УДК 327.3

НАУЧНЫЙ ЖУРНАЛ
«БИЗНЕС И ОБЩЕСТВО»

Войнов Александр Сергеевич

студент бакалавриата
Московский государственный юридический
университет имени О. Е. Кутафина
Волго-Вятский институт (филиал)
Киров, Россия

СРАВНЕНИЕ ВНЕШНЕЙ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РФ И КНР

Аннотация

Рассматриваются вопросы влияния внешней политики в сфере обеспечения международной безопасности на взаимоотношения государств. Проводится сравнительно-правовой анализ Стратегии международного сотрудничества в киберпространстве Китайской Народной Республики и Основ государственной политики Российской Федерации в области международной информационной безопасности. Результатом работы является вывод о влиянии различий во внешней политике государств на их взаимоотношения.

Ключевые слова: внешняя политика, информационная безопасность

В современном мире кибербезопасность стала одной из наиболее актуальных и важных тем. Развитие информационных технологий и сети «Интернет» привело к тому, что всё больше стран оказываются в зависимости от уровня развития информационных технологий. Чем больше задействованы информационные технологии, прежде всего, в экономике, а также в осуществлении государством своих функций, тем более такое государство уязвимо к кибератакам и иным формам оказания давления через информацию и информационные технологии, будь то доступ к новейшим разработкам более продвинутых государств или угроза от них введением информационной блокады. Сложившаяся обстановка вынуждает государства всё больше обращать внимание на защиту своих сетей от подобного рода посягательств на суверенитет. Сложившуюся ситуацию отражают как акты каждого государства по отдельности, так и международные договоры.

Тем временем, наблюдается и ещё одна немаловажная тенденция – отказ России от «западного пути» и её сближение с азиатскими странами, прежде всего с Китаем. Сближение России и Китая обусловлено, отчасти их взаиморасположением и долгой историей взаимоотношений. Однако, ввиду вышеупомянутой тенденции к увеличению значимости информационных технологий в жизни государств, мы считаем необходимым понять различия и сходства в подходах России и Китая в обеспечении международной информационной безопасности. Предполагается, что такое сравнение позволит, в дальнейшем, при сохранении обоих тенденций, понять и оценить,

насколько «тесным» будет взаимодействие России и Китая, и в какой форме оно будет протекать. Наиболее эффективно это можно сделать через сравнение законодательства.

Как правило, намерения государства действовать так или иначе, можно понять через анализ документов. Государства, имеющие идентичные по содержанию и структуре акта, в данной сфере будут действовать достаточно схожим образом. В свою очередь, это утверждение влечёт следующий вывод – государства, действующие схожим образом, будут вынуждены объединяться в блоки против государств, не разделяющих их точку зрения и не одобряющих их действия. Данное утверждение же, в свою очередь, позволяет нам предположить, что, при условии наличия определённой взаимосвязи между государствами ранее (взаимопомощь, договоры, общие военные действия, если обобщить, – любой положительный опыт взаимодействия между государствами) и признания регулируемой сферы достаточно важной для обоих государств, объединение государств в блоки приведёт к сближению государств и в остальных сферах. Суть вышесказанного можно вывести в простую взаимосвязь – чем важнее регулируемая сфера и чем более схожи акты различных государств в данной сфере, тем эффективнее будет взаимодействие данных государств.

Однако, важно прояснить и ещё один момент – акты должны быть направлены именно на внешнюю политику. Обосновано это, прежде всего логикой предыдущего абзаца. Акт, регулирующий внутренние общественные отношения в сфере обеспечения информационной безопасности, не будет оказывать сильного влияния на другое государство. Соответственно, разногласиями во внутренней политике, для достижения общих целей, государства могут пренебречь. В то же время, действия, предпринимаемые государством во внешней политике, прямо или косвенно затрагивают другие страны и заставляют ощущать на себе последствия каждого шага, предпринимаемого государством-оппонентом.

Также, для полноты картины, важно понимать уровень информационного развития сравниваемых стран, так как именно он напрямую влияет на уровень зависимости государства от информационно-коммуникационных технологий (далее – ИКТ). На момент 18 января 2023 года, по данным, опубликованным на сайте Роспатента, Китай занимает первое место по развитию цифровых технологий, тогда как Россия – 20 [23]. Так же необходимо учесть то, что и на Россию, и на Китай

оказывается достаточно сильное информационное внешнее давление со стороны других стран. В частности, количество кибератак на российские организации в 2023 году заметно выросло [24]. При том, и сами вышеупомянутые страны могут проводить кибератаки на ряд стран. К примеру, Американская компания Symantec, занимающаяся разработками в области кибербезопасности, выявила кибератаку из Китая на компании в США и Юго-Восточной Азии. По данным Symantec, за атакой стоят хакеры из группы Thrip, которая образовалась в 2013 году [25].

Для того, чтобы показать сходства и различия Российской Федерации и Китайской Народной Республики использованы два документа, определяющих основы государственной политики в сфере ИКТ. Основным документом для Российской Федерации будут являться Основы государственной политики в Российской Федерации в области международной информационной безопасности (Основы), а для Китая – Стратегии международного сотрудничества в киберпространстве (Стратегии) со стороны Китайской Народной Республики (КНР). Первый документ утверждён Указом Президента РФ от 12 апреля 2021 г. № 213, а второй подлежал публикации 2 марта 2017 года. Оба акта являются доктринальными документами стратегического планирования. Иными словами, данные акты являются «предвестниками» будущих нормативно правовых актов и, следовательно, предопределяют политику государства на некоторый период.

Стоит отметить стиль речи, использующийся в документах. В общих положениях Основ используется официально-деловой стиль речи, на который указывает точность формулировок, а также отсутствие достаточного количества средств выразительности. По сравнению с Основами, текст Стратегий КНР составлен менее формально. Присутствуют средства выразительности: эпитеты «стремительное развитие информационных технологий», градация «активизировать коммуникации, расширять консенсус и углублять сотрудничество», метафора «глобальную деревню». Таким образом, можно сказать, что стиль текста Стратегий КНР не является официально-деловым. Так же, наличие средств выразительности, таких как метафора, указывает на то, что в тексте могут присутствуют многозначные слова, которые, по сравнению с Основами, допускают больше вариаций для трактовки смысла стратегий.

Начать следует с сущности сравниваемых актов. Оба документа содержат в себе положения как направленные на продвижение на международной арене подходов государств, так и на внутреннее регулирование.

Отдельно стоит отметить, что содержательная сторона данных документов практически одинакова. Сущностные различия проступают только в отдельных формулировках. В частности, в отличие от Стратегий КНР, в Основах присутствует фраза «продвижение российских подходов» [2], которая явно идёт в разрез с используемой в Стратегиях «поощрять международное сообщество объединяться для … построения мирного … киберпространства». Принципиальное различие заключается в том, что первую фразу мы можем истолковать как призыв к государствам использовать Российские подходы, тогда как вторая фраза призывает нас прежде всего к объединению и выработке подходов, прежде всего, совместными усилиями. Соответственно, формулировка, представленная в Стратегии, является более демократичной и «привлекательной» для окружающих стран.

Схожи, так же, и внешние киберугрозы для стран. Чтобы показать необходимость принятия акта и обозначить проблему, оба акта содержат в себе перечисление угроз. Так, к угрозам оба акта относят терроризм в сфере информационных технологий и нарушение суверенитета менее развитых стран более развитыми, путём злоупотребления последних своим уровнем информационного развития. Однако, помимо вышеперечисленных угроз, КНР выделяет то, что «Существующая глобальная система управления основными ресурсами Интернета вряд ли отражает желания и интересы большинства стран. … Вмешательство во внутренние дела других стран путем злоупотребления ИКТ и массированной деятельности по кибернаблюдению происходит время от времени» [6]. Иными словами, помимо прочих внешних IT-угроз, направленных непосредственно на Китай, Стратегии содержат и проблему, современного международного информационно-политического общества, которая заключается в том, что «Страны-обладатели высокоразвитых технологий могут начать диктовать условия» [18]. Напрямую эта проблема Китая не касается поскольку, как говорилось выше, его уровень информационных технологий гораздо выше, чем у ряда других стран. Следовательно, данная проблема не может полноценно считаться проблемой Китая, зато однозначно является проблемой всего мирового сообщества.

Отметим, что Российская Федерация тоже указывает на данную проблему, но под несколько иным углом. Одной из целей основ, указанных в дальнейшем, является «создание условий для … преодоления информационного неравенства между

развитыми и развивающимися странами» [2], что косвенно даёт нам понять об осведомлённости РФ в отношении данной киберугрозы.

Цели государственной политики в данной сфере также не предоставляют больших различий. Очевидно, что и Россия, и Китай стремятся не допустить возможных конфликтов в киберпространстве, посредствам установления системы международной кибербезопасности. Внимание стоит обратить и на тот факт, что в Стратегии, помимо простого перечисления (как это закреплено в Основах), даётся и разъяснение (трактовка) целей КНР, которая позволяет наиболее полно отразить позицию Китая.

Следующие положения, нуждающиеся в сравнении – основные принципы. Российское законодательство ссылается прежде всего общепринятые нормы международного права [2], а КНР стремится выработать свои принципы.

Стратегии выделяют четыре основных принципа:

1) Мир;

2) Суверенитет;

3) Совместное управление;

4) Общие выгоды.

Каждому принципу даётся разъяснение. Принципы содержат в себе и обязательства. Так, например, в пояснении к принципу Общих выгод прямо говорится: «Международное сообщество должно способствовать большей открытости и сотрудничеству .... Страны должны содействовать развитию сотрудничества на двустороннем, региональном и международном уровнях» [6].

И последнее, что хотелось бы отметить – нормы, связанные с реализацией актов. Российское законодательство делает упор на международное сотрудничество. Однако, большая часть взаимодействия с другими странами заключается в проведении мер по обеспечению кибербезопасности. В то же время китайский «План действий» основан именно на мирном сотрудничестве в целях развития. При этом Стратегии утверждают, что, для достижения целей, необходимо создание нового информационного общества, в котором Китай выступит основным посредником между странами. Данный пункт напрямую указывает на положение «мирового посредника», которое стремится занять Китай в международных отношениях.

Отдельного внимания также заслуживают и «каналы связи» – иными словами, посредством каких контрагентов будут достигнуты данные цели. Российская

федерация практически единственным контрагентом видит ООН. Любой элемент реализации, прописанный в Основах, может быть осуществлён либо непосредственно РФ, либо через ООН. В то же время КНР видит также возможности реализации и в других международных организациях.

В результате всего вышеперечисленного, нельзя не сделать ряд выводов о данных актах. Прежде всего, документы действительно схожи. Они ставят одни цели и призваны бороться с одними и теми же проблемами. Но, при этом, каждое государство видит возможности разрешения и результаты по разному Если Российская Федерация видит возможности решения проблем в сфере ИКТ путём совершенствования своих технологий и периодическом взаимодействии с другими странами для обмена опытом по строго-оговорённым вопросам, то Китайская Народная Республика, в соответствии с тенденциями глобализации, видит путём решения проблемы – создание на базе ООН постоянно действующего международного содружества, которое предоставляло бы всем своим членам возможности доступа к более развитым информационным технологиям. По сути своей Стратегии КНР являются более глобалистскими. Они содержат в себе не только отдельные высказывания, но и предлагают государствам возможный вариант объединения, что может счесться как выказывание Китаем гораздо более серьёзные намерений и его возможность перейти к действиям.

Таким образом, можно полагать, что Российская Федерация и Китайская Народная Республика будут достаточно долго и тесно взаимодействовать. На это нам указывает прежде всего тот факт, что оба государства преследуют одни цели, имеют схожие проблемы и пути решения. Безусловно, при сравнении был обнаружен ряд разногласий, однако они не являются достаточными, чтобы быть препятствием сближению стран.

Список использованных источников

1. Федеральный закон от 28 июня 2014 г. № 172-ФЗ (ред. от 13 июля 2024г.) «О стратегическом планировании в Российской Федерации» // Российская газета, № 146, 03.07.2014.

2. Указ Президента РФ от 12 апреля 2021г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СЗ РФ, 19 апреля 2021г., № 16 (Часть I), ст. 2746.

3. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ, 12 декабря 2016, № 50, ст. 7074.

4. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ, 05 июля 2021, № 27 (часть II), ст. 5351

5. Указ Президента РФ от 31 марта 2023 г. № 229 «Об утверждении Концепции внешней политики Российской Федерации» // СЗ РФ, 03 апреля 2023, № 14, ст. 2406

6. Международная стратегии сотрудничества в киберпространстве Китайской народной Республики от 2 марта 2017. [Электронный ресурс] URL: https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html (дата обращения: 26.01.2025)

7. Международные стратегии сотрудничества в киберпространстве (中英文对照网络空间国际合作战略（кит.）（全文）/ 发布时间：2017-03-07 [Электронный ресурс] URL: http://www.catl.org.cn/2017-03/07/content_40498343.htm (дата обращения: 26.01.2025)

8. Окинавская Хартия Глобального информационного общества [Электронный ресурс] URL: http://www.kremlin.ru/supplement/3170 (дата обращения: 26.01.2025)

9. Коврижных Л. А. Основы государственной политики в области информатизации : Учеб. пособие / Л. А. Коврижных. – Киров : Старая Вятка, 2006. – 75 с. – ISBN 5-91061-019-8. – EDN: QWXJRR

10. Губеладзе, Д. В. Тенденции глобализации в современном мире / Д. В. Губеладзе. — Текст : непосредственный // Молодой ученый. — 2019. — № 23 (261). — С. 144-146. – EDN: ZCFDGH

11. Лопатин Ю. Н. Информационная безопасность в России. Проблемы, поиски решений / Ю. Н. Лопатин – Текст : электронный // Гуманитарные исследования в Восточной Сибири и на Дальнем Востоке. – 2008. – №2. – С. 51-57. – URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-rossii-problemy-poiski-resheniy (дата обращения: 26.01.2025). – EDN: MDXEHP

12. Михайлова А. А. Россия и Китай в международном цифровом пространстве / А. А. Михайлова – Текст : электронный // Вестник Балтийского федерального университета им. И. Канта. Серия: Естественные и медицинские науки. – 2023. – №2. – С. 31-45. – URL: https://cyberleninka.ru/article/n/rossiya-i-kitay-v-mezhdunarodnom-

tsifrovom-prostranstve (дата обращения: 26.01.2025). – DOI: 10.5922/gikbfu-2023-2-3. – EDN: GNKXOF

13. Ромашкина Н.П. Эволюция политики КНР в области информационной безопасности / Н. П. Ромашкина, В. Г. Задремайлова. – Текст : электронный // Пути к миру и безопасности. – 2020. – С. 122-138. – URL: https://cyberleninka.ru/article/n/evolyutsiya-politiki-knr-v-oblasti-informatsionnoy-bezopasnosti (дата обращения: 26.01.2025)

14. Чекменёва Т. Г., Ершов Б. А., Трубицын С. Д., Остапенко А. А. Стратегия Китая по обеспечению информационной безопасности: политический и технический аспекты / Т. Г. Чекменёва. – Текст : электронный // Bulletin Social-Economic and Humanitarian Research. – 2020. – №7 (9). – С. 78-97. – URL: https://cyberleninka.ru/article/n/strategiya-kitaya-po-obespecheniyu-informatsionnoy-bezopasnosti-politicheskiy-i-tehnicheskiy-aspekty (дата обращения: 26.01.2025). – DOI: 10.5281/zenodo.3911320. – EDN: KBYJRD

15. Разумов Е. А. Политика КНР по обеспечению кибербезопасности — Текст : непосредственный // Россия и АТР. — 2017. — № 4. — С. 156-170. – EDN: YMTCGH

16. Липень С. В. Прогностическая методология в юридических исследованиях — Текст : непосредственный // Журнал российского права — 2019. — № 8. — С. 5-7. – DOI: 10.12737/jrl.2019.8.1. – EDN: DZFYZA

17. Федеральная служба по интеллектуальной собственности Российской Федерации (Роспатент) : официальный сайт. – Москва. – Обновляется в течение суток. – URL: https://rospatent.gov.ru/ru (дата обращения: 26.01.2025). – Текст : электронный.

18. Токаев, К. Страны-обладатели высокоразвитых технологий могут начать диктовать условия/ К. Токаев. – Текст : электронный // Liter.kz : [сайт]. – 2020. – 4 дек. – URL: https://liter.kz/strany-obladateli-vysokorazvityh-tehnologij-mogut-nachat-diktovat-svoi-usloviya-tokaev/ (дата обращения: 26.01.2025)

19. Китай – ВВП – Текст : электронный // Trading Economics : [сайт]. – URL: https://ru.tradingeconomics.com/china/gdp (дата обращения: 26.01.2025)

20. Россия – ВВП – Текст : электронный // Trading Economics : [сайт]. – URL: https://ru.tradingeconomics.com/russia/gdp (дата обращения: 26.01.2025)

21. Бевза, Д. Количество кибератак на российские организации в 2023 году заметно выросло / Д. Бевза. https://rg.ru/2023/07/27/kolichestvo-kiberatak-na-rossijskie-organizacii-v-2023-godu-zametno-vyroslo.html (дата обращения: 26.01.2025)

22. Symantec сообщила о китайской кибератаке на компании в США и Азии – Текст : электронный // РБК : [сайт]. – 2018. – 20 июнь. – URL: https://www.rbc.ru/rbcfreenews/5b29efa39a7947a75b0dbbf5 (дата обращения: 21.01.2025)

23. Россия вошла в топ-20 стран по развитию цифровых технологий [Электронный ресурс] URL: https://rospatent.gov.ru/ru/news/top-20-stran-cifrovyh-tehnologiy-18012923#:~:text=Россия%20заняла%2014-е%20место%20в,Южная%20Корея%2C%20Франция%20и%20

24. Дмитрий Бевза Количество кибератак на российские организации в 2023 году заметно выросло [Электронный ресурс] URL: https://rg.ru/2023/07/27/kolichestvo-kiberatak-na-rossijskie-organizacii-v-2023-godu-zametno-vyroslo.html

25. РБК - Symantec сообщила о китайской кибератаке на компании в США и Азии [Электронный ресурс] URL: https://www.rbc.ru/rbcfreenews/5b29efa39a7947a75b0dbbf5