ГАО ЮЕ
аспирант, Московский государственный университет имени М.В. Ломоносова, Москва, Россия
gaoyue199412@gmail.com

GAO YUE
Postgraduate student of Lomonosov Moscow State University, Moscow, Russia
gaoyue199412@gmail.com

Особенности и перспективы российско-китайского сотрудничества в сфере обеспечения информационной безопасности / Features and prospects of Russian-Chinese cooperation in the field of information security

Аннотация

В настоящей статье исследуется актуальная проблематика стратегического взаимодействия между Российской Федерацией и Китайской Народной Республикой в области информационной безопасности. На основе исследования нормативно-правовых документов информационной политики обоих государств автором дается оценка актуального состояния взаимоотношений между Россией и КНР в сфере обеспечения суверенного киберпространства.

Вместе с тем автором отдельно рассмотрены такие стороны информационной безопасности, как кибертерроризм и кибератаки. Предложены методы и механизмы, направленные на предотвращение и минимизацию эффекта киберагрессии.

В конце статьи автором проведено сравнение ключевых элементов информационной политики как России, так и Китая, и обозначены перспективы сотрудничества этих стран в условиях формирующегося нового миропорядка.

Ключевые слова

Китай; киберагрессия; кибертерроризм; информационная безопасность; ШОС; ОДКБ.

Abstract

This article examines the topical issues of strategic cooperation between the Russian Federation and the People's Republic of China in the field of information security. Based on the study of the normative legal documents of the information policy of both states, the author assesses the current state of relations between Russia and China in the sphere of ensuring sovereign cyberspace.

At the same time, the author separately considered such a side of information security as cyberterrorism and cyberattacks. Methods and mechanisms aimed at preventing and minimizing the effect of cyber aggression are proposed.

At the end of the article, the author compares the key elements of the information policy of both Russia and China and outlines the prospects for

cooperation between these countries in the emerging new world order.

Keywords

China; cyber aggression; cyberterrorism; information security; SCO; CSTO.

Наблюдаемое в настоящее время ускоренное развитие новых цифровых технологий во многом обуславливает потребность в усилении информационной безопасности большинства стран мира. В данном плане Россия и Китай не являются исключением. Цифровая среда содержит два источника угроз: опасность кибератак и ее становление плацдармом для «манипуляции общественным мнением»[1]. Так, китайские технологические гиганты в 2019-2020 гг. подверглись хакерским атакам. В том числе пострадали Huawei, Alibaba, ZTE[2]. 14 апреля 2022 г. МИД РФ также заявил о резком росте числа кибератак на Россию[3]. Как представляется некоторым исследователям, например Исаеву А.С., с мнением которого мы полностью согласны, обеспечение безопасности информационной политики и компьютерных технологий является многоуровневой проблемой из-за высокого уровня проникновения Интернета во все сферы жизни современных обществ, поэтому от эффективности мер в киберпространстве также зависят экономическая, энергетическая, социально-политическая, военная безопасность и стабильность общества[4].

И Китай, и Россия предпринимают комплексные меры для защиты собственных цифровых сред, в том числе, в сотрудничестве друг с другом. Главный шаг к этой цели – создание устойчивых сетей интернет и телекоммуникаций, а также «внутреннего интернета» компаний и госструктур. При этом обе страны понимают, что обеспечение безопасности информационно-коммуникационных технологий «тесно связано с вопросами обеспечения глобальной конкурентоспособности и безопасности»[5].

Очевидно, что эффективность борьбы с киберугрозами зависит от понимания принципов работы Интернета и факторов риска всем мировым сообществом. В связи с этим особенно важно взаимодействие России и Китая по обеспечению безопасности ИКТ, особенно на фоне усиления взаимодействия в науке и технике и противодействия общим

[1]Иванов И.С., Се Ф. 20-летие Договора о добрососедстве, дружбе и сотрудничестве между РФ и КНР. РСМД, 2021. С. 58.

[2] Там же. С. 58.

[3][Электронный ресурс]. Режим доступа: https://ria.ru/20220414/kiberbezopasnost-1783470960.html (дата обращения: 22.08.22).

[4] Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности. Китай в мировой и региональной политике. История и современность - ИДВ РАН, Т. 23 №23, 2018. С. 226.

[5] Иванов И.С., Се Ф. 20-летие Договора о добрососедстве, дружбе и сотрудничестве между РФ и КНР. РСМД, 2021. С. 58.

вызовам.

Так, в сентябре 2021 г. на 25-ом заседании Российско-Китайской подкомиссии по научно-техническому сотрудничеству обе страны договорились расширить сотрудничество в научно-технической и инновационной сферах[1], а в декабре 2021 г. замглавы МИД РФ Олег Сыромолотов подтвердил намерение о совместной борьбе с терроризмом и другими вызовами[2].

Вместе с тем в последнее десятилетие некоторые западные страны стали видеть именно в КНР и России угрозу собственной информационной кибербезопасности. Так, власти США, Канады и ряда других стран включают обе страны в списки источников угрозы национальной безопасности[3]. С точки зрения некоторых российских исследователей, «Коллективный Запад» может использовать информационное пространство для оправдания собственных геополитических планов. Похожая тактика использовалась для обоснования агрессии против Югославии, Ирака, Ливии, Сирии и других государств[4]. Ожесточенное противостояние в информационном пространстве на современном этапе является еще одной причиной для России и Китая добиться собственного суверенитета в области управления интернет-пространством и исключить любые попытки внешнего негативного информационного вмешательства во внутренние дела.

Очень важно, что обе страны сходятся в понимании основных направлений работы в киберпространстве.

Во-первых, это схожее определение комплексного характера атак и угроз, которые исходят из киберпространства (включение террористических угроз, возможность политических онлайн-провокаций и политической дестабилизации и т.д.). Перечисление подобных источников опасности киберпространства часто встречается в выступлениях высших должностных лиц обеих стран[5].

Во-вторых, это схожие шаги по созданию «защищенного интернета», а также национальных социальных сетей. Китай давно начал создание суверенного интернета: в 2011 г. был создан полностью китайский аналог мессенджеров WeChat, аналог Twitter – Weibo, аналог YouTube – Youku. Однако в России граждане активно пользуются

[1] [Электронный ресурс]. Режим доступа: https://minobrnauki.gov.ru/press-center/news/?ELEMENT_ID=40118 (дата обращения: 22.08.22).

[2] [Электронный ресурс]. Режим доступа: https://tass.ru/politika/13268039?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 22.08.22).

[3] См.: Иванов И.С., Се Ф. 20-летие Договора о добрососедстве, дружбе и сотрудничестве между РФ и КНР. РСМД, 2021.

[4] Лузянин С.Г. Российско-китайский диалог: модель 2017: доклад № 18/2015. С. 31-32.

[5] [Электронный ресурс]. Режим доступа: https://tass.ru/politika/11006783?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 22.08.22) и http://www.cac.gov.cn/2018-12/27/c_1123907720.htm (дата обращения: 22.08.22).

как национальными платформами (такими, как VK и Одноклассники), так и международными платформами.

Однако несмотря на то, что Россия пока не так радикальна в своих мерах, как Китай, обе страны регулярно подтверждают намерения совместных усилий в этой сфере, в том числе на базе Шанхайской организации сотрудничества (ШОС) и БРИКС, где РФ и Китай занимают ведущие роли. На данный момент законодательства России и КНР стали более системными и эффективными в сфере регулирования информационной безопасности и противодействию терроризму и экстремизму в интернет-пространстве.

Преимущество современного цифрового развития Китая – это комплексный подход к задаче цифровизации. Он включает как меры по цифровизации традиционных отраслей, так и физическое обеспечение растущих потребностей в скорости Интернета для передачи больших данных, так и поддержании устойчивости электросетей, генерации, хранения и передачи электроэнергии на большие расстояния и проведения Интернета по всей стране.

Отдельно стоит остановиться на основных этапах плана развития цифровой экономики КНР:

- «Сделано в Китае-2025» (2013 г.);
- «Интернет +» (2015 г.);
- «Национальный план развития информатизации» (2016 г.);
- «Национальная стратегия взаимодействия в кибер-пространстве» (2017 г.);
- «Новая инфраструктура» (2020 г.) и др.

Для обеспечения цифровой безопасности стратегии регулируются «Закон о национальной безопасности», «Закон об информационной безопасности» и т.д.[1]. Первый был принят в 2015 г., второй вступил в силу 2017 г. «Закон об информационной безопасности» можно назвать главным законом, регулирующим деятельность в цифровой среде КНР. В этих перечисленных документах и планах прописаны главные цели политики КНР в сфере Интернета: оградить отечественную цифровую среду от возможных утечек, атак иностранных спецслужб и хакеров, а также поднять уровень цифровизации страны. Данные законы дали толчок развитию рынка сервисов обеспечения цифровой безопасности. Так, с 2014 г. по 2019 г. он вырос с $2,11 млрд до $3,62 млрд.[2]

Россия также активно работает над созданием национальных проектов по развитию безопасности в интернет-сфере. Например, была принята комплексная программа «Цифровая экономика» на 2019–2024 гг. Одним из направлений работы стала информационная безопасность. На ее реализацию планируется выделить 34,204 млрд. руб. На направление «Цифровые технологии» в рамках

[1]Иванов И.С., Се Ф. 20-летие Договора о добрососедстве, дружбе и сотрудничестве между РФ и КНР. РСМД, 2021.

[2] Там же.

программы будет выделено 451,809 млрд. руб. При этом основные расходы программы (17,984 млрд. руб.) будут финансироваться из государственного бюджета.[1]

С ростом информатизации увеличилось количество потребляемой и поступающей в Интернет информации, поэтому защита данных является одним из важнейших вопросов кибербезопасности. В современном Китае мы можем выделить три ключевых нормативно-правовых акта, регулирующих данную сферу отношений: Закон КНР «О безопасности данных», «О сетевой безопасности» и «О защите персональных данных»[2].

Отметим немаловажный факт, что «Закон о безопасности данных» был принят Постоянным комитетом Всекитайского собрания народных представителей (ПК ВСНП) и вступил в силу 1 сентября 2021 г. Он стал юридической базой в сфере обеспечения сохранности информации, так как в нем впервые объясняется понятие «данные» (кит. 数据), сбора, хранения, передачи, управления информацией, а также определяется правовая ответственность за их нарушение[3]. Данные классифицируются по уровню значимости для государства и вреда, которые их утечка сможет причинить, а также определяются различные способы и механизмы защиты информации. Вместе с тем данный закон наделяет региональную власть достаточно большой самостоятельностью в вопросах информационной безопасности, так как местные правительства могут индивидуально определять приоритеты развития и защиты информационного пространства.

Учитывая естественное желание национального правительства оградить страну от возможных кибератак, законодательство Китая в области регулирования данных строго следит за безопасностью личной информации собственных граждан. Мониторинг за соблюдением законодательства осуществляет Государственная канцелярия по делам интернет-информации (CAC) (кит. 中华人民共和国国家互联网信息办公室). Операторы данных, в том числе иностранные, ведущие деятельность на территории КНР, по «Закону о безопасности данных» стали обязаны передавать регулятору отчетность об объеме хранимой важной информации, количестве совершенных кибератак и т.п. CAC также может запросить отчет о сетевой безопасности деятельности операторов за границей[4].

---

[1] [Электронный ресурс]. Режим доступа: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 22.08.22).

[2] [Электронный ресурс]. Режим доступа: https://ru.chinajusticeobserver.com/law/x/data-security-law-of-the-people-s-republic-of-china20210610 (дата обращения: 22.08.22); [Электронный ресурс]. Режим доступа: https://chinalaw.center/business_law/china_cybersecurity_law_2016_russian/ (дата обращения: 22.08.22).

[3] [Электронный ресурс]. Режим доступа: https://cnlegal.ru/china_economic_law/china_data_security_law_2021/ (дата обращения: 22.08.22).

[4] [Электронный ресурс]. Режим доступа: https://ru.chinajusticeobserver.com/law/x/data-security-law-of-the-people-s-republic-of-china20210610 (дата обращения: 22.08.22).

Другие два закона (Закон КНР «О сетевой безопасности»[1], вступивший в силу 1 июля 2017 г., и Закон КНР «О защите персональных данных»[2], вступивший в силу 1 ноября 2021 г.), дополняют правовую основу, прописанную в «Законе о безопасности данных», и формируют эффективную правовую систему в области защиты и регулирования персональной информации и больших объемов данных.

Одновременно с усилением охраны безопасности данных правительство КНР создает общую систему регулирования отечественной цифровой инфраструктуры, включающую новейшие технологические инновации. Для этого в апреле 2020 г. Национальная комиссия по развитию и реформам (кит. 中华人民共和国国家发展和改革委员会) опубликовала следующую классификацию:

– Информационная инфраструктура как основа технологического развития. Технологии увеличения скорости передачи данных и увеличения объема собираемых, обрабатываемых и хранящихся данных (5G, Интернет вещей (IoT), промышленный Интернет, искусственный интеллект (AI), облачные вычисления, блокчейн, центры обработки данных (ЦОД) и сетевая инфраструктура интернет-коммуникаций);

– Инновационная инфраструктура. Строительство объектов, которые обеспечивают развитие научно-технического прогресса. Например, научно-исследовательские институты, инновационные парки и т.д.;

– Интегрированная инфраструктура. Внедрение Интернета, больших данных, искусственного интеллекта и т.д. для модернизации традиционных транспортных и энергетических инфраструктур внутри страны[3].

Вместе с тем отметим, что КНР в области информационной политики ведет себя достаточно стратегически, так как стремится предоставить другим странам доступ к своим продуктам в сфере безопасности, чтобы создать общее пространство с определенным уровнем безопасности и регулирования. Для этого в 2020 г. запустили международную программу инновационной безопасности[4]. А 21 апреля 2022 г. Си Цзиньпин на Боаоском Азиатском Форуме выступил с инициативой обеспечения Глобальной безопасности. По мнению Си Цзиньпина, глобальная безопасность не может быть достигнута без обеспечения мировой кибербезопасности. Также китайский лидер проблематику информационной безопасности ставит в один ряд с экологическими проблемами, терроризмом и другими глобальными

[1] [Электронный ресурс]. Режим доступа: https://chinalaw.center/business_law/china_cybersecurity_law_2016_russian (дата обращения: 22.08.22).

[2] [Электронный ресурс]. Режим доступа: https://chinalaw.center/business_law/china_personal_information_protection_law_2021_russian/ (дата обращения: 22.08.22).

[3] [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/4483436 (дата обращения: 24.08.22).

[4] Иванов И.С., Се Ф. 20-летие Договора о добрососедстве, дружбе и сотрудничестве между РФ и КНР. РСМД, 2021. С. 17.

угрозами, что лишний раз подчеркивает важность поиска путей противодействия кибер-атакам в современных условиях[1].

Действительно, Китай готов делиться своими достижениями в сфере интернет-безопасности. Например, компания KingsoftCorp. предоставляет бесплатный доступ пользователям со всего мира своему антивирусу KingsoftInternetSecurity. Также популярен китайский антивирус 360 Total Security, разработанный компанией Qihoo 360 и т.д.

Россия также выступает с международными инициативами в сфере кибербезопасности. Так, 25 сентября 2020 г. В.В. Путин выступил с инициативой «О комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности (МИБ)». А 6 декабря ООН приняла резолюция США и РФ по международной информационной безопасности[2].

На фоне развития сфер кибербезопасности как РФ, так и КНР, данные страны уверенно формируют механизм двустороннего сотрудничества через следующие институциональные структуры:

- подкомиссии по связи и информационным технологиям Российско-Китайской комиссии по подготовке регулярных встреч глав правительств;
- в рамках ООН, ШОС, БРИКС;
- в рамках договоренностей ЕАЭС с другими странами-партнерами;
- в рамках китайской инициативы «Один пояс, один путь»;
- сотрудничество оборонных структур РФ и КНР;
- диалог и взаимодействие на экспертном уровне[3].

Российско-Китайская Подкомиссия разрабатывает решения расширения сфер высокотехнологического сотрудничества: от систем хранения данных и механизмов укрепления сетевой безопасности до способов повышения эффективности управления и развития глобального информационного пространства[4].

Правовой основой взаимодействия России и КНР друг с другом, а также на международной арене в киберпространстве можно считать «Соглашения между правительствами государств-членов ШОС о сотрудничестве в области международной информационной безопасности»[5], подписанное в 2009 г., но вступившее в силу только в 2015 г. Площадка ШОС и прописанные правила взаимодействия в ИКТ

[1] [Электронный ресурс]. Режим доступа: http://www.news.cn/politics/leaders/2022-04/21/c_1128580296.htm (дата обращения: 24.08.22).

[2] См.: [Электронный ресурс]. Режим доступа: https://tass.ru/info/13536027 (дата обращения: 24.08.22).

[3] Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности. Китай в мировой и региональной политике. История и современность - ИДВ РАН, Т. 23 №23, 2018. С. 223-237.

[4] Там же. С. 233.

[5] [Электронный ресурс]. Режим доступа: https://www.prlib.ru/item/1283353 (дата обращения: 28.08.22).

также помогают для продвижения идей в ООН и других международных площадках.

В 2016 г. на Петербургском международном экономическом форуме (ПМЭФ) В.В. Путин подчеркнул необходимость глобального взаимодействия в условиях ускорения информатизации и «цифровой революции». Президент выразил надежду, что Евразийский экономический союз (ЕАЭС) сможет стать основой взаимодействия стран Центральной Азии и стран-партнеров, в том числе Китая в рамках проекта «Большая Евразия»[1].

Со своей стороны Китай развивает инициативу «Один пояс, один путь», который охватывает более 60 стран Азии, Европы и Африки, в том числе Россию. В рамках проекта реализуется строительство «Цифрового Шелкового пути», включающее создание трансграничных оптических кабелей и межконтинентальных подводных оптических линий, совершенствование воздушных и спутниковых информационных каналов, улучшение региональной международной связи. Однако цифровизация стран вдоль Пути усиливает угрозу кибербезопасности этих стран. В связи с этим ведется широкая кооперация в этом направлении. В том числе Россия планирует сотрудничать в рамках «Большой Евразии», а не в двустороннем порядке[2].

Международная координация осуществляется также через платформы Международного союза электросвязи при ООН, в ходе Всемирных встреч на высшем уровне по вопросам информационного общества, в БРИКС, АТЭС и т.д. Также в 2018 г. Генассамблея ООН приняла российский проект резолюции о глобальной кибербезопасности[3], из чего можно сделать вывод о высокой роли РФ в разработке международных стандартов Интернет-безопасности, что делает страну равным партнером Китая в этой сфере.

При этом сотрудничество в международных рамках не гарантирует соблюдение своих же договоренностей. Так, в 2016 г. пакистанская группировка хакеров признала взлом более 7 тыс. индийских сайтов[4]. Поэтому двусторонняя кооперация России с КНР особенно важна для достижения максимальных результатов в реализации общих целей.

Принципиальное значение для взаимодействия двух стран имеет подписанное в 2015 г. на межправительственном уровне российско-китайское «Соглашение о сотрудничестве в области обеспечения международной информационной безопасности». Можно сказать, что «Соглашение» «стало правовой и организационной основой сотрудничества России и КНР в области обеспечения международной

[1] [Электронный ресурс]. Режим доступа: https://rg.ru/2016/06/19/reg-szfo/vladimir-putin-proekt-bolshoj-evrazii-otkryt-i-dlia-evropy.html (дата обращения: 28.08.22).=

[2] [Электронный ресурс]. Режим доступа: https://rg.ru/2016/06/19/reg-szfo/vladimir-putin-proekt-bolshoj-evrazii-otkryt-i-dlia-evropy.html (дата обращения: 28.08.22).

[3] [Электронный ресурс]. Режим доступа: https://d-russia.ru/ustav-oon-primenim-v-informacionnom-prostranstve-sovmestnoe-zajavlenie-rf-i-knr.html (дата обращения: 28.08.22).

[4] Индия и Пакистан были приняты в ШОС в 2017 г.

информационной безопасности»[1]. В нем содержится список главных угроз в международном киберпространстве и определяются основные формы и механизмы совместной борьбы с ними.

Основными сферами взаимодействия были названы:

- борьба с угрозой подрыва международной информационной безопасности;
- недопущение использования ИКТ террористическими организациями;
- предупреждение вмешательства во внутренние дела, подрыва суверенитета государства и разжигания конфликтов на национальной и религиозной почве и т.д.[2]

Пандемия и перевод сотрудников на удаленный режим работы усилили опасность кибератак на рабочие и личные компьютеры сотрудников, поэтому перед Россией и Китаем встала задача обеспечения кооперации между интернет-провайдерами и мобильными операторами.

Подобные вопросы партнерства обсуждаются в рамках рабочих групп по электросвязи, информационным технологиям и, в том числе, кибербезопасности российско-китайской Подкомиссии по связи и информационным технологиям.

Крупные ИТ-компании тоже выходят на рынки РФ и КНР. В России давно работают Alibaba, Huawei, Xiaomi и др., а в Китае – российский «Яндекс»[3].

Подобные соглашения позволяют на практике реализовывать стратегии сотрудничества, прописанные в межправительственных соглашениях. Главными плюсами являются общее понимание угроз киберпространства и общее видение методов борьбы с ними. Высокий уровень регулирования цифровой среды в КНР и понимание общих целей с РФ позволяют добиться максимальной продуктивности кооперации двух стран в данной сфере. Принимая во внимание большое количество межправительственных встреч, работу в рамках ШОС и других международных организаций можно сказать, что в настоящее время российско-китайское сотрудничество в сфере кибербезопасности находится на очень высоком уровне и в обозримой перспективе будет только улучшаться.

БИБЛИОГРАФИЯ

1. Иванов И.С., Се Ф. 20-летие Договора о добрососедстве, дружбе и сотрудничестве между РФ и КНР. РСМД, 2021. С. 58.
2. Исаев А.С. Российско-китайское взаимодействие по вопросам

[1] [Электронный ресурс]. Режим доступа: https://d-russia.ru/rossiya-i-kitaj-podpisali-soglashenie-o-sotrudnichestve-v-oblasti-informacionnoj-bezopasnosti.html(дата обращения: 28.08.22).

[2] Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности. Китай в мировой и региональной политике. История и современность - ИДВ РАН, Т. 23 №23, 2018. С. 235.

[3] [Электронный ресурс]. Режим доступа: https://www.interfax.ru/business/465878 (дата обращения: 28.08.22).

обеспечения информационной безопасности. Китай в мировой и региональной политике. История и современность - ИДВ РАН, Т. 23 №23, 2018. С. 226.
3. Лузянин С.Г. Российско-китайский диалог: модель 2017: доклад № 18/2015. С. 31-32.
4. [Электронный ресурс]. Режим доступа: https://ria.ru/20220414/kiberbezopasnost-1783470960.html (дата обращения: 22.08.22).
5. [Электронный ресурс]. Режим доступа: https://minobrnauki.gov.ru/press-center/news/?ELEMENT_ID=40118 (дата обращения: 22.08.22).
6. [Электронный ресурс]. Режим доступа: https://tass.ru/politika/13268039?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (дата обращения: 22.08.22).
7. [Электронный ресурс]. Режим доступа: https://digital.gov.ru/ru/activity/directions/858/ (дата обращения: 22.08.22).
8. [Электронный ресурс]. Режим доступа: https://cnlegal.ru/china_economic_law/china_data_security_law_2021/ (дата обращения: 22.08.22).
9. [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/4483436 (дата обращения: 24.08.22).
10. [Электронный ресурс]. Режим доступа: http://www.news.cn/politics/leaders/2022-04/21/c_1128580296.htm (дата обращения: 24.08.22).
11. [Электронный ресурс]. Режим доступа: https://rg.ru/2016/06/19/reg-szfo/vladimir-putin-proekt-bolshoj-evrazii-otkryt-i-dlia-evropy.html (дата обращения: 28.08.22).
12. [Электронный ресурс]. Режим доступа: https://d-russia.ru/rossiya-i-kitaj-podpisali-soglashenie-o-sotrudnichestve-v-oblasti-informacionnoj-bezopasnosti.html (дата обращения: 28.08.22).
13. [Электронный ресурс]. Режим доступа: https://spbdnevnik.ru/news/2015-09-16/telekom-rossii-i-kitaya-ukreplyaeyt-svyazi (дата обращения: 28.08.22).
14. [Электронный ресурс]. Режим доступа: https://www.interfax.ru/business/465878 (дата обращения: 28.08.22).

REFERENCES

1. Ivanov I.S., Ce F. 20th anniversary of the Treaty on Good Neighborliness, Friendship and Cooperation between the Russian Federation and China [*20-letie Dogovora o dobrososedstve, druzhbe i sotrudnichestve mezhdu RF i KNR*]. INF, 2021. C. 58.
2. Isaev A.S. Russian-Chinese cooperation on information security. China in world and regional politics. History and Modernity [*Rossijsko-kitajskoe vzaimodejstvie po voprosam obespecheniya informacionnoj bezopasnosti. Kitaj v mirovoj i regional'noj politike. Istoriya i sovremennost'*] - IDV RAS, Vol. 23 No.23, 2018. p. 226.
3. Luzyanin S.G. Russian-Chinese Dialogue: Model 2017 [*Rossijsko-kitajskij dialog: model' 2017*]: Report No. 18/2015. pp. 31-32.
4. [Electronic resource]. Access mode: https://ria.ru/20220414/kiberbezopasnost-1783470960.html (accessed: 08/22/2012).
5. [Electronic resource]. Access mode: https://minobrnauki.gov.ru/

press-center/news/?ELEMENT_ID=40118 (date of reference: 08/22/2012)
6. [Electronic resource]. Access mode: https://tass.ru/politika/13268039 ?utm_source=google.com&utm_medium=organic&utm_campaign=google.com&utm_referrer=google.com (date of reference: 08/22/2012).
7. [Electronic resource]. Access mode: https://digital.gov.ru/ru/activity/directions/858 / (accessed: 08/22/2012).
8. [Electronic resource]. Access mode: https://cnlegal.ru/china_economic_law/china_data_security_law_2021 / (accessed: 08/22/2012).
9. [Electronic resource]. Access mode: https://www.kommersant.ru/doc/4483436 (date of reference: 24.08.22).
10. [Electronic resource]. Access mode: http://www.news.cn/politics/leaders/2022-04/21/c_1128580296.htm (date of reference: 24.08.22).
11. [Electronic resource]. Access mode: https://rg.ru/2016/06/19/regszfo/vladimir-putin-proekt-bolshoj-evrazii-otkryt-i-dlia-evropy.html (date of reference: 28.08.22).
12. [Electronic resource]. Access mode: https://d-russia.ru/rossiya-i-kitaj-podpisali-soglashenie-o-sotrudnichestve-v-oblasti-informacionnoj-bezopasnosti.html (accessed: 28.08.22).
13. [Electronic resource]. Access mode: https://spbdnevnik.ru/news/2015-09-16/telekom-rossii-i-kitaya-ukreplyaeyt-svyazi (date of reference: 28.08.22).
14. [Electronic resource]. Access mode: https://www.interfax.ru/business/465878 (accessed: 28.08.22).