Секция «Региональные проблемы международных отношений: Восток»

Особенности и перспективы взаимодействия России и Китая в сфере кибербезопасности

Научный руководитель – Цветков Иван Александрович

Янькова Александра Дмитриевна
Студент (бакалавр)
Санкт-Петербургский государственный университет, Факультет международных отношений, Санкт-Петербург, Россия
E-mail: yankova.alex97@yandex.ru

В настоящий момент мир переживает информационную революцию, охватывающую все сферы человеческой деятельности. Скорость развития ИКТ свидетельствуют о том, что влияние цифровых технологий будет возрастать; это значит, что кибербезопасность станет ключевой задачей для дальнейшего внедрения информационных технологий и развития цифровой экономики. Россия и Китай являются активными участниками данных мировых процессов. За последние годы эти страны ускорили формирование новой интернет стратегии на евразийском континенте. Россия и КНР, наряду с США, Японией и другими государствами, входят в десять лидирующих стран мира по числу интернет пользователей и использованию киберпространства в целом.

Киберпространство стало источником новых возможностей для взаимодействия, обмена информацией, реализация финансовых, торговых и других операций. Однако, помимо преимуществ, оно также привело к появлению новых вызовов и угроз, включающих в себя проблему безопасности и стабильности в киберпространстве, которую целесообразно решать на международном уровне. Если не предпринимать необходимые меры по укреплению международного сотрудничества в этой области, киберугрозы будут создавать серьезные риски для равномерного развития и устойчивости мировой экономики.

Россия и Китай ведут активное политическое сотрудничество, в том числе в рамках международных организаций. Совместное обеспечение безопасности является одним из важнейших аспектов их взаимодействия. В последние годы к понятию традиционной безопасности добавилась информационная. В связи с появлением новых угроз Китай начал активную трансформацию своей системы кибербезопасности, включающей модернизацию нормативно-правовой базы (в том числе, принятие нового Закона о кибербезопасности [5]), а также совершенствование структуры, состоящей из специализированных подразделений КПК, министерств и подразделений НОАК, образующих интеграцию гражданский и военных структур. По мнению экспертов, КНР продолжит модернизацию правовой базы в этом направлении, а также разработку военной стратегии, допускающей ведение информационной войны [3]. Опыт Китая в этой сфере остается крайне интересным для России.

Базовый Закон о кибербезопасности Китая включает в себя документ о «Международной стратегии сотрудничестве в киберпространстве», который частично перекликается с российской стратегией, согласно «Основам государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Российские и китайские практические ведомства и аналитики изучают и отчасти используют опыт друг друга в нормативно-правовом обеспечении кибербезопасности [1].

Опасность милитаризации информационной среды подталкивает страны к взаимодействию. Несмотря на то, что определяющим для Китая в этом вопросе является мнение и отношения с США [2], российско-китайский диалог в сфере кибербезопасности все же

можно считать налаженным. Помимо взаимодействия в рамках ШОС и БРИКС и подписания рамочных соглашений, таких как «Соглашение о сотрудничестве в области обеспечения международной информационной безопасности» 2015 г., он включает в себя работу Российско-китайской подкомиссии по связи и информационным технологиям и взаимодействие на уровне экспертов. Россия не осуждает даже жестких мер контроля и цензуры в интернете КНР. В относительно недавних попытках установления контроля над интернетом в РФ можно разглядеть отголоски китайского опыта. Взаимодействие оборонных ведомств, специализирующихся на кибербезопасности также является показательным. В данном случае скорее КНР делится своим опытом, чем происходит равноправный обмен. Тем не менее, яркими примерами реальных действий служат российско-китайские компьютерные командно-штабные учения ПРО, заключающиеся в компьютерном моделировании различных ситуаций, и планы по созданию совместной технологической платформы для отражения киберугроз [4].

Реальный процесс решения практических проблем информационной безопасности очень сложен, даже не смотря на наличие соглашений и постоянных контактов. Доверие, традиционное для взаимодействующих в рамках одной международной организации стран, утрачивается в киберпространстве. Его восстановление - одна из важней задач сотрудничества России и Китая. Проблемы недоверия возникают в результате регулярных хакерских атак с китайских IP-адресов на индустриальные, финансовые и исследовательские сети, в том числе и Российской Федерации. Большинство таких сетей имели стратегическое значение и входили в зону пересечения интересов Китая с другими странами АТР [1]. Доказательства и источники атак почти невозможно раскрыть с помощью традиционных средств наблюдения и верификации, которыми на данный момент располагают дипломаты и военные. В перспективе, в рамках ШОС возможно создание специальных программ по расширению возможностей ведения сетевых войн и обороне в цифровом пространстве; однако, для реализации таких планов требуется время, консолидация усилий и политическая воля всех членов [1].

Основным достижением отношений России и КНР в вопросах кибербезопасности является то, что между государствами созданы благоприятные условия для дальнейшего диалога по политическим и военным каналам, а также для обмена технологиями и продуктами ИКТ. Формирование условий для сотрудничества в технологической сфере, активное участие в цифровом взаимодействии и глобальном управлении цифровой экономикой, объединенные с отстаиванием собственных интересов, могут в перспективе стать основой единой платформы по предотвращению новых киберугроз.

Источники и литература

1) Исаев А.С. Российско-китайское взаимодействие по вопросам обеспечения информационной безопасности // Китай в мировой и региональной политике. История и современность, М., 2018. С. 223-237

2) Кашин В.Б. КНР и «третья стратегия компенсации» Министерства обороны США // Вестник Московского университета. Серия 25: Международные отношения и мировая политика, Изд-во Моск. ун-та (М.), Том 8, № 3, 2016.

3) Ball D. China's cyber warfare capabilities. Security Challenges, 7(2), 2011.

4) Учения России и Китая: Война на компьютерах // Газета.RU: https://www.gazeta.ru/army/2017/12/15/11489156.shtml

5) Law of the People's Republic of China on cybersecurity: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm