее ярких примеров: Глобальная инициатива по безопасности данных (2020), обеспечение информационной безопасности и борьба с международным терроризмом в рамках Региональной антитеррористической структуры Шанхайской организации сотрудничества (РАТС ШОС), Ежегодное проведение Всемирной интернет-конференции, в рамках которой страна продвигает китайскую модель управления Интернетом, а также участие в Рабочей группе по безопасности в использовании ИКТ в рамках БРИКС с целью расширения механизмов взаимодействия и создания новых совещательных форматов в рамках обмена опытом в сфере регулирования киберпространства. КНР демонстрирует понимание необходимости защиты глобального информационного пространства от современных угроз, таких как киберпреступность, терроризм и шпионаж. В этом контексте Китай вносит вклад в развитие и укрепление международной информационной безопасности, предлагая свой опыт и ресурсы для создания эффективных механизмов защиты.

Противостояние с США. Китай обеспечивает тотальный контроль китайской интернет-сети, создавая необходимый информационный климат внутри Китая и ограничивая внешнее влияние. Регламентация как технических и организационных действий, так и поведения пользователей в киберпространстве является основным отличием Интернета в Китае [4, с. 181], что провоцирует возникновение противоречий государства с другими странами мира, в частности с США. Взаимодействие Китая и США в сфере кибербезопасности характеризуется в большей степени конкуренцией, чем сотрудничеством.

Упомянутая конкуренция между Китаем и США в информационном пространстве вызывает опасения относительно потенциала киберконфликта между этими двумя мировыми державами. Появление новых технологий и увеличение взаимосвязанности государств сделали киберпространство важной и уязвимой областью международной безопасности. В результате как Китай, так и США инвестируют значительные средства в кибертехнологии, включая наступательные и защитные, и активно разрабатывают кибердоктрины и стратегии.

Наиболее пристальному вниманию в контексте конфронтации между КНР и США подвергаются материалы, связанные с территориальными вопросами, например сепарацией Тибета и Тайваня, а также с конфликтом в Южно-Китайском море [7, с. 389, 392]. Это соперничество, по словам исследователей, оказывает значительное влияние на общемировую военную ситуацию, ускоряя милитаризацию киберпространства, провоцируя напряженность и втягивая в гонку кибервооружений остальные страны [1, с. 43]. Подобные киберугрозы, которые касаются политических, экономических, социальных и других сфер, оказывают негативное воздействие на дальнейшее существование глобальной интернет-сети, имеющее непреходящее значение для развития мирового сообщества.

Для борьбы с этой растущей угрозой необходимо международное сотрудничество и диалог по вопросам кибербезопасности. Разработка норм и правил поведения для государств в киберпространстве,

в создании которых активно участвует Китайская Народная Республика, способствует предотвращению эскалации киберконфликтов, а также стабильности и безопасности в этой области. Кроме того, Китай инвестирует значительные средства в технологии, обеспечивающие кибербезопасность, особенно в критическую инфраструктуру для защиты от потенциальных кибератак, что свидетельствует о ведущей роли Поднебесной не только в решении внутренних проблем, но и о возрастающем влиянии на международную информационную безопасность.

Литература

1. *Антипов К. В.* Киберконфликт в китайско-американских отношениях и поиски диалога // Проблемы Дальнего Востока. 2013. № 6. С. 39–54. EDN: RVWILZ
2. *Булавин А. В.* О подходах США и Китая к обеспечению кибербезопасности // Общество: политика, экономика, право. 2014. № 1. С. 27–31. EDN: RUJYSB
3. *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: образование, наука, новая экономика. 2021. Т. 16. № 3. С. 7–33. EDN: RHBSFR. DOI: 10.17323/1996-7845-2021-03-01
4. *Ибрагимова Г.* Стратегия КНР в области управления интернетом и обеспечения информационной безопасности // Индекс безопасности. 2013. Т. 19. № 1 (104). С. 169–184. EDN: PILMBR
5. *Кулажников В. В.* Нормативно-правовое и технологическое обеспечение информационной безопасности КНР // Образование и право. 2019. № 7. С. 24–30. EDN: ZUPYRL
6. *Локшин Г. М.* Филиппины против Китая в Гаагском арбитраже // Юго-Восточная Азия: актуальные проблемы развития. 2015. № 28. С. 126–133. EDN: VZEOCN
7. *Понька Т. И., Рамич М. С., У Юйяо*. Информационная политика и информационная безопасность КНР: развитие, подходы и реализация // Вестник Российского университета дружбы народов. Сер.: Международные отношения. 2020. Т. 20. № 2. С. 382–394. EDN: UANODL. DOI: 10.22363/2313-0660-2020-20-2-382-394
8. *Разумов Е. А.* Политика КНР по обеспечению кибербезопасности // Россия и АТР. 2017. № 4 (98). С. 156–170. EDN: YMTCGH
9. *Ромашкина Н. П., Задремайлова В. Г.* Эволюция политики КНР в области информационной безопасности // Пути к миру и безопасности. 2020. № 58. С. 122–138. EDN: UAUVRE. DOI: 10.20542/2307-1494-2020-1-122-138
10. *Чекменева Т. Г., Ершов Б. А., Трубицын С. Д., Остапенко А. А.* Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты // Бюллетень социально-экономических и гуманитарных исследований. № 7 (9). 2020. С. 78–97. DOI: 10.5281/zenodo.3911320. EDN: KBYJRD
11. *Lindsay J. R., Cheung T. M., Reveron D. S.* China and Cybersecurity Espionage: Strategy, and Politics in the Digital Domain. Oxford University Press, 2015. 379 p.
12. *Lindsay J. R.* The Impact of China on Cybersecurity: Fiction and Friction // International Security. 2015. Vol. 39. No. 3. P. 7–47. DOI: 10.1162/ISEC_a_00189
13. *Ventre D.* Chinese Cybersecurity and Defense. London : Wiley ISTE, 2014. 301 p. DOI: 10.1002/9781119009009
14. *Zack Beauchamp.* The New US-China Cybersecurity Agreement: A Brief Guide [Электронный ресурс] // VOX.com. 25.09.2015. URL: https://www.vox.com/2015/9/25/9399117/obama-xi-cyber-economic (дата обращения: 06.06.2024).
15. 方滨兴，杜阿宁， 张熙， 王忠儒. 国家网络空间安全国际战略研究 = *Фан Биньсин, Чжун Си, Ван Яжунжу*. Исследование международной стратегии национальной безопасности в области киберпространств // 中国工程科学2016年第18卷第6期 13-16页 = Журнал Китайской инженерной академии. 2016. № 6. P. 13–16. (На китайском)
16. 王桂芳. 大国网络竞争与中国网络安全战略选择 = *Ван Гуйфан*. Киберконкуренция между Великими державами и стратегический выбор кибербезопасности Китая // 国际安全研究. 2017年第2期第27-46页 = Исследования международной безопасности. 2017. № 2. P. 27–46. (На китайском)

Об авторе:

Семенов Борис Романович, аспирант факультета международных отношений и политических исследований Северо-Западного института управления РАНХиГС (Санкт-Петербург, Российская Федерация);
e-mail: bsemenov-13@edu.ranepa.ru

References

1. Antipov K. V. Cyber Conflict in Sino-American Relations and the Search for Dialogue // Far Eastern Studies [Problemy Dal'nego Vostoka]. 2013. No. 6. P. 39–54. (In Russ.) EDN: RVWILZ
2. Bulavin A. V. Concerning Approaches of the USA and China to Cybersecurity // Society: Politics, Economics, Law [Obshchestvo: politika, ekonomika, pravo]. 2014. No. 1. P. 27–31. (In Russ.) EDN: RUJYSB
3. Degterev D. A., Ramich M. S., Piskunov D. A. U.S. & China Approaches to Global Internet Governance: "New Bipolarity" in Terms of "The Network Society" // International Organisations Research Journal [Vestnik mezhdunarodnykh organizatsii: obrazovanie, nauka, novaya ekonomika]. 2021. Vol. 16. No. 3. P. 7–33. (In Russ.) EDN: RHBSFR. DOI: 10.17323/1996-7845-2021-03-01
4. Ibragimova G. China's Strategy in Cyberspace: The Issues Internet Governance and Information Security // Security Index [Indeks bezopasnosti]. 2013. Vol. 19. No. 1 (104). P. 169–184. (In Russ.) EDN: PILMBR
5. Kulazhnikov V. V. Regulatory Legal and Technological Support of China's Information Security // Education and Law [Obrazovanie i pravo]. 2019. No. 7. P. 24–30. (In Russ.) EDN: ZUPYRL
6. Lokshin G. M. The Philippines against China in the Haig Tribunal // Southeast Asia: Actual Problems of Development [Yugo-Vostochnaya Aziya: aktual'nye problemy razvitiya]. 2015. No. 28. P. 126–133. (In Russ.) EDN: VZEOCN
7. Ponka T. I., Ramich M. S., Y. Wu. Information Policy and Information Security of PRC: Development, Approaches and Implementation // Vestnik RUDN. International Relations [Vestnik Rossiiskogo universiteta druzhby narodov. Ser.: Mezhdunarodnye otnosheniya]. 2020. Vol. 20. No. 2. P. 382–394. (In Russ.) EDN: UANODL. DOI: 10.22363/2313-0660-2020-20-2-382-394
8. Razumov E. A. PRC's Cybersecurity Policy // Russia and the Pacific Region [Rossiya i ATR]. 2017. No. 4 (98). P. 156–170. (In Russ.) EDN: YMTCGH
9. Romashkina N. P., Zadremailova V. G. Evolution of China's Information Security Policy // Pathways to Peace and Security [Puti k miru i bezopasnosti]. 2020. No. 58. P. 122–138. (In Russ.) EDN: UAUVRE. DOI: 10.20542/2307-1494-2020-1-122-138
10. Chekmeneva T. G., Ershov B. A., Trubitsyn S. D., Ostapenko A. A. China's Information Security Strategy: Political and Technical Aspects // Bulletin Social-Economic and Humanitarian Research [Byulleten' sotsial'no-ekonomicheskikh i gumanitarnykh issledovanii]. 2020. No. 7 (9). P. 78–97. (In Russ.) EDN: KBYJRD. DOI: 10.5281/zenodo.3911320
11. Lindsay J. R., Cheung T. M., Reveron D. S. China and Cybersecurity Espionage: Strategy, and Politics in the Digital Domain. Oxford University Press, 2015. 379 p.
12. Lindsay J. R. The Impact of China on Cybersecurity: Fiction and Friction // International Security. 2015. Vol. 39. No. 3. P. 7–47. DOI: 10.1162/ISEC_a_00189
13. Ventre D. Chinese Cybersecurity and Defense. London: Wiley ISTE, 2014. 301 p. DOI: 10.1002/9781119009009
14. Zack Beauchamp. The New US-China Cybersecurity Agreement: A Brief Guide [Electronic resource] // VOX.com. 25.09.2015. URL: https://www.vox.com/2015/9/25/9399117/obama-xi-cyber-economic (accessed: 06.06.2024).
15. Fan Bingsin, Zhong Xi, Wang Yazhong. Research on the International Strategy of National Security in the Field of Cyberspace // Chinese Academy of Engineering Journal. 2016. No. 6. P. 13–16. (In Chinese)
16. Wang Guifan. Cyber-competition between Great Powers and China's strategic choice in cybersecurity // International Security Research. 2017. No. 2. P. 27–46. (In Chinese)

About the author:

Boris R. Semenov, graduate student at the Faculty of International Relations and Political Studies at the North-West Institute of Management of the RANEPA (Saint Petersburg, Russian Federation);
e-mail: bsemenov-13@edu.ranepa.ru