Зарубежный опыт. Международной сотрудничество

СПЕЦИФИКА СОТРУДНИЧЕСТВА РФ И КНР В ОБЛАСТИ ИКТ

Статья рекомендована к публикации членом редакционного совета А.А. Стрельцовым 25.04.2022.

Малчинова Айсура Эжеровна

Магистр
Московский государственный университет имени М.В.Ломоносова, факультет глобальных процессов
Москва, Российская Федерация
aysura.malchinova@gmail.com

Аннотация

В статье рассматривается понятие международной информационной безопасности, а также специфика киберугроз. Поднимается вопрос актуальности обеспечения глобальной информационной безопасности. Изучается подход Российской Федерации и Китайской Народной Республики к проблеме защищенности информационного пространства. Автором рассмотрено взаимодействие двух стран в вопросе обеспечения кибербезопасности, выявлена специфика сотрудничества.

Ключевые слова

кибербезопасность; киберугрозы; международная информационная безопасность; информационно-коммуникационные технологии; информационное пространство; Российская Федерация Китайская Народная Республика; Организация Объединенных Наций; многосторонность; коллективная безопасность

Возникновение и активное развитие цифровизации уже стало отличительной чертой XXI века. С появлением современных технологий общество переходит на новый этап своего развития – информационный [1]. С этого времени информационные технологии интегрируются в мировое развитие, закрепляя существование информационного общества. Процессы цифровизации с каждым годом оказывают все большее влияние на жизнь людей, отдельные домохозяйства и мировую экономику. Вместе с огромными возможностями, предоставляемыми цифровыми данными и технологиями, современное общество сталкивается с угрозами нового порядка. К ним можно отнести: проблему неравенства доходов в развитых и развивающихся государствах, отсутствие единой основы в сфере регулирования цифровых услуг и киберугрозы, представляющие опасность как государству, так и личности. Интернет-пользователи заинтересованы в безопасном пользовании глобальной сети, защите от кибератак и различных видов киберпреступности. Всесторонняя информатизация общества также обостряет уязвимость государств перед угрозами информационных атак. Информационный ресурс является мощным оружием в руках государств, способное оказать значительное влияние на геополитические процессы и воздействовать на ситуацию в других государствах. На сегодняшний день, информационное пространство – необходимое условие для развития государства и платформа политического противостояния. Таким образом, обеспечение информационной безопасности становится одним из приоритетных направлений деятельности государств современного миропорядка.

Международная информационная безопасность - состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности [2]. В Организации Объединенных Наций под данным термином подразумевается состояние защищенности глобальной информационной системы от террористических, преступных и военно-политических угроз [3].

https://doi.org/10.52605/16059921_2022_04_96

Отличительной чертой проблемы информационной безопасности является ее многоаспектность. Она включает в себя не только информационную составляющую, но также экономическую, коммуникационную, политическую, энергетическую, военную и т.д. Более того, транснациональность – характеристика проблемы обеспечения безопасности в киберпространстве. Обеспечение информационной безопасности достигается путем технической и юридической деятельности. Природа информационных угроз едина для всего мирового сообщества, в связи с этим механизмы регулирования в сфере киберпространства также требуют унификации. Следует отметить, что в вопросе выработки единых принципов регулирования Интернет-пространства, не следует допускать навязывания правил одним государством или группой стран, необходимо одобрение мирового сообщества. В противном случае, будет это может негативно сказаться на информационном пространстве.

Упорядочивание процессов в Интернете усложняется влиянием общемировой обстановки. Нормы регулирования киберпространства вырабатываются как на национальном, так и на региональном уровне. Развитые государства в последние годы ведут активную работу над созданием технической и юридической защиты от киберугроз: создание систем распознавания, предупреждения и уничтожения попыток информационных атак и развитие регулирования информационного пространства на законодательном уровне. Тем не менее, в силу глобальности мировой сети Интернет, необходимость в многостороннем взаимодействии при решении проблем киберугроз становится все более очевидной. Государства-союзники работают над созданием совместных программ по противодействию информационным угрозам, развивают сотрудничество в сфере информационно-коммуникационных технологий. Активная деятельность в сфере обеспечения информационной безопасности ведется на площадке ООН, Европейского союза, БРИКС, ШОС, ЕАЭС, СНГ и т.д.

«Развитие безопасного информационного пространства, защита российского общества от деструктивного информационно-психологического воздействия» - один из пунктов национальных интересов и стратегических национальных приоритетов России согласно Стратегии национальной безопасности Российской Федерации от 02.07.2021 [4]. Таким образом, вопрос обеспечения информационной безопасности – неотъемлемый элемент системы национальной безопасности нашего государства.

Противодействие угрозам информационной безопасности на национальном уровне в России рассматриваются в Доктрине информационной безопасности [5]. Самостоятельность государства в международном информационном сообществе и независимость в выборе источников информации – основа борьбы с дезинформационными атаками. Информационная безопасность нации состоит из нескольких компонентов. Информация является главным фактором поддержания государства в политической, социальной, экономической и военной сферах.

Информационную безопасность в Российской Федерации, как известно, поддерживают следующие службы: Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Министерство цифрового развития, связи и массовых коммуникаций, а также различные ведомственные и межведомственные подразделения.

Россия активно содействует расширению сотрудничества в сфере кибербезопасности на международном уровне. Реализация государственной политики в обеспечении международной информационной безопасности предполагается на площадке Организации Объединенных Наций как площадки для многостороннего диалога и выработки Конвенции. Кроме того, обсуждение и сотрудничество по данному вопросу проходит в рамках других межгосударственных организаций: СНГ, БРИКС, ОДКБ, ШОС, АСЕАН и т.д [6].

Говоря о вкладе России в сфере развития международной безопасности, следует отметить инициативу российских дипломатов в 1998 году. Генеральной Ассамблеей Организации Объединенных Наций была принята резолюция «Достижение в сфере информатизации и телекоммуникации в контексте международной безопасности». Принятия данного документа означало постановку вопроса международной информационной безопасности на глобальном уровне. С этого момента мировое сообщество обратило свое внимание на существование информационных угроз и начало вырабатывать единый механизм регулирования для обеспечения и укрепления системы безопасности от атак на информационном пространстве.

Рассмотрим систему информационной безопасности Китая. Глобальная сеть появилась в Китае в 1987 году, массовое пользование Интернетом началось после 1995 года. С конца 1990-ъх годов начались массовые кибератаки на информационную сеть Китайской Народной Республики. Серьезный ущерб информационной безопасности Китая в 1999 году нанес вирус, созданный на Тайване. Он повредил около полумиллиона компьютеров, треть которых находились на материковом Китае. В начале 2000-х годов под удар информационных атак попали правительственные сайты страны.

Начиная с 1991 года Китайская Народная Республика начала активную работу по выработке нормативно-правовых актов, регулирующих информационное пространство. К первым документам в сфере информационного регулирования относятся: «Общегосударственный регламент организации труда по информационным компьютерным системам и противодействию интернет-вирусам» 1991 г., «Временные положения администрирования компьютерно-информационных систем и международной сети Интернет» 1996 г. и др [7].

В настоящее время в Китае киберпространство регламентируется следующими документами:

1. Закон о кибербезопасности 2017 года. Принятие данного закона привело к усилению государственного контроля над информационной деятельностью компаний в Интернет пространстве. Закон определяет операции серверов с пользовательскими данными, специфику обеспечения информационной безопасности в стратегически важных отраслях.

2. Национальная стратегия по безопасности в киберпространстве. В Стратегии отмечается, что для обеспечения информационной безопасности в стране необходимо предотвращать любые вмешательства во внутреннюю жизнь государства: в политическую, социальную и культурную сферы. В Стратегии указывается главный проект кибербезопасности Китая – «Золотой щит» - система фильтрации интернет-контента.

3. Стратегия международного сотрудничества в киберпространстве 2017 года. Первый официальный нормативно-правовой акт, закрепляющий вопросы участия Китая в международном сотрудничестве в сфере обеспечения международной информационной безопасности.

Деятельность в области обеспечения международной информационной безопасности Китая осуществляется на площадке Организации Объединенных Наций, Шанхайской организации сотрудничества и БРИКС.

Высшим органом системы обеспечения кибербезопасности Китая является Центральный военный совет. Полномочиями по реализации системы информационной безопасности обладают: Бюро общественной информации и надзора за сетевой безопасностью, Министерство государственной безопасности, Министерства науки и технологий и др.

Отличительной особенностью регулирования информационного пространства Китайской Народной Республики является влияние Коммунистической партии Китая. В целях координации обеспечения кибербезопасности создана Центральная комиссия по киберпространству, в состав которой входит высшее руководство страны и руководители профильных ведомств.

Большую роль в разграничении контента играет Государственное управление по делам радиовещания, кинематографии и телевидения. Оно ответственно за блокировку нежелательной информации в китайском Интернете. Значительный вклад в обеспечение кибербезопасности вносит Народно-освободительная армия Китая. В обязанности китайских военных структур входит разведывательная деятельность в Интернете, поиск уязвимостей в национальной системе защиты информационной безопасности, а также выработка комплекса мер по предотвращению кибератак.

Сущность китайской системы обеспечения безопасности в информационном пространстве заключается в совокупности технических мер по поддержанию защитной системы устройств и контроле национальной инфраструктуры сети Интернет. Особое внимание уделяется государственному суверенитету в сфере информационной безопасности. Согласно закону о кибербезопасности, интернет-провайдеры обязаны хранить персональные данные пользователей на территории КНР.

Китайская Народная Республика заявляет об открытости к международному сотрудничеству в сфере информационного противоборства. В 2019-2020 гг. Китай испытал сильные атаки на предлагаемые им технологии: облачные хранилища, технологии 5G [8]. Вопрос развития информационно-коммуникационных технологий для Китая связан с насущными вопросами обеспечения глобальной информационной безопасности.

Взаимодействие Китая и России в данной сфере на сегодняшний день является одним из самых продвинутых в сравнении с другими странами. И Китай, и Россия предпринимают действия по усилению национальных систем защит от киберугроз и созданию суверенного Интернета. Рассмотрим взаимодействие РФ и КНР в области информационно-коммуникационных технологий в ретроспективе.

В 2002 году была создана Российско-китайская рабочая группа по сотрудничеству в области СМИ, ее первое заседание проводилось в Пекине. Это положило начало для взаимного сотрудничества стран в сфере телевидения, радио, информационных служб. Страны обменивались опытом, техническими достижениями, начал складываться фундамент для создания договорно-правовой базы сотрудничества. В 2008 году данный формат сотрудничества был преобразован в Подкомиссию по сотрудничеству в области СМИ Российско-Китайской комиссии по гуманитарному сотрудничеству.

В 2015 году в Санкт-Петербурге был проведен российско-китайский медиа-форум. В ходе обсуждений затрагивались вопросы освещения СМИ стратегических проектов, сотрудничество сетевых СМИ, совместное освещение международных вопросов. Кульминацией развития сотрудничества двух стран в области информационно-коммуникационных технологий стало Соглашение о сотрудничестве в области обеспечения международной информационной безопасности. главами внешнеполитических ведомств России и Китая в 2015 году [9]. Целью соглашения была также провозглашена совместная деятельность по обеспечению национальной и международной информационной безопасности. Два государства обязались сотрудничать в противостоянии использованию информационно-коммуникационных технологий в преступных целях. В 2016-2017 годах в России и Китае были проведены «Годы китайских и российских СМИ».

Китай и Россия – единомышленники в вопросе создания системы обеспечения международной информационной безопасности. Более двадцати лет государства совместно продвигают внедрение систем многостороннего регулирования Интернета в Организации Объединенных Наций. Обе страны негативно оценивали систему ICAAN, которая предоставляла США возможность быть монополистом в управлении глобальной сети.

В 2011 году Китай и Россия выступили с инициативой концепции Конвенции «Об обеспечении международной информационной безопасности». Российско-китайское предложение включало в себя правила поведения государств при взаимодействии в киберпространстве в целях обеспечения информационной безопасности. Однако данная инициатива не получила должной реакции у стран Запада, привела к противостоянию взглядов на проблему международной информационной безопасности: западная модель с монополизацией безопасности и альтернативный российско-китайский подход с коллективной системой международной безопасности. После дела Эдварда Сноудена в 2013 году в информационном сообществе начался процесс демонополизации системы безопасности.

Два государства ведут сотрудничество по вопросам международной информационной безопасности в региональных форматах. Так в 2011 году в рамках Шанхайской Организации Сотрудничества было подписано соглашение между правительствами государств-членов в области обеспечения кибербезопасности [10]. В 2020 году Совет глав государств-членов ШОС в Московской декларации подчеркнул необходимость разработки единых стандартов на основе норм международного права. В рамках БРИКС вопрос информационной безопасности затрагивается в Форталезской и Уфимской декларациях [11].

Сотрудничество Китая и России в сфере информационно-коммуникационных технологий обусловлено тем фактом, что обе страны считаются киберугрозами для стран Запада. В последнее время оба государства все чаще придерживаются конфронтационных отношений с Западом в информационной области: критика действий Запада, отрицание критики своей страны западным блоком, продвижение собственного видения на международном инфополе. Отдельно отмечается сходство инструментов Китая и России, используемых в целях критики западного режима. Некоторые исследователи утверждают, что соглашения между странами в области информационно-коммуникационных технологий носят символический характер. Несмотря на общность целей Китая и России в информационном пространстве, а к ним относят противостояние Западу, защита собственных политических режимов, продвижение идей и тезисов, выгодных России и Китая, на пути достижения этих целей два государства действуют параллельно, не организовывая единый фронт [12].

Рассмотрим на общности позиций двух государств. Во-первых, единое понимание и представления природы информационных атак и угроз. Во-вторых, работа над созданием суверенного и защищенного интернета. законодательства, регулирующие информационную сферу, обоих государств являются одними из самых жестких в мире. В-третьих, готовность к взаимодействию в области информационно-коммуникационных технологий не только на межнациональном уровне, но и на региональных площадках (ШОС, БРИКС).

Однако существуют и препятствия для более тесной совместной деятельности в данном направлении. Несмотря на подписанные соглашения по сотрудничеству, СМИ государств, информационные службы всегда ставят интересы собственного государства превыше других. Необходимо учитывать данный фактор при дальнейшем развитии российско-китайского взаимодействия в информационном пространстве.

Более того, стоит обратить внимание, на курс внешней политики Китайской Народной Республики. Декларируя открытость к сотрудничеству со всем миром, Китай все же остается крайне прагматичным: каждому партнеру отводится определенная роль. В случае с взаимодействием с Россией в области информационно-коммуникационных технологий, заинтересованность Китая заключается в политическом и пропагандистском аспектах [13].

Стоит отметить, что сотрудничество государств в области масс-медиа осуществляется при поддержке правительств двух стран, с использованием административного ресурса. Данный подход обеспечивает общность информационной повестки при освещении международных вопросов, так и внутригосударственных. Однако при таком методе невозможно полное информационное согласие.

Отличительной чертой позиции России и Китая по вопросу обеспечения международной безопасности является многосторонность. Страны призывают к разработке универсальных принципов безопасности в информационном пространстве. Принцип коллективности в аспектах, связанных с обеспечением глобальной безопасности, прослеживается в позициях стран по другим международным вопросам.

Литература

1. Науменко Т.В. Информационное общество и глобализация проблемы идентификации. // Информационное общество. 2017. №6. С.4-10.
2. Указ Президента РФ от 12.04.2021 N 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности". URL: https://www.consultant.ru/document/cons_doc_LAW_381999/ (дата обращения: 04.03.2022).
3. Зиновьева Е.С. Международная информационная безопасность // МГИМО Университет, 2014. URL: https://mgimo.ru/about/news/experts/256505/ (дата обращения: 04.03.2022).
4. Указ Президента Российской Федерации от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации". URL: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=8&rangeSize=1 (дата обращения: 04.03.2022).
5. Указ Президента Российской Федерации от 05.12.2016 № 646 "Об утверждении Доктрины информационной безопасности Российской Федерации". URL: http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1 (дата обращения: 04.03.2022).
6. Указ Президента РФ от 12 апреля 2021 г. № 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности". URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (дата обращения: 04.03.2022).
7. Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности // Китай в мировой и региональной политике. История и современность, 2018. №23. URL: https://cyberleninka.ru/article/n/rossiysko-kitayskoe-vzaimodeystvie-po-voprosam-obespecheniya-informatsionnoy-bezopasnosti (дата обращения: 07.03.2022).

8. Маслов А. Перспективы и вызовы цифровому будущему // Специальный проект RG.RU Digital, 2021. URL: https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html (дата обращения 07.03.2022)
9. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 года (вступило в силу 10 августа 2016 года). URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (дата обращения: 07.03.2022).
10. Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. URL: https://docs.cntd.ru/document/902289626 (дата обращения: 07.03.2021).
11. Уфимская декларация. VII саммит БРИКС (Уфа. 9 июля 2015 г.) URL: https://base.garant.ru/71480256/ (дата обращения: 07.03.2022).
12. Габуев А., Ковачич Л. Товарищи по твитам: становятся ли Россия и Китай партнерами в информационной сфере? // Московский центр Карнеги, 2021. URL: https://carnegie.ru/2021/06/11/ru-pub-84741 (дата обращения: 07.03.2022).
13. Исаев А.С. Институты формирования общественного сознания КНР и вопросы сотрудничества СМИ России и Китая // Китай в мировой и региональной политике. История и современность, 2016. №21. URL: https://cyberleninka.ru/article/n/instituty-formirovaniya-obschestvennogo-soznaniya-knr-i-voprosy-sotrudnichestva-smi-rossii-i-kitaya (дата обращения: 08.03.2022).

SPECIFICS OF COOPERATION BETWEEN THE RUSSIAN FEDERATION AND CHINA IN THE FIELD OF ICT

Malchinova Aysura Ezherovna

Master
Lomonosov Moscow State University, Faculty of global studies
Moscow, Russian Federation
Aysura.malchinova@gmail.com

Abstract

The article discusses the concept of international information security, as well as the specifics of cyber threats. The question of the relevance of ensuring global information security is raised. The approach of the Russian Federation and the People's Republic of China to the problem of information space security is being studied. The author considers the interaction of the two countries in the issue of ensuring cybersecurity, reveals the specifics of cooperation.

Keywords

cyber security; cyber threats; international information security; information and communication technologies; information space; Russian Federation, People's Republic of China; United Nations; versatility; collective security

References

1. Naumenko T.V. Informacionnoe obshchestvo i globalizaciya problemy identifikacii. // Informacionnoe obshchestvo. 2017. №6. P.4-10.
2. Ukaz Prezidenta RF ot 12.04.2021 N 213 "Ob utverzhdenii Osnov gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti". URL: https://www.consultant.ru/document/cons_doc_LAW_381999/ (data obrashcheniya: 04.03.2022).
3. Zinov'eva E.S. Mezhdunarodnaya informacionnaya bezopasnost' // MGIMO Universitet, 2014. URL: https://mgimo.ru/about/news/experts/256505/ (data obrashcheniya: 04.03.2022).
4. Ukaz Prezidenta Rossijskoj Federacii ot 02.07.2021 № 400 "O Strategii nacional'noj bezopasnosti Rossijskoj Federacii". URL: http://publication.pravo.gov.ru/Document/View/0001202107030001?index=8&rangeSize=1 (data obrashcheniya: 04.03.2022).
5. Ukaz Prezidenta Rossijskoj Federacii ot 05.12.2016 № 646 "Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii". URL: http://publication.pravo.gov.ru/Document/View/0001201612060002?index=0&rangeSize=1 (data obrashcheniya: 04.03.2022).
6. Ukaz Prezidenta RF ot 12 aprelya 2021 g. № 213 "Ob utverzhdenii Osnov gosudarstvennoj politiki Rossijskoj Federacii v oblasti mezhdunarodnoj informacionnoj bezopasnosti". URL: https://www.garant.ru/products/ipo/prime/doc/400473497/ (data obrashcheniya: 04.03.2022).
7. Isaev A.S. Rossijsko-kitajskoe vzaimodejstvie po voprosam obespecheniya informacionnoj bezopasnosti // Kitaj v mirovoj i regional'noj politike. Istoriya i sovremennost', 2018. №23. URL: https://cyberleninka.ru/article/n/rossiysko-kitayskoe-vzaimodeystvie-po-voprosam-obespecheniya-informatsionnoy-bezopasnosti (data obrashcheniya: 07.03.2022).
8. Maslov A. Perspektivy i vyzovy cifrovomu budushchemu // Special'nyj proekt RG.RU Digital, 2021. URL: https://rg.ru/2021/07/15/pozicii-rossii-i-kitaia-po-voprosam-kiberbezopasnosti-vo-mnogom-sovpali.html (data obrashcheniya 07.03.2022).
9. Soglashenie mezhdu Pravitel'stvom Rossijskoj Federacii i Pravitel'stvom Kitajskoj Narodnoj Respubliki o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti ot 8 maya 2015 goda (vstupilo v silu 10 avgusta 2016 goda). URL: http://publication.pravo.gov.ru/Document/View/0001201608100001?rangeSize=1 (data obrashcheniya: 07.03.2022).

10. Soglashenie mezhdu pravitel'stvami gosudarstv - chlenov Shankhajskoj organizacii sotrudnichestva o sotrudnichestve v oblasti obespecheniya mezhdunarodnoj informacionnoj bezopasnosti. URL: https://docs.cntd.ru/document/902289626 (data obrashcheniya: 07.03.2021).
11. Ufimskaya deklaraciya. VII sammit BRIKS (Ufa. 9 iyulya 2015 g.) URL: https://base.garant.ru/71480256/ (data obrashcheniya: 07.03.2022).
12. Gabuev A., Kovachich L. Tovarishchi po tvitam: stanovyatsya li Rossiya i Kitaj partnerami v informacionnoj sfere? // Moskovskij centr Karnegi, 2021. URL: https://carnegie.ru/2021/06/11/ru-pub-84741 (data obrashcheniya: 07.03.2022).
13. Isaev A.S. Instituty formirovaniya obshchestvennogo soznaniya KNR i voprosy sotrudnichestva SMI Rossii i Kitaya // Kitaj v mirovoj i regional'noj politike. Istoriya i sovremennost', 2016. №21. URL: https://cyberleninka.ru/article/n/instituty-formirovaniya-obschestvennogo-soznaniya-knr-i-voprosy-sotrudnichestva-smi-rossii-i-kitaya (data obrashcheniya: 08.03.2022).